How to use the User Access feature to configure RBAC for services hosted on the Red Hat Hybrid Cloud Console
How to use the User Access feature to configure RBAC for services hosted on the Red Hat Hybrid Cloud Console
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. 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.
Table of Contents

CHAPTER 1. USER ACCESS CONFIGURATION GUIDE FOR ROLE-BASED ACCESS CONTROL (RBAC) .................. 3
1.1. USER ACCESS AND THE SOFTWARE AS A SERVICE (SAAS) ACCESS MODEL 3
1.2. WHO CAN USE USER ACCESS 3
1.3. HOW TO USE USER ACCESS
   1.3.1. The Default admin access group 4
   1.3.2. The Default access group 4
   1.3.3. The Custom default access group 4
   1.3.4. The User Access groups, roles, and permissions 5
   1.3.5. Additive access 5
   1.3.6. Access structure 5

CHAPTER 2. PROCEDURES FOR CONFIGURING USER ACCESS ......................................................... 7
2.1. CREATING A USER ACCESS ADMINISTRATOR 7
2.2. VIEWING ROLES AND PERMISSIONS 8
2.3. VIEWING USER PERMISSIONS 8
2.4. MANAGING GROUP ACCESS WITH ROLES AND MEMBERS 9
   2.4.1. Adding a role to a group 10
   2.4.2. Adding a user to a group 11
2.5. RESTRICTING SERVICE ACCESS TO A SINGLE USER 11
2.6. INCLUDING AN ORGANIZATION ADMINISTRATOR IN A GROUP 13
2.7. DISABLING GROUP ACCESS 13
2.8. GRANULAR PERMISSIONS FOR USER ACCESS 14
   2.8.1. Adding custom User Access roles 14
   2.8.2. Creating a role from scratch 15
   2.8.3. Copying an existing role 16
   2.8.4. Creating an application-specific role 17
   2.8.5. Creating cost management application roles 18
   2.8.5.1. Cost management example for creating a role from scratch 18
   2.8.6. Editing custom role names 19
   2.8.7. Removing permissions from a custom role 20
   2.8.8. Restoring the Default access group 20

CHAPTER 3. HOW TO ENABLE RED HAT ACCOUNT TEAM ACCESS FOR CUSTOMER SUPPORT ............. 22
3.1. USING THE ACCESS REQUEST FEATURE TO PROVIDE ACCESS TO A CUSTOMER ACCOUNT 22
   3.1.1. Approving access to your account 22
   3.1.2. Denying access to your account 23
   3.1.3. Requesting access to a customer account (Red Hat support team) 24

CHAPTER 4. PREDEFINED USER ACCESS ROLES ................................................................. 26

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION ......................................................... 33
CHAPTER 1. USER ACCESS CONFIGURATION GUIDE FOR ROLE-BASED ACCESS CONTROL (RBAC)

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 the Hybrid Cloud Console.

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 the Red Hat Hybrid Cloud Console. With the User Access features, an Organization Administrator can manage user access to services hosted on the 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. See Configuring access to clusters in OpenShift Cluster Manager in the Openshift Cluster Manager documentation for details.

1.2. WHO CAN USE USER ACCESS

To initially view and manage User Access on the 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 the Red Hat Hybrid Cloud Console.

1.3. HOW TO USE USER ACCESS

The User Access feature is based on managing roles rather than by individually assigning permissions 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.

**NOTE**

You can make changes to the **Default access** group. However, when you do so, its name changes to **Custom default access** group.

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.

1.3.1. The Default admin access group

The **Default admin access** group is provided by Red Hat on the [Red Hat Hybrid Cloud Console](https://redhathybridcloudconsole.com). 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 the [Red Hat Hybrid Cloud Console](https://redhathybridcloudconsole.com).

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 [Predefined User Access roles](#), for the roles are included in the **Default admin access** group.

1.3.2. The Default access group

The **Default access** group is provided by Red Hat on the [Red Hat Hybrid Cloud Console](https://redhathybridcloudconsole.com). It contains a set of roles that are predefined in the [Red Hat Hybrid Cloud Console](https://redhathybridcloudconsole.com). The **Default access** group includes all authenticated users in your organization. The **Default access** group is automatically updated when **Default access** group roles are added in the [Red Hat Hybrid Cloud Console](https://redhathybridcloudconsole.com).

**NOTE**

The **Default access** group contains a subset of all predefined roles. For more information, see section [Predefined User Access roles](#).

As an Organization Administrator, you can add roles to and remove roles from the **Default access** group. When you do so, its name changes to **Custom default access** group. The changes you make to this group affect all authenticated users in your organization.

1.3.3. The Custom default access group

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 the [Red Hat Hybrid Cloud Console](https://redhathybridcloudconsole.com).

From that point forward, an Organization Administrator is responsible for all updates and changes to the **Custom default access** group. The group is no longer managed or updated by the [Red Hat Hybrid Cloud Console](https://redhathybridcloudconsole.com).
**1.3.4. 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.

**1.3.5. Additive access**

User access on the Red Hat Hybrid Cloud Console uses an additive model, which means that there are no **deny** roles. In other words, actions are only permitted. To control access, assign the appropriate roles with the desired permissions to groups, then add 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.

**1.3.6. 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 the Red Hat Hybrid Cloud Console.
CHAPTER 2. PROCEDURES FOR CONFIGURING USER ACCESS

As an Organization Administrator or User Access administrator, you can click ➡️ Identity & Access Management to view, configure, and modify the User Access groups, roles, and permissions.

2.1. 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 are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.

Procedure


2. Click Create group.

3. 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.
You can click the **Back** button to go back and make changes, or the **Cancel** button to cancel the action.

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

### 2.2. VIEWING ROLES AND PERMISSIONS

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

#### NOTE

You cannot modify a predefined role.

#### Prerequisites

- You are logged in to the **Red Hat Hybrid Cloud Console** as a user who has Organization Administrator permission.
- 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. Navigate to the **Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles**. User Access roles are displayed. You can scroll through the list of all Roles.

2. 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.

    **Cost Price List Viewer**

    A cost management role that grants read permissions on cost models.

    | Application     | Resource type | Operation | Resource definitions | Last commit     |
    |-----------------|---------------|-----------|----------------------|-----------------|
    | cost-management | cost_model    | read      | N/A                  | 19 May 2021     |

    **NOTE**

    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.

### 2.3. VIEWING USER PERMISSIONS
You can view a user’s permissions and other access-related information from the user details page.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.

- 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. Navigate to the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users to view a list of users in your organization.

2. Click a Username to view more details about that user.

3. On the user details page, you can view:
   - If the user is an Organization Administrator in your organization
   - The user’s email address
   - The user’s username on the Hybrid Cloud Console (also known as a Red Hat login)
   - A list of roles associated with the user. To view more details about each role:
     - Click the count in the Groups column to show the groups with this role assigned.
     - Click the count in the Permissions column to show permissions the role provides.

   NOTE

   If you are not an Organization Administrator, you can view your own permissions for different services by navigating to the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > My User Access.

2.4. 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 Members 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.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.

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

Procedure


2. Click Create group.

3. Follow the guided actions provided by the wizard to add users and roles.

4. To grant additional group access, edit the group and add additional roles.

2.4.1. Adding a role to a group

Add a role to an existing group to provide additional permissions to all members of that group. You can view user details to add roles to a group that the user belongs to.

NOTE

You can add a role to a group from the Users page, or by editing a group from the Groups page. These steps show you how to edit the group from the user details page.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.

- 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. Navigate to the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users to open the Users list.

2. Click the Username for a user to open the user details page.

3. Click the count in the Groups column for a role. This shows the groups the user is a member of that have this role assigned.

NOTE

You can view the permissions a role provides by clicking the count in the Permissions column.

4. Click Add role to this group next to the group name to add additional role(s) to the group. This opens the Add roles dialog.

5. Select the checkbox for each role(s) you want to add to the group. (Only roles not yet associated with the group are listed.) Click Add to group.
6. Reload the user details page to see the roles you added to the group.

The group now has these additional permissions in the console.

### 2.4.2. Adding a user to a group

Add a user to an existing group to provide that user with the permissions granted by the roles assigned to that group.

This can be useful when a new team member joins your organization and you want to provide them with all necessary permissions for their work.

**NOTE**

You can add a user to a group from the Users page, or by editing a group from the Groups page. These steps show you how to add a user to a group from the user details page.

#### Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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. Navigate to the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users to open the Users list.

2. Click the username for the user you want to edit.

3. On the user details page, click **Add user to a group**. A dialog opens showing a list of groups the user is not a member of.

4. Select the checkbox for one or more groups to add the user to and click **Add to group**.

5. Reload the user details page to see the roles you added.

The user now has the permissions granted by the group(s) they were added to.

### 2.5. 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.

For more information about predefined roles, see section **Predefined User Access roles**.
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, the Default access group name changes to Custom default access. The Custom default access group is no longer updated with changes pushed out by Red Hat from the Red Hat Hybrid Cloud Console.

**TIP**

You can restore the Default access group, which removes the Custom default access group and any changes you made. See Restoring the Default access group.

**Prerequisites**

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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**


2. 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.

   a. Select the checkbox above the roles list to select all roles in the group.
   
   b. Click the more options icon (⋮) > Remove.
   
   c. Click Remove roles to confirm.

3. Save the changes to Default access group. The name changes to Custom default access.

4. 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 service.

   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.
NOTE
If you want an Organization Administrator to have access, add the Organization Administrator user to the group.

2.6. 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.

NOTE
This procedure assumes that you want to modify an existing group and add an Organization Administrator to the group. Alternatively, you can add an Organization Administrator to a group when you create a new group.

Prerequisites
- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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. For more information, see Managing group access with roles and members.

Procedure
2. Click the group Name to display details about the group.
3. On the group details page, click the Members tab to display a list of authorized users who are a member of the group.
4. Click the Add member tab.
5. 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.
6. Verify the name list is complete and click the Add to group action.

Notification pop-ups appear when the action successfully completes.

2.7. 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 are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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

2. Click the Group Name that you want to modify.
3. Click the Roles tab.
4. 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.
5. Click the more options menu icon that is next to the Add role tab, and then click Remove from group.
6. 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.

2.8. 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>
<tr>
<td>Cost Price List Viewer</td>
<td>cost-management</td>
<td>cost_model</td>
<td>read</td>
</tr>
</tbody>
</table>

By creating a new role, you can define the applications, resources, and operations that are specific to that role.

2.8.1. 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.

For a list of predefined roles provided by Red Hat, see section Predefined User Access roles.

NOTE
You cannot modify a predefined role.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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.


2. 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.

2.8.2. 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

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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.

### 2.8.3. 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. For a list of predefined roles provided by Red Hat, see section **Predefined User Access roles**.

**NOTE**

You cannot modify a predefined role.

**Prerequisites**

- You are logged in to the *Red Hat Hybrid Cloud Console* as a user who has Organization Administrator permission.
- 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.

### 2.8.4. 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 are logged in to the **Red Hat Hybrid Cloud Console** as a user who has Organization Administrator permission.
- 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.
2.8.5. 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 are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization
  Administrator permission.
- 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 cloud integration 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.

2.8.5.1. Cost management example for creating a role from scratch

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization
  Administrator permission.
- 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 cloud integration 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.

2.8.6. 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 are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.

• 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. Navigate to the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles. The Roles window appears. In the Roles window, a custom role has (more options) to the right of its name.

2. Click (more options).

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

4. 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.
5. A confirmation window appears. After you confirm that this action cannot be undone, the custom role is deleted.

2.8.7. Removing permissions from a custom role

You can remove permissions from a custom role.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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. Navigate to the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles. The Roles window appears. In the Roles window, a custom role has (more options) to the right of its name.

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

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

4. A confirmation window appears. Click Remove permission.

2.8.8. Restoring the Default access group

You can restore the Default access group to its state as provided by Red Hat services. When you do so, the Custom default access group is removed along with any changes made to that group.

There is no way to recover the Custom default access group when you restore the Default access group.

Reasons to restore the Default access group:

- You made changes to the Default access group that were not intended.
- You want to start over with the Default access group.
- You want to remove the Custom default access group.
- You want to pick up changes to the the Default access group pushed out by Red Hat services and abandon the Custom default access group.

NOTE

One of the default groups, either the Default access group or the Custom default access group, always exists on your system.
Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- 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.
- The Custom default access group must exist.

Procedure

2. Click Custom default access on the Groups page.
3. Click Restore to default and accept the caution message. Default access appears on the Groups page.
CHAPTER 3. HOW TO ENABLE RED HAT ACCOUNT TEAM ACCESS FOR CUSTOMER SUPPORT

When a customer has a question about their account on the Red Hat Hybrid Cloud Console, they can grant temporary access to their account to a Red Hat associate, usually a Red Hat Technical Account Manager (TAM) or a Red Hat Customer Experience and Engagement support engineer. After the customer grants account access, the Red Hat TAM or support engineer can log in to the customer account and access the account information on the Red Hat Hybrid Cloud Console as though they were a member of the customer’s account.

For more information about Red Hat support services, see Red Hat Service offerings.

When a Red Hat Technical Account Manager (TAM) or a Red Hat Customer Experience and Engagement support engineer requests access to a customer account, what they can see and do is limited by which user access roles are assigned to the access request and is also limited to customer account information that is available on the Red Hat Hybrid Cloud Console.

For more information about default user access roles, see reference section, Predefined User Access roles.

3.1. USING THE ACCESS REQUEST FEATURE TO PROVIDE ACCESS TO A CUSTOMER ACCOUNT

Direct access to a customer account can help resolve issues when screen shots and remote viewing sessions are not successful. By using the access request feature, the Red Hat support team collaborates with the customer who consents to the level of access and the duration of access.

In a typical situation, the customer opens a support case with the Red Hat support team. The Red Hat support team works with the customer to arrange access to the customer’s account and log in to their Red Hat Hybrid Cloud Console.

Make sure to verify the following information before beginning any access request actions:

- The customer account number.
- The duration of the access which includes a maximum duration up to 12 months.
- The default user access roles the customer wants granted to the Red Hat support team.

With the access request feature, system access is always controlled by the customer. The customer can deny access permissions at any time.

NOTE

Any access request action is associated with the unique username of the Red Hat associate on the support team who made the request. This means each Red Hat access request is visible only to the Red Hat associate who made the request, and only that associate can access the customer system. If a different Red Hat support engineer is brought into the support case and needs access, a new access request action is required for that unique Red Hat username.

3.1.1. Approving access to your account
As a customer and Organization Administrator, you grant access to your account by approving the Red Hat access request. An access request notification popup appears briefly when the Organization Administrator is logged in and receives a request.

You can view a list of all account access requests for your system and the status of each from the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Red Hat Access Requests.

**NOTE**

Only the Organization Administrator can approve or deny an access request. The User Access administrator role does not provide permissions to approve or deny an access request.

**Prerequisites**

Collaborate with a Red Hat support engineer and provide the following information so that the support engineer can create an access request request for your approval.

- You are logged in to the Red Hat Hybrid Cloud Console as a user who has Organization Administrator permission.
- Your Red Hat customer account number.
- A start date for system access.
- An end date for system access.
- An understanding of which user access roles the access request will grant to the Red Hat support engineer.

**Procedure**

1. Navigate to the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Red Hat Access Requests. A list of all access requests is displayed.

2. The recommended approach is that you click on the Request ID number, a string of hexadecimal digits.

3. Carefully review the request details and the Roles requested.

4. Click Approve to approve the request. The action is confirmed and the status changes to Approved.

5. Use the edit function to change your response.

**3.1.2. Denying access to your account**

As a customer and Organization Administrator, you deny access to your account by denying the Red Hat access request.

You can view a list of all account access requests and their statuses from the Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > Red Hat Access Requests.
NOTE

Only the Organization Administrator can approve or deny an access request. The User Access administrator role does not provide permissions to approve or deny an access request.

Prerequisites

- A Red Hat support engineer created an access request.
- The access request appears in the Red Hat Account Requests list.

Procedure

   A list of all access requests is displayed.

2. The recommended approach is that you click on the Request ID number, a string of hexadecimal digits.

3. Carefully review the request details and the Roles requested.

4. Click Deny to approve the request. The action is confirmed and the status changes to Denied.

5. Use the edit function to change your response.

3.1.3. Requesting access to a customer account (Red Hat support team)

A member of the Red Hat support team uses the access request feature to gain access to a customer's account. After receiving the access request, the customer can approve or deny the request.

NOTE

The access request feature is available only to Red Hat associates who have a validated Red Hat associate user account. The access request feature is not visible to a non-associate. This information is provided as an aid to Red Hat Technical Account Manager (TAM) or a Red Hat Customer Experience and Engagement support engineer, and to enhance the communications of requirements between the customer and the Red Hat support team member.

Prerequisites

Make sure to verify the following information before beginning any access request actions.

- The customer account number
- The customer organization ID
- The duration of the access which includes a maximum duration up to 12 months
- The user access roles the customer wants granted to the Red Hat support team

Procedure
1. Use one of the following methods to obtain the customer organization ID:

- Ask the customer to provide it.
- On the Red Hat Subscription Admin page, search by the customer account number.

**NOTE**
You must be a Red Hat associate on the Red Hat VPN to view the Red Hat Subscription Admin page.

2. Log in to the Red Hat Hybrid Cloud Console.

3. Click your user avatar in the upper right of the Red Hat Hybrid Cloud Console window. A drop-down list appears.

4. On the drop-down list, click Internal.

5. After the Internal window appears, click Access Requests.

6. Click Create request. A wizard guides you through the steps.

7. After you create an access request, and before the customer approves or denies the request, you can edit the request or cancel the request.

**Verification**
A list of accounts to which you have access appears in a context switcher in the masthead of your Red Hat Hybrid Cloud Console account. This list includes your personal account.

When you choose another account from the context switcher, a banner appears in your Red Hat Hybrid Cloud Console window, for example, "Viewing as account 654321.”

**TIP**
The Access Requests window shows the status of all access requests that you submitted. Account requests are linked to your username and are unique to you. No other Red Hat associate can view or act on the requests that you created.
CHAPTER 4. 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>
<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>Account Staleness and Deletion Administrator</td>
<td>Be able to read and edit Account Staleness and Deletion data.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Account Staleness and Deletion Viewer</td>
<td>Be able to read Account Staleness and Deletion data.</td>
<td></td>
<td></td>
</tr>
<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 Approver</td>
<td>An approval approver role that grants permissions to read and approve requests.</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>X</td>
</tr>
<tr>
<td></td>
<td>request, and read workflows.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation Analytics Administrator</td>
<td>An Automation Analytics Administrator role that grants ALL permissions.</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>Automation Analytics Editor</td>
<td>An Automation Analytics Editor role that grants read-write permissions.</td>
<td></td>
<td>X</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>Automation Services Catalog administrator</td>
<td>A catalog administrator roles grants create, read, update, delete and order permissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation Services Catalog user</td>
<td>A catalog user roles grants read and order permissions</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Compliance administrator</td>
<td>A Compliance role that grants full access to any Compliance resource.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance viewer</td>
<td>A Compliance role that grants read access to any Compliance resource.</td>
<td></td>
<td>X</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 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>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>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 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>Drift analysis administrator</td>
<td>Perform any available operation against any Drift Analysis resource.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Drift viewer</td>
<td>Perform read only operation against Drift Analysis resources.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Hybrid Committed Spend viewer</td>
<td>View any Hybrid Committed Spend report.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RHEL Advisor administrator</td>
<td>Perform any available operation against any RHEL Advisor resource.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Inventory Groups Administrator</td>
<td>Be able to read and edit Inventory Groups data.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Inventory Groups Viewer</td>
<td>Be able to read Inventory Groups data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inventory Hosts Administrator</td>
<td>Be able to read and edit Inventory Hosts data.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Inventory Hosts Viewer</td>
<td>Be able to read Inventory Hosts data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inventory administrator</td>
<td>Perform any available operation against any Inventory resource.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch Administrator</td>
<td>An launch administrator role that grants read and write permissions.</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>Launch Viewer</td>
<td>An launch role that grants read permissions on launch reservation and related resources.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Launch on AWS User</td>
<td>An AWS launch role that grants write permissions on launch reservation and related resources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch on Azure User</td>
<td>An Azure launch role that grants write permissions on launch reservation and related resources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Launch on Google Cloud User</td>
<td>An Google Cloud launch role that grants write permissions on launch reservation and related resources.</td>
<td></td>
<td></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>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>X</td>
</tr>
<tr>
<td>OCM Cluster Autoscaler Editor</td>
<td>Grants permission to edit cluster autoscaler</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCM Cluster Editor</td>
<td>Grants permission to edit clusters</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>OCM Cluster Provisioner</td>
<td>Grants permission to provision clusters</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>OCM Cluster Viewer</td>
<td>Grants permission to view clusters</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>OCM Idp Editor</td>
<td>Grants permission to edit idps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCM Machine Pool Editor</td>
<td>Grants permission to edit machine pools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCM Organization Admin</td>
<td>Grants administrative permissions associated organization’s clusters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCP Advisor administrator</td>
<td>Perform any available operation against any OCP Advisor resource.</td>
<td>X</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>Patch viewer</td>
<td>Read 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>Policies viewer</td>
<td>Perform read only operation against any Policies resource.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RHC administrator</td>
<td>Perform any operations on RHC manager</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RHC viewer</td>
<td>Can view the current configurations on RHC manager</td>
<td>X</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>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>Remediations user</td>
<td>Perform create, view, update, delete operations against any Remediations resource.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Repositories administrator</td>
<td>Perform any available operation against any repositories resource.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Repositories viewer</td>
<td>Perform read only operations against repositories resources.</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>X</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>X</td>
</tr>
<tr>
<td>Subscriptions administrator</td>
<td>Perform any available operation against any Subscriptions resource.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subscriptions user</td>
<td>View any Subscriptions resource.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Tasks administrator</td>
<td>Perform any available operation against any Tasks resource.</td>
<td></td>
<td>X</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>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>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>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>
We appreciate your feedback on our documentation. Provide as much detail as possible so that your request can be addressed.

**Prerequisites**

- You have a Red Hat account. If you do not have a Red Hat account, you can create one by clicking **Register** on the **Red Hat Customer Portal** main page.
- You are logged in to your Red Hat account.

**Procedure**

1. To provide your feedback, click the following link: **Create Issue**
2. Describe the issue or enhancement in the **Summary** text box.
3. Provide more details about the issue or enhancement in the **Description** text box.
4. If your Red Hat user name does not automatically appear in the **Reporter** text box, enter it.
5. Scroll to the bottom of the page and then click the **Create** button. A documentation issue is created and routed to the appropriate documentation team.

Thank you for taking the time to provide feedback.