Subscription Central 2023

Getting started with activation keys on the Hybrid Cloud Console
Subscription Central 2023 Getting started with activation keys on the Hybrid Cloud Console

Red Hat Customer Content Services
Abstract

Administrative users in your organization can create, configure, edit, and delete activation keys in the Red Hat Hybrid Cloud Console. When a preconfigured activation key is used to register a system from the command line, all of the system-level feature configurations set on the activation key are automatically applied to the system during the registration process.
# Table of Contents

CHAPTER 1. CREATING AND MANAGING ACTIVATION KEYS ........................................... 3
  1.1. VIEWING AN ACTIVATION KEY ......................................................... 3
  1.2. CREATING AN ACTIVATION KEY ..................................................... 4
  1.3. DELETING AN ACTIVATION KEY ..................................................... 5

CHAPTER 2. USING ACTIVATION KEYS ................................................................. 6

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION ....................................... 7
CHAPTER 1. CREATING AND MANAGING ACTIVATION KEYS

An activation key is a preshared authentication token that enables authorized users to register and auto-configure systems. Running a registration command with an activation key and organization ID combination, instead of a username and password combination, increases security and facilitates automation.

Administrative users in your organization can create and manage activation keys on the Red Hat Hybrid Cloud Console. When an authorized user enters a preconfigured activation key to register a system on the command line, all of the system-level settings configured on the activation key are automatically applied to the system during the registration process. You can also use an activation key in a Kickstart file to bulk-provision the registration of multiple Red Hat Enterprise Linux (RHEL) instances without exposing personal username and password values.

Your organization’s activation keys and organization ID are displayed on the Activation Keys page in the Hybrid Cloud Console.

Each user’s access to your organization’s activation keys is managed through a role-based access control (RBAC) system for the Hybrid Cloud Console. For example:

- Only users with the RHC viewer role can view the activation keys on the Activation Keys page.
- Only users with the RHC administrator role can create, configure, edit, and delete activation keys.
- Only users with root privileges or their equivalent can enter an activation key and organization ID with a registration command to connect and automatically configure systems from the command line.

Users in the Organization administrator group for your organization use the RBAC system to assign roles to other users in your organization. An Organization administrator has the RHC administrator role by default. If you have questions about your access permissions, ask an Organization administrator in your organization.

1.1. VIEWING AN ACTIVATION KEY

With the RHC viewer role, you can view your organization’s numeric identifier (organization ID) and available activation keys on the Activation Keys page in the Hybrid Cloud Console. You can also view additional details, such as the Workload setting and additional enabled repositories for each activation key in your organization.

The **Key Name** column shows the unique name of the activation key.

The **Role** column shows the role value for the system purpose attribute set on the key. A potential role value is *Red Hat Enterprise Linux Server*.

The **SLA** column shows the service level agreement value for the system purpose attribute set on the key. A potential service level agreement value is *Premium*.

The **Usage** column shows the usage value for the system purpose attribute that is set on the key. A potential usage value is *Production*.

If the RHC administrator sets no system purpose attributes on the activation key, then the Role, SLA, and Usage columns show no values.

**Prerequisites**
You are logged in to the Red Hat Hybrid Cloud Console.

You have the RHC viewer or RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To view the activation keys for your organization in the Hybrid Cloud Console, complete the following step:

1. From the Hybrid Cloud Console Home page, click Settings > Remote Host Configuration > Activation Keys.

NOTE

Activation keys are listed alphabetically by default.

1.2. CREATING AN ACTIVATION KEY

With the RHC administrator role, you can use the Hybrid Cloud Console interface to create activation keys that root users in your organization can use as an authentication token. During the creation process, you can configure the activation key to set system-level features, such as system purpose attributes, to host systems. When an authorized user uses the preconfigured activation key to register a system to Red Hat, the selected attributes are automatically applied to the system during the registration process.

When creating the activation key, you must give it a unique name that meets the specified naming criteria. Use this name to locate the key in the table on the Activation Keys page or to specify the key that you want to use in a Kickstart script or CLI command.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.
- You have the RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To create an activation key in the Hybrid Cloud Console, complete the following steps:

1. From the Hybrid Cloud Console Home page, click Settings > Remote Host Configuration > Activation Keys.

2. From the Activation Keys page, click Create activation key.

3. In the Name field, enter a unique name for the activation key. Click Next.

NOTE

This is the name that you will enter to use the activation key on the command line. If you enter a name that already exists for an activation key in your organization, you will receive an error message and the key will not be created.

4. Optional: Select a workload option to associate an appropriate selection of repositories with the activation key. Click Next.
5. Optional: In the Role, Service Level Agreement (SLA), and Usage fields, select the system purpose attribute value that you want to set on the activation key from the drop-down list. Click Next.

**NOTE**

Only the system purpose attributes that are available to your organization’s account are selectable.

6. Review the information that you entered into each field. If the information is correct, click Create.

**Result**

The new activation key is listed on the Activation Keys page of the Hybrid Cloud Console.

### 1.3. DELETING AN ACTIVATION KEY

With the RHC administrator role, you can use the Hybrid Cloud Console interface to delete an activation key from the table on the Activation Keys page. You might want to delete an unwanted or compromised activation key for security or maintenance purposes. However, deleting an activation key that is referenced in an automation script will impact the ability of that automation to function. To avoid any negative impacts to your automated processes, either remove the unwanted activation key from the script or retire the automation script prior to deleting the key.

**Prerequisites**

- You are logged in to the Red Hat Hybrid Cloud Console.
- You have the RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

**Procedure**

To delete an activation key in the Hybrid Cloud Console, complete the following steps:

1. From the Hybrid Cloud Console Home page, click Settings > Remote Host Configuration > Activation Keys.

2. From the Activation Keys page, locate the row containing the activation key that you want to delete. Click More options and select Delete from the overflow menu.

3. In the Delete Activation Key window, review the information about deleting activation keys. If you want to continue with the deletion, click Delete.

**IMPORTANT**

Deleting this activation key will impact any automation that references it. To avoid any negative consequences of deleting this key, retire any automation script that uses this key or remove any references of this key from your Kickstart scripts.
CHAPTER 2. USING ACTIVATION KEYS

With root privileges, you can use an activation key with a registration command to connect your system to Red Hat from the command line. Using an activation key and organization ID combination instead of a username and password combination increases security and facilitates automation. If an RHC administrator has preconfigured the activation key with system-level features, then the selected features are automatically applied to the system during the registration process.

Additional resources

- For more information about using activation keys to register your system to Red Hat, see Registering a RHEL system with command line tools in Getting Started with RHEL System Registration

- For more information about using activation keys with automation scripts, see Automating RHEL system registration with a Kickstart file in Getting Started with RHEL System Registration
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.