Red Hat Connect for Technology Partners

Getting Started Guide - Container Zone

Prepared for: Product Managers and Technical Staff
Draft Version: 20180904 (preliminary release)

Table of Contents

Introduction

Welcome to Red Hat Connect for Technology Partners. This guide provides instructions on how to register for the Red Hat Connect for Technology Partner program.
This document will also guide you through the process of obtaining a "Red Hat Certified" designation for an application that you have made deployable via a Linux container using Red Hat technology.

The process involves preparing your containerized application so that it meets certain criteria as specified in the Red Hat Certification Policy Guide, submitting it to Red Hat for review and certification, and publishing it so that the containerized application is available for consumption.

It should be noted that the ability to maintain the certification requires a commitment to maintaining the trustworthiness of the container, i.e., updating it as needed for security or other reasons.

Register for RHC4TP & Request Technology Partnership

Go to connect.redhat.com and click *LOG IN* at the upper right of the page.
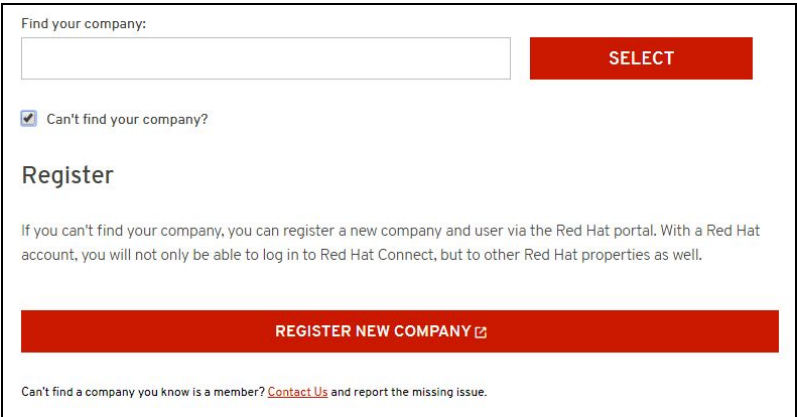
Click *REGISTER*.

Check to see if you have an existing account by searching your Red Hat account login Username.

If you do not have an existing User Account, check if your Company has an existing account by clicking *SEARCH FOR YOUR COMPANY*.

NOTE: If you find your company in the search field, please email connect@redhat.com to find out who the Org Admin is for your company, so they can add you to the existing account.
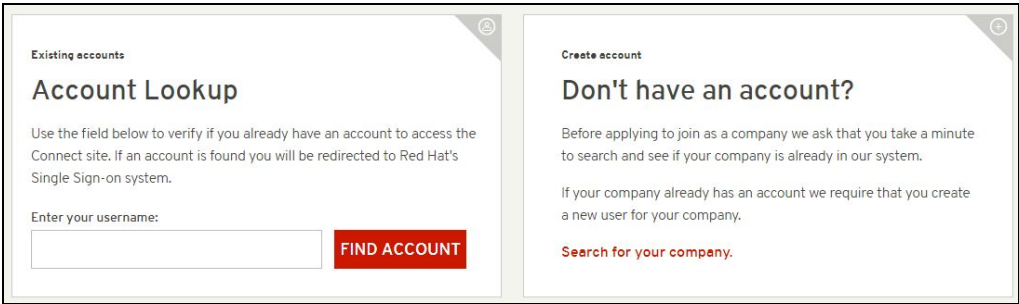
If your company does not have an existing account, click *CAN'T FIND YOUR COMPANY* and then click *REGISTER NEW COMPANY*.

Fill in all required fields and *SUBMIT.*

A confirmation Email will be sent (example email)

Once your Email has been confirmed, log in to your RHC4TP account at connect.redhat.com. You will be redirected to the *Getting Started* page.

NOTE: If you are not redirected, please click *MANAGE COMPANY* and then click *BECOME A PARTNER*

You will now be required to complete the following sections (clicking *Next* after filling in the required information):

> Company Details
> Connect Details
> My Profile

Once the Profile section is complete, you will need to review and accept the Technology Partner Program Agreement..

Request Zone Access

When you're ready to certify your product on Red Hat Software, you will need to request Zone access and then create a Certification Project.

Go to connect.redhat.com and click *LOG IN* at the upper right of the page.

Click on *COMPANY DASHBOARD*
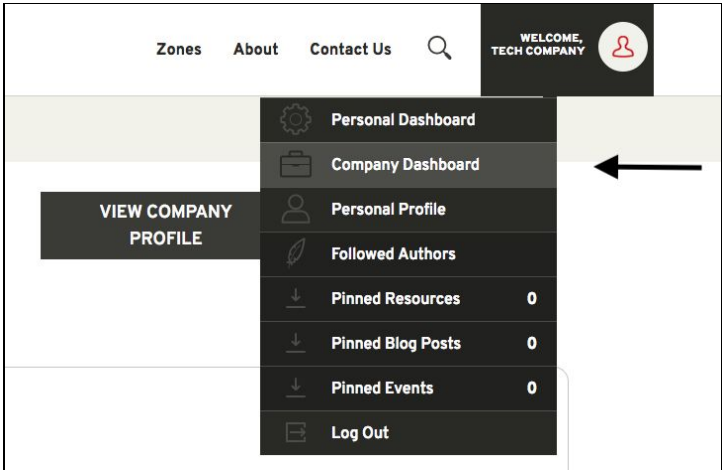
Then select *EDIT COMPANY PROFILE*

Complete all mandatory fields marked with an * and then click *SUBMIT* at the end of the page

Click on *ZONES* at the top of the page.

Scroll down to Join a Zone section.

Under the Zone you wish to join, click *APPLY FOR ZONE ACCESS.*

You will be notified via Email upon approval of your Zone Request.

Add a Product

Log in to your RHC4TP account at connect.redhat.com.

Select the *Human* icon at the top right of the screen and select *Company Dashboard* from the dropdown menu.

Scroll down to *Products* section.

Click *ADD A PRODUCT*.

Fill in all required information and click *SUBMIT*.

If your Product requires more than one container, add the container names separately under Product Version. Example:

Note: The product information you enter will be used to feed the certified product catalog after certification is complete and approved by Red Hat, therefore verify all information is correct.

Add a New User to the RHC4TP Account

Login to your RHC4TP account at *connect.redhat.com*

Click on the *Human* icon at the top right of the page and select *Company Dashboard* from the drop-down menu
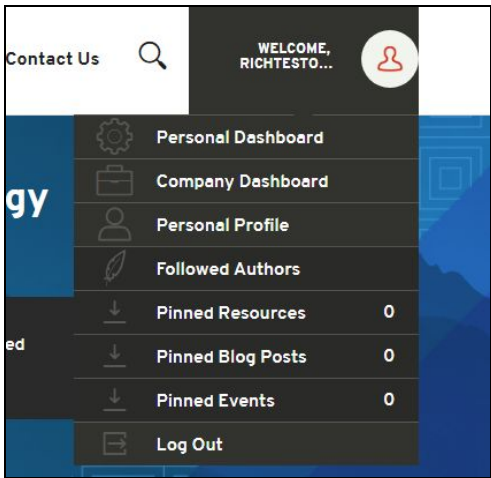
Scroll down to *Users* section and click *MANAGE USERS*.

Click *ADD NEW USER*

Fill in required information, then click *SAVE.*

> **NOTE:** For a User to access software and certification tools, you must check the Organization Administrator (Org Admin) box. Multiple users can be Organization Administrators.

Request Software Access

Log in to your RHC4TP account at connect.redhat.com.

Scroll down to the *As a program member you receive section* and click *LEARN MORE* under *Software access.*

On the Red Hat Software Access Page, scroll down to *PLATFORMS* and click *REQUEST SUBSCRIPTION* under the software you need

You will receive an email once software access has been granted.

Access granted software entitlements

Go to access.redhat.com

Click *DOWNLOADS* under Quick links at the bottom of the page

Choose the product family

Then follow the instructions to download

Create a Certification Project

Log in to your RHC4TP account at connect.redhat.com.

Select *ZONES* at the top of the page.

Scroll down to the Zone you wish to create the Project under and click *CREATE A PROJECT*.

Complete the required fields and click *SUBMIT*.

Primed & Container Certification

To find the Checklist for Primed and Container Certification go to your Project Page and select Certification Checklist located on the left menu under Actions.

Primed

Primed is a technical readiness designation for applications that interoperate with OpenShift. Through Primed, partners indicate that they have verified their product's functionality on OpenShift, taking the first step towards the ongoing commitment of container certification. Primed is also the suggested path for products that integrate with OpenShift but are not packaged as containers.

To achieve the Primed designation, complete the Primed section of the Container Checklist
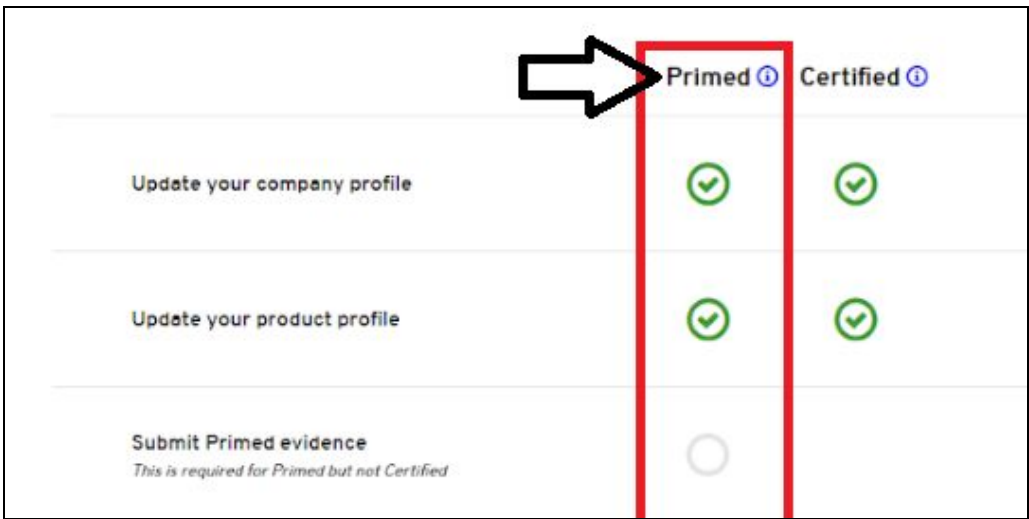
Primed Listing

To find the Checklist for Primed Listing go to your Project Page and select Certification Checklist located on the left menu under Actions.

11
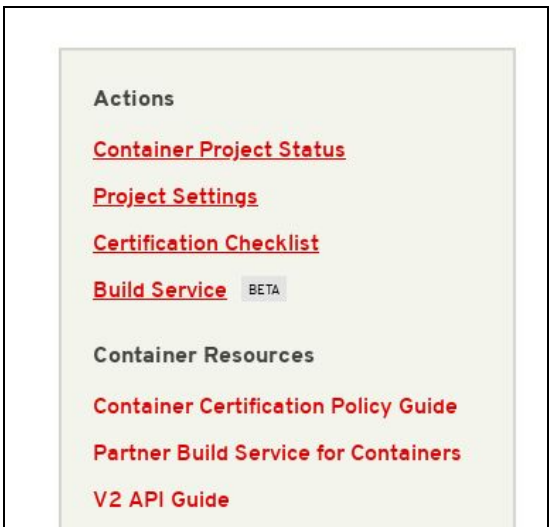
Submitting Primed Evidence

Evidence must be submitted for review. To submit your evidence click on the *START* button for the item located on the Checklist.

This will now take you to the Settings Page of your Project. Fill out all mandatory fields.

Scroll all the way to the section: Supporting Documentation for Primed and add all evidence links.

Click *SUBMIT* at the end of the page.

Now you will have completed that item on the checklist. The check marked box only indicates that the evidence has been submitted, NOT approved. Once the evidence is submitted, you will need to click *GET LISTED* button on the Certification Checklist Page.
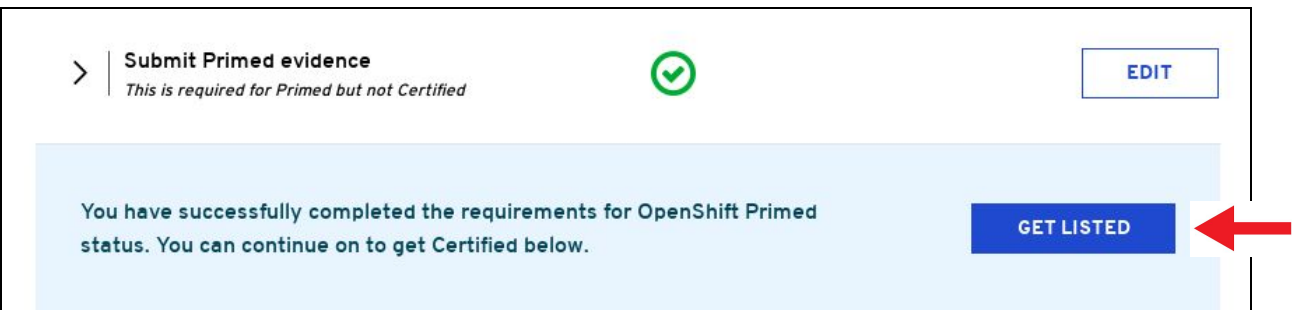
Fill out the Contact form for your evidence to be reviewed.

Your evidence will reviewed and if your application successfully demonstrates running on the latest release of OpenShift, it will be listed in in the OpenShift Primed page found here.

https://access.redhat.com/openshift-primed/

Container Certification Checklist

Certified containers are applications that meet Red Hat's best practices for packaging, distribution and maintenance. Certified containers imply a commitment from partners to maintain their images up to date and represent the highest level of trust and supportability for Red Hat customers container-capable platforms, including OpenShift

For Container Certification, complete the *Certified* section of the checklist and publish the image. The certified container will be published in the Red Hat Container Catalog (RHCC)

Example of Container Checklist in progress:

<u>Container Checklist</u>

The certified container will be published in the Red Hat Container Catalog (RHCC) along with containers published by Red Hat and those published by other software companies. The RHCC is the public-facing website that showcases the containerized applications suitable for enterprise consumption. RHCC pages will allow for publishing information about the partner company, and company's products, as well as technical information about the containerized application. There will also be a way to link in assets from the partner company (by URL) that provide additional information about the product, for example a datasheet, a solution brief, a pre-recorded webinar, a case study, etc. The data populating the RHCC is sourced from the Connect site. Therefore, it is important to review the company and product entries on Connect prior to publishing the container to RHCC.

Before your image gets published you must complete the Certification Checklist. Once all items are completed and your image has passed the scan, you will be able to publish to the Red Hat Container Catalog.

Each item on the Checklist has more information, you can select the drop down arrow located to the left of each item to Learn More.
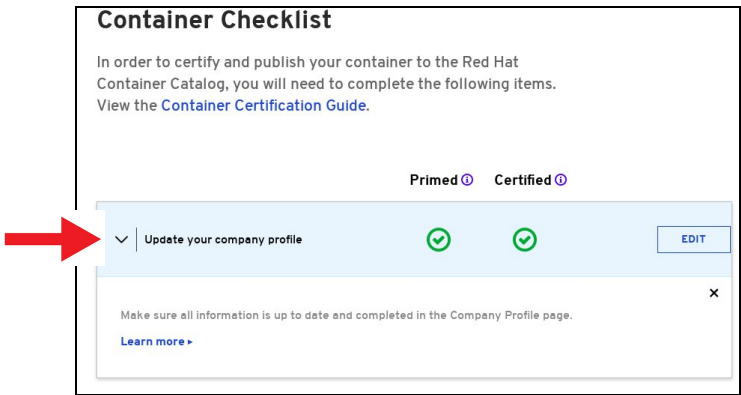
Certification Checklist Section Descriptions

- *Update your company profile*
  - This page is to ensure that your company profile is up to date. Edit if necessary.
- *Update your product profile*
  - This page relates to the product's profile such as product type, description, repository URL, version, contact distribution list, etc.
- *Accept the OpenStack Appendix*
  - Site Agreement to the Container Terms.
- *Update project profile*
  - This section relates more to the image/container settings such as Auto Publish feature, registry namespace, release category, supported platforms.
- *Package and test your application as a container*
  - Follow the instructions on this page to configure the build service. The build service will be dependent on the complete of the previous steps.
- *Upload documentation and marketing materials*
  - This will bring you to the product page. Scroll to the bottom and click on ***Add new Collateral*** to upload your product information.

> **NOTE:** A minimum of 3 materials are required, with 1 being a mandatory "document" type. This is where you add your product information to your product page.

- *Provide a container registry namespace*
  - This is the same as the project page profile page.
- Provide sales contact information

- ○ Again, this information is the same as the company profile.
- ● Obtain distribution approval from Red Hat
  - ○ Red Hat will take care of this step.
- ● Configure Automated Build Service
  - ○ The build service is where Red Hat will automatically build your container/image by utilizing the Dockerfile provided in your repository. The advantage of setting up the automated build service is that your image will update whenever the underlying base image/OS is updated, to ensure up-to-date security. Part of the agreement of using Red Hat's services requires that your container meets a high security standard. See section "Build Service" to get started with this.

Red Hat Partner Logo

To download the *Red Hat Technology Partner logo*, please go to
https://connect.redhat.com/benefits/marketing

If you have a product certified on Red Hat Technology, please contact us at connect@redhat.com so that we can send you the *Certified Product* logo.

Please contact connect@redhat.com for any questions or concerns.

Dockerfile Requirements

You can use this link as a reference to how the Dockerfile needs to be configured to have your image build and pass the scan successfully. Depending on your zone, navigate to the appropriate directory. Here's an example of a Dockerfile for a service you may want to build on RHEL 7.

Note: Although labels and licenses are not required to successfully build a running container, they are required for the Red Hat build service and scanner.

---

1. Base image must be Red Hat. Any images using Ubuntu, Debian, CentOS, etc as a base will **not** pass the scanner.
2. You must configure the required labels (name, maintainer, vendor, version, release, summary)
3. Software license(s) must be included within the image.
4. You must configure a user other than root.

Below is a snippet of a Dockerfile which includes the aforementioned requirements:

Dockerfile Example:

```
FROM registry.access.redhat.com/rhel7
MAINTAINER NAME <EMAIL@ADDRESS>

### Required Atomic/OpenShift Labels - https://github.com/projectatomic/ContainerApplicationGenericLabels
LABEL name="APPLICATION NAME" \
      maintainer="EMAIL@ADDRESS" \
      vendor="COMPANY NAME" \
      version="VERSION NUMBER" \
      release="RELEASE NUMBER" \
      summary="APPLICATION SUMMARY" \
      description="APPLICATION DESCRIPTION" \

### add licenses to this directory
COPY licenses /licenses

### Add necessary Red Hat repos here
RUN REPOLIST=rhel-7-server-rpms,rhel-7-server-optional-rpms \

### Add your package needs here
    INSTALL_PKGS="PACKAGES HERE" && \
    yum -y update-minimal --disablerepo "*" --enablerepo rhel-7-server-rpms --setopt=tsflags=nodocs \
      --security --sec-severity=Important --sec-severity=Critical && \
    yum -y install --disablerepo "*" --enablerepo ${REPOLIST} --setopt=tsflags=nodocs ${INSTALL_PKGS} && \

### Install your application here -- add all other necessary items to build your image
RUN "ANY OTHER INSTRUCTIONS HERE"
```

The Build Service

What does it do?

This service automates the rebuilding of your image whenever an updated Red Hat package is available. It also scans your image (after a successful build) for any security vulnerabilities that may be present prior to publishing your image to the Container Catalog.

How does it work?

The build service clones your Github/Gitlab repository onto a build server, and uses the Dockerfile to build your image.

Why is this recommended?

It is a requirement from Red Hat to properly maintain your image by keeping up to date with the latest security updates. By not using the automated build service, you are opting into manually maintaining and rebuilding your image every time an update is released.

Configuration

Configuration is very easy and straightforward. Follow the steps below:

In the left hand box, click on Build Service:
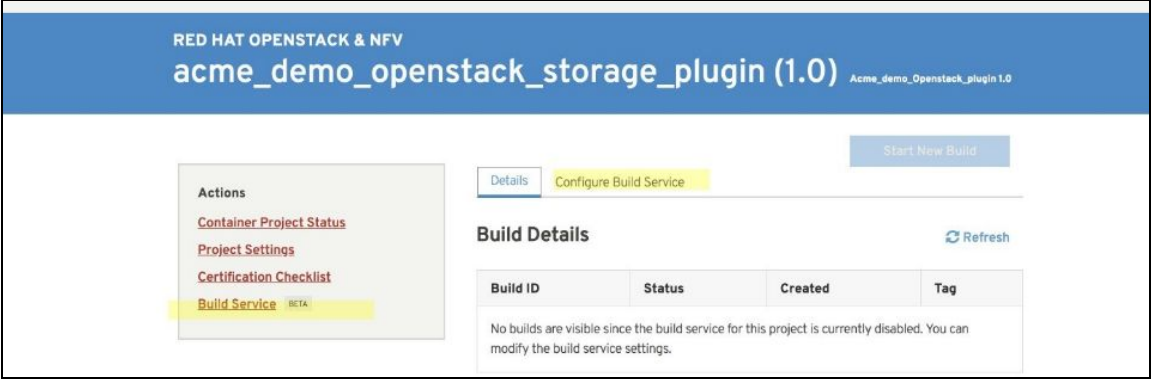
Click on the Configure Automated Build Service tab and fill in the git repo and the Dockerfile name if it has a name other than "Dockerfile".

If your repository is public, then all that is needed is the git source URL (HTTPS link). If your repository is *private,* then you must configure the build service with the SSH link and a private ssh key. The git repository needs the public ssh key associated with the private key in order to successfully clone. It is recommended to create a new public and private ssh key just for the project. Never use your own personal private key.

Click "Start New Build" button at the top of the page.

Enter a tag number (the version number of the plugin) and click *SUBMIT* to begin the build and scan process.

NOTE: The Build Service must first be completed before it can begin the scanning process for certification. If your Build Service fails or does not complete, make sure the details you entered under the Configure Build Service tab is correct and confirm that your Dockerfile conforms to the examples provided in this link.

Once the image has completed the scan in Red Hat Connect repository, the image will show the results of the scan. Scans normally take about 10-15 minutes to complete.

The "View" button will expand on the scan results. The "Publish" button will publish the image to the Red Hat Container Catalog. It will change to "Unpublish" once and image has been published. The "Remove" button allows you to remove an image that you do not want to use or need anymore.

NOTE: The Build Service must first be completed before it can begin the scanning process for certification. If your Build Service fails or does not complete, make sure the details you entered under the Configure Build Service tab is correct

Manually Upload Your Image

This information can be located in the UPLOAD YOUR IMAGE tab on the Projects page.

Cut and paste the following line to your terminal.

        # docker login -u unused -e none scan.connect.redhat.com

When prompted for the password copy and paste the *Registry Key* located on the *Upload Your Image* tab in the project. This Registry Key is unique per project, please make sure you are using the correct password for the project you are working on.

Downloading Your Unpublished Container

It is possible to download your unpublished container to test it on a local environment. To do so, visit the *Upload Your Image* tab and copy the last command for *Push Your Container*. Change

the word "push" to "pull" and replace the data in the brackets with the data appropriate to your project. Use either one of the command formats below to pull your image from the registry.

- **If your image was built using the build service:**

#docker pull scan.connect.redhat.com/[pid]/partner-build-service:[image-tag]

example: # docker pull scan.connect.redhat.com/p78693833236cdf211b0b7767fec4f6fe2a25b4e51/partner-build-service:1.2.2

- **If your image was built locally and pushed manually**

#docker pull scan.connect.redhat.com/[pid]/[image-name]:[image-tag]

example: # docker pull scan.connect.redhat.com/p78693833236cdf211b0b7767fec4f6fe2a25b4e51/my-awesome-plugin:1.2.2

Image Scan

After the image has completed being uploaded, the image will display "Scan In-Progress" in the "Status" column.

NOTE: It may be necessary to refresh the browser page to see the current status.

Once the image has completed the scan in Red Hat Connect repository, the image will show the results of the scan. Scans normally take about 10-15 minutes to complete.

The "View" button will expand on the scan results. The "Publish" button will publish the image to the Red Hat Container Catalog. It will change to "Unpublish" once and image has been published. The "Remove" button allows you to remove an image that you do not want to use or need anymore.

Image Results

If the image returns a "Failed" scan status, the results will automatically be displayed. Click on the name of the failed item (in this example, "has_licenses") for reference to the policy guide.

Name	Value ▲
has_licenses	X
not_running_privileged	✓
rpm_list_successful	✓
rpm_verify_successful	✓
is_rhel	✓
vendor_label_exists	✓
free_of_critical_vulnerabilities	✓
good_tags	✓
good_layer_count	✓
release_label_exists	✓
not_running_as_root	✓
version_label_exists	✓
name_label_exists	✓

Scan Details

▼ **Assessments**

---

*NOTE: If you receive an "Access Denied" link when accessing the Policy Guide, please reach out to connect@redhat.com

---

Export Compliance Questionnaire

Red Hat Export Questionnaire and Resource Links

This section references a set of questions provided by the Red Hat legal team for evaluation of export compliance by third party software vendors.
The resource links and questions should be reviewed and answered by a legal representative of the partner.
Completion and returning this document does not guarantee export compliance approval, but begins the evaluation process by Red Hat.
Depending on the answers provided, a set of follow-up questions may be necessary.
In the event that you have insufficient information to complete the questionnaire, some additional resources are provided in Part 2 below.

The evaluation process is outlined below:
  Step 1: Red Hat provides questionnaire to partner to complete
  Step 2: Partner engages their legal team to review and respond to questionnaire
  Step 3: Partner returns completed questionnaire to Red Hat
  Step 4: Within approximately 5 business days, Red Hat legal evaluates responses and
    a. Approves partner
    b. Defers decision
    c. Requests more information
    d. Declines partner

Part I: Red Hat Questionnaire
Please access and complete this export questionnaire.

  At this time, Red Hat is NOT able to accept applications that are authorized for export as encryption items under License Exception ENC §740.17(b)(2) and/or License Exception ENC §740.17(a) of the U.S. Export Administration Regulations.

Part II: Resources
In the event that your company has not previously gone through the process of obtaining an export classification, or if you have not gone through this process for the product that you

intend to publish in the Red Hat Container Catalog, the U.S. Department of Commerce's Bureau of Industry and Security provides these resources.

Unfortunately Red Hat cannot provide any guidance or help with our partners' export control compliance.

EAR/Encryption Overview	https://bis.doc.gov/index.php/1-encryption-items-not-subject-to-the-ear/15-policy-guidance/encryption	Guidance for determining whether your item is subject to the EAR.
Encryption items not subject to the EAR	https://bis.doc.gov/index.php/1-encryption-items-not-subject-to-the-ear	
Flowchart 1	https://bis.doc.gov/index.php/documents/new-encryption/1654-flowchart1/file	Item designed to use encryption NOT controlled under Category 5, Part 2
Flowchart 2	https://bis.doc.gov/index.php/documents/new-encryption/1655-flowchart-2-1/file	Item classified under an ECCN in Category 5, Part 2
License Exception ENC §740.17/ Mass Market Chart	https://bis.doc.gov/index.php/documents/new-encryption/1651-740-17-enc-table/file	
Chambers & Global - US Export Control Lawyers	http://www.chambersandpartners.com/12788/525/editorial/5/1	
Red Hat Export Control Product Matrix (for example purposes)	https://www.redhat.com/en/about/export-control-product-matrix	

Maintaining Certified Images

Image Maintenance Requirements

As software package vulnerabilities are discovered it is important to rebuild container images to keep them up-to-date. Without automation this process quickly becomes onerous and reflects poorly on the catalog listing. Organizations frequently run vulnerable software but few

want to download vulnerable software. It is a requirement of Red Hat Connect Partner Program that the partner maintain the image certification. Red Hat publishes a "Container Health Index" (or CHI) as described here to inform partners about those situations where an image might need to be updated.

Reference: https://access.redhat.com/articles/2803031

If a container image falls below an "A" grade, a periodic email from connect@redhat.com will be sent out to the partner contact list.

In order to keep the image up to date, it is recommended that the partner use the Red Hat Connect **Build Service** located in the Project section of Red Hat Connect. The option Auto-Rebuild will automatically rebuild your container and automatically publish it.

The only requirement to use this service is that the image bits be accessible via github/gitlab. If the github is internal, ssh access to the bits is required. This service automates the rebuilding of the image whenever an updated Red Hat package is available.

Top FAQs

1. **Who can upload images through the Portal?**

   A. The administrator account created for your organization may upload images. However, this account may grant permissions to other user accounts so that those accounts may also upload images.

2. **Can I change the Product Version after I created a Project?**

   A. No you cannot; therefore make sure you set it up correctly before starting any project with that product version. Keep in mind that the product version should be considered as the name of the image, the version can be specified later on when you Tag your image during the project.

3. **Can a container be built on another version of Linux other than Red Hat?**

   A. No, the Red Hat certification is a validation that the container, which is a combination of application software and Linux, is made of genuine Red Hat parts. Currently, Red Hat has just a little over one million paying customers today. Our customers do not use other versions of Linux and pay us for the services and support we provide to them. Therefore, your container needs to be built on a version of Red Hat Linux.

4. **Will the catalog support an ISO or virtual machine image as the container image?**

   A. No, this certification process is specifically for containers. Therefore, your image needs to be in Dockerfile format. You can find an example provided by Red Hat Engineering: Dockerfile Examples

5. **What path should my licenses be on?**

   A. Should be on / (the root or home directory of where the application resides). You can find an example provided by RH Engineer:Dockerfile Example

6. **How do I change the namespace and repository name of my project?**

   A. First, unpublish all containers. Then change the namespace/repo in the project settings. Finally, re-publish your containers.

7. **How do I download my unpublished container?**

   A. First log into the registry (scan.connect.redhat.com) using the appropriate registry key as the password for the project. Then use this docker pull command if you have used the build service (#docker pull scan.connect.redhat.com/[pid]/partner-build-service:[image-tag]), otherwise, use (#docker pull scan.connect.redhat.com/[pid]/[image-name]:[image-tag]). Look at the *Downloading Your Unpublished Container* section above for more information.

   For a full list of FAQs please visit: http://people.redhat.com/~pchriste/.faq/

Online Resources

Learn Kubernetes by Example	http://kubernetesbyexample.com/
OpenShift Interactive Learning Portal	https://learn.openshift.com/
Partner Openshift Onboarding Guide	https://www.openshift.com/partners/get-started/index.html
OpenShift Documentation	https://docs.openshift.com/container-platform/
Red Hat Atomic Recommended Practices for Container Development	https://access.redhat.com/articles/1483053

Continuous integration Examples	https://rhsyseng.github.io/containerzone-pipeline-library/#_example_jenkins_pipeline_using_docker
Examples of scan ready Dockerfiles	https://github.com/RHC4TP/starter.git
Docker tagging	https://docs.docker.com/engine/reference/commandline/tag/