Managing Signing Keys

Overview

RSA key pairs are used to sign and verify the Alpine Linux index files in JFrog Artifactory, while GPG key pairs are used to sign and validate packages integrity in JFrog Distribution. The JFrog Platform enables you to manage multiple RSA and GPG signing keys through the Keys Management UI and REST API. The JFrog Platform supports managing multiple pairs of GPG signing keys to sign packages for authentication of several package types such as Debian, Opkg, and RPM through the Keys Management UI and REST API.

Artifactory signs repository metadata (not packages) for RPM, Debian, Opkg, and Alpine.

Page Contents

Managing RSA and GPG Key Pairs

In the JFrog Platform, you can upload, view or remove the RSA/GPG Keys in the **Administration module**, under **Artifactory | Security | Keys Management | Signing Key Pairs**.

Adding RSA Keys Pairs

JFrog Platform lets you manage multiple pairs of RSA signing keys, so you can sign Alpine packages for authentication.

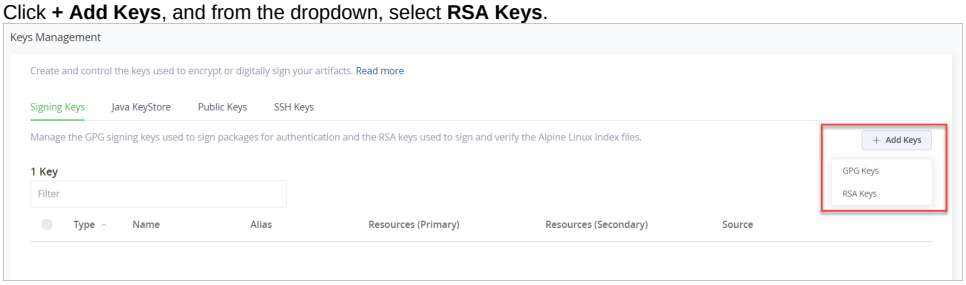
Generating Keys

The way to generate keys is platform-dependent. For more information, see Build a Public and Private RSA Key.

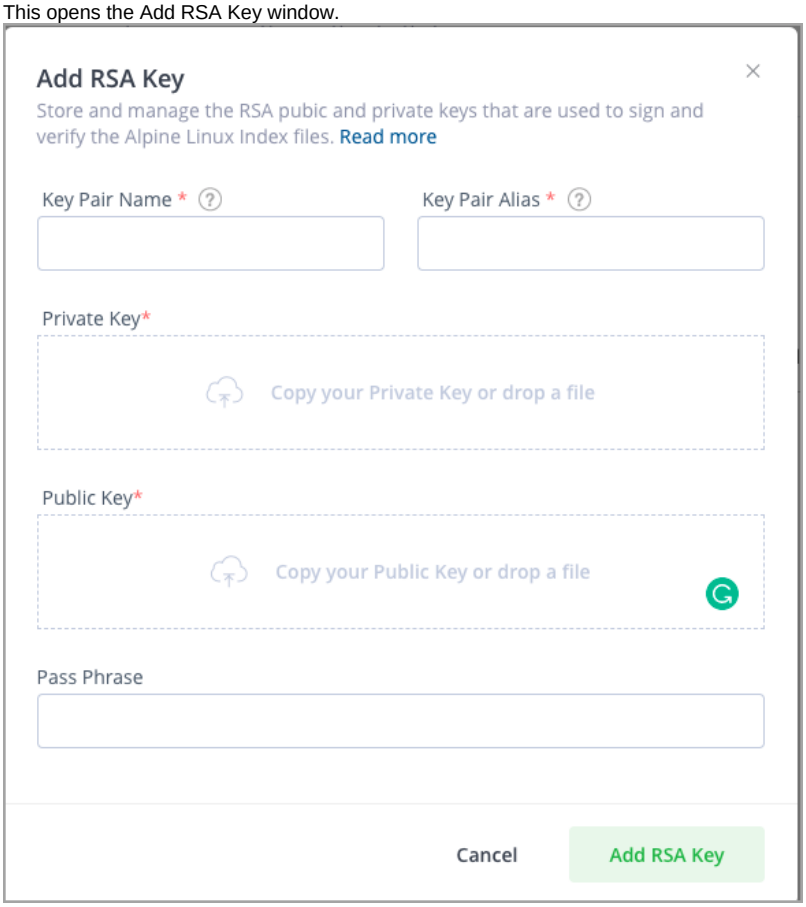
Uploading Keys

1. In the JFrog Platform UI, go to the **Administration module** and then go to **Artifactory | Security | Keys Management**.

2. Click **+ Add Keys**, and from the dropdown, select **RSA Keys**.



This opens the Add RSA Key window.



3. Enter the RSA parameters generated when creating the RSA Key Pair.
4. Click **Test** to test the configuration.
5. If the test is successful, click **Add RSA Key** to save the new key.

Configuring Alpine Repositories

Alpine Linux requires RSA keys by default.

To learn more about configuring keys for Alpine Linux packages, see Configuring Alpine Package Manager to work with Artifactory.

Adding GPG Key Pairs

JFrog Platform lets you manage a pair of GPG signing keys so you can sign packages for authentication in several formats such as Debian, Opkg and YUM.

Generating Keys

The way to generate keys is platform-dependent. The example below shows how to generate the public and private keys on Linux:

Generating GPG keys

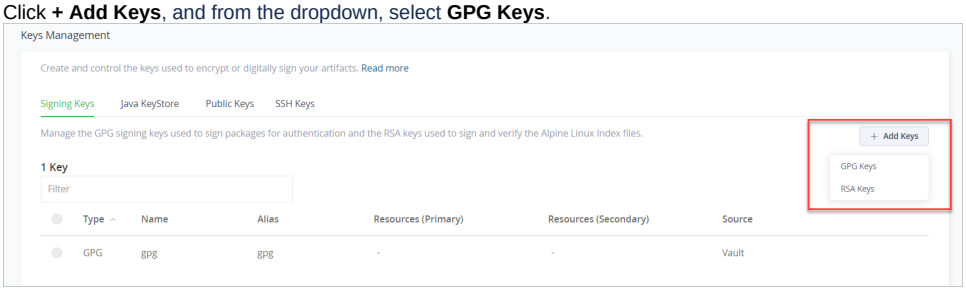
```
# generate the keys
gpg --gen-key

# list all keys in your system and select the pair you want to use in Artifactory
```

```
gpg --list-keys

# resolve the key-id from the lists-keys by selecting the relevant license
pub   2048R/8D463A47 2015-01-19
uid   JonSmith (Jon) <jon.smith@jfrog.com>
key-id =  8D463A47

#export the private key with the specified id to a file
gpg --output {private key file name and path} --armor --export-secret-keys {key-id}

#export the public key with the specified id to a file
gpg --output {public key file name and path} --armor --export {key-id}
```

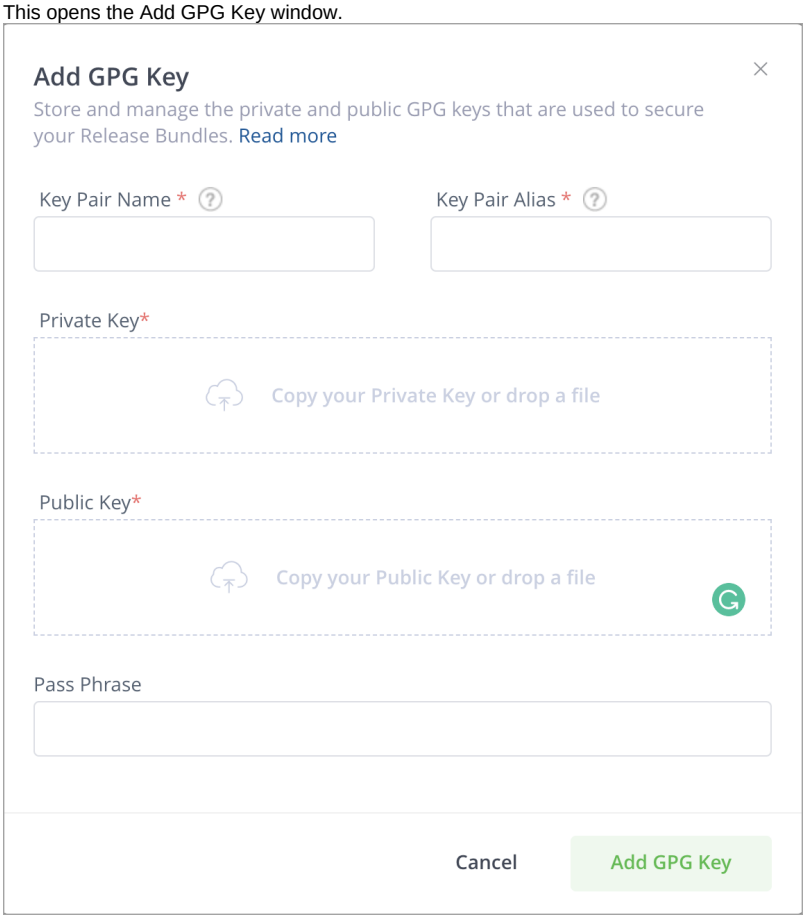
You also need to specify a passphrase that must be used together with the signing keys. The passphrase can be saved, or passed with a REST API call.

Uploading Keys

1. To upload your signing keys, go to the **Administration module** and then go to **Artifactory | Security | Keys Management**.
2. Click **+ Add Keys**, and from the dropdown, select **GPG Keys**.



This opens the Add GPG Key window.



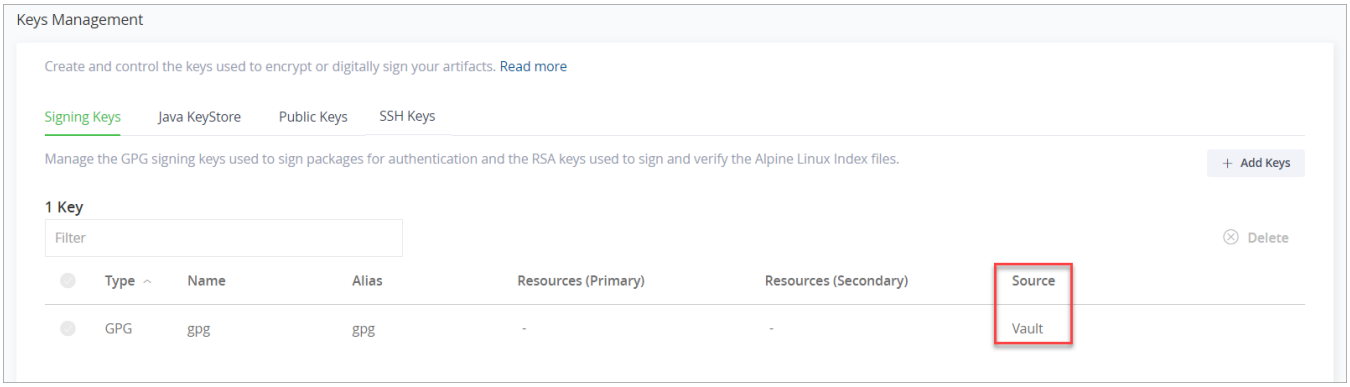
3. Enter the details for the GPG key.
4. Click **Test** to test the configuration.
5. If the test is successful, click **Add GPG Key** to save the new key.
6. Artifactory will indicate when the keys are installed, and you can click the **Public key is installed** link to download the public key.

Once you have uploaded your signing GPG keys, you can use them GPG signing for JFrog Distribution. For more information, see JFrog Distribution GPG Signing.

Managing Vault RSA and GPG Key Pairs

In addition to uploading keys, you can also choose to store your signing keys in HashiCorp Vault as secrets, and retrieve them in the JFrog Platform. For more information on configuring and enabling HashiCorp Vault, see Vault Integration.

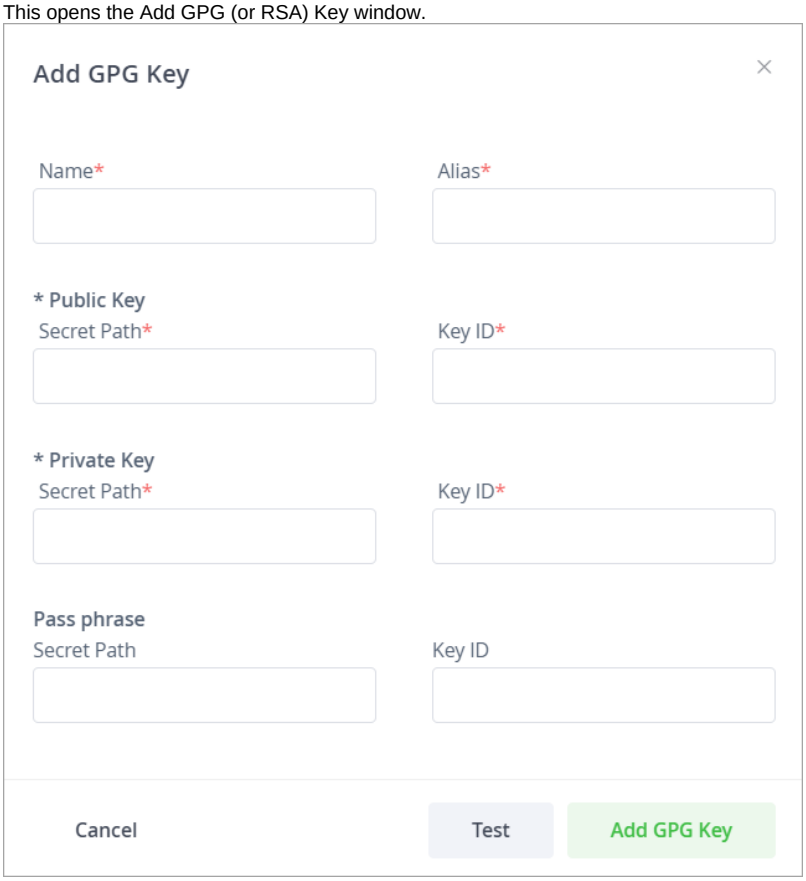
When Vault is enabled in your JFrog Platform, keys that have been stored in Vault will appear in the Source column under "Vault".



When Vault is enabled, you can either add new RSA/GPG keys and store them in Vault, or change the uploaded keys with Vault ones.

Setting up a New RSA/GPG Key in Vault

1. Click **+Add Keys** and select **GPG** or **RSA**.
   This opens the Add GPG (or RSA) Key window.



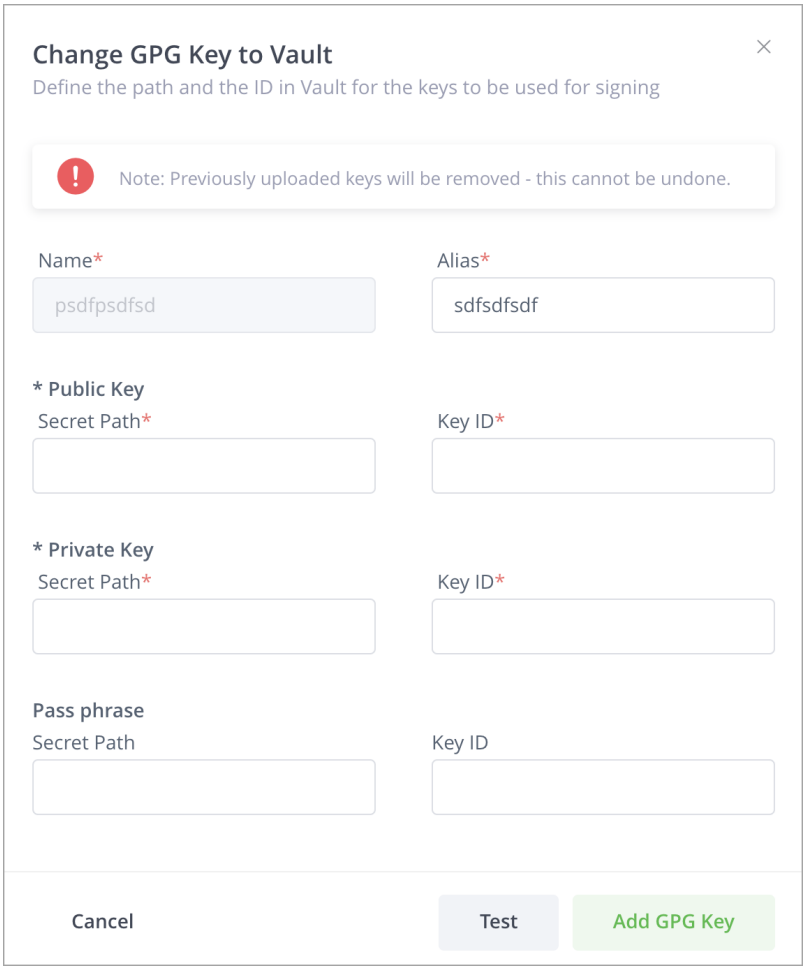
2. From the Vault Connector dropdown list, select the Vault connector you wish to use for the key.
3. Enter the details for the key.
4. Click **Test** to test the configuration.
5. If the test is successful, click **Add GPG (RSA) Key** to save the new key.

Change an Uploaded Key with a Vault Key

> **Important**
>
> Once you change an uploaded key to a Vault one, the uploaded key will be deleted; this action cannot be undone.

1. In the Signing Key list of keys, go to the arrow next to the uploaded key you wish to change to Vault and click it.

This opens the Change GPG/RSA Key to Vault window.



2. From the Vault Connector dropdown list, select the Vault connector you wish to use for the key.
3. Enter the details for the key.
4. Click **Test** to test the configuration.
5. If the test is successful, click **Add GPG (RSA) Key** to save the new key.

REST API Commands

The JFrog Platform supports managing multiple pairs of GPG signing keys using a set of REST APIs. This feature enables you to assign a signing key pair per repository, providing you with the granularity to choose which keys to use to sign the artifacts in repositories instead of using the same key pair to sign all artifacts.

You can perform the following Key Pair REST API commands:

- Create RSA Key Pair
- Get Key Pair
- Delete Key Pair
- Get Key Pair Public Key Per Repository
- Set Key
- Delete Key
- Download Primary Key
- Download Secondary Public Key
- Set Primary Key
- Set Secondary Key
- Delete Primary Key
- Delete Secondary Key
- Promote
- Update Key Pair
- Verify Key Pair
- Get All Key Pairs