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. **Note SIP must be disabled for OSX, more details can be found here: https://fresponse.com/blog/f-response-apple-sip-ohm **



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.

13	License Ma	nager Mo	nitor	×		
<u>F</u> ile				_		
Ŧ	License Ma	nager Sett	ings			
	TCP Port	5682				
	Username mshannon					
	Password					
1						
Ť	License Ma	nager Con	trol			
	-		Enable Autostart			
	=		Start			
	- -		Stop			
	Runn	ing	ResetKey			
			OK			
		Business				

Step 2: Confirm the Deployment Settings

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

File Cloud	Deployment	Subject	Messages	Help	
Data Sources	Deploy o	overt Sub	ject via the N	Vetwork	
F-Respons	Export c	overt Micr	osoft Softwa	are Installer (MSI)	
Subje Export G		UI Subject	t executable.		
	Deployment Settings				
	Linux (1) Apple (0)				

Deployment Settings

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	Service Name	
Service Description Test Description Service Executable subject-text.exe Service Port 3263 Set Windows Service Startup Type to Automatic (Default is Manual) .icense Manager URI	F-Response Test	
Test Description Service Executable subject-text.exe Service Port 3263 Set Windows Service Startup Type to Automatic (Default is Manual) icense Manager URI	Service Description	
Service Executable subject-text.exe Service Port 3263 Set Windows Service Startup Type to Automatic (Default is Manual) icense Manager URI	Test Description	
subject-text.exe Service Port 3263 Set Windows Service Startup Type to Automatic (Default is Manual) .icense Manager URI	Service Executable	
Service Port 3263 Set Windows Service Startup Type to Automatic (Default is Manual) License Manager URI	subject-text.exe	
	Service Port 3263	
192.168.1.63:5682	Set Windows Service Startup Ty	pe to Automatic (Default is Manual)

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.

Deployment Credentials	
In order to deploy F-Response to remote machines you must have valid credentials, remove credentials.	use this button to add or Configure Credentials
Deploy or Undeploy F-Response Subject Software	
Input a comma separated list of IP addresses and or machine names to add or removing 192, 168, 1, 1)	ve F-Response from. (ex. MACHINE1, MACHINE2,
	Install/Start F-Response
	Stop/Uninstall F-Response
/lessages	A

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.

ser Account	Assume Root	Password		
User	×	User Password		
		Root Password	•••••	
Root		SSH Key		

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.

Deploy or Undeploy F-Response Subject Software	
Input a comma separated list of IP addresses and or machine names to add or removed 192.168.1.1) $\!\!\!$	ve F-Response from. (ex. MACHINE1, MACHINE2,
x64-win10-sub, 192.168.1.22	Install/Start F-Response
	Stop/Uninstall F-Response

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

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.

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. F-Response Management Console

	Activity		
ıb Attach Drive			
ub			
Subject Targets			
Subject Targets			
Name	Type	Size	^
scd0	drive	383MB	
vg_x64linuxsub-lv_swap	drive	3GB	
vg_x64linuxsub-lv_root	drive	26GB	
sr0	drive	383MB	
sdd	drive	16GB	
sdc1	drive	4GB	
sdc	drive	5GB	
sdb	drive	2GB	
sda2	drive	29GB	
sda1	drive	500MB	~
	ib Attach Drive sub Subject Targets Name scd0 vg_x64linuxsub-lv_swap vg_x64linuxsub-lv_root sr0 sdd sdc1 sdc sdb sda2 sda1	Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Activity Subject Targets Name Type scd0 drive vg_x64inuxsub-lv_swap drive vg_x64inuxsub-lv_root drive scd0 drive scd2 drive scda1 drive sc	Attach Drive Attach Drive Attach Drive Subject Targets Name Type Size scd0 drive 383MB vg_x64linuxsub-lv_swap drive 3GB vg_x64linuxsub-lv_root drive 26GB sr0 drive 383MB sdd drive 16GB sdc1 drive 4GB sdc1 drive 4GB sdc2 drive 2GB sda1 drive 29GB sda1

Subject and Targets

ltems	Activity	
хб4-linux-sub	x64-linux-sub sdb \\.\PhysicalDrive1	

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.

inage boarce	Name	Туре	Size	^		
	scd0	drive	383MB			
	vg_x64linuxsub-lv_root	drive	26GB	~		
Image Name	sdbimage					
Image Path	J:\					
Hash	md5 V Total Available Space = 12189MB					
Examiner Name	Joe					
Case Number	fres2					
Evidence Number	2					
Evidence Number	SDB					
Unique Description	SDB			Direct Image of remote disk		

Start Imaging Process...

ltems	Activity		
x64-linux-sub	sdbimage started 8 MB/s - 3%		

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.



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.