



Red Hat Hybrid Cloud Console 2023

User Access Configuration Guide for Role-based Access Control (RBAC)

Red Hat Hybrid Cloud Console 2023 User Access Configuration Guide for Role-based Access Control (RBAC)

Legal Notice

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

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 DOCUMENTATION	4
CHAPTER 1. USER ACCESS CONFIGURATION GUIDE FOR ROLE-BASED ACCESS CONTROL (RBAC)	5
1.1. WHAT IS USER ACCESS	5
1.1.1. User Access and the Software as a Service (SaaS) access model	5
1.1.2. Who can use User Access	5
1.1.3. How to use User Access	5
1.1.3.1. The Default admin access group	6
1.1.3.2. The Default access group	6
1.1.3.3. The Custom default access group	6
1.1.3.4. The User Access groups, roles, and permissions	7
1.1.3.5. Additive access	7
1.1.3.6. Access structure	7
CHAPTER 2. PROCEDURES FOR CONFIGURING USER ACCESS	9
2.1. PROCEDURES FOR CONFIGURING USER ACCESS	9
2.1.1. Creating a User Access administrator	9
2.1.2. Viewing roles and permissions	10
2.1.3. Managing group access with roles and members	10
2.1.4. Restricting service access to a single user	11
2.1.5. Including an Organization Administrator in a group	12
2.1.6. Disabling group access	13
2.1.7. Granular permissions for User Access	14
2.1.7.1. Adding custom User Access roles	14
2.1.7.2. Creating a role from scratch	15
2.1.7.3. Copying an existing role	15
2.1.7.4. Creating an application-specific role	16
2.1.7.5. Creating cost management application roles	17
2.1.7.5.1. Cost management example for creating a role from scratch	18
2.1.7.6. Editing custom role names	18
2.1.7.7. Removing permissions from a custom role	19
2.1.7.8. Restoring the Default access group	19
CHAPTER 3. PROCEDURES FOR TEMPORARILY ACCESSING A CUSTOMER ACCOUNT	21
3.1. WHEN TO USE THE ACCESS REQUEST FEATURE	21
3.2. USING THE ACCESS REQUEST FEATURE TO PROVIDE ACCESS TO A CUSTOMER ACCOUNT	21
3.2.1. Approving access to your account	21
3.2.2. Denying access to your account	22
3.2.3. Requesting access to a customer account (Red Hat support team)	23
CHAPTER 4. PREDEFINED USER ACCESS ROLES	25
4.1. PREDEFINED USER ACCESS ROLES	25

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 DOCUMENTATION

We appreciate your feedback on our documentation. To provide feedback, highlight text in a document and add comments.

Prerequisites

- You are logged in to the Red Hat Customer Portal.
- In the Red Hat Customer Portal, the document is in the **Multi-page HTML** viewing format.

Procedure

To provide your feedback, perform the following steps:

1. Click the **Feedback** button in the top-right corner of the document to see existing feedback.



NOTE

The feedback feature is enabled only in the **Multi-page HTML** format.

2. Highlight the section of the document where you want to provide feedback.
3. Click the **Add Feedback** pop-up that appears near the highlighted text.
A text box appears in the feedback section on the right side of the page.
4. Enter your feedback in the text box and click **Submit**.
A documentation issue is created.
5. To view the issue, click the issue link in the feedback view.

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.



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.

1.1.3.1. 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 [Chapter 4, 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 [Chapter 4, 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.

1.1.3.3. 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 [Red Hat Hybrid Cloud Console](#).

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 [Red Hat Hybrid Cloud Console](#).



IMPORTANT

You cannot delete the **Default access** group or **Custom default access** group. You can restore the **Default access** group, which removes the **Custom default access** group and any changes you made. See [Section 2.1.7.8, “Restoring the Default access group”](#).

1.1.3.4. 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.

1.1.3.5. Additive access

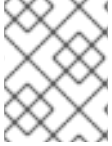
User access on [Red Hat Hybrid Cloud Console](#) uses an additive model, which means that there are no **deny** roles. In other words, actions are only permitted. You control access by assigning the appropriate roles with the desired permissions to groups then adding users to those groups. The access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

1.1.3.6. 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 [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 navigate to [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access](#) 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 are logged in to [Red Hat Hybrid Cloud Console](#) as a user who has Organization Administrator permission.

Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access > Groups](#).
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.
 - g. 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.

2.1.2. Viewing roles and permissions

You can view the roles and permissions for User Access at [Red Hat Hybrid Cloud Console](#). See [Chapter 4, Predefined User Access roles](#) for a list of predefined roles provided by Red Hat.



NOTE

You cannot modify a predefined role.

Prerequisites

- You are logged in to [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 [Red Hat Hybrid Cloud Console](#) > [Settings menu \(gear icon\)](#) > [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.

Application	Resource type	Operation	Last commit
cost-management	cost_model	read	4 months ago

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.

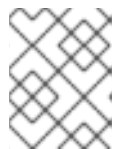
2.1.3. Managing group access with roles and members

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 are logged in to [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.



NOTE

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

Procedure

1. Navigate to [Red Hat Hybrid Cloud Console](#) > [Settings menu \(gear icon\)](#) > [Identity & Access Management](#) > [User Access](#) > [Groups](#). The **Groups** page is displayed.
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.

2.1.4. 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.

For more information about predefined roles, see [Section 4.1, “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 [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 [Section 2.1.7.8, “Restoring the Default access group”](#).

Prerequisites

- You are logged in to [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 [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access > Groups](#). The **Groups** page is displayed.
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**.
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 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.



NOTE

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

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.



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 [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.
Section 2.1.3, “Managing group access with roles and members”

Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access > Groups](#). The **Groups** page displays.
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.


2.1.6. Disabling group access

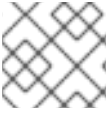
You can disable group access by removing roles from a group. Because the roles and their permissions determine the type of access granted to the group, removing roles disables group access for that role.

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. Navigate to [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access > Groups](#), and log in if necessary. The **Groups** page is displayed.
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.

2.1.7. 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.

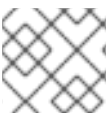
Role	Application	Resource	Operation
Cost Administrator	cost-management	* (all)	* (all)
Cost Price List Viewer	cost-management	cost_model	read

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 4, 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.
 1. You are logged in to [Red Hat Hybrid Cloud Console](#) as a user who has Organization Administrator permission.

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. Navigate to [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access > Roles](#). The **Roles** window appears.

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.

2.1.7.2. 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

- 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.

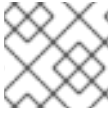
7. Click the **Next** button to review details. You can click the **Submit** button to submit the role, the **Back** button to go back and make changes, or the **Cancel** button to cancel the action.

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 4, 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 are logged in to [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 [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > 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.



2.1.7.7. Removing permissions from a custom role

You can remove permissions from a custom role.

Prerequisites

- You are logged in to [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 [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > 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**.

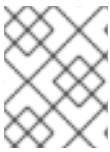
2.1.7.8. Restoring the Default access group

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 **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 [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

1. Navigate to [Red Hat Hybrid Cloud Console](#) > [Settings menu \(gear icon\)](#) > [Identity & Access Management](#) > [User Access](#) > [Groups](#). The **Groups** page is displayed.
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. PROCEDURES FOR TEMPORARILY ACCESSING A CUSTOMER ACCOUNT

3.1. WHEN TO USE THE ACCESS REQUEST FEATURE

When a customer has a question about their account on [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 [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 [Red Hat Hybrid Cloud Console](#).

For more information about default user access roles, see [Section 4.1, "Predefined User Access roles"](#)

3.2. 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.

3.2.1. 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 on [Red Hat Hybrid Cloud Console](#) 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 [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > 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 [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 [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > 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.

3.2.2. 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 status from  (**Settings**) on [Red Hat Hybrid Cloud Console](#).

**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

1. Navigate to the [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access > Red Hat Access Requests](#) window.
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.

3.2.3. 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 on [Red Hat Hybrid Cloud Console](#). 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 or 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. Log in to [Red Hat Hybrid Cloud Console](#).

2. Click your user avatar in the upper right of the [Red Hat Hybrid Cloud Console](#) window. A drop-down list appears.
3. On the drop-down list, click **Internal**.
4. After the **Internal** window appears, click **Access Requests**.
5. Click **Create request**. A wizard guides you through the steps.
6. 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

4.1. 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 4.1. Predefined roles provided with User Access

Role name	Description	Default access group	Default admin access group
Approval Administrator	An approval administrator role that grants permissions to manage workflows, requests, actions, and templates.		
Approval User	An approval user role which grants permissions to create/read/cancel a request and read workflows.	true	
Approval Approver	An approval approver role that grants permissions to read and approve requests.		
Automation Analytics Administrator	An Automation Analytics Administrator role that grants ALL permissions.		
Automation Analytics Editor	An Automation Analytics Editor role that grants read-write permissions.	true	

Role name	Description	Default access group	Default admin access group
Automation Analytics Viewer	An Automation Analytics Viewer role that grants read permissions.		
Automation Services Catalog administrator	A catalog administrator roles grants create, read, update, delete and order permissions		
Automation Services Catalog user	A catalog user roles grants read and order permissions	true	
Compliance administrator	A Compliance role that grants full access to any Compliance resource.		true
Compliance viewer	A Compliance role that grants read access to any Compliance resource.	true	
RHC administrator	Perform any operations on RHC manager		true
RHC viewer	Can view the current configurations on RHC manager	true	
Cost Administrator	A cost management administrator role that grants read and write permissions.		true
Cost Price List Administrator	A cost management role that grants read and write permissions on cost models.		
Cost Price List Viewer	A cost management role that grants read permissions on cost models.		

Role name	Description	Default access group	Default admin access group
Cost Cloud Viewer	A cost management role that grants read permissions on cost reports related to cloud sources.		
Cost OpenShift Viewer	A cost management role that grants read permissions on cost reports related to OpenShift sources.		
Drift analysis administrator	Perform any available operation against any Drift Analysis resource.	true	
Drift viewer	Perform read only operation against Drift Analysis resources.	true	
RHEL Advisor administrator	Perform any available operation against any RHEL Advisor resource.	true	
Inventory administrator	Perform any available operation against any Inventory resource.	true	
Malware detection administrator	Perform any available operation against any malware-detection resource.		true
Malware detection viewer	Read any malware-detection resource.		
Migration Analytics administrator	Perform any available operation against any Migration Analytics resource.	true	
Notifications administrator	Perform any available operation against Notifications and Integrations applications.		true

Role name	Description	Default access group	Default admin access group
Notifications viewer	Read only access to notifications and integrations applications.		
OCP Advisor administrator	Perform any available operation against any OCP Advisor resource.	true	
Patch administrator	Perform any available operation against any Patch resource.	true	
Policies administrator	Perform any available operation against any Policies resource.	true	
User Access administrator	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.		
User Access principal viewer	Grants a non-org admin read access to principals within user access.		
Remediations administrator	Perform any available operation against any Remediations resource		
Remediations user	Perform create view update delete operations against any Remediations resource.	true	
Resource Optimization administrator	Perform any available operation against any Resource Optimization resource.		true

Role name	Description	Default access group	Default admin access group
Resource Optimization user	A Resource Optimization user role that grants read only permission.	true	
Sources administrator	Perform any available operation against any Source		
Subscriptions administrator	Perform any available operation against any Subscriptions resource.		true
Subscriptions user	View any Subscriptions resource.	true	
Vulnerability administrator	Perform any available operation against any Vulnerability resource.	true	
Vulnerability viewer	Read any Vulnerability resource.		