



## ***Red Hat Enterprise Linux Release 9.2 Manual Pages on 'podman-image-trust.1' command***

### ***\$ man podman-image-trust.1***

podman-image-trust(1)      General Commands Manual      podman-image-trust(1)

#### **NAME**

podman-image-trust - Manage container registry image trust policy

#### **SYNOPSIS**

podman image trust set|show [options] registry[/repository]

#### **DESCRIPTION**

Manages which registries to trust as a source of container images based on its location. (This option is not available with the remote Podman client, including Mac and Windows (excluding WSL2) machines)

The location is determined by the transport and the registry host of the image. Using this container image `docker://docker.io/library/busybox` as an example, `docker` is the transport and `docker.io` is the registry host.

Trust is defined in `/etc/containers/policy.json` and is enforced when a user attempts to pull a remote image from a registry. The trust policy in `policy.json` describes a registry scope (registry and/or repository) for the trust. This trust can use public keys for signed images.

The scope of the trust is evaluated from most specific to the least specific. In other words, a policy may be defined for an entire registry. Or it could be defined for a particular repository in that registry. Or it could be defined down to a specific signed image inside of the registry.

For example, the following list includes valid scope values that could

be used in policy.json from most specific to the least specific:

docker.io/library/busybox:notlatest      docker.io/library/busybox

docker.io/library docker.io

If no configuration is found for any of these scopes, the default value (specified by using "default" instead of REGISTRY[/REPOSITORY]) is used.

Trust type provides a way to:

Allowlist ("accept") or Denylist ("reject") registries or Require a simple signing signature (?signedBy?), Require a sigstore signature ("sigstoreSigned").

Trust may be updated using the command podman image trust set for an existing trust scope.

## OPTIONS

--help, -h

Print usage statement.

set OPTIONS

--pubkeysfile, -f=KEY1

A path to an exported public key on the local system. Key paths will be referenced in policy.json. Any path to a file may be used but locating the file in /etc/pki/containers is recommended. Options may be used multiple times to require an image be signed by multiple keys. The --pubkeysfile option is required for the signedBy and sigstoreSigned types.

--type, -t=value

The trust type for this policy entry.

Accepted values:

signedBy (default): Require simple signing signatures with corresponding list of

public keys

sigstoreSigned: Require sigstore signatures with corresponding list of

public keys

accept: do not require any signatures for this

registry scope

reject: do not accept images for this registry scope

show OPTIONS

--json, -j

Output trust as JSON for machine parsing

--noheading, -n

Omit the table headings from the listing.

--raw

Output trust policy file as raw JSON

## EXAMPLES

Accept all unsigned images from a registry

```
sudo podman image trust set --type accept docker.io
```

Modify default trust policy

```
sudo podman image trust set -t reject default
```

Display system trust policy

```
podman image trust show
```

TRANSPORT	NAME	TYPE	ID	STORE
all	default	reject		
repository	docker.io/library	accept		
	repository		registry.access.redhat.com	signed
				security@redhat.com

<https://access.redhat.com/webassets/docker/content/sigstore>

repository	registry.redhat.io	signed	security@redhat.com	<a href="https://registry.redhat.io/containers/sigstore">https://registry.redhat.io/containers/sigstore</a>
repository	docker.io	reject		
docker-daemon		accept		

Display trust policy file

```
podman image trust show --raw
```

```
{
  "default": [
    {
      "type": "reject"
    }
  ],
  "transports": {
```

```

"docker": {
  "docker.io": [
    {
      "type": "reject"
    }
  ],
  "docker.io/library": [
    {
      "type": "insecureAcceptAnything"
    }
  ],
  "registry.access.redhat.com": [
    {
      "type": "signedBy",
      "keyType": "GPGKeys",
      "keyPath": "/etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release"
    }
  ],
  "registry.redhat.io": [
    {
      "type": "signedBy",
      "keyType": "GPGKeys",
      "keyPath": "/etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release"
    }
  ]
},
"docker-daemon": {
  "": [
    {
      "type": "insecureAcceptAnything"
    }
  ]
}

```

```
}  
}
```

Display trust as JSON

```
podman image trust show --json
```

```
[  
  {  
    "transport": "all",  
    "name": "* (default)",  
    "repo_name": "default",  
    "type": "reject"  
  },  
  {  
    "transport": "repository",  
    "name": "docker.io",  
    "repo_name": "docker.io",  
    "type": "reject"  
  },  
  {  
    "transport": "repository",  
    "name": "docker.io/library",  
    "repo_name": "docker.io/library",  
    "type": "accept"  
  },  
  {  
    "transport": "repository",  
    "name": "registry.access.redhat.com",  
    "repo_name": "registry.access.redhat.com",  
    "sigstore": "https://access.redhat.com/webassets/docker/content/sigstore",  
    "type": "signed",  
    "gpg_id": "security@redhat.com"  
  },  
  {  
    "transport": "repository",
```

```
"name": "registry.redhat.io",
"repo_name": "registry.redhat.io",
"sigstore": "https://registry.redhat.io/containers/sigstore",
"type": "signed",
"gpg_id": "security@redhat.com"
},
{
"transport": "docker-daemon",
"type": "accept"
}
]
```

## SEE ALSO

containers-policy.json(5)

## HISTORY

January 2019, updated by Tom Sweeney (tsweeney at redhat dot com) December 2018, originally compiled by Qi Wang (qiwan at redhat dot com)

podman-image-trust(1)