Lesson 12 Roles and Permissions

12.1 Requirements

In this exercise, investigate the Security Dictionary and then explore the capabilities for certain users and roles to better understand these functions of PolicyCenter. You will create a new role and assign a user to that role.

12.2 Explore permissions and roles

Activity

Use the Security Dictionary to learn about permissions and roles.

Determine which permission grants the ability to perform the listed task, and which role has that permission. The first item is already completed to provide an example.

1. **Create account**
   a) Permission: accountcreate
   b) Roles: Producer, Producer Code – Basics, Superuser, Underwriter, Underwriter Assistant, Underwriting Supervisor
2. **Create a sensitive note**
   a) Permission:
   b) Roles:
3. **View the Authority Profile**
   a) Permission:
   b) Roles:
4. **View underwriting companies**
   a) Permission:
   b) Roles:
5. **Edit a sensitive note**
   a) Permission:
   b) Roles:
6. **View Team tab**
   a) Permission:
   b) Roles:

12.3 List users with roles

Activity

List users with certain roles.

1. **Log in to PolicyCenter as su/gw**
2. **List the following users from the Users page**
   a) All users with the role, Premium Auditor
   b) All Underwriters whose first name begins with “A”
   c) All Producers whose last name begins with the string “arm” and Role: Producer

12.4 Assign a user a specific role

Activity

Configure a user and assign roles and view permissions.

1. **Log in using su/gw**
2. **Create a user named Terry ProcessorXX (replace XX with student number)**
3. **Assign Terry the role of Processor and add the following details**
   - First name: Terry
   - Last name: ProcessorXX (replace XX with student number)
   - Password: Final
   - Confirm password: Sensitive
   - Active: Letter Sent
   - External user: No
   - User type: Other
   - Primary Phone: Work
   - Work Phone: 555-555-5555
4. **Log out and log in as tprocessorXX/gw**
5. **Observe what Terry can do or access within PolicyCenter**

   For example, what is available in the Menu items and the Administration tabs?

6. **The Underwriting department manager has requested access to PolicyCenter for an underwriting clerk.**

   Create a role UW ClerkXX (replace XX with student number) and add three create permissions, three search permissions and three view permissions that you think an underwriting clerk would need. Refer to the underwriter roles in PolicyCenter for a sample permission set.

7. **Assign the role you created, UW ClerkXX, to the user, Terry ProcessorXX**

8. **Verification**
    a) Log out
    b) Log in as tprocessorXX
    c) Verify that Terry has access to the appropriate tasks

Stop

12.5 Solutions

12.5.1 Explore permissions and roles

Solution

Use the Security Dictionary to learn about permissions and roles.

Determine which permission grants the ability to perform the listed task, and which role has that permission. The Security Dictionary is in the folder PolicyCenter/build/dictionary/security. Open the index.html file.

1. **Create account**
    a) Permission: accountcreate
    b) Roles: Producer, Producer Code – Basics, Superuser, Underwriter, Underwriter Assistant, Underwriting Supervisor
2. **Create a sensitive note**
    a) Permission: *createsensnote*
    b) Roles: *Superuser, Underwriter, Underwriting Supervisor*
3. **View the Authority Profile**
    c) Permission: *authprofileview*
    d) Roles: *Community Admin, Superuser, Underwriter, Underwriting Supervisor, User Admin*
4. **View underwriting companies**
    a) Permission: *uwview*
    b) Roles: *Superuser*
5. **Edit a sensitive note**
    a) Permission: *editsensnote*
    b) Roles: *Superuser, Underwriting Supervisor*
6. **View Team tab**
    a) Permission: *viewteam*

b) Roles: *Audit Supervisor, Community Admin, Superuser, Underwriting Supervisor, User Admin*

12.5.2 List users with roles

Solution

List users with certain roles.

1. **Log in to PolicyCenter as su/gw**
2. **List the following users from the Users page**
   a) All users with the role, Premium Auditor
      - Select Role Premium Auditor from the Role dropdown in the Users page
      - Select only on the Role. Do not select any other criteria
      - The only Premium Auditor is **Adam Auditor**
      - All Underwriters whose first name begins with “A”
   b) All Underwriters whose first name begins with “A”
   c) All Producers whose last name begins with the string “arm” and Role: Producer

      First name: “A” and Role: Underwriters are Alice Applegate, Adele Levin, Allie Lee, Albert Munoz, Amy Baxter.

   d) All Producers whose last name begins with the string “arm” and Role: Producer

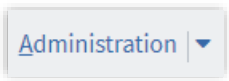
      Archie Armstrong, Peyton Armstrong, Eli Armstrong

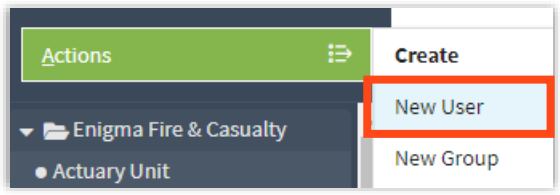
12.5.3 Assign a user a specific role

Solution

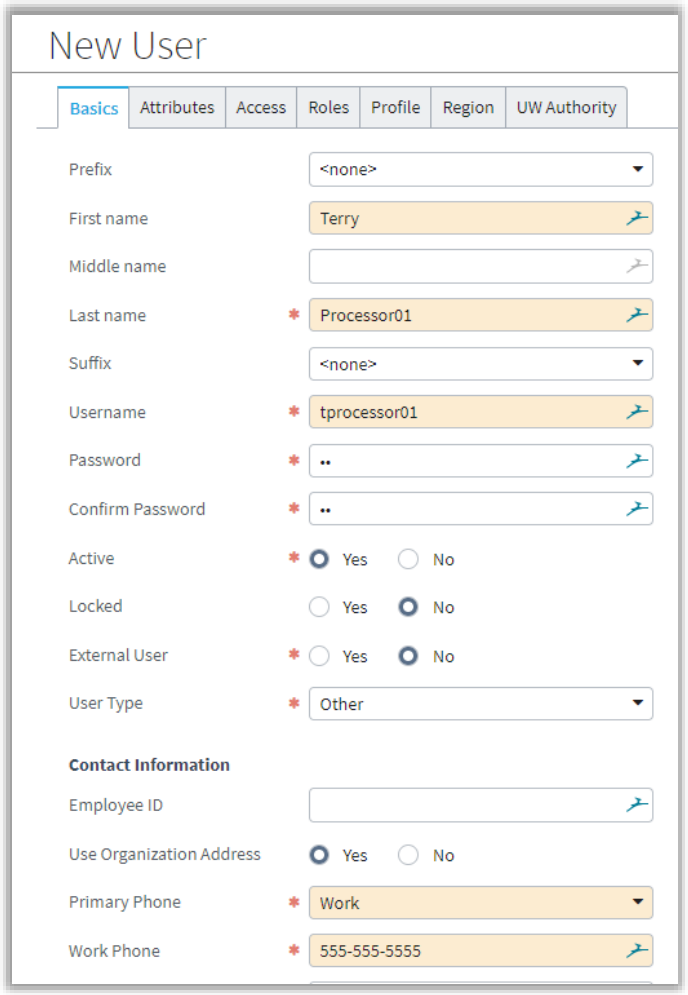
Configure a user and assign roles and view permissions.

1. **Log in using su/gw**
2. **Create a user named Terry ProcessorXX (replace XX with student number)**
3. **Assign Terry the role of Processor and add the following details**
   a) Select the Administration tab, then select **Actions → New User** from the left navigation pane





b) Enter the details in the New User interface. Select Update in the upper right corner when done.



4. **Log out. Log in as tprocessorXX/gw**
5. **Observe what Terry can do or access within PolicyCenter**

   For example, what is available to him in the Menu items and the Administration tabs?

   He can only see the Policy and Contacts tab and Search for Contacts. He has very few functions under the Administration tab.

6. **The Underwriting department manager has requested access to PolicyCenter for an underwriting clerk.**

Create a role UW ClerkXX (replace XX with student number) and add three create permissions, three search permissions and three view permissions that you think an underwriting clerk would need. Refer to the underwriter roles in PolicyCenter for a sample permission set.

a) Log out and log in as su/gw

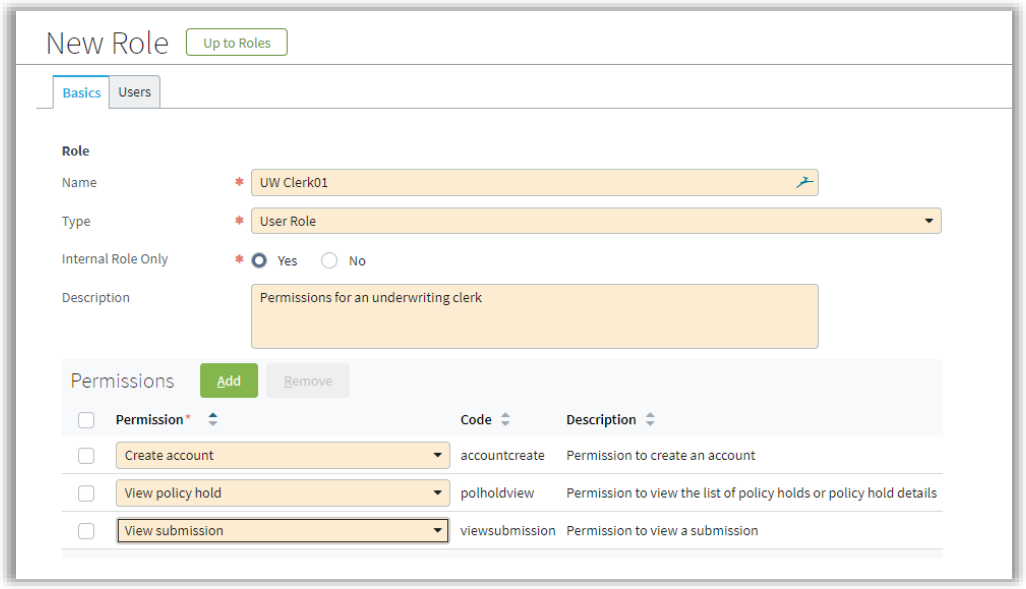
b) Go to Administration → Users & Security → Roles, and New Role

c) Enter information for the new Role

d) Add permissions. Answers vary. This example only allows three permissions

e) Enter the localization text for the name and description of the role. You can use the same text for all languages.

f) Click Update in the upper right corner to save the new information



7. Assign the role you created, UW ClerkXX, to the user, Terry ProcessorXX

a) Find the user in the User screen (Administration → Users & Security → Users)

b) Open the user and click the Roles tab

c) Add role UW ClerkXX to the user

8. Verification

a) Log out

b) Log in as tprocessorXX

c) Verify that Terry has access to the appropriate tasks

Various results will be displayed depending on the permissions granted.

12.6 References

12.6.1 Roles and permissions

Review

A system permission is a granular ability to see or do something within PolicyCenter. It is defined in the SystemPermissionType typelist. The entire list of system permissions can be seen in the Security Dictionary. Whether a user has a given permission can determine what they can view/navigate, create, edit, delete, own, or act upon. A user's permissions are determined during login. A role is a named collection of permissions used to simplify the assignment of permissions to users. Typically, a role maps to a job title or a job function. Each user is given one or more roles and has all the permissions included in the roles assigned to them.

A role type indicates which entities that role can be assigned to.

- A user role can be assigned only to a user
- A producer code role can be assigned to a producer code only
- A user producer code role can be assigned to either users or producer codes

Managing roles

1. **Managing roles through Administration ->Users & Security -> Roles**
2. **Click "New Role" to add a new role**
3. **Roles can also be deleted. Be careful not to delete roles that are already assigned to users.**

Creating a new role

1. **Enter name**
2. **Choose role type**
3. **Specify if the role is internal only**
4. **Add permissions**
5. **Click Update**

Assigning roles to a user

1. **Go to the Roles tab**
2. **In edit mode, add or remove, or change rules if you need to**
3. **Click Update to save the changes**

12.6.2 Security dictionary

Review

The Security Dictionary is a series of HTML pages documenting the permissions and roles in the application. The Security dictionary is located at: <serverdirectory>\build\dictionary\security\ index.html. The dictionary has four main sections:

An application permission key is a set of one or more system permissions. PolicyCenter defines application permission keys internally as a method to improve system performance. For example, the accountedit permission key represents the system permissions for editing an account, and accountreopen to reopen a withdrawn account. Application permission keys appear in the files used to specify the user interface, therefore, its users must know what they are and how they act. Users cannot create or modify application permission keys. **The Application Permission Keys** section of the security dictionary lists each application permission key, the set of system permissions it contains, and the pages and elements in the user interface that reference the application permission key.

The **Pages** section of the security dictionary lists each page in the user interface and the permissions needed to view or edit that page (if any). By clicking on any of the permissions listed in the right pane, the user is taken to the list of pages that have that permission set.

The System permissions are permissions defined in the SystemPermissionType typelist. Permissions that appear grayed are internal and cannot be modified. The **System Permissions** section of the security dictionary lists each system permission, the roles containing the system permission, and the pages and elements in the user interface referencing the system permission.

The **Roles** section of the security dictionary lists each role and the permissions it contains. The security dictionary is a series of static HTML pages. If changes are made to the permissions in each role, the security dictionary must be regenerated to reflect those changes. Users can update the security dictionary through a command-line utility tool, “regen-dictionary”, which is covered in the Insurance Suite Fundamentals course.

Stop