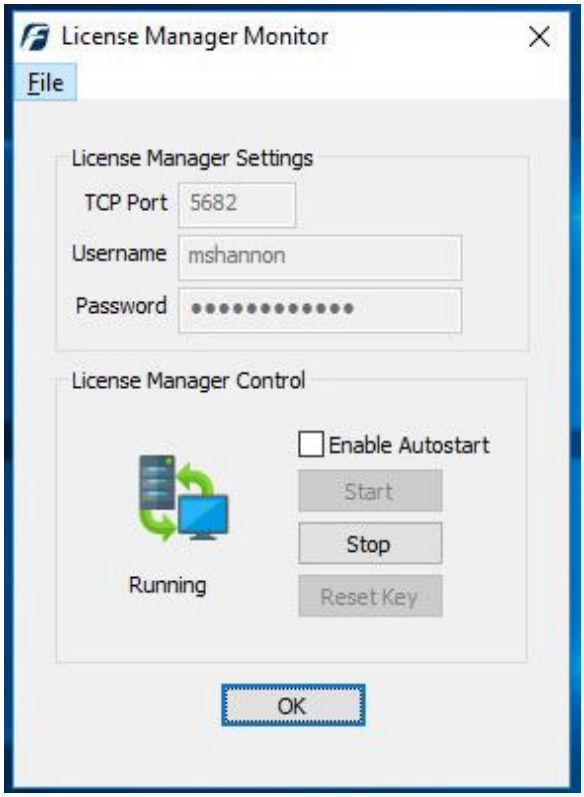
Mission Guide: Covert Deploy

Your Mission: Use F-Response to covertly connect to a remote Non-Windows machine

Using F-Response to deploy and connect to a remote Non-Windows (Apple, Linux, etc.,) machines and access one or more targets

Step 1: Open and start the F-Response License Manager Monitor (If you have not already done so)

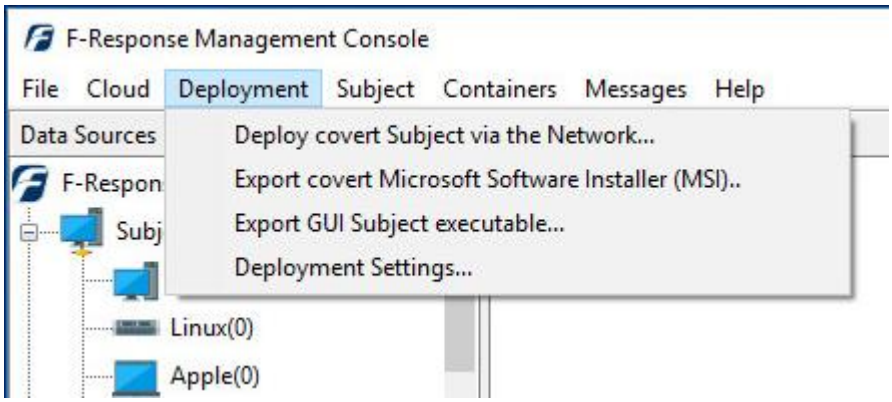
Open the F-Response License Manager Monitor and enter a username and password that will be used specifically for F-Response. These credentials are purely to control access to F-Response on the remote subject, they are NOT a domain account or system account. Once you have set the username and password be sure to press "Start" to start the License Manager Service.



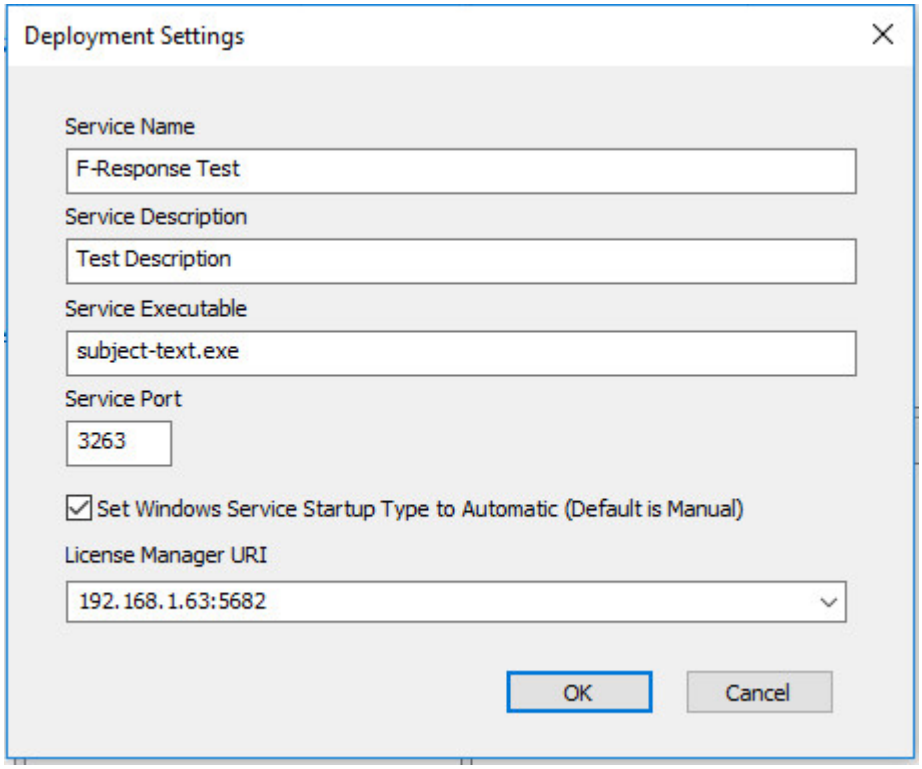
F-Response License Manager Monitor

Step 2: Confirm the Deployment Settings

Open the F-Response Management Console and go to Deployment->Deployment Settings.



Deployment Settings



Deployment Settings Dialog

Many of the options will be pre-populated for you, however you are welcome to adjust them to meet your needs.

Service Name: When F-Response is deployed to the remote machine this is the name of the Windows service that will be created (in this case, we are not connecting to Windows so you can ignore the data here).

Service Description: When F-Response is deployed to the remote machine this is the service description that will be assigned. created (in this case, we are not connecting to Windows so you can ignore the data here).

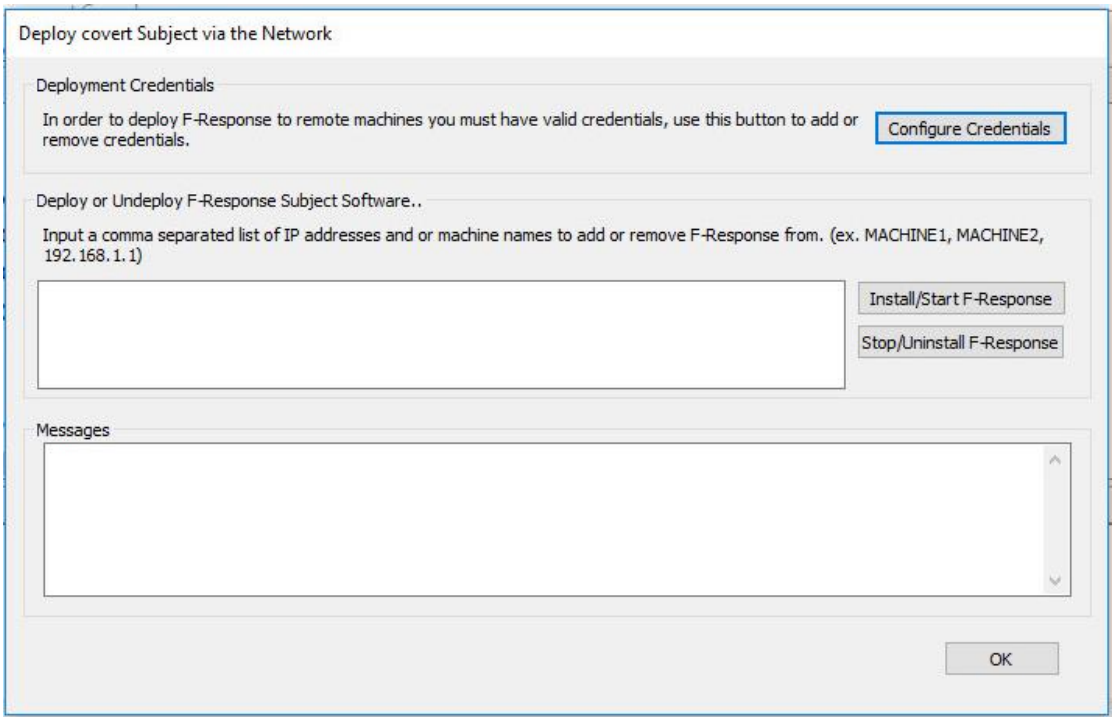
Service Executable: When F-Response is deployed to the remote machine this is the executable name that will be assigned.

Service Port: This is the default TCP port that F-Response will use when listening on the remote machine.

License Manager URI: This is the IP or Hostname plus Port that F-Response will attempt to use to locate your license manager (see step 1). Most of the time it will be easy to determine what to select here, however keep in mind the address you select must be accessible to the remote machine.

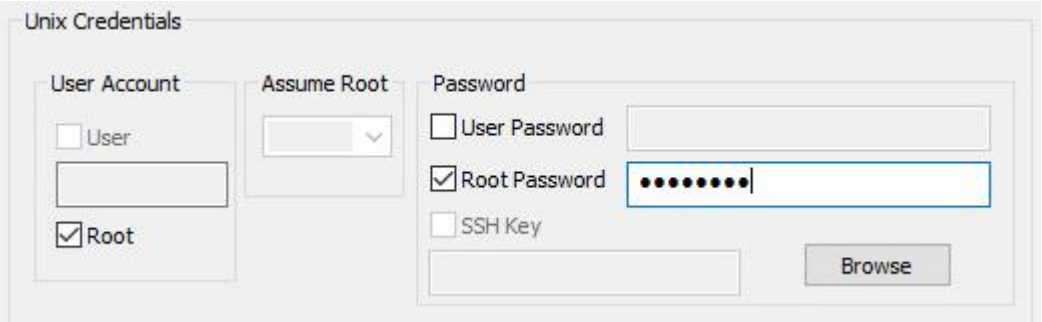
Step 3: Begin the deployment process by adding credentials

Open the Deployment->Deploy covert Subject via the Network… dialog to begin the deployment process.



Deploy covert Subject via the Network…

Now that we've opened the dialog the first order of business is to configure credentials to use for deployment. Keep in mind that unlike previous versions of F-Response, starting in version 7, F-Response stores the deployment credentials encrypted in the examiner's registry. Press Configure Credentials to get started.

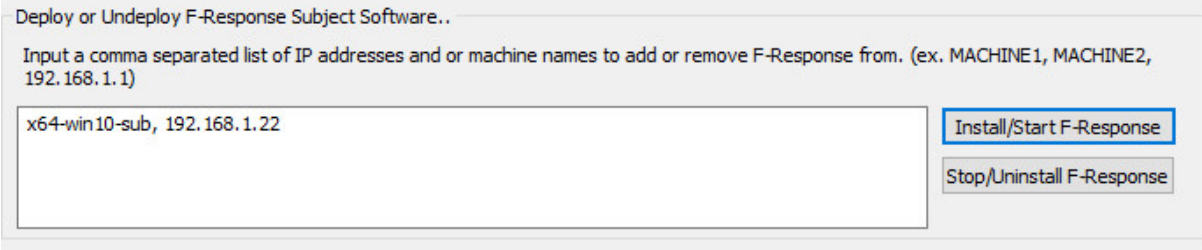


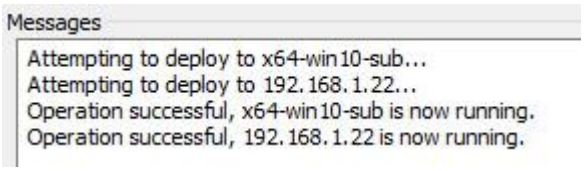
Adding Non-Windows Deployment Credentials

You will want to input one or more credentials to use for deployment and click the Add button for each one. Press OK when complete.

Step 4: Scan for one or more remote machines

After adding at least one credential you will be able to use the Deploy or Undeploy box to add one or more comma delineated hostnames or IP addresses. Once you've added them you must press the Install/Start F-Response button to begin the scanning and deployment process.



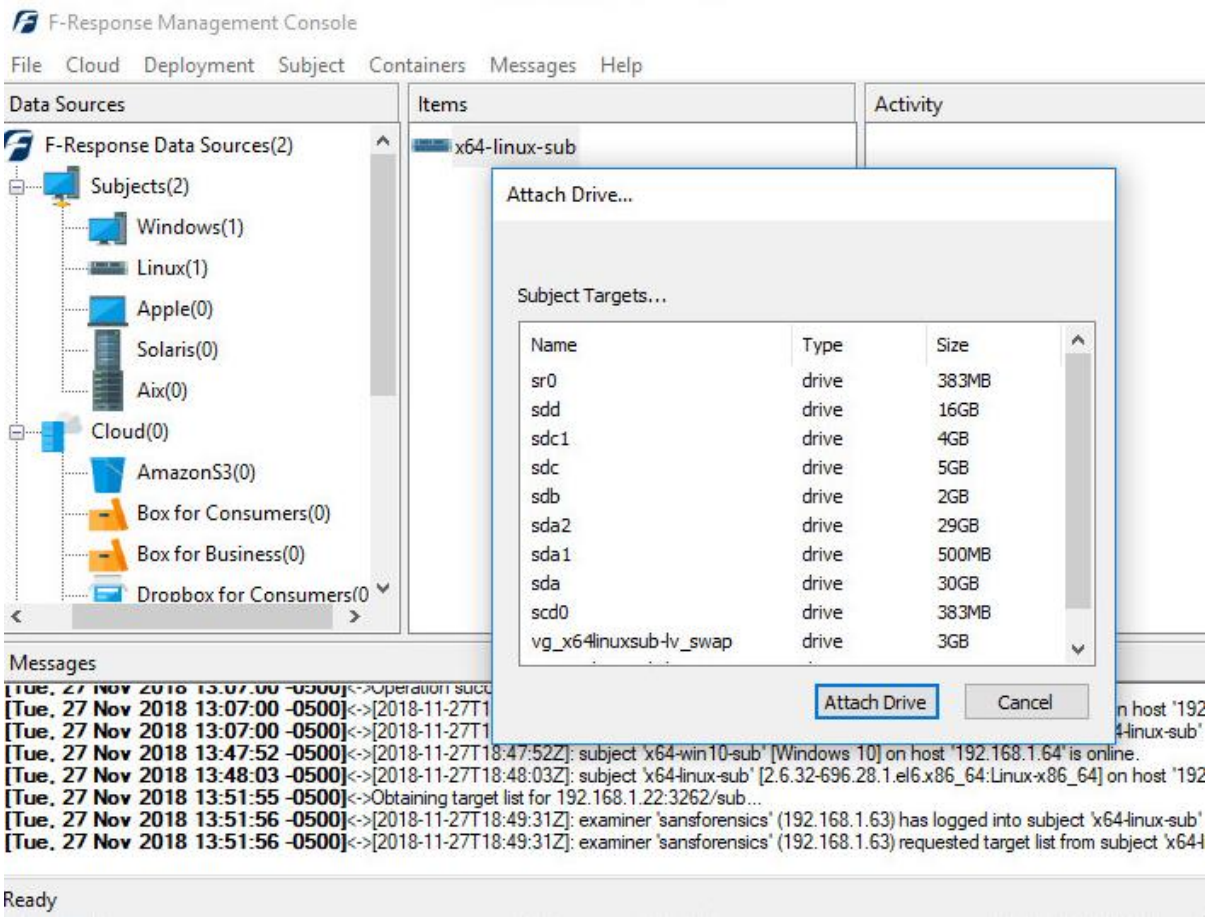


The results will appear below in the Messages section of the dialog. Provided your credentials were successful and the machine was available on the network you should see the following response. If not, please check your credentials and try again, failing that we recommend you consult the Troubleshooting section at the end of this document.

Click OK to return to the main window of the F-Response Management Console.

Step 5a: List the available targets and attach one or more to your local machine

After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Double-Click on any subject to open a dialog for attaching a subject disk, or use the Subject menu for attaching a disk or starting a direct image of one or more subject targets.

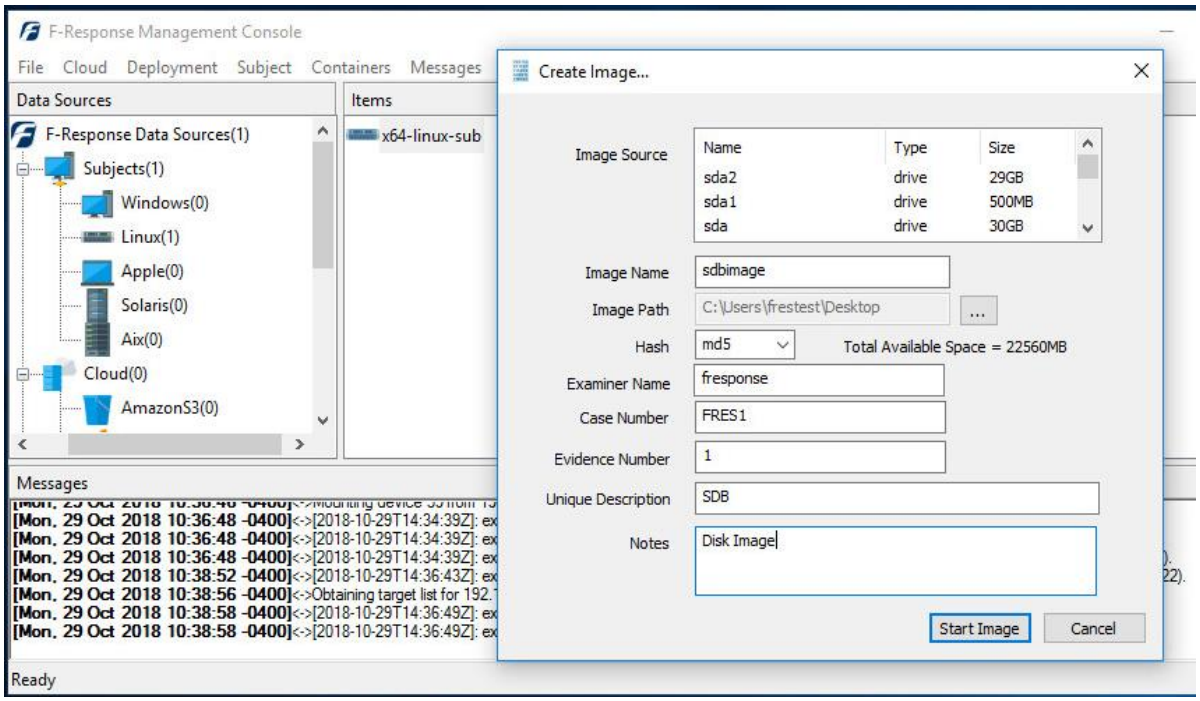


Subject and Targets

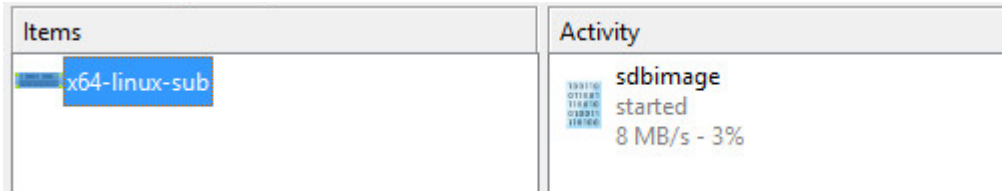
Active Targets

Step 5b: List the available targets and image one or more to your local machine directly(optional)

After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Right click on any subject and select Image Subject Target menu option to commence a direct image of one or more subject targets.



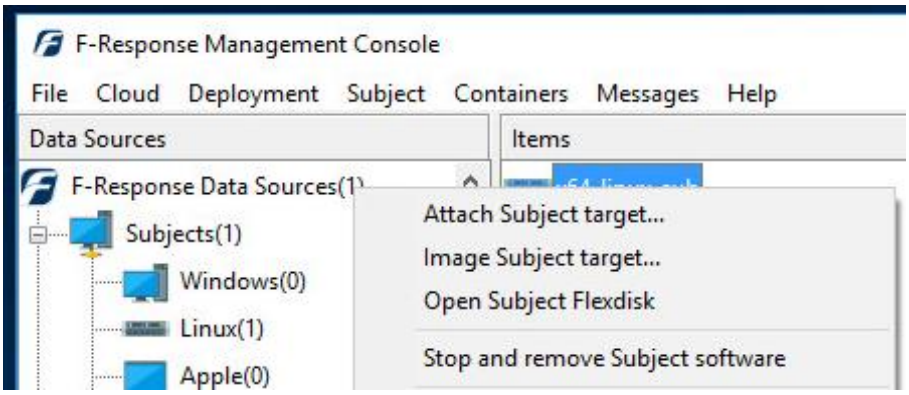
Start Imaging Process…



Active Images

Step 6: Removing F-Response from the remote machine

When you are finished using F-Response on the remote machine it can be readily removed using the Subject menu. First disconnect any active disks or images by right clicking on them in the Activity panel and selecting Cancel/Detach. Once all targets are detached, simply select the subject machine in the Items panel and right-click to select the "Stop and Remove Subject Software" to stop and remove all F-Response software from the remote machine.



Stopping and removing F-Response from the remote machine.

Troubleshooting

I can deploy F-Response, but when I try to start I get an error telling me it could not connect to License Server?

Most of the time this is due to the local firewall on your examiner machine. Check that you do not have a local or network firewall rule blocking access to your license manager from the remote subject(s).

I can deploy F-Response, but when I try to start I get an "error code zero" message.

This is usually due to an AV or security product on the subject computer, try disabling the AV or whitelist the executable.

I can successfully deploy to the remote machine but cannot get a listing of targets, why might that be?

This is typically the case when a firewall on the remote machine is keeping you from being able to communicate with the F-Response software on that machine. You may need to set firewall exceptions for the F-Response software, or alternatively disable the firewall temporarily while you are connected to the machine.