Red Hat Insights 2020-10

User Access Configuration Guide for Red Hat Insights

Last Updated: 2020-12-09

Legal Notice

Abstract

This guide is for Red Hat Insights users who want to use the User Access feature to configure role-based access control (RBAC) in Red Hat Insights, cloud management services for Red Hat Linux (RHEL), and other services hosted at cloud.redhat.com. Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.

Table of Contents

CHAPTER 1. WHAT IS USER ACCESS

The User Access feature is an implementation of role-based access control (RBAC) that controls user access to Red Hat Insights, cloud management services for Red Hat Enterprise Linux, and other services hosted at cloud.redhat.com. User access is supported on cloud.redhat.com.

1.1. WHO CAN USE USER ACCESS

To view and manage User Access on cloud.redhat.com, you must be the Organization Administrator (org admin). This is because User Access requires user management capabilities that are designated from access.redhat.com and belong solely to the org admin.

1.2. 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 has the permissions of the roles in that group.

This might sound complicated, but by creating different groups and adding or removing roles for that group, you control the permissions allowed for that group. When you add users to a group, those users can perform all actions that are allowed for that group.

Red Hat provides a **Default user access** group for User Access. This default group contains many of the roles provided with User Access. The **Default user access** group also contains all authenticated users in your organization.

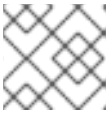
Red Hat provides a set of predefined roles. Depending on the application, the predefined roles for each supported application might have different permissions that are tailored to the application.

1.3. 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 cloud.redhat.com. With the User Access features, the org admin can manage user access to services hosted on cloud.redhat.com.

Some of the cloud.redhat.com services supported by User Access to which your account is subscribed or entitled include the following:

- Red Hat Insights
- Vulnerability
- Compliance
- Drift
- Cost Management



NOTE

User access is available for other services hosted at cloud.redhat.com.

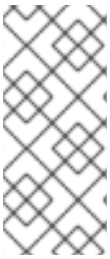
1.3.1. The Default user access group

The **Default user access** group is provided by Red Hat on cloud.redhat.com. It contains many of the predefined roles provided with User Access. The **Default user access** group also includes all authenticated users in your organization.

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

When you change the **Default user access** group, the system no longer updates it with new predefined roles that might be available through cloud.redhat.com. The group name changes to **Custom default user access**, which indicates it was modified.

The **Default user access** group or **Custom default user access** group cannot be deleted. You can create new groups that use roles provided by Red Hat on cloud.redhat.com.



NOTE

If you change and save the **Default user access** group, its name changes to **Custom default user access**. You cannot revert or undo the name change. From that point forward, the org admin is responsible for all updates and changes to the group. The **Custom default user access** group is no longer managed or updated by cloud.redhat.com.

1.3.2. The User Access groups, roles, and permissions

Similar to RBAC, User Access uses the following categories to determine the level of user access that the org admin permits to the supported cloud.redhat.com 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. The org admin 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 lets all members of that group read and write to that service.

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

The org admin adds or deletes roles and users to groups. The group can be a new group created by the org admin 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 cloud.redhat.com 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.

1.3.3. Additive access

User access on cloud.redhat.com 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.

1.3.4. 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 user access** group.

NOTE

Any user added to a group must be an authenticated user for the organization account on cloud.redhat.com.

CHAPTER 2. PROCEDURES FOR CONFIGURING USER ACCESS

As the Organization Administrator (org admin), you can click  (**Settings**) to view, configure, and modify the User Access groups, roles, and permissions.

2.1. VIEWING ROLES AND PERMISSIONS

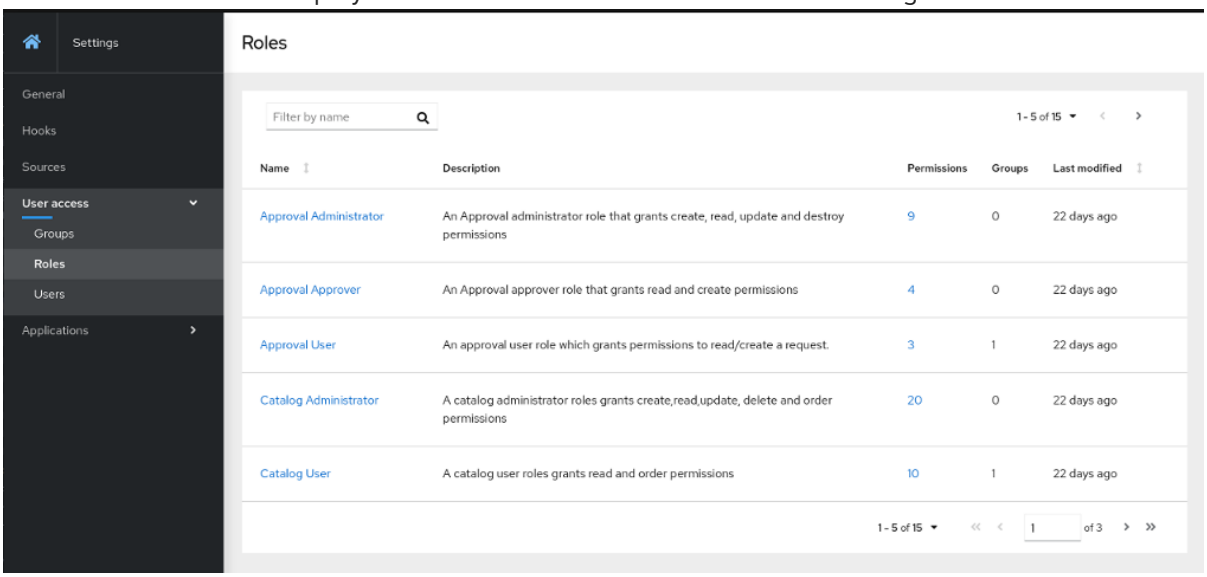
You can view the roles and permissions for User Access at cloud.redhat.com.

Prerequisites

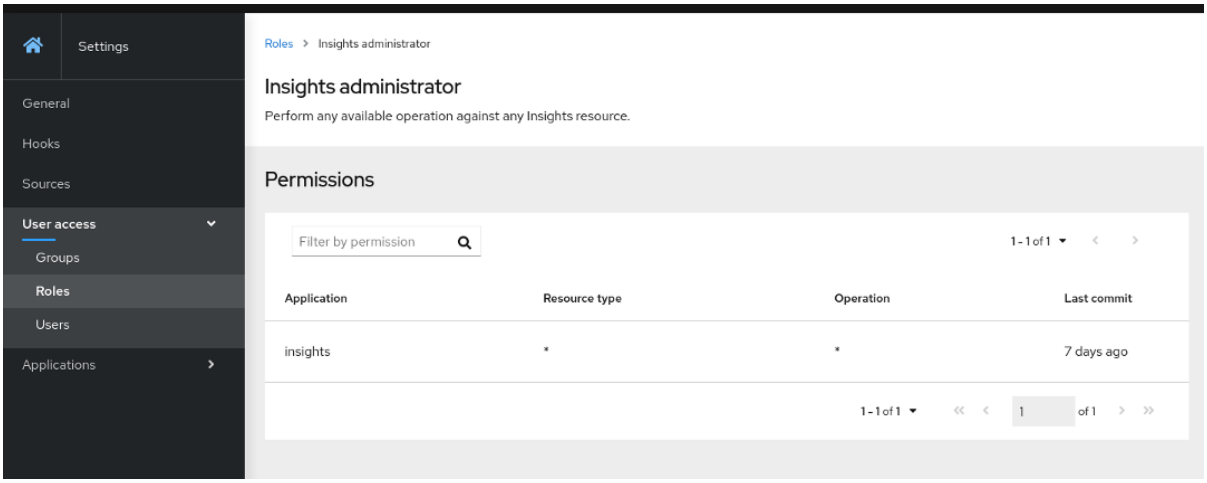
- You must be the Organization Administrator (org admin).

Procedure

1. Log in to your Red Hat organization account at cloud.redhat.com.
2. Click the Settings icon (gear) to open the **Settings** page.
3. On the **Settings** page, click on the **User access** tab to expand it.
4. Click the **Roles** tab to display the User Access roles. You can scroll through the list of all Roles.



5. In the table, click either the role **Name** or the role **Permissions** to see details about the permissions assigned to the role. For example, if you click on the **Insights administrator** role, you see the following information.



The asterisks * indicate all resources and all operations are allowed in this role.

2.2. MANAGING GROUP ACCESS WITH ROLES AND MEMBERS

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

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

Prerequisite

- You must be the Organization Administrator (org admin).

Procedure

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

2.3. 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 must be from the predefined list of roles provided with User Access. The current implementation of User Access does not support creating new roles. For more information about predefined roles, see Chapter 3, *Predefined User Access roles*.

NOTE

If you previously used RBAC to create roles that limit access to cost management resources, those roles appear in the list of available roles.

Any user you add to the new group also inherits the permissions of any other group that the user belongs to in addition to the permissions of the new group.

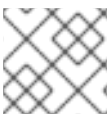
In this procedure you modify the **Default user access** group. When you modify the **Default user access** group its name changes to **Custom default user access** You cannot restore the **Default user access** group. The **Custom default user access** group is not automatically updated with changes to the default roles pushed out by Red Hat.

Prerequisites

- You must be the Organization Administrator (org admin).

Procedure

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



NOTE

If you want the org admin to have access, add the org admin user to the group.

2.4. INCLUDING THE ORG ADMIN IN A GROUP

You can include the Organization Administrator (org admin) in a group. You add the org admin user to a group if you want the org admin to have the roles assigned to that group. The org admin does not inherit all available roles for all cloud.redhat.com applications. Non-inherited roles must be assigned through

group membership.

NOTE

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

Prerequisites

- You must be the Organization Administrator (org admin).
- Create a group if one does not exist.
  Section 2.2, “Managing group access with roles and members”

Procedure

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

Notification pop-ups appear when the action successfully completes.

2.5. DISABLING GROUP ACCESS

You can disable group access by removing roles from a User Access 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 the Organization Administrator (org admin).

Procedure

1. Log in to your Red Hat organization account at cloud.redhat.com.

2. Click the Settings icon (gear) to open the **Settings** page.
3. On the **Settings** page, click the **User access** tab to expand it.
4. Click the **Groups** tab to display the **Groups** page.
5. Click the Group **Name** that you want to modify.
6. Click the **Roles** tab.
7. Click the check box next to roles **Name** that you want to remove.
   You can click the check box at the top of the **Name** column to select all roles.
8. Click the more action menu (three stacked dots) that is next to the **Add role** tab and click **Remove from group**.
9. In the confirmation window that appears, click either **Remove role** or **Cancel** to complete the action.

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

2.6. ADDING AND MODIFYING CUSTOM USER ACCESS ROLES

User Access provides a number of predefined roles that you can add to groups. (Predefined roles are also called default roles.) In addition to using the default roles, you can create and modify User Access roles.

Prerequisites

- You must be the Organization Administrator (org admin).

Procedure

A guided wizard leads you through the steps for adding a role or modifying an existing role. You modify an existing role by making a copy of it. The following steps describe how to use the **Create role** wizard.

1. Log in to cloud.redhat.com as a user who has org admin privileges.
2. From the home page after you log in, click  (**Settings**) to open the Settings window.
3. Click the **User Access** tab to expand the drop-down choices.
4. Click the **Roles** tab. The **Roles** window appears.
5. Click the **Create role** button. This starts the **Create role** wizard.

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

2.6.1. Creating a role from scratch

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

Prerequisites

- You must be the Organization Administrator (org admin).
- 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 applications to include in your role. By default, permissions are listed by application.
6. Optionally use the filter drop-down to 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.

2.6.2. 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.

Prerequisites

- You must be the Organization Administrator (org admin).
- 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 applications to include in your role. By default, permissions are listed by application.

7. Optionally use the filter drop-down to 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.

2.6.3. 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 the Organization Administrator (org admin).
- 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.

2.6.4. Creating cost management application roles

You can create or 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

- You must be the Organization Administrator (org admin).
- You started the **Create role** wizard.

Procedure

This procedure describes how to create a cost management role from scratch that supports

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 list of cost management appears, click on each the check box for each application 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 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.

2.6.4.1. Cost management example for creating a role from scratch

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.

2.6.5. Editing custom role names

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

Prerequisites

- You must be the Organization Administrator (org admin).

- One or more custom role must exist.

Procedure

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

   TIP

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

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

2.6.6. Removing permissions from a custom role

You can delete permissions from a custom role.

NOTE

To add permissions to a custom role, you must create a new custom role. You cannot add permissions to an existing custom role.

Prerequisites

- You must be the Organization Administrator (org admin).
- One or more custom role must exist.

Procedure

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

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

6. A confirmation window appears. Click **Remove permission**.

CHAPTER 3. PREDEFINED USER ACCESS ROLES

The following table lists the predefined roles provided with User Access. For more information about viewing predefined roles, see Section 2.1, “Viewing roles and permissions” .

NOTE

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

Table 3.1. Predefined roles provided with Insights

Role name	Description
Approval Administrator	An approval administrator role that grants permissions to manage workflows, requests, actions, and templates.
Approval Approver	An approval approver role that grants permissions to read and approve requests.
Approval User	An approval user role which grants permissions to create/read/cancel a request, and read workflows.
Catalog Administrator	A catalog administrator roles grants create,read,update, delete and order permissions.
Catalog User	A catalog user roles grants read and order permissions.
Compliance administrator	Perform any available operation against any Compliance resource.
Cost Administrator	A cost management administrator role that grants read and write permissions.
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.
Cost Price List Administrator	A cost management role that grants read and write permissions on price list rates.
Cost Price List Viewer	A cost management role that grants read permissions on price list rates.
Drift analysis administrator	Perform any available operation against any Drift Analysis resource.

Role name	Description
Insights administrator	Perform any available operation against any advisor resource.
Inventory administrator	Perform any available operation against any Inventory resource.
Role name	Description
Inventory permissions	A description of Inventory permissions.
Migration Analytics administrator	Perform any available operation against any Migration Analytics resource.
Patch administrator	Perform any available operation against any Patch resource.
Policies administrator	Perform any available operation against any Policies resource.
Remediations administrator	Perform any available operation against any Remediations resource.
Remediations user	Perform create, view, update, delete operations against any Remediations resource..
Subscription Watch administrator	Perform any available operation against any Subscription Watch resource.
Vulnerability administrator	Perform any available operation against any Vulnerability resource.