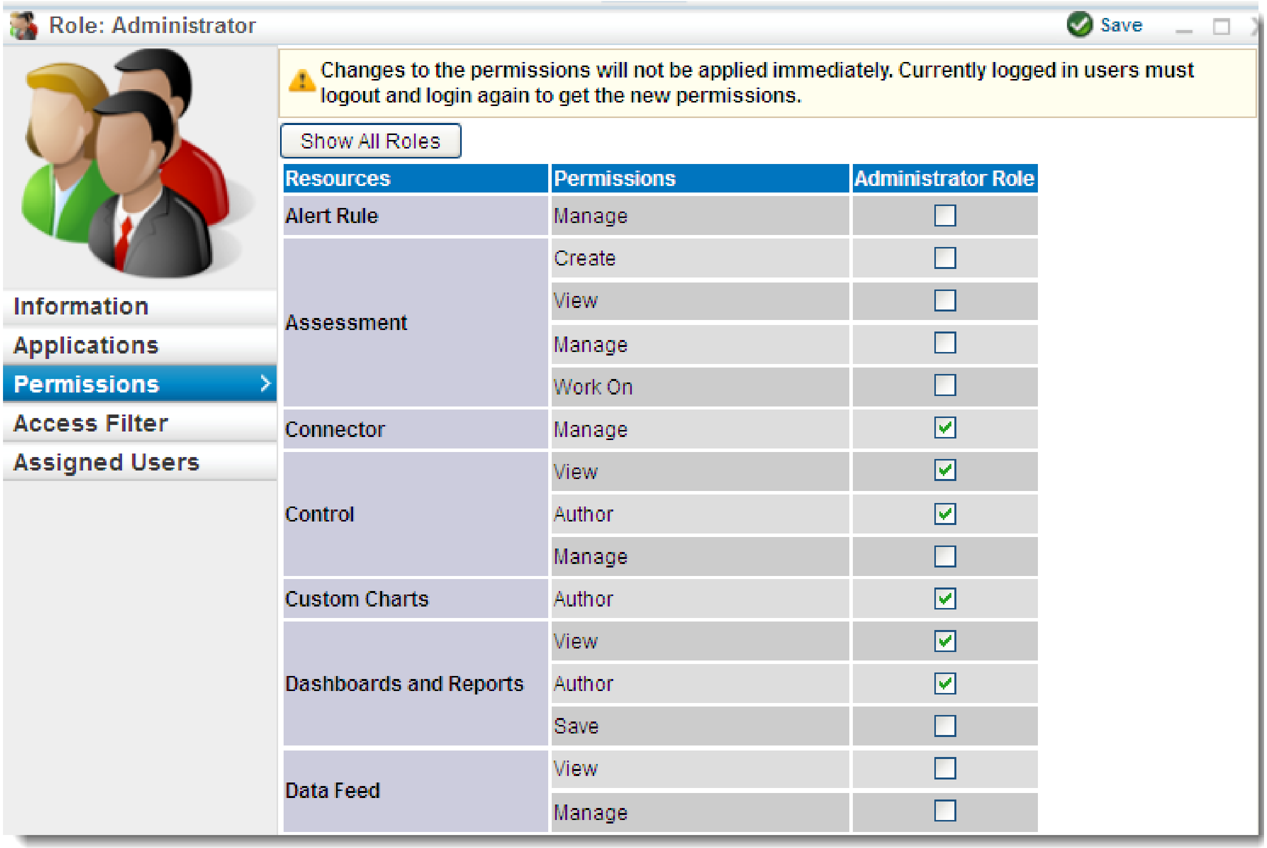
Configuring a Role

When you modify a role, users assigned to the role have the new privilege and access settings the next time they log in. If the user is logged in when you change the role, the new settings will apply within a few minutes.

If you assign more than one role to a user, the user has the highest level of permission in all the roles for each privilege and can access all the entities of each role.

To modify permissions:

1. In the Administration application, go to **Users** > **Roles**.
2. Select a role and click **Details**.
3. Go to the **Permissions** tab and click **Edit**.



Changes to the permissions will not be applied immediately. Currently logged in users must logout and login again to get the new permissions.

Resources	Permissions	Administrator Role
Alert Rule	Manage	□
Assessment	Create	□
	View	□
	Manage	□
	Work On	□
Connector	Manage	☑
Control	View	☑
	Author	☑
	Manage	□
Custom Charts	Author	☑
Dashboards and Reports	View	☑
	Author	☑
	Save	□
Data Feed	View	□
	Manage	□

1. To grant a permission to a role, check the box that is available next to the permission level of a resource type .
2. To remove a permission, clear the selection for that particular permission.
3. Click **Save** when you finish making the changes.

Warning: Clicking **X** at the top right corner of the pane, instead of clicking**Save**, changes the permissions.

To manage entity access for a role:

1. In the Administration application, go to **Users** > **Roles**.
2. Select a role, go to the **Access Filters** tab, and click **Add Filter**.
3. The **Filter** dialog appears. You can apply an **Entity** and **Incident** filter type for a role. Then select the filter type drop-down box to apply a filter based on an entity or an incident.
4. Expand the **Filter** tree to select the desired filter and then click **OK**.

   To delete a filter, select a filter and then click **Delete**.

To manage a role:

1. In the Administration application, go to **Users** > **Roles**.
2. Select a role, then go to the **Assigned Users** tab to view any users that are assigned to that role.
3. To add a user, click **Add**. The **Select Users** dialog appears. In the select user drop-down box, choose the same role that appears on the top-left side of the Role's pane or enter text in the **User Name** field and then click **Search** for users. Based on your search criteria, the usernames appear for you to make a selection. Select a user name and then click **OK**.
4. To remove a user, select a username and then click **Remove**.

Note: By default, all users with the Incident Manage permission can create new incident types and subtypes. If you want to restrict users with the Incident Manage permission from creating new incident types and subtypes, you can use the allow.incident.type.subtype.creation.toRole=User_Role property value to require that, in addition to having to have Manage permissions, users have a specific role in order to be able to create new incident types and subtypes