**How to Use Client Tool to Prepare a Virtual Machine Image for Secure Launch**

After running Client\_build.sh:

1. Create the directory /root/manifest\_files

# mkdir /root/manifest\_files

2. Change to the directory of the latest build

# cd /opt/RP\_$Current\_Date/ManifestTool

3. Provide the necessary values in resources/config.properties file

To run the client tool to create and upload a manifest for a Virtual Machine binary:

In resources/config.properties:

Host\_Manifest=false

To run the client tool to create a manifest for a TCB boot using rootfs.tar.gz;

In resources/config.properties:

Host\_Manifest=true

How to set up the Client Tool machine after setting up a new Mt Wilson server:

Default password is changeit

1. Retrieve Mt. Wilson server public certificate

# ./retrieve-cert.sh $mtwilson\_ip:8181 > ./mtwcert.pem

1.a. Delete the old mtwcert certificate from the java keystore:

# keytool -delete -noprompt -trustcacerts -alias mtwcert -keystore /usr/lib/jvm/jdk1.7.0\_55/jre/lib/security/cacerts

2. Add the certificate to java keystore

# keytool -import -noprompt -trustcacerts -alias mtwcert -file ./mtwcert.pem -keystore /usr/lib/jvm/jdk1.7.0\_55/jre/lib/security/cacerts

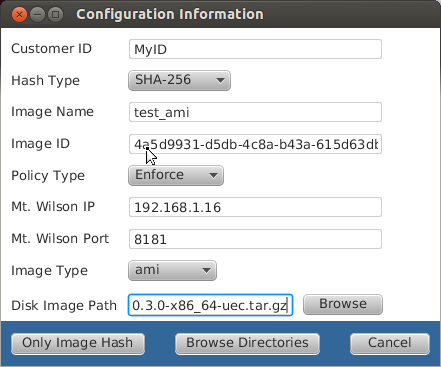
3. Verify the certificate added to keystore

# keytool -list -keystore /usr/lib/jvm/jdk1.7.0\_55/jre/lib/security/cacerts -alias mtwcert

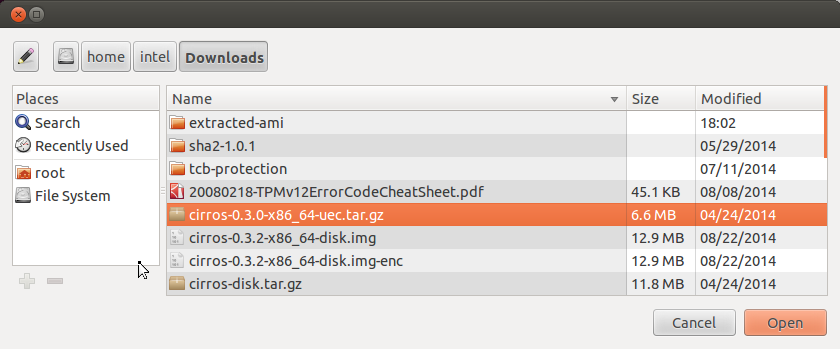
3. Run the client tool and provide the 'Mt. Wilson IP' and 'Mt. Wilson Port' in the GUI

# java -jar dist/lib/ManifestToolApp.jar

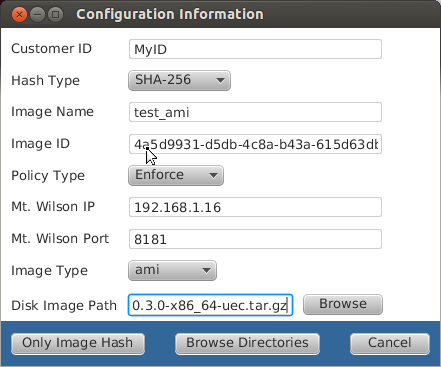
In the first window, shown below, fill in all the blanks and click on the ‘Browse’ button. This first example shows how to prepare an AMI image for secure launch.



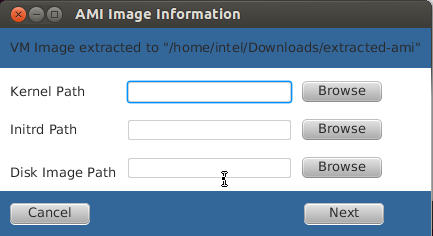
After clicking on ‘Browse’ you will see this file selector dialog. The AMI image is smaller than the QCOW2 image and is a gzipped tar file.



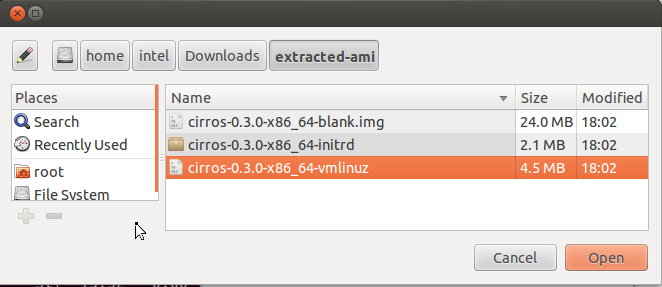
After double clicking on the AMI image selection or clicking on ‘Open’ after selecting it, you will see this main window again. Then click the ‘Browse Directories’ button.



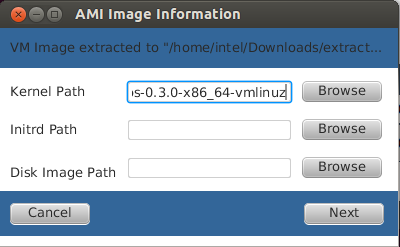
Then you will see this dialog which allows you categorize the files extracted from the gzipped tar file. Next click on the ‘Browse’ button next to the Kernel Path.



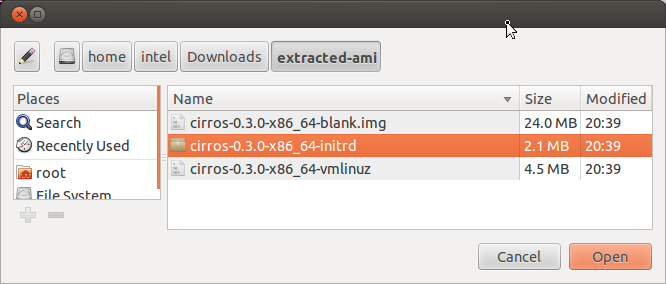
In this dialog box, double click on the vmlinuz file name.



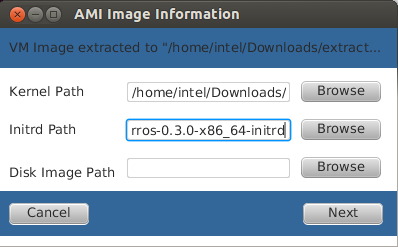
Now click the ‘Browse’ button next to ‘Initrd Path’.



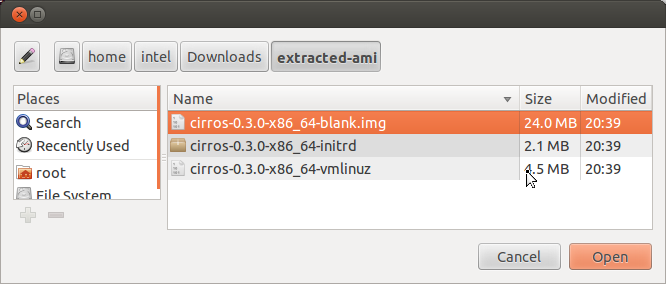
In this dialog box, double click on the initrd file name.



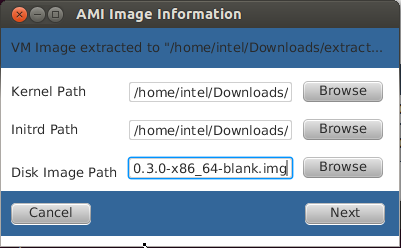
Now click the ‘Browse’ button next to ‘Disk Image Path’.



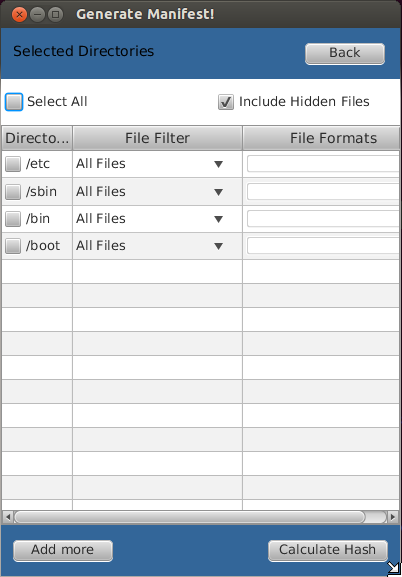
In this dialog box, double click on the .img file name.



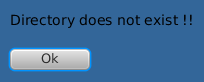
Now click the ‘Next’ button.



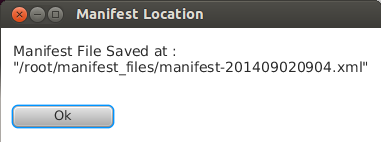
Click the ‘Select All’ check box to unselect all the directories for the AMI version of image. Then click the ‘Calculate Hash’ button.



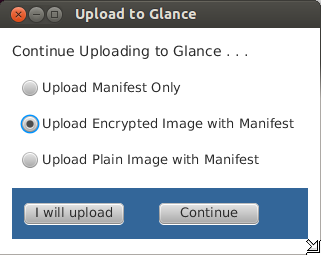
If you do not unselect the directories before clicking on ‘Calculate Hash’ in the previous dialog, you will get this error message for AMI:



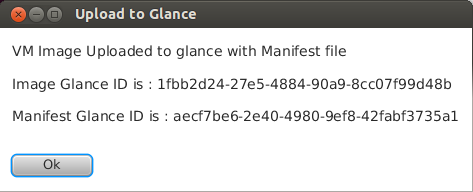
If the directories were unselected above, you will see this informational dialog. You can make note of this file if desired, but this is not necessary. Then click on the ‘Ok’ button.



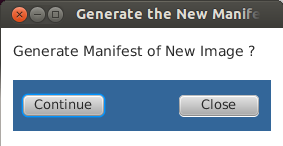
In this dialog, first click on the ‘Upload Encrypted Image with Manifest’ radio button and then click the ‘Continue’ button.



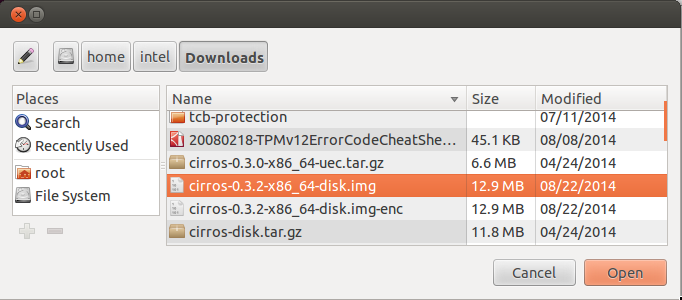
After the upload is complete, you will see this informational dialog. Again, you can make note of this information if desired, but it is not necessary. Then click on the ‘Ok’ button.



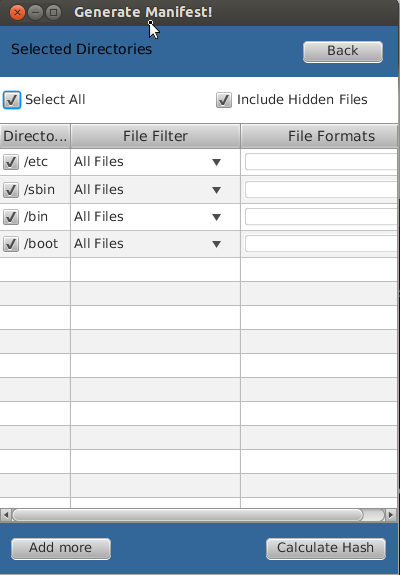
Clicking on the ‘Continue’ button will start the program at the beginning again so another VM image file can be processed. Clicking on ‘Close’ will close the Client Tool.



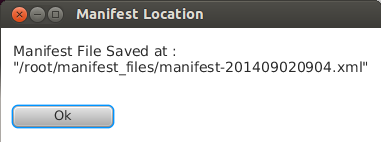
If the QCOW2 image type is selected on the first window, this is the file that should be selected as shown below.



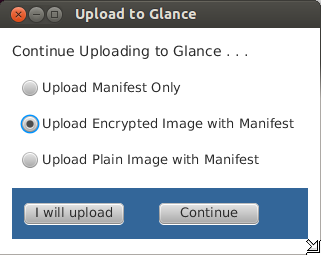
After selecting ‘Browse Directories’, this dialog will come up. For the QCOW2 image, all the directories should remain selected and then click on the ‘Calculate Hash’ button.



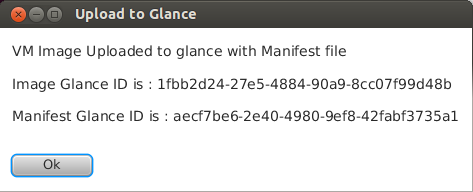
You can make note of this file if desired, but this is not necessary. Then click on the ‘Ok’ button.



In this dialog, first click on the ‘Upload Encrypted Image with Manifest’ radio button and then click the ‘Continue’ button.



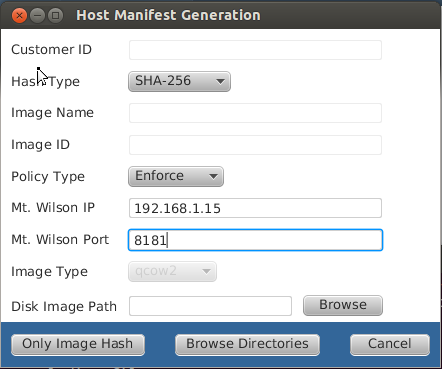
After the upload is complete, you will see this informational dialog. Again, you can make note of this information if desired, but it is not necessary. Then click on the ‘Ok’ button.



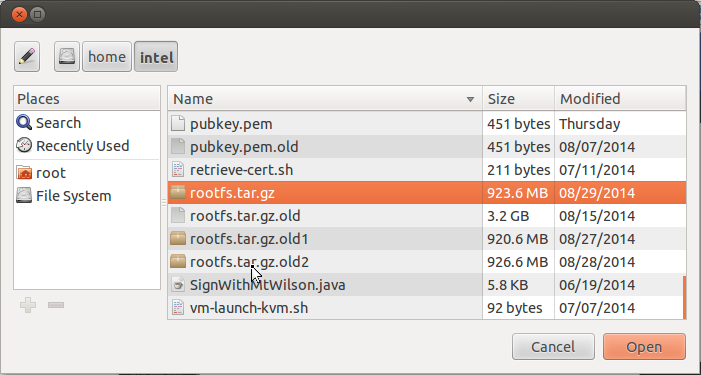
The next step in the process of launching a secure Virtual Machine image is to select the uploaded image and launch it from the OpenStack Dashboard: <http://controller_name_or_IP/horizon>

**How to Use Client Tool to Create a Signed Manifest for rootfs.tar.gz**

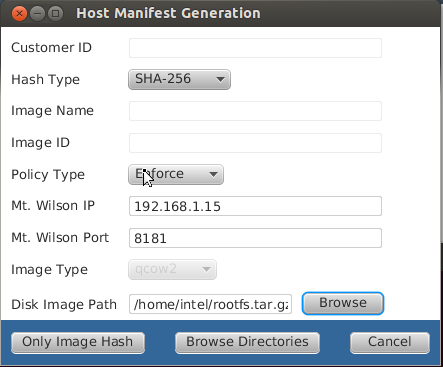
In the first window, shown below, fill in the Mt. Wilson information and click on the ‘Browse’ button. This second example shows how to create a signed manifest xml file for rootfs.tar.gz.



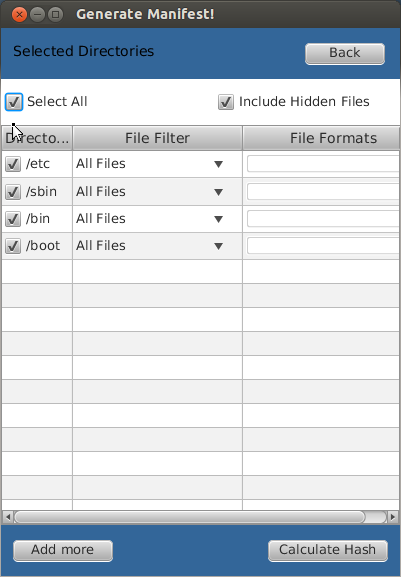
After clicking on ‘Browse’ you will see this file selector dialog. Double click on rootfs.tar.gz or select it and click on the ‘Open’ button.



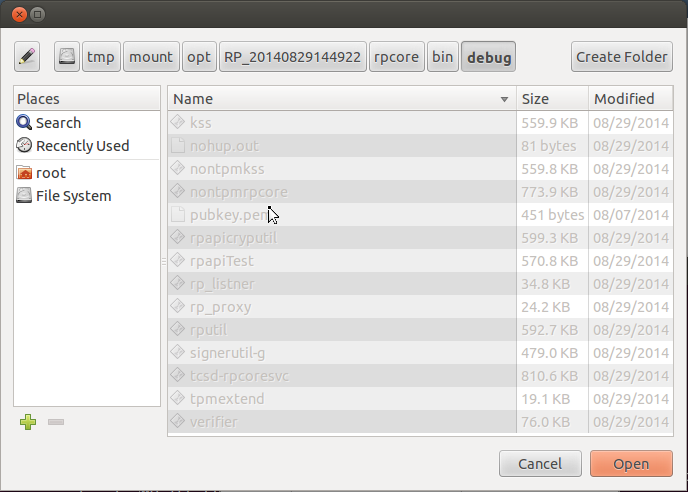
After double clicking on the rootfs.tar.gz selection or clicking on ‘Open’ after selecting it, you will see this main window again. Then click the ‘Browse Directories’ button.



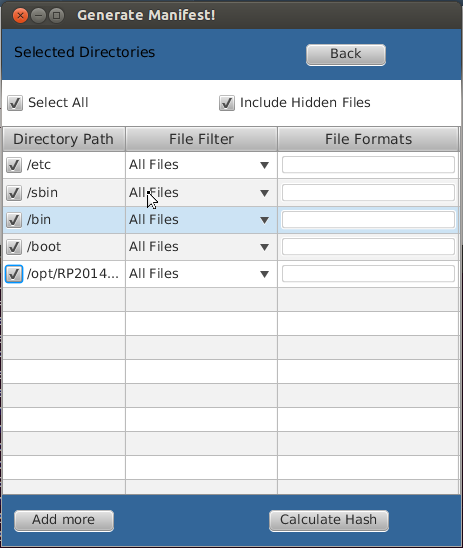
After selecting ‘Browse Directories’, this dialog will come up. Then click on the ‘Add more’ button.



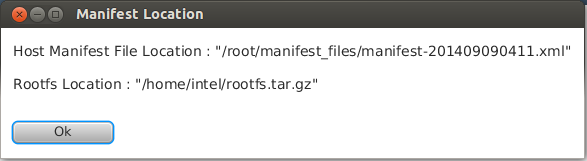
Then in this directory select dialog, select the rpcore/bin/debug directory as shown and click the ‘Open’ button.



For the rootfs.tar.gz image, all the directories should remain selected and then click on the ‘Calculate Hash’ button.



This shows the location of the manifest file just created. You may want to make a note of it to be sure you copy the correct file back to the computer that generated the rootfs.tar.gz file.



Clicking on the ‘Continue’ button will start the program at the beginning again so another rootfs.tar.gz image file can be processed. Clicking on ‘Close’ will close the Client Tool.

