



Smarter Balanced Assessment Consortium: Permissions System User Guide

© Smarter Balanced Assessment Consortium, 2014



Table of Contents

INTRODUCTION TO THIS USER GUIDE	4
SECTION I. OVERVIEW OF THE PERMISSIONS SYSTEM	5
User Roles and Access	5
Interrelated Smarter Balanced Systems	5
SECTION II. GETTING STARTED WITH THE PERMISSIONS SYSTEM	6
Logging in to the Permissions System	6
Understanding the Permissions System Layout	7
Header	7
Task Icons	8
SECTION III. PERFORMING PERMISSIONS TASKS	9
Creating and Managing Components	9
Creating and Managing Roles	11
Creating and Managing Permissions	13
Mapping Roles to Component Permissions	15

Table of Figures

Figure 1. Login Screen	6
Figure 2. Permissions System Home Screen.....	7
Figure 3. Header	7
Figure 4. Permissions Task Icons.....	8
Figure 5. Navigation Menu.....	8
Figure 6. Manage Components Screen.....	9
Figure 7. Manage Roles Screen.....	11
Figure 8. Manage Component Permissions Screen	13
Figure 9. Map Roles to Component Permissions Screen	15





INTRODUCTION TO THIS USER GUIDE

This user guide supports individuals using the Permissions System to manage the roles and permissions associated with a tenant's deployed components. This introduction describes the contents of this document and includes a key for identifying icons and elements.

This user guide provides information about the Permissions System in a series of three sections, as follows:

- [Section I. Overview of the Permissions System](#) provides an overview of the system, its interrelation with other Smarter Balanced systems, and the user roles for accessing the system.
- [Section II. Getting Started with the Permissions System](#) explains how to log in to the Permissions System and describes the overall layout of the Permissions System user interface.
- [Section III. Performing Permissions Tasks](#) describes how to perform different permissions management tasks, including adding roles, adding permissions, and mapping roles to permissions.

Table 1. Key Icons and Elements

Icon	Description
	Warning: This symbol appears with text that contains extremely important information regarding actions that may cause errors.
	Caution: This symbol appears with text that contains important information regarding a task.
	Note: This symbol appears next to text that contains helpful information or reminders.
	Text that appears in gray boxes provides instructions relevant to the task described. <ul style="list-style-type: none"> • Numbered (ordered) lists provide step-by-step instructions. • Bulleted lists provide instructions that do not need to be done in a specific order.
[Text]	Bold text in brackets is used to indicate a link or button that is clickable.
<i>Text</i>	Text in italics indicates field names or labels.
"Text"	Text in quotation marks indicates the value specified for a field.

SECTION I. OVERVIEW OF THE PERMISSIONS SYSTEM

The Permissions System is a web-based system for Smarter Balanced. It is one of the core applications that you must deploy with any other component used at any given deployment level.

The Permissions System serves as a repository of the roles and permissions associated with a tenant's deployed components. When a user signs in to one of these deployed components, the Permissions System checks his or her role and grants access to only those features associated with that role.

User Roles and Access

The Permissions System is a core infrastructural application and is accessible to a limited number of users. Currently, only users with the Administrator role can access and perform all the tasks within the Permissions System.

Interrelated Smarter Balanced Systems

The Permissions System manages user roles and permissions for the following Smarter Balanced systems:

- **Test Authoring System (TAS):** This system allows users to construct the tests that are provided to students in the Test Delivery System.
- **Administration and Registration Tools (ART):** This system configures assessment attributes, registers students for assessments, and manages records for entities, personnel, and students.
- **Digital Library:** This system stores professional development resources that educational personnel can use to monitor their professional learning goals.
- **Test Delivery System (TDS):** This system delivers assessments to the students.
- **TDS Backend:** This system supports the services of the Test Delivery System.
- **Computer Adaptive Testing (CAT) Simulator:** This system runs simulations on test packages created in TAS to ensure that the adaptive segments in a test function according to the blueprint.
- **Portal:** The portal allows users to access and log in to the various Smarter Balanced systems.
- **Item Authoring:** This system allows users to construct the items to be included in operational and field-test assessments.

SECTION II. GETTING STARTED WITH THE PERMISSIONS SYSTEM

This section provides information about getting started with the Permissions System:

- Logging in to the Permissions System
- Understanding the Permissions System layout

Logging in to the Permissions System

To access the Permissions System, you must have an authorized user name and password. Your system administrator will be responsible for setting up your user account and providing you with the login credentials.

The Permissions System uses the Single Sign-On System, which is responsible for user authentication and authorization, and allows you to log in to the Smarter Balanced systems. After logging in, you can switch between systems without having to log in and out of each system.

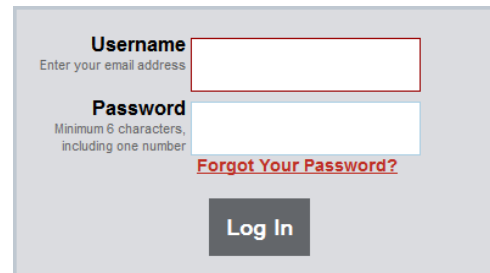
To log in to the Permissions System:

1. Open your web browser and navigate to the Permissions System using the URL provided to you.

You will be directed to the Single Sign-On **Login** screen shown in [Figure 1](#).

2. In the *Username* field, enter your user name.
3. In the *Password* field, enter your password.
4. Click [**Log In**]. You will be directed to the Permissions System home screen, provided your login is authenticated.

Figure 1. Login Screen

The screenshot shows a login interface with a light gray background. At the top, the word "Username" is in bold, followed by the instruction "Enter your email address" and a white text input field with a red border. Below this, the word "Password" is in bold, followed by the instruction "Minimum 6 characters, including one number" and a white password input field with a red border. To the right of the password field is a red link that says "Forgot Your Password?". At the bottom center is a dark gray button with the text "Log In" in white.

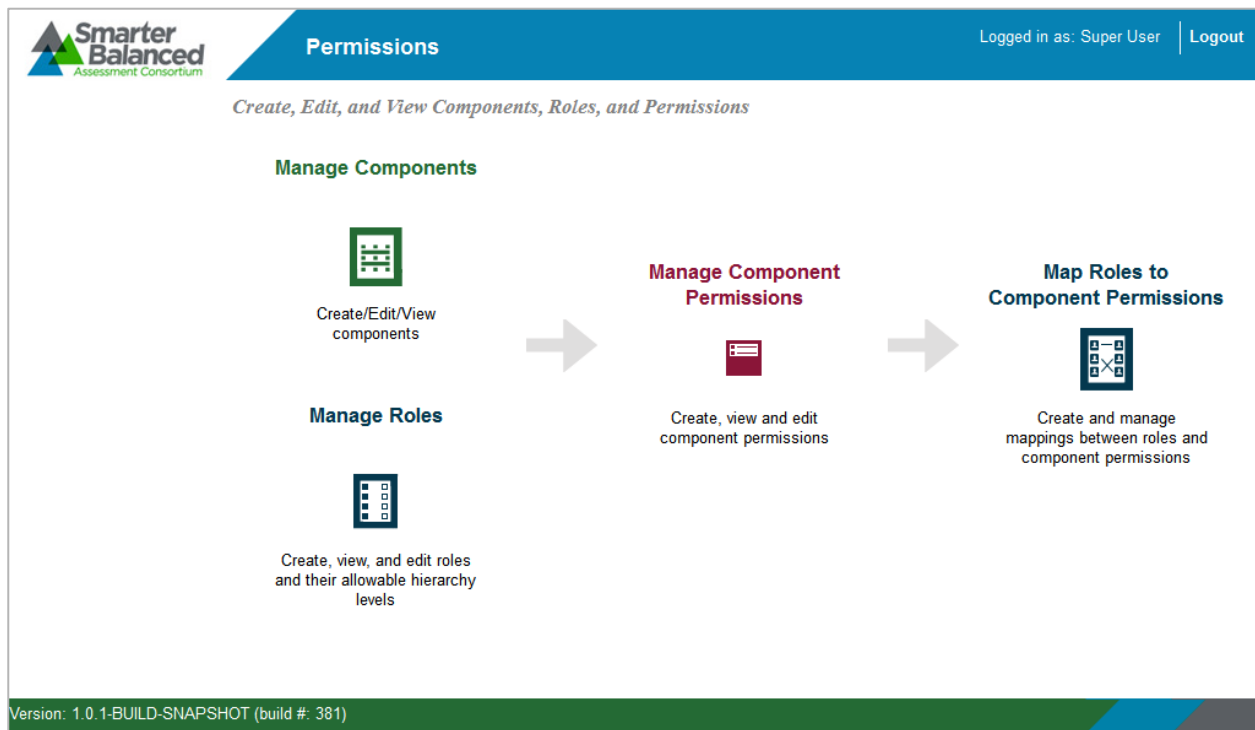
Understanding the Permissions System Layout

You can access the different features of the Permissions System from the home screen (see [Figure 2](#)) that appears when you first log in to the system.



Use the on-screen tools and buttons to navigate within the system. Do not use your web browser's back button, as this could result in a loss of information or accidental sign-out.

Figure 2. Permissions System Home Screen



The Permissions System layout includes the features described below.

Header

The header that appears on every screen (see [Figure 3](#)) provides information about the logged-in user and includes tools and buttons to perform different tasks.

Figure 3. Header



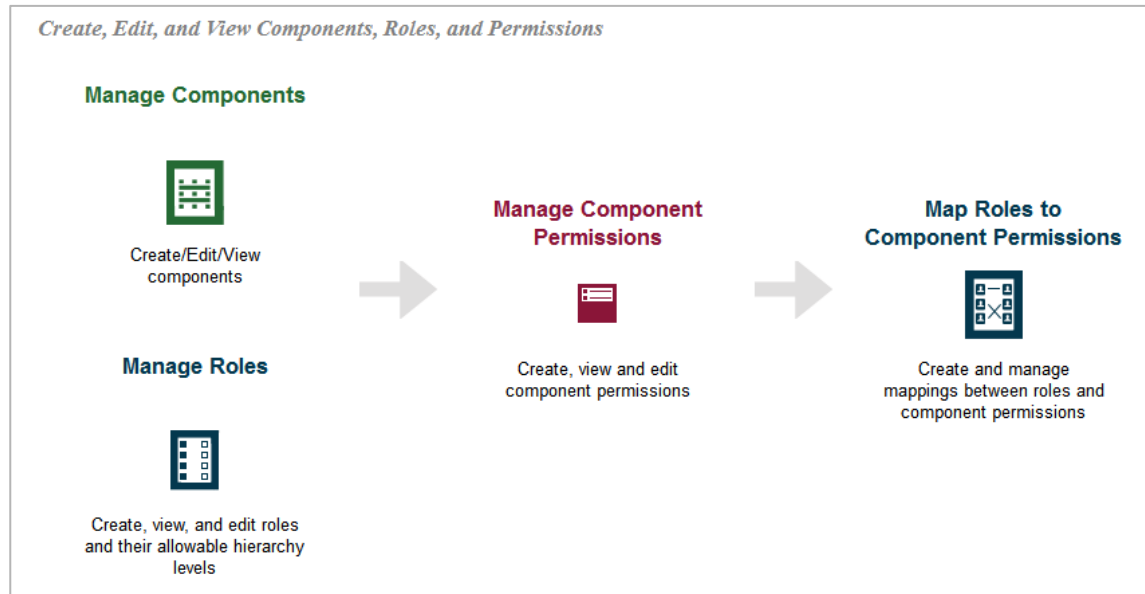
The header consists of the following features:

- **User Identification:** When you log in to the Permissions System, the header displays your name and user role.
- **Smarter Balanced Logo:** This logo acts as a button that returns you to the home screen.
- **[Logout]:** This button enables you to log out of the system.

Task Icons

The different permissions management tasks are displayed as icons on the home screen. Each task icon acts as a link that takes you to the corresponding task screen.

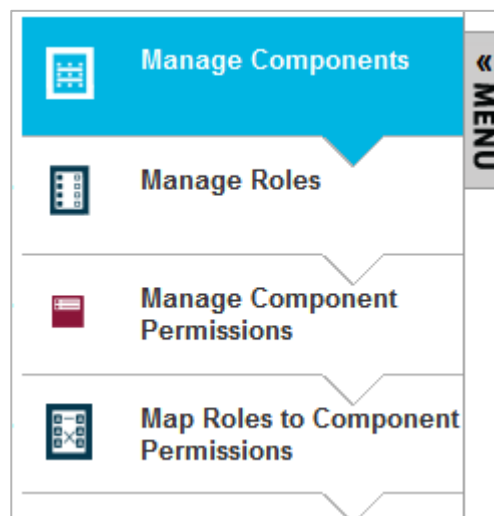
Figure 4. Permissions Task Icons



When you select a task, a collapsible menu displays on the left side of the screen (see [Figure 5](#)). You can use this menu to navigate through the available tasks.

- To collapse the navigation menu, click [**Menu**].
- To expand the collapsed navigation menu, click [**Menu**] again.

Figure 5. Navigation Menu



SECTION III. PERFORMING PERMISSIONS TASKS

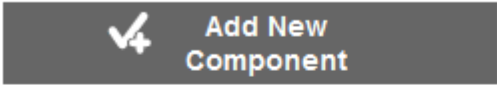








This section describes how to manage roles and permissions. The overall process is as follows:

1. Add your tenant's deployed components.
2. Create the roles and associate them with an entity level.
3. Create the permissions for each component.
4. Map the roles to the appropriate permissions.

Creating and Managing Components

In order to create the roles and permissions for a component, you must first add the component to the Permissions System. You should add any deployed component that restricts access to its features based on users' roles.

Figure 6. Manage Components Screen


Manage Components	
	
Component	Action
CATSimulator	 
CoreStandards	 
DigitalLibrary	 
Item Authoring	 

You can add and edit components on the **Manage Components** screen (see [Figure 6](#)). The components that you add to the Permissions System are displayed in the table on this screen. You can add, edit, and delete the components in this table.

To add a component:

1. On the Permissions System home screen, click [**Manage Components**]. The **Manage Components** screen loads.
2. On the **Manage Components** screen, click [**Add New Component**]. The *Add New Component* popup window opens.
3. In the *Component* field, enter the name of the component.
4. To save the new component, click [**Save**]. To save the component and enter another one, click [**Save and Add More**]. To cancel the operation without adding the component, click [**Cancel**].

To edit an existing component:

1. On the **Manage Components** screen, click [] in the Action column next to a component displayed in the table. The *Edit Component* pop-up window opens.
2. In the *Component* field, edit the component name.
3. To save your changes, click [**Save**].

To delete an existing component:

1. On the **Manage Components** screen, click [] in the Action column next to a component displayed in the table.
2. In the warning box that pops up, click [**Yes, delete...**].










Creating and Managing Roles

After adding components to the Permissions System, you can create user roles. A user role can be associated with zero, one, or multiple entity levels. The entity with which a role is associated determines the access level for users with that role. For example, an Administration and Registration Tools (ART) user associated with the state entity level will be able to manage entity records within his or her state.

Roles can be associated with the following entity levels in the Smarter Balanced hierarchy:

- Client
- Group of States
- State
- Group of Districts
- District
- Group of Institutions
- Institution

Figure 7. Manage Roles Screen

Manage Roles									
<div>  Add New Role  Save  Cancel </div>									
Role	Client	Group of States	State	Group of Districts	District	Group of Institutions	Institution	Protected Role	
AccommodationsUpload	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 
Admin Role1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 
Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	 

You can add and edit roles on the **Manage Roles** screen (see [Figure 7](#)). The table on this screen displays the roles that you add to the Permissions System along with their associated entity levels. You can add, edit, and delete the roles in this table, as well as associate roles with entity levels.



This table also includes a Protected Role column. If you mark the checkbox in this column for a role, then only users with that role will be able to add other users with that role in ART. For example, marking the Protected Role checkbox for the Administrator role would mean that only an Administrator can add other Administrator user records in ART.


To add a new role:

1. On the Permissions System home screen, click [**Manage Roles**]. The **Manage Roles** screen loads.
2. On the **Manage Roles** screen, click [**Add New Role**]. The *Add New Role* pop-up window opens.
3. In the *Role* field, enter the name of the new role.
4. To save the new role, click [**Save**]. To save the role and enter another one, click [**Save and Add More**].


To establish entity-role associations:

1. On the **Manage Roles** screen, mark the checkbox in the required role's row for each entity that should be associated with the role.
 - To remove a role's association with an entity level, clear the checkbox for that entity level.
2. To restrict a role so that only users with that role can add other users with that role, mark the checkbox in the Protected Role column.
3. To save your changes, click [**Save**].

To edit a role:

1. On the **Manage Roles** screen, click [] in the Action column next to a role displayed in the table. The *Edit Role* pop-up window opens.
2. In the *Role* field, edit the name of the role.
3. To save your changes, click [**Save**].

To delete a role:

1. On the **Manage Roles** screen, click [] in the Action column next to a role displayed in the table.
2. In the warning box that pops up, click [**Yes, delete...**].


Creating and Managing Permissions









After adding roles to the Permissions System, you can create permissions. Each permission must be associated with a component. If multiple components share a common permission, (e.g., “View only”), then you must create a unique record of that permission for each component.

Figure 8. Manage Component Permissions Screen

Manage Component Permissions

Component: View all components


Add New Permission

Component	Permission	Action
CATSimulator	CATSimulator	 
CoreStandards	Administrator	 
DigitalLibrary	DL Read	 
Item Authoring	Item Authoring	 


You can manage permissions on the **Manage Component Permissions** screen (see [Figure 8](#)). The table on this screen displays the permissions that you add to the Permissions System along with their associated components. You can add, edit, and delete the permissions in this table.

The *Component* drop-down list above the table allows you to filter the table to display only those permissions associated with a selected component. This drop-down list contains only the components that were added on the **Manage Components** screen (see [Figure 6](#)).

To create a new permission for a component:

1. On the Permissions System home screen, click [**Manage Component Permissions**].
2. On the **Manage Component Permissions** screen, click [**Add New Permission**]. The *Add New Permission* pop-up window opens.
3. From the *Component* drop-down list, select the component to which the permission belongs.
4. To add a component permission, enter the permission name in the *Enter New Permission* field.
5. To save the new component permission, click [**Save**]. To save and enter another component permission, click [**Save and Add More**].

To edit an existing component permission:

1. On the **Manage Permissions** screen, click [Edit Permission pop-up window opens.
2. In the *Permission* field, edit the name of the permission. You can use this field to enter a new permission that does not already exist in the system. When changing the permission to another existing permission, you must enter the permission manually. *Note: You cannot edit the permission's associated component in this window.*
3. To save your changes, click [**Save**].

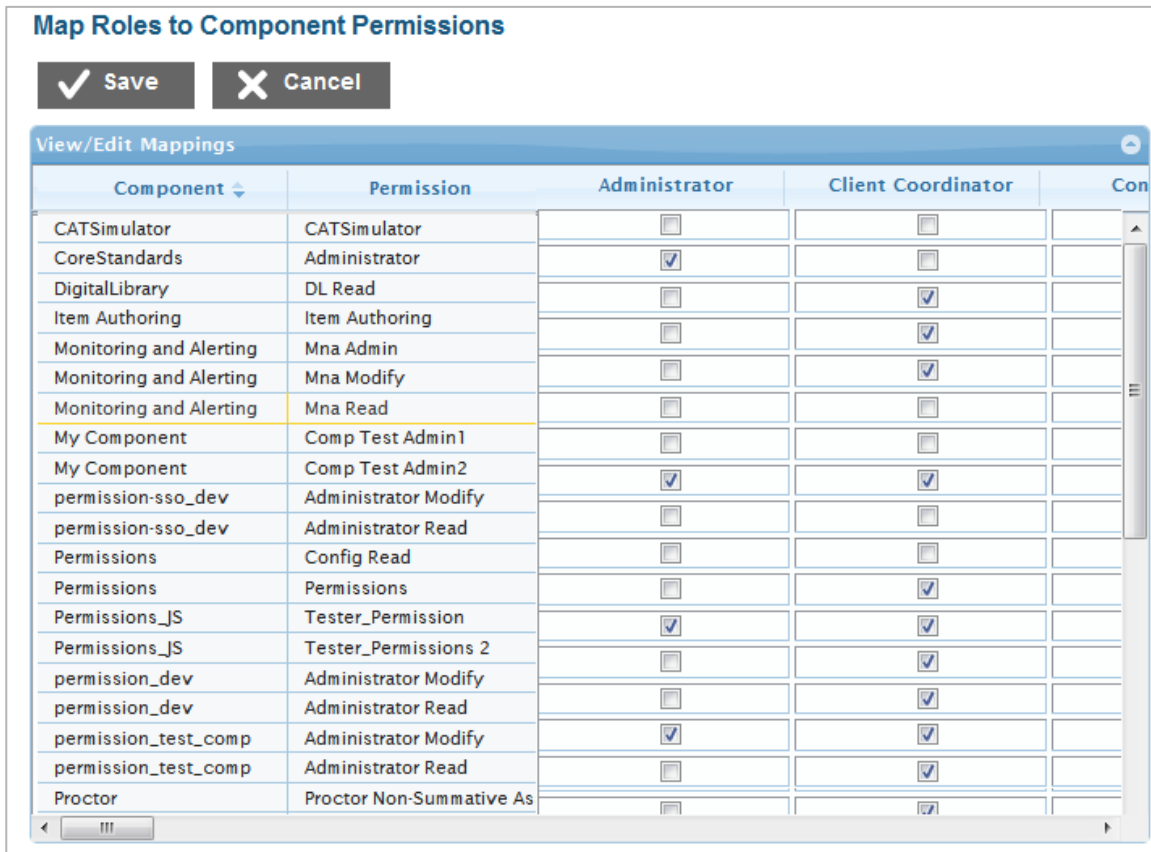
To delete a component permission:

1. On the **Manage Permissions** screen, click [- 2. In the warning box that pops up, click [**Yes, delete...**].

Mapping Roles to Component Permissions

After adding roles and component permissions to the system, you can map the roles to the component permissions. This task allows you to designate which permissions will be available to each role. You can map a single role to multiple permissions, and you can map a single permission to multiple roles.

Figure 9. Map Roles to Component Permissions Screen



Component	Permission	Administrator	Client Coordinator	Con
CATSimulator	CATSimulator	<input type="checkbox"/>	<input type="checkbox"/>	
CoreStandards	Administrator	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
DigitalLibrary	DL Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Item Authoring	Item Authoring	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Monitoring and Alerting	Mna Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Monitoring and Alerting	Mna Modify	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Monitoring and Alerting	Mna Read	<input type="checkbox"/>	<input type="checkbox"/>	
My Component	Comp Test Admin1	<input type="checkbox"/>	<input type="checkbox"/>	
My Component	Comp Test Admin2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
permission-sso_dev	Administrator Modify	<input type="checkbox"/>	<input type="checkbox"/>	
permission-sso_dev	Administrator Read	<input type="checkbox"/>	<input type="checkbox"/>	
Permissions	Config Read	<input type="checkbox"/>	<input type="checkbox"/>	
Permissions	Permissions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Permissions_JS	Tester_Permission	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Permissions_JS	Tester_Permissions 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
permission_dev	Administrator Modify	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
permission_dev	Administrator Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
permission_test_comp	Administrator Modify	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
permission_test_comp	Administrator Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Proctor	Proctor Non-Summative As	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

You can map permissions to roles on the table provided on the **Map Roles to Component Permissions** screen (see [Figure 9](#)). The first two columns in this table list the components and associated permissions you added to the Permissions System. The subsequent columns display checkboxes for each role that you added to the Permissions System.

To map a role to permissions:

1. Mark the checkbox in the row for each permission that should be associated with the role.
 - To remove a permission association for a role, clear the checkbox for that permission.
2. When you are finished, click **[Save]**.