Verify OVA Images

You must verify the integrity of OVA images and upgrade scripts before you install or upgrade Cisco IoT FND. This verification ensures that the files are authentic and untampered.

Contents of OVA Images and Upgrade Scripts

Table 1: Contents of the .zip files

Zip File Name	Contents
CISCO-IOTFND-VPI-K9-<release>-<build number>.zip	Contains Postgres/Influx for gateway management. • iot-fnd-<release>-<build number>.iso • iot-fnd-<release>-<build number>.iso.signature

Zip File Name	Contents
CISCO-IOTFND-VPI-K9-CGMS-TOOLS-<release>-<build number>.zip **Note** The CGMS tools file is bundled with CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>.zip.	Includes cgms tools rpm for Postgres deployments. • cgms-tools-<release>-<build number>.x86_64.rpm • FND_RPM_SIGN-CCO_RELEASE.pem — Cisco signed x.509 end-entity certificate containing public key that is used to verify the signature. This certificate is chained to Cisco root CA and sub CA posted on https://www.cisco.com/security/pki/. • cisco_openpgp_verify_release.py — Signature verification program for verifying the Open-pgp Complaint Public Key against x.509 end-entity certificate. • cisco_openpgp_verify_release.py.signature — Signature generated for the script cisco_openpgp_verify_release.py. • FND-rel-binary.gpg — Open-pgp public key is used for verification of signed RPM. • FND-rel-ascii.gpg — Open-pgp public key is used for verification of signed RPM.
CISCO-IOTFND-VPI-K9-UPGRADE-SCRIPTS-<release>-<build number>.zip	Includes upgrade scripts for upgrading FND-Postgres/Influx OVA. • upgrade-ova-<release>-<build number>.rpm — Signature embedded RPM image. • FND_RPM_SIGN-CCO_RELEASE.pem — Cisco signed x.509 end-entity certificate containing public key that is used to verify the signature. This certificate is chained to Cisco root CA and sub CA posted on https://www.cisco.com/security/pki/. • cisco_openpgp_verify_release.py — Signature verification program for verifying the Open-pgp Complaint Public Key against x.509 end-entity certificate. • cisco_openpgp_verify_release.py.signature — Signature generated for the script cisco_openpgp_verify_release.py. • FND-rel-binary.gpg — Open-pgp public key is used for verification of signed RPM. • FND-rel-ascii.gpg — Open-pgp public key is used for verification of signed RPM.

Verify OVA Signature

Use the instructions provided in this section to verify the OVA signature:

Here are the contents of the OVA zip file for different use cases:

Use case	Contents
Oracle-based deployments	**iot-fnd-oracle-<release>-<build number>_SHA1_signed.ova**
TPS-related deployments	**iot-tps-<release>-<build number>_SHA1_signed.ova**

Before you begin

The following knowledge is required to verify OVA signature:

- Python 2.7.x
- OpenSSL
- Internet connection

Procedure

Use the `ovftool` command on your terminal to verify the signed OVA file.

Example:

```
ovftool iot-fnd-<release>-<build number>_SHA256_signed.ova
```

This command checks the integrity and authenticity of the OVA file by verifying its signature.

Example

```
Opening OVA source: iot-fnd-<release>-<build number>_SHA256_signed.ova
The manifest validates
Completed successfully
```

What to do next

Verify the upgrade RPM signature

Verify RPM Signatures

The following steps collectively ensure the security and integrity of the files before proceeding with any installations or upgrades.

Before you begin

The following knowledge is required to verify OVA signature:

- Python 2.7.x
- OpenSSL
- Internet connection

Procedure

Step 1 Unzip the file **iot-fnd-<release>-<build number>-signed.zip** and change directory to the folder **iot-fnd-<release>-<build number>-signed**

Example:

```
unzip iot-fnd-<release>-<build number>-signed.zip

           cd iot-fnd-<release>-<build number>-signed
```

Step 2 Extract the public key from the public certificate:

Example:

```
openssl x509 -pubkey -noout -in FND_RPM_SIGN-CCO_RELEASE.pem > FND-EE-cert.pubkey

FND-EE-cert.pubkey is created under the same folder
```

Step 3 Verify the scripts using the public key and signature files:

Example:

```
openssl dgst -sha512 -verify FND-EE-cert.pubkey -signature cisco_x509_verify_release.py.signature
cisco_x509_verify_release.py
openssl dgst -sha512 -verify FND-EE-cert.pubkey -signature cisco_openpgp_verify_release.py.signature
 cisco_openpgp_verify_release.py
```

Expected Result: Verified OK

Step 4 Verify the ISO file:

Example:

```
./cisco_x509_verify_release.py -e FND_RPM_SIGN-CCO_RELEASE.pem -s iot-fnd-<release>-<build
number>.iso.signature -i iot-fnd-<release>-<build number>.iso -v dgst -sha512

Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
 Successfully retrieved and verified crcam2.cer.
 Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
 Successfully retrieved and verified innerspace.cer.
 Successfully verified root, subca and end-entity certificate chain.
 Successfully fetched a public key from FND_RPM_SIGN-CCO_RELEASE.pem.
 Successfully verified the signature of iot-fnd-<release>-<build number>.iso using
FND_RPM_SIGN-CCO_RELEASE.pem
```

Step 5 Install the ISO image file:

Example:

```
cd /mnt
mkdir iso
mount -t iso9660 -o loop <path>/iot-fnd-<release>-<build number>.iso /mnt/iso
mkdir /tmp/ISO
cp -pRf /mnt/iso /tmp/ISO
umount /mnt/iso/
```

Step 6 Verify the delivered binary and ascii keys have matching fingerprints:

Example:

```
gpg FND-rel-binary.gpg

gpg FND-rel-ascii.gpg

pub 2048R/F7D5ED29 2017-01-01 user (FND.rel)
```

Step 7 Verify the binary GPG key against EE cert:

Example:

```
./cisco_openpgp_verify_release.py -e FND_RPM_SIGN-CCO_RELEASE.pem -G FND-rel-binary.gpg

Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...

            Successfully downloaded crcam2.cer.

           Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer
 ...

            Successfully downloaded innerspace.cer.

            Successfully verified Cisco root, subca and end-entity certificate chain.

            Successfully fetched a public key from FND_RPM_SIGN-CCO_RELEASE.pem.

            Successfully authenticated FND-rel-binary.gpg key using Cisco X.509 certificate trust
chain.
```

Step 8 Verify RPM Signature using the GPG ASCII key:

Example:

```
sudo rpm --import FND-rel-ascii.gpg

            rpm -K /tmp/ISO/iso/cgms-<release>-<build number>.x86_64.rpm

 /tmp/ISO/iso/cgms-<release>-<build number>.x86_64.rpm: rsa sha1 (md5) pgp md5 OK
```

Step 9 Repeat the step 8 to verify all the RPM signatures. For example, CGMS tools RPM for Postgres Signature.

You've successfully verified the RPM signatures.

What to do next

Proceed to installing or upgrading the RPMs.

Export an OVF File

Before you begin

An OVF template captures the state of a virtual machine or vApp into a self-contained package. The disk files are stored in a compressed sparse format.

Procedure

To export an OVF file using VMware vSphere see, Export an OVF Template.