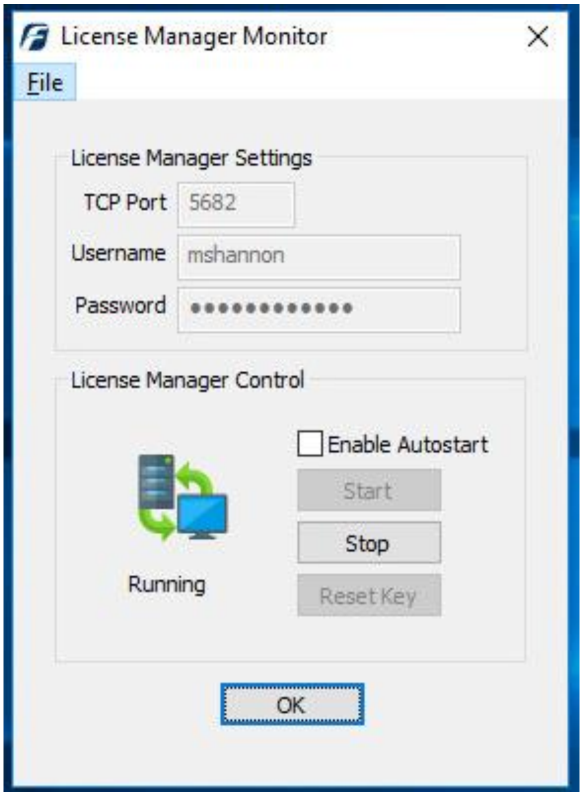
Mission Guide: Covert Deploy

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

Using F-Response to deploy and connect to a remote Windows machine 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 create 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.



License Manager Settings

TCP Port 5682

Username mshannon

Password ●●●●●●●●●●●●●

License Manager Control

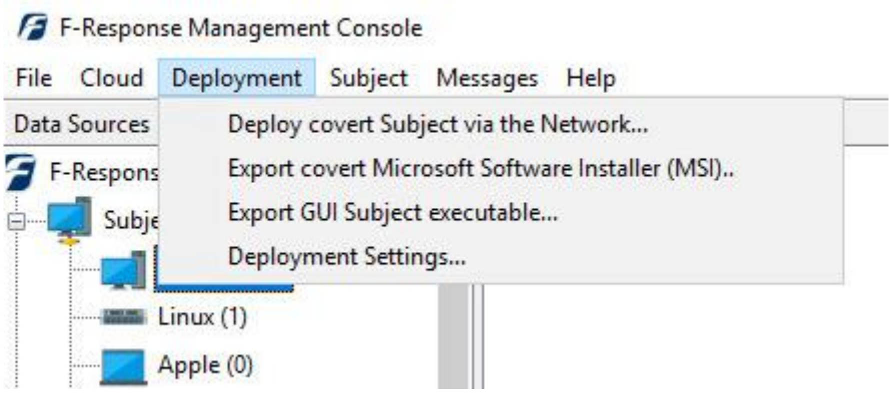
□ Enable Autostart

Running

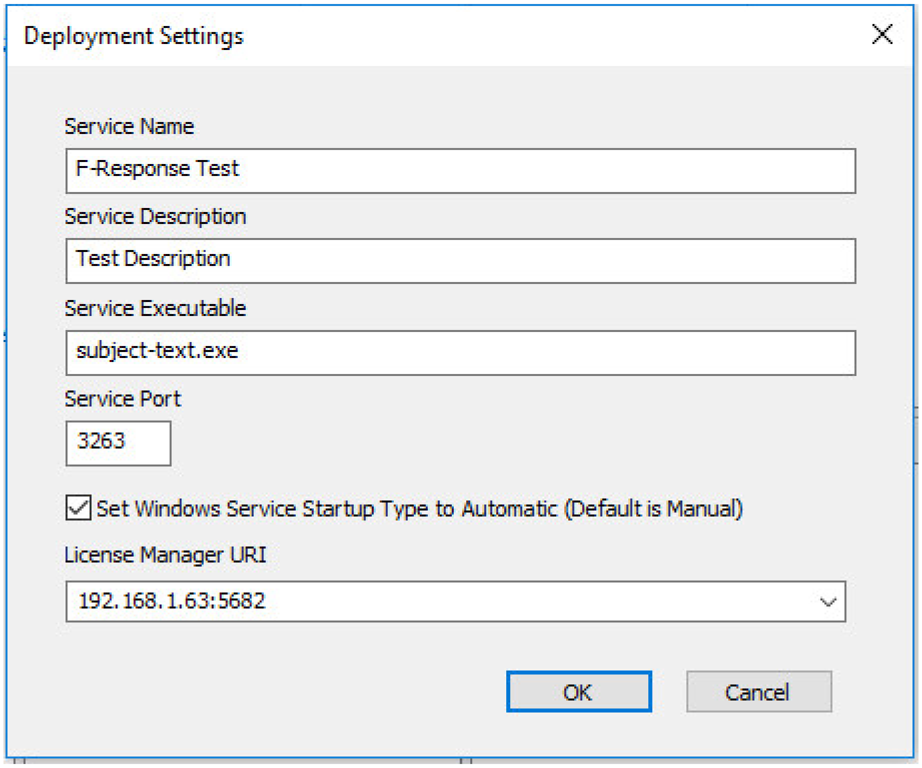
F-Response License Manager Monitor

Step 2: Confirm the Deployment Settings

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


F-Response Management Console
File
Cloud
Deployment
Subject
Messages
Help
Data Sources
Deploy covert Subject via the Network...
Export covert Microsoft Software Installer (MSI)..
Export GUI Subject executable...
Deployment Settings...
F-Respons
Subje
Linux (1)
Apple (0)

Deployment Settings



Deployment Settings

Service Name

F-Response Test

Service Description

Test Description

Service Executable

subject-text.exe

Service Port

3263

☑ Set Windows Service Startup Type to Automatic (Default is Manual)

License Manager URI

192.168.1.63:5682

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.

Service Description: When F-Response is deployed to the remote machine this is the service description that will be assigned.

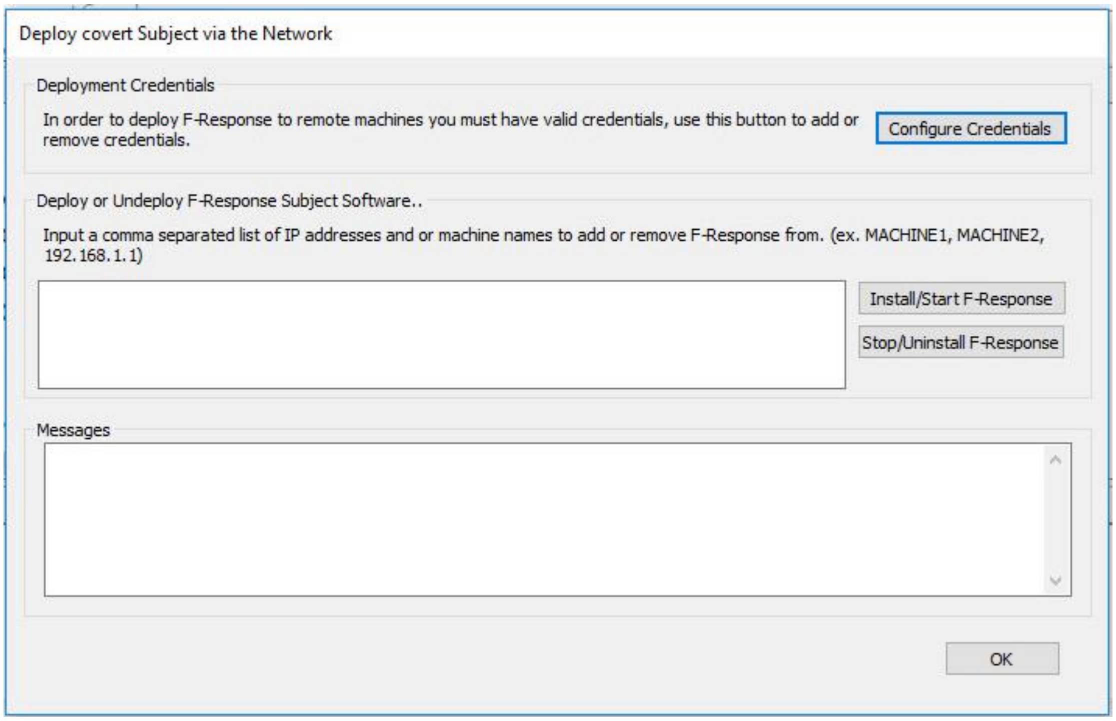
Service Executable: When F-Response is deployed to the remote machine this is the executable name that will be assigned.

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

Deployment Credentials

In order to deploy F-Response to remote machines you must have valid credentials, use this button to add or remove credentials.

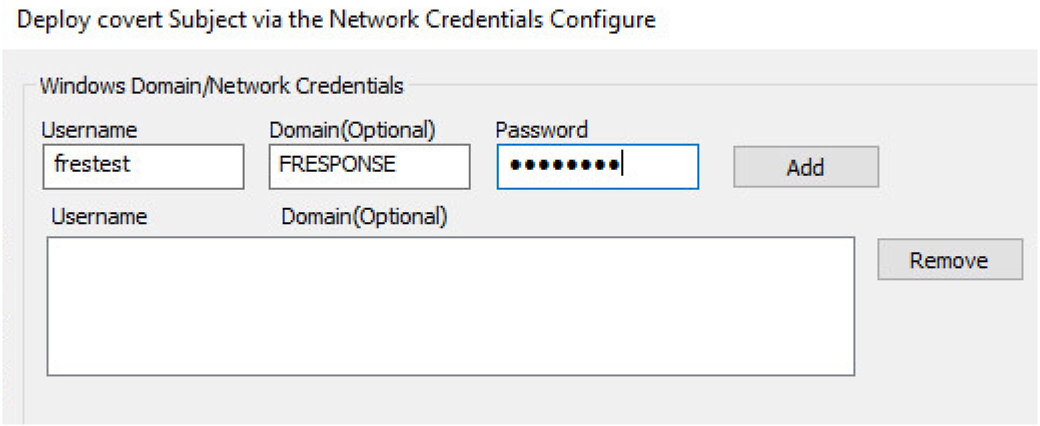
Deploy or Undeploy F-Response Subject Software..

Input a comma separated list of IP addresses and or machine names to add or remove F-Response from. (ex. MACHINE1, MACHINE2, 192.168.1.1)

Messages

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. Press Configure Credentials to get started.



Deploy covert Subject via the Network Credentials Configure

Windows Domain/Network Credentials

Username: frestest

Domain(Optional): FRESPONSE

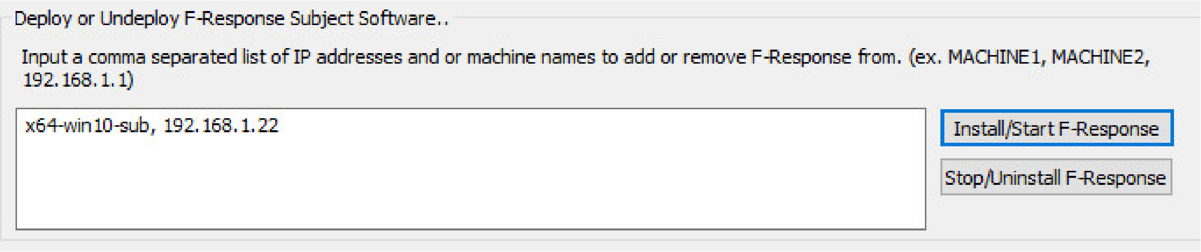
Password: ••••••••

Adding Windows Deployment Credentials

You will want to input one or more Username/Domain/Password combinations to use for deployment. Please keep in mind that some credentials will not work properly even when they are accurate due to Microsoft Workgroup and Domain policies. If you are having issues with credentials, please see the Troubleshooting section at the end of this document.

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.

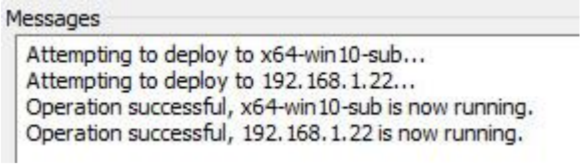


Deploy or Undeploy F-Response Subject Software..

Input a comma separated list of IP addresses and or machine names to add or remove F-Response from. (ex. MACHINE1, MACHINE2, 192.168.1.1)

x64-win10-sub, 192.168.1.22

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.



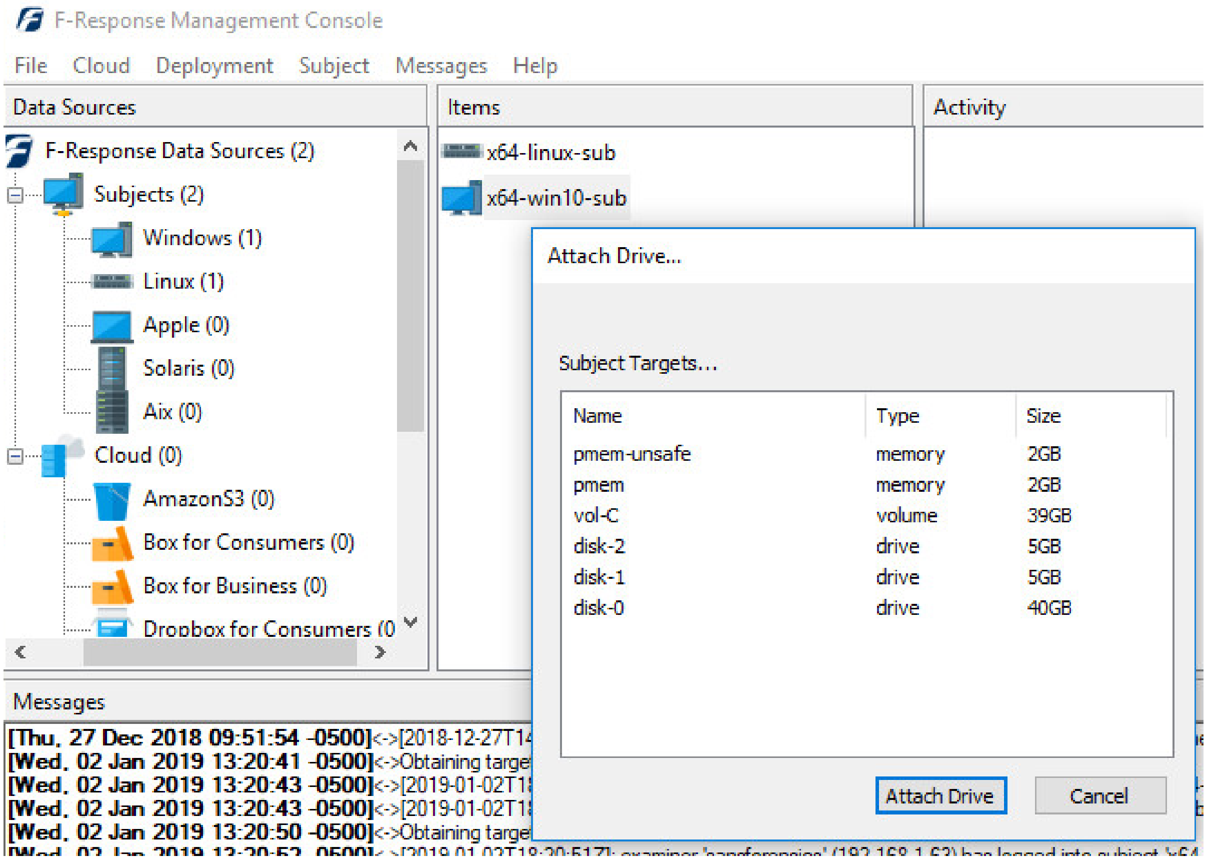
Messages

```
Attempting to deploy to x64-win10-sub...
Attempting to deploy to 192.168.1.22...
Operation successful, x64-win10-sub is now running.
Operation successful, 192.168.1.22 is now running.
```

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

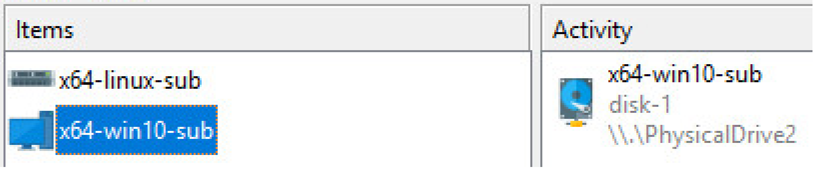
After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Double-Click on any subject to open a dialog for attaching a subject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



Name	Type	Size
pmem-unsafe	memory	2GB
pmem	memory	2GB
vol-C	volume	39GB
disk-2	drive	5GB
disk-1	drive	5GB
disk-0	drive	40GB

```
[Thu, 27 Dec 2018 09:51:54 -0500]<->[2018-12-27T14
[Wed, 02 Jan 2019 13:20:41 -0500]<->Obtaining targe
[Wed, 02 Jan 2019 13:20:43 -0500]<->[2019-01-02T1
[Wed, 02 Jan 2019 13:20:43 -0500]<->[2019-01-02T1
[Wed, 02 Jan 2019 13:20:50 -0500]<->Obtaining targe
```

Subject and Targets

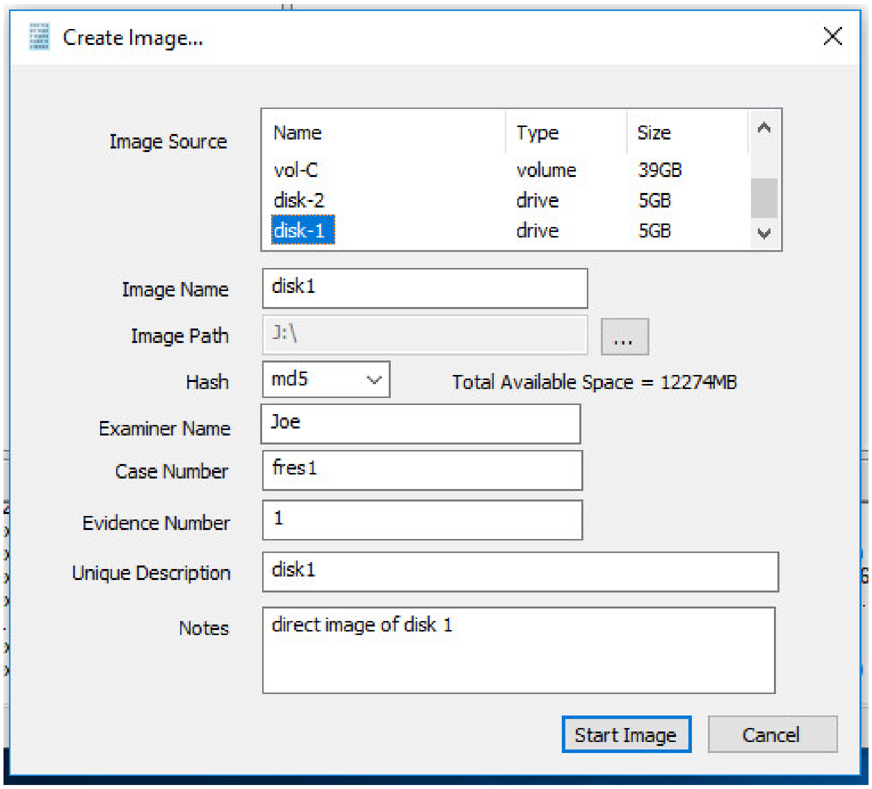


Active Targets

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

Please remember F-Response is first and foremost a vendor-neutral connectivity tool. You can use any forensic/eDiscovery/IR tool you'd like against the write-protected F-Response connected disk. That being said, the F-Response Console does have a built-in full-disk imaging option that will maximize the F-Response connection to its fullest capabilities (for individual file collection, you'd need to leverage a different imaging tool from your kit). For full details on imaging from the F-Response Console, please refer to the manual on our website.

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.



Create Image...

Image Source

Name	Type	Size
vol-C	volume	39GB
disk-2	drive	5GB
disk-1	drive	5GB

Image Name: disk1

Image Path: J:\

Hash: md5 — Total Available Space = 12274MB

Examiner Name: Joe

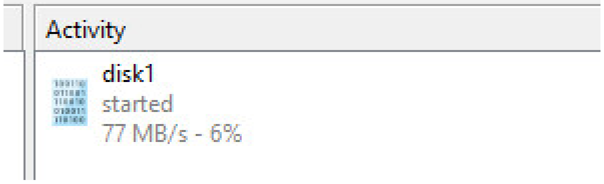
Case Number: fres1

Evidence Number: 1

Unique Description: disk1

Notes: direct image of disk 1

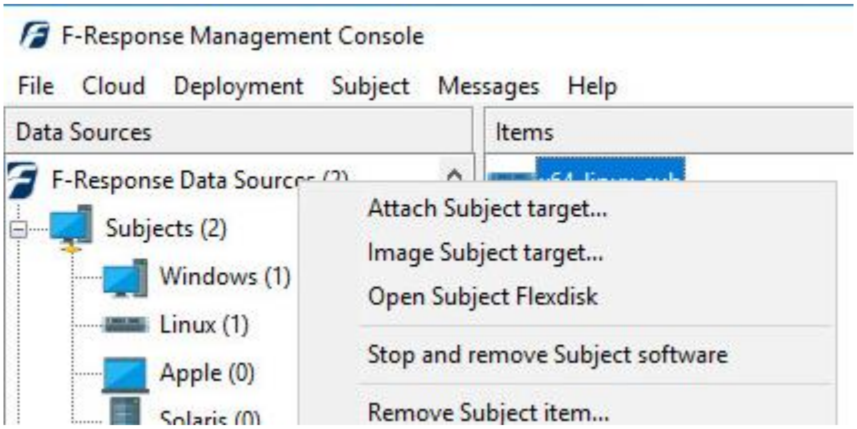
Start Imaging Process...



Imaging Activity

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 it 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.

When I attempt to deploy F-Response using the console I cannot, even though I have valid credentials?

This is typically the case when attempting to connect to Windows machines that are not part of a Domain.

Your target machine is most likely a Windows machine not running in "Classic" mode for credential authentication. To switch the target machine to Classic you must open the Local Security Policy Administration Tool under Control Panel, Administrative Tools. You will then select Local Policies->Security Options and change the value of "Network Access: Sharing and Security Model for Local Accounts" to "Classic – Local Users authenticate as themselves". This is only necessary when using the Console to deploy F-Response to computers that are not part of a Windows Domain. If the target machine is a Windows 7 or newer Windows OS and not joined to a Domain (ie. Workgroup Member) then a key will need to be added to the registry of the target machine. You can manually create and add it the registry by following these steps:

To create your registry key, copy the following information into Notepad:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

Save this file as LocalAccountTokenFilterPolicy.reg, and then copy it to your target machine. Double click this file on the target machine to populate the registry with this key.

To remove follow the same steps as above this time with the following information:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000000
```