Abstract

This guide is for Red Hat account users who want to use the User Access feature to configure role-based access control (RBAC) for services hosted on the Red Hat Hybrid Cloud Console.
# Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE .......................................................... 3

PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION .................. 4

CHAPTER 1. USER ACCESS CONFIGURATION GUIDE FOR ROLE-BASED ACCESS CONTROL (RBAC) .... 5
    1. WHAT IS USER ACCESS .......................... 5
        1.1. User Access and the Software as a Service (SaaS) access model 5
        1.2. Who can use User Access 5
        1.3. How to use User Access 5
            1.3.1. The Default admin access group 6
            1.3.2. The Default access group 6
            1.3.3. The User Access groups, roles, and permissions 6
            1.3.4. Additive access 7
            1.3.5. Access structure 7

CHAPTER 2. PROCEDURES FOR CONFIGURING USER ACCESS ............................................. 8
    2. PROCEDURES FOR CONFIGURING USER ACCESS .......................... 8
        2.1. Creating a User Access administrator 8
        2.2. Viewing roles and permissions 9
        2.3. Managing group access with roles and members 10
        2.4. Restricting service access to a single user 10
        2.5. Including an Organization Administrator in a group 12
        2.6. Disabling group access 13
        2.7. Granular permissions for User Access 13
            2.7.1. Adding custom User Access roles 14
            2.7.2. Creating a role from scratch 14
            2.7.3. Copying an existing role 15
            2.7.4. Creating an application-specific role 16
            2.7.5. Creating cost management application roles 17
                2.7.5.1. Cost management example for creating a role from scratch 18
            2.7.6. Editing custom role names 18
            2.7.7. Removing permissions from a custom role 19

CHAPTER 3. PREDEFINED USER ACCESS ROLES ....................................................... 20
    3. PREDEFINED USER ACCESS ROLES ........................................... 20
MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
PROVIDING FEEDBACK ON RED HAT HYBRID CLOUD CONSOLE DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so, create a Bugzilla ticket:

1. Go to the Bugzilla website.
2. As the Component, use Documentation.
3. Fill in the Description field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
4. Click Submit Bug.
CHAPTER 1. USER ACCESS CONFIGURATION GUIDE FOR ROLE-BASED ACCESS CONTROL (RBAC)

1.1. WHAT IS USER ACCESS

The User Access feature is an implementation of role-based access control (RBAC) that controls user access to various services hosted on the Red Hat Hybrid Cloud Console. You configure the User Access feature to grant user access to services hosted on Hybrid Cloud Console.

1.1.1. User Access and the Software as a Service (SaaS) access model

Red Hat customer accounts might have hundreds of authenticated users, yet not all users need the same level of access to the SaaS services available on Red Hat Hybrid Cloud Console. With the User Access features, an Organization Administrator can manage user access to services hosted on Red Hat Hybrid Cloud Console.

NOTE

User Access does not manage OpenShift Cluster Manager permissions. For OpenShift Cluster Manager, all users in the organization can view information, but only an Organization Administrator and cluster owners can perform actions on clusters.

1.1.2. Who can use User Access

To initially view and manage User Access on Red Hat Hybrid Cloud Console, you must be an Organization Administrator. This is because User Access requires user management capabilities that are designated from the Red Hat Customer Portal at Customer Portal. Those capabilities belong solely to the Organization Administrator.

The User Access administrator role is a special role that the Organization Administrator can assign. This role allows users who are not Organization Administrator users to manage User Access on Red Hat Hybrid Cloud Console.

1.1.3. How to use User Access

The User Access feature is based on managing roles rather than by assigning permissions individually to specific users. In User Access, each role has a specific set of permissions. For example, a role might allow read permission for an application. Another role might allow write permission for an application.

You create groups that contain roles and, by extension, the permissions assigned to each role. You assign users to groups. This means each user in a group is assigned the permissions of the roles in that group.

By creating different groups and adding or removing roles for that group, you control the permissions allowed for that group. When you add one or more users to a group, those users can perform all actions that are allowed for that group.

Red Hat provides two default access groups for User Access:

- Default admin access group. The Default admin access group is limited to Organization Administrator users in your organization. You cannot change or modify the roles in the Default admin access group.
Default access group. The Default access group contains all authenticated users in your organization. These users automatically inherit a selection of predefined roles.

Red Hat provides a set of predefined roles. Depending on the application, the predefined roles for each supported application might have different permissions that are tailored to the application.

1.1.3.1. The Default admin access group

The Default admin access group is provided by Red Hat on Red Hat Hybrid Cloud Console. It contains a set of roles that are assigned to all users who have an Organization Administrator role on your system. The roles in this group are predefined in Red Hat Hybrid Cloud Console.

The roles in the Default admin access group cannot be added to or modified. Because this group is provided by Red Hat, it is automatically updated when Red Hat assigns roles to the Default admin access group.

The benefit of the Default admin access group is that it allows roles to be assigned automatically to Organization Administrators.

See Section 3.1, “Predefined User Access roles” for the roles are included in the Default admin access group.

1.1.3.2. The Default access group

The Default access group is provided by Red Hat on Red Hat Hybrid Cloud Console. It contains a set of roles that are predefined in Red Hat Hybrid Cloud Console. The Default access group includes all authenticated users in your organization. One advantage of the Default access group is that it is automatically updated when Default access group roles are added in Red Hat Hybrid Cloud Console.

NOTE

The Default access group contains a subset of all predefined roles. See Section 3.1, “Predefined User Access roles”.

As an Organization Administrator, you can add roles to and remove roles from the Default access group. Changes you make to the Default access group affect all authenticated users in your organization.

When you manually modify the Default access group, its name changes to Custom default access, which indicates it was modified. Moreover, it is no longer automatically updated from Red Hat Hybrid Cloud Console.

NOTE

If you change and save the Default access group, its name changes to Custom default access. You cannot revert or undo the name change. From that point forward, an Organization Administrator is responsible for all updates and changes to the group. The Custom default access group is no longer managed or updated by Red Hat Hybrid Cloud Console.

The Default access group or Custom default access group cannot be deleted. You can create new access groups that use predefined roles, custom roles, or a combination of both.

1.1.3.3. The User Access groups, roles, and permissions
User Access uses the following categories to determine the level of user access that an Organization Administrator can grant to the supported Red Hat Hybrid Cloud Console services. The access provided to any authorized user depends on the group that the user belongs to and the roles assigned to that group.

- **Group**: A collection of users belonging to an account which provides the mapping of roles to users. An Organization Administrator can use groups to assign one or more roles to a group and to include one or more users in a group. You can create a group with no roles and no users.

- **Roles**: A set of permissions that provide access to a given service, such as Insights. The permissions to perform certain operations are assigned to specific roles. Roles are assigned to groups. For example, you might have a read role and a write role for a service. Adding both roles to a group grants all members of that group read and write permissions to that service.

- **Permissions**: A discrete action that can be requested of a service. Permissions are assigned to roles.

An Organization Administrator adds or deletes roles and users to groups. The group can be a new group created by an Organization Administrator or the group can be an existing group. By creating a group that has one or more specific roles and then adding users to that group, you control how that group and its members interact with the Red Hat Hybrid Cloud Console services.

When you add users to a group, they become members of that group. A group member inherits the roles of all other groups they belong to. The user interface lists users in the Members tab.

### 1.1.3.4. Additive access

User access on Red Hat Hybrid Cloud Console uses an additive model, which means that there are no deny roles. In other words, actions are only permitted. You control access by assigning the appropriate roles with the desired permissions to groups then adding users to those groups. The access permitted to any individual user is a sum of all roles assigned to all groups to which that user belongs.

### 1.1.3.5. Access structure

The following points are a summary of the user access structure for User Access:

- **Group**: A user can be a member of one or many groups.

- **Role**: A role can be added to one or many groups.

- **Permissions**: One or more permissions can be assigned to a role.

In its initial default configuration, all User Access account users inherit the roles that are provided in the Default access group.

**NOTE**

Any user added to a group must be an authenticated user for the organization account on Red Hat Hybrid Cloud Console.
CHAPTER 2. PROCEDURES FOR CONFIGURING USER ACCESS

2.1. PROCEDURES FOR CONFIGURING USER ACCESS

As an Organization Administrator or User Access administrator, you can click (Settings) to view, configure, and modify the User Access groups, roles, and permissions.

2.1.1. Creating a User Access administrator

The User Access administrator is a special role that the Organization Administrator assigns to a group. All users in this group can perform User Access administration roles, such as adding, modifying, or deleting groups and roles. The User Access administrator role does not inherit the roles defined in the Default Admin Access group.

The User Access administrator role cannot create or modify a User Access administrator group. Only the Organization Administrator can create, modify, or delete a group that is assigned the User Access administrator role.

By having the User Access administrator role, users who are not the Organization Administrator can perform many of the Organization Administrator functions for managing the User Access features. The User Access administrator role does not inherit the roles of the Default admin access group. The roles in that group are restricted to the Organization Administrator.

Prerequisites

- You must be an Organization Administrator.
- You started the Create role wizard.
- You are at the Add permissions step in the wizard.

Procedure

1. Log in to your Red Hat organization account at Red Hat Hybrid Cloud Console.
2. Click the Settings icon (gear) to open the Settings page.
3. On the Settings page, click the User access tab to expand it.
4. Click the Groups tab to display the Groups page.
5. Click Create group.
6. Follow the guided actions provided by the wizard to create the group and add users and roles.
   a. Name the group with a recognizable name: User Access Admin.
   b. Provide a meaningful description: User Access Organization Administrator permissions
   c. Click the Next button to add roles.
   d. Search for the User Access administrator role and click the selection box to add this role to the group. Optionally, select additional roles.
e. Click the **Next** button to add members to the group.

**NOTE**

Any member you add must be an active member of the organization account.

f. After you select the members for the group, click the **Next** button to review the details.

g. You can click the **Back** button to go back and make changes, or the **Cancel** button to cancel the action.

7. Click the **Submit** button to complete the **Create group** wizard. The new group will appear in the **Groups** tab.

### 2.1.2. Viewing roles and permissions

You can view the roles and permissions for User Access at Red Hat Hybrid Cloud Console. See Chapter 3, *Predefined User Access roles* for a list of predefined roles provided by Red Hat.

**NOTE**

You cannot modify a predefined role.

**Prerequisites**

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the **User Access administrator** role assigned to it.

**Procedure**

1. Log in to your Red Hat organization account at Red Hat Hybrid Cloud Console.

2. Click the Settings icon (gear) to open the **Settings** page.

3. On the **Settings** page, click on the **User access** tab to expand it.

4. Click the **Roles** tab to display the User Access roles. You can scroll through the list of all Roles.
5. In the table, click either the role **Name** or the role **Permissions** to see details about the permissions assigned to the role. For example, if you click on the **Cost Price List Viewer** role, you see the following information.

<table>
<thead>
<tr>
<th>Application</th>
<th>Resource type</th>
<th>Operation</th>
<th>Last commit</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost-management</td>
<td>cost.model</td>
<td>read</td>
<td>4 months ago</td>
</tr>
</tbody>
</table>

An asterisk * indicates a wildcard permission. A wildcard permission grants access to all resource types and allows all operations for the applications in a role.

### 2.1.3. Managing group access with roles and members

You can manage group access by creating a group and adding roles and users to the group. The roles and their permissions determine the type of access granted to all members of the group.

The **Member** tab shows all users that you can add to the group. When you add users to a group, they become members of that group. A group member inherits the roles of all other groups they belong to.

**Prerequisite**

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the **User Access administrator** role assigned to it.

**NOTE**

Only the Organization Administrator can assign the **User Access administrator** role to a group.

**Procedure**

1. Log in to your Red Hat organization account at [Red Hat Hybrid Cloud Console](https://www.redhat.com).
2. Click the Settings icon (gear) to open the **Settings** page.
3. On the **Settings** page, click the **User access** tab to expand it.
4. Click the **Groups** tab to display the **Groups** page.
5. Click **Create group**
6. Follow the guided actions provided by the wizard to add users and roles.
7. To grant additional group access, edit the group and add additional roles.

### 2.1.4. Restricting service access to a single user
You can create a new group that contains a single user and add a role to that group. The role you add provides the service access permissions you want that single user to have. If you add other users to the group, the added users will have the same group permissions.

The roles you add to the group can be from the predefined list of roles provided with User Access, from custom roles created by an Organization Administrator, or a combination of both.

When you add a user to a new group, the user acquires the permissions of the new group and also inherits the permissions of all other groups they belong to. The permissions of the new group are added to their existing permissions.

**IMPORTANT**

In this procedure you modify the Default access group. Once modified, you cannot restore the Default access group. When you modify the Default access group its name changes to Custom default access. The Custom default access group is no longer updated with changes pushed out by Red Hat from Red Hat Hybrid Cloud Console.

**Prerequisites**

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.

**Procedure**

1. Log in to your Red Hat organization account at Red Hat Hybrid Cloud Console.
2. Click the Settings icon (gear) to open the Settings page.
3. On the Settings page, click the User access tab to expand it.
4. Click the Groups tab to display the Groups page.
5. Remove all roles from the Default access group.
   Because all users in your organization belong to the Default access group, you cannot add or remove single users in Default access to create access control. By removing all roles, users do not inherit role permissions from Default access.
6. Save the changes to Default access group. The name changes to Custom default access.
7. Create a new group that contains the users and roles for the allowed access permissions.
   For example, create a group Security Admin that contains the users who will have full access to Vulnerability services.
   a. Create a group Security Admin.
   b. Add one or several users to the group from the Members list.
   c. Add the Vulnerability administrator role.
      Each user you add to this group has full access to the Vulnerability service.
2.1.5. Including an Organization Administrator in a group

You can include an Organization Administrator in a group. You add an Organization Administrator user to a group if you want an Organization Administrator to have the roles assigned to that group. An Organization Administrator does not inherit all available roles for all Red Hat Hybrid Cloud Console applications. Any roles not inherited by means of the Default access group or the Default admin access group must be assigned through group membership.

Prerequisites

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.
- Create a group if one does not exist.
  
  Section 2.1.3, “Managing group access with roles and members”

Procedure

1. Log in to your Red Hat organization account at Red Hat Hybrid Cloud Console.
2. Click the Settings icon (gear) to open the Settings page.
3. On the Settings page, click the User access tab to expand it.
4. Click the Groups tab to display the Groups page.
5. Click the group Name to display details about the group.
6. On the group details page, click the Members tab to display a list of authorized users who are a member of the group.
7. Click the Add member tab.
8. On the Add members to the group page that appears, find the Organization Administrator user name and click the check box next to the name.
   For example, if the Organization Administrator user name is smith-jones, find that name and click the check box next to smith-jones. You can add additional names.
9. Verify the name list is complete and click the Add to group action.

Notification pop-ups appear when the action successfully completes.
2.1.6. Disabling group access

You can disable group access by removing roles from a group. Because the roles and their permissions determine the type of access granted to the group, removing roles disables group access for that role.

Prerequisite

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.

Procedure

1. Log in to your Red Hat organization account at Red Hat Hybrid Cloud Console.
2. Click the Settings icon to open the Settings page.
3. On the Settings page, click the User access tab to expand it.
4. Click the Groups tab to display the Groups page.
5. Click the Group Name that you want to modify.
6. Click the Roles tab.
7. Click the check box next to roles Name that you want to remove. You can click the check box at the top of the Name column to select all roles.
8. Click the More options menu icon that is next to the Add role tab, and then click Remove from group.
9. In the confirmation window that appears, click either Remove role or Cancel to complete the action.

**NOTE**

Groups can contain no roles and no members and still be a valid group.

2.1.7. Granular permissions for User Access

Granular permissions allow an Organization Administrator to define role permissions for one or more applications. Many of the predefined roles provide wildcard permissions, which is equivalent to a super user role with full access to all actions.

By defining granular permissions, you can create (or modify) roles with limited permissions, such as read-only, or read and update but not delete.

As an example, compare the predefined roles of Cost Administrator and Cost Price List Viewer.

<table>
<thead>
<tr>
<th>Role</th>
<th>Application</th>
<th>Resource</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Administrator</td>
<td>cost-management</td>
<td>* (all)</td>
<td>* (all)</td>
</tr>
</tbody>
</table>
By creating a new role, you can define the applications, resources, and operations that are specific to that role.

### 2.1.7.1. Adding custom User Access roles

User Access provides a number of predefined roles that you can add to groups. In addition to using the predefined roles, you can create and manage custom User Access roles with granular permissions for one or more applications.

See Chapter 3, Predefined User Access roles for a list of predefined roles provided by Red Hat.

**NOTE**

You cannot modify a predefined role.

**Prerequisites**

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.

**Procedure**

A guided wizard leads you through the steps for adding a role. The following steps describe how to use the Create role wizard.

1. Log in to Red Hat Hybrid Cloud Console as a user who has Organization Administrator privileges.

2. From the home page after you log in, click \(\) (Settings) to open the Settings window.

3. Click the User Access tab to expand the drop-down choices.

4. Click the Roles tab. The Roles window appears.

5. Click the Create role button. This starts the Create role wizard.

At this point in the wizard, you can create a role from scratch or copy an existing role.

### 2.1.7.2. Creating a role from scratch

Create a role from scratch when you want to create a role with specific granular permissions. For example, you can create a single role for your organization that provides read-only permissions across all resources for all available applications. By adding and managing this role in your default access group, you can change default access to read-only.

**Prerequisites**

<table>
<thead>
<tr>
<th>Role</th>
<th>Application</th>
<th>Resource</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Price List Viewer</td>
<td>cost-management</td>
<td>cost_model</td>
<td>read</td>
</tr>
</tbody>
</table>
You must be an Organization Administrator.

If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.

You started the Create role wizard.

Procedure

1. In the Create role wizard, click the Create a role from scratch button.

2. Enter a Role name, which is required.

3. Optionally, enter a Role description.

4. Click the Next button. If the role name already exists, you must provide a different name before you can proceed.

5. Use the Add permissions window to select the application permissions to include in your role. By default, permissions are listed by application.

6. Optionally use the filter drop-down to filter by Applications, Resources, or Operations.

TIP

Use the list at the top of the wizard page to view all the permissions added to the role. You can click a permission to delete it.

7. Click the Next button to review details. You can click the Submit button to submit the role, the Back button to go back and make changes, or the Cancel button to cancel the action.

The role you created is available to add to a User Access group.

2.1.7.3. Copying an existing role

Copy an existing role when that role already contains many of the permissions you want to use and you need to change, add, or remove some permissions.

An existing role can be one of the predefined roles provided by Red Hat or it can be a previously created custom role. See Chapter 3, Predefined User Access roles for a list of predefined roles provided by Red Hat.

NOTE

You cannot modify a predefined role.

Prerequisites

- You must be an Organization Administrator.

- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.

- You started the Create role wizard.
Procedure

1. In the Create role wizard, click the Copy an existing role button.

2. Click the button next to the role you want to copy.

3. Click the Next button.

4. The Name and description window shows a copy of the Role name and the existing Role description filled in. Make changes as needed.

5. Click the Next button. If the role name already exists, you must provide a different name before you can proceed.

6. Use the Add permissions window to select the application permissions to include in your role. By default, permissions are listed by application.

   **TIP**
   
   Custom roles only support granular permissions. Wildcard permissions, such as `approval:*:*` are not copied into a custom role.

7. Optionally use the filter drop-down to filter by Applications, Resources, or Operations.

   **TIP**
   
   Use the list at the top of the wizard page to view all the permissions added to the role. You can click a permission to delete it.

8. Click the Next button to review details. You can click the Submit button to submit the role, the Back button to go back and make changes, or the Cancel button to cancel the action.

The role you created is available to add to a User Access group.

2.1.7.4. Creating an application-specific role

Use the filters provided by the Create role wizard to create a role for a specific application. When you create a role for a specific application, the filters display the allowed Resource type and Operation for the selected application.

You can create application-specific roles that include more than one application.

**Prerequisites**

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.
- You started the Create role wizard.
- You are at the Add permissions step in the wizard.

**Procedure**
1. In the Add permissions window, click in the Filter by application field.

2. Choose the application by typing the first few letters of application name. The wizard shows the matching permissions for that application.

3. Optionally, use the navigation tools to scroll through the list of available applications and permissions.

4. Click the check box next to the permissions that you want in the application-specific role.

5. Click the Next button to review details. You can click the Submit button to submit the role, the Back button to go back and make changes, or the Cancel button to cancel the action.

2.1.7.5. Creating cost management application roles

You can create a role that is specific to the cost management application. When you create a cost management role, you define cost management resource definitions for that role. Other application roles do not provide that choice.

Prerequisites

- Cost management operator is installed and configured.
- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.
- A minimum of one source is configured for cost management.
- You started the Create role wizard.

Procedure

This procedure describes how to create roles with cost management permissions from scratch.

1. In the Create role window, click on the radio button Create a role from scratch

2. Enter a Role name (required) and a Role description (optional).

3. Click the Next button to display the Add permissions window.

4. Enter cost in the Filter by application field to display the cost management application and click on the cost-management check box.

5. When the Add permissions window appears, click on the check box for each cost management permission to include in this role.

6. Click on the Next button to display the Define Cost Management resources window.

7. You will see a drop-down list of available Resource definitions for each application permission you added to the role. You must click on the check box for at least one resource in each cost management permission.

8. Click the Next button to review details. You can click the Submit button to submit the role, the Back button to go back and make changes, or the Cancel button to cancel the action.
2.1.7.5.1. Cost management example for creating a role from scratch

**Prerequisites**

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.
- A minimum of one source is configured for cost management.
- You started the Create role wizard.

**Procedure**

1. Start the Create role wizard and click on Create a role from scratch
2. Enter AWS Org Unit Cost Viewer for Role name and then click the Submit button. A description is not required.
3. Enter cost in the Filter by application field to display the cost management application and click on the cost-management check box.
4. Click the check box on the line that contains aws.organizational_unit and then click the Next button to display a drop-down list of available Resource definitions for the permission.
5. Click on the check box for at least one resource listed in the Resource definitions list and then click the Next button to review details.
6. After you review the details for this role, which show the Permissions and Resource definitions, click the Submit button to submit the role.

2.1.7.6. Editing custom role names

You can change the name of a custom role from the main roles page or from the Permissions page.

**Prerequisites**

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.
- One or more custom role must exist.

**Procedure**

1. From the home page after you log in, click Settings to open the Settings window.
2. Click the User Access tab to expand the drop-down choices.
3. Click the Roles tab. The Roles window appears. In the Roles window, a custom role has (more options) to the right of its name.
4. Click (more options).

5. Click on Edit to change the role name or description.

6. Click on Delete to remove the custom role.

TIP

You can also click on the role name to open the Permissions window and then click on the (more options) to the right of the role name to access the Edit and Delete actions.

7. A confirmation window appears. After you confirm that this action cannot be undone, the custom role is deleted.

2.1.7.7. Removing permissions from a custom role

You can remove permissions from a custom role.

Prerequisites

- You must be an Organization Administrator.
- If you are not an Organization Administrator, you must be a member of a group that has the User Access administrator role assigned to it.
- One or more custom role must exist.

Procedure

1. From the home page after you log in, click (Settings) to open the Settings window.

2. Click the User Access tab to expand the drop-down choices.

3. Click the Roles tab. The Roles window appears. In the Roles window, a custom role has (more options) to the right of its name.

4. Click on a custom role name to open the Permissions window.

5. In the Permissions list, click the (more options) to the right of an application permission name and click Remove.

6. A confirmation window appears. Click Remove permission.
CHAPTER 3. PREDEFINED USER ACCESS ROLES

3.1. PREDEFINED USER ACCESS ROLES

The following table lists the predefined roles provided with User Access. Some of the predefined roles are included in the Default access group, which includes all authenticated users in your organization.

Only the Organization Administrator users in your organization inherit the roles in the Default admin access group. Because this group is provided by Red Hat, it is updated automatically when Red Hat assigns roles to the Default admin access group.

For more information about viewing predefined roles, see Chapter 2, Procedures for configuring User Access.

NOTE

Predefined roles are updated and modified by Red Hat and cannot be modified. The table might not contain all currently available predefined roles.

Table 3.1. Predefined roles provided with User Access

<table>
<thead>
<tr>
<th>Role name</th>
<th>Description</th>
<th>Default access group</th>
<th>Default admin access group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Administrator</td>
<td>An approval administrator role that grants permissions to manage workflows</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>requests actions and templates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approval User</td>
<td>An approval user role which grants permissions to create/read/cancel a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>request and read workflows.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Approval Approver</td>
<td>An approval approver role that grants permissions to read and approve</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>requests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation Analytics</td>
<td>An Automation Analytics Administrator role that grants ALL permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation Analytics</td>
<td>An Automation Analytics Editor role that grants read-write permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Editor</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Role name</td>
<td>Description</td>
<td>Default access group</td>
<td>Default admin access group</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Automation Analytics Viewer</td>
<td>An Automation Analytics Viewer role that grants read permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog Administrator</td>
<td>A catalog administrator roles grants create/read/update/delete and order permissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalog User</td>
<td>A catalog user roles grants read and order permissions</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Compliance administrator</td>
<td>Perform any available operation against any Compliance resource.</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>RHC Administrator</td>
<td>Perform any operations on the service enablement dashboard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RHC Viewer</td>
<td>Can view the service enablement dashboard</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cost Administrator</td>
<td>A cost management administrator role that grants read and write permissions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost Price List Administrator</td>
<td>A cost management role that grants read and write permissions on cost models.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost Price List Viewer</td>
<td>A cost management role that grants read permissions on cost models.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost Cloud Viewer</td>
<td>A cost management role that grants read permissions on cost reports related to cloud sources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role name</td>
<td>Description</td>
<td>Default access group</td>
<td>Default admin access group</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Cost OpenShift Viewer</td>
<td>A cost management role that grants read permissions on cost reports related to OpenShift sources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drift analysis administrator</td>
<td>Perform any available operation against any Drift Analysis resource.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Insights administrator</td>
<td>Perform any available operation against any RHEL Advisor resource.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Inventory administrator</td>
<td>Perform any available operation against any Inventory resource.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Malware detection administrator</td>
<td>Perform any available operation against any malware-detection resource.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware detection viewer</td>
<td>Read any malware-detection resource.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Migration Analytics administrator</td>
<td>Perform any available operation against any Migration Analytics resource.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Notifications administrator</td>
<td>Perform any available operation against Notifications and Integrations applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notifications viewer</td>
<td>Read only access to notifications and integrations applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCP Advisor administrator</td>
<td>Perform any available operation against any OCP Advisor resource.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Role name</td>
<td>Description</td>
<td>Default access group</td>
<td>Default admin access group</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Patch administrator</td>
<td>Perform any available operation against any Patch resource.</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Policies administrator</td>
<td>Perform any available operation against any Policies resource.</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>User Access administrator</td>
<td>Grants a non-org admin full access to configure and manage user access to services hosted on console.redhat.com. This role can only be viewed and assigned by Organization Administrators.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Access principal viewer</td>
<td>Grants a non-org admin read access to principals within user access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediations administrator</td>
<td>Perform any available operation against any Remediations resource.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediations user</td>
<td>Perform create view update delete operations against any Remediations resource.</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Resource Optimization administrator</td>
<td>Perform any available operation against any Resource Optimization resource.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Optimization user</td>
<td>A Resource Optimization user role that grants read only permission.</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Sources administrator</td>
<td>Perform any available operation against any Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscription Watch administrator</td>
<td>Perform any available operation against any Subscriptions resource.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role name</td>
<td>Description</td>
<td>Default access group</td>
<td>Default admin access group</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Subscriptions user</td>
<td>View any Subscriptions resource.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Vulnerability administrator</td>
<td>Perform any available operation against any Vulnerability resource.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Vulnerability viewer</td>
<td>Read any Vulnerability resource.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>