

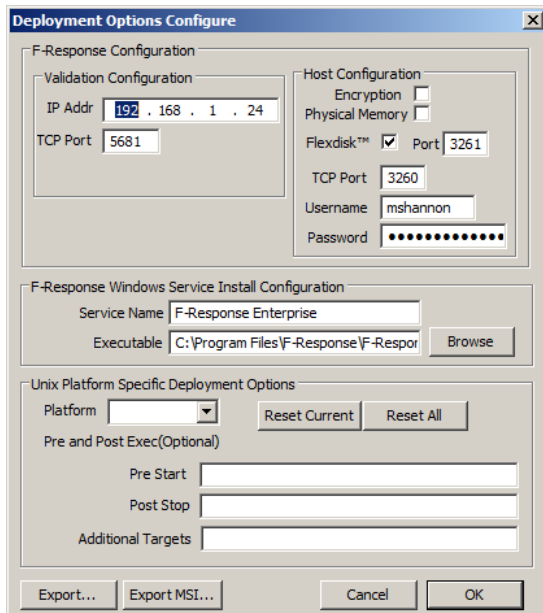
Your Mission: Using F-Response Consultant Edition with the Enterprise Management Console

Note: This guide assumes you have installed F-Response Enterprise Edition, your F-Response licensing dongle is plugged into your analyst machine, the F-Response License Manager Monitor is installed and running, and the F-Response Enterprise Management Console (FEMC) has been started. For more information, please reference the F-Response User Manual, or the [F-Response Enterprise Edition Training Video](#) on the F-Response Website.

Step 1: Export the Configuration

In order to use the F-Response Consultant edition executable quickly and easily with F-Response Enterprise you will need to export the configuration file with your settings.

In the FEMC go to File – Configure Options... and the Deployment Options Configure window will open.



Now press the "Export..." button to export the necessary configuration information. You will want to save this information to an easy to access folder, in our example we have saved the F-Response export files to our Desktop.

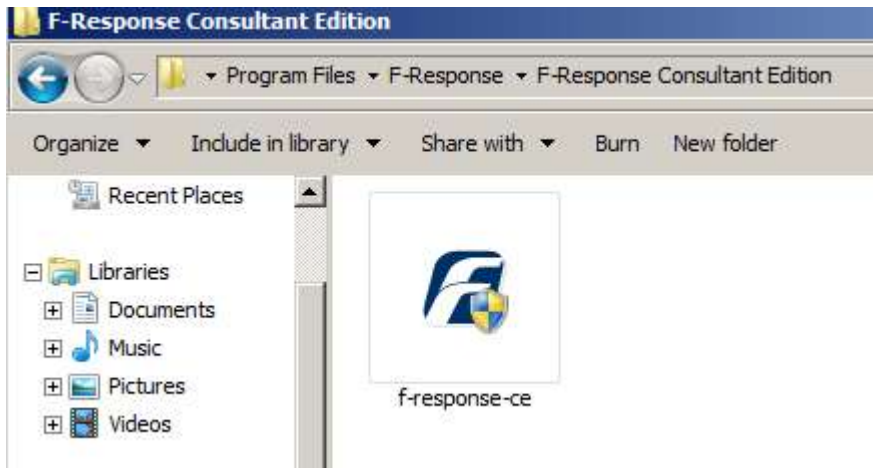


First you can delete the f-response-ent.exe file as we will not be using it for this task. Next rename the f-response-ent.exe.ini file to fresponse.ini as pictured below.



Now we will need to navigate to the F-Response Enterprise installation folder and copy the Consultant Edition executable to our Desktop.

The Consultant edition windows executable is "f-response-ce.exe" and is located in C:\Program Files\F-Response\F-Response Consultant Edition.



After placing this file on the desktop you should have the following executable and configuration file ready to run on your target machine(s).

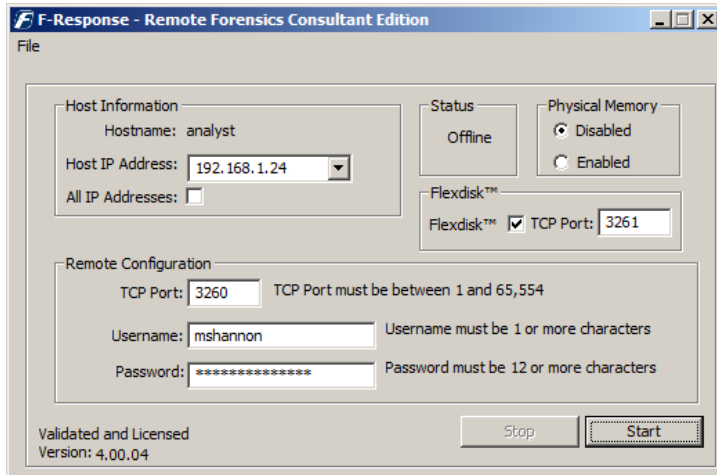


Step 2: Copy and execute the resulting bundle on one or more target Windows machines

You will want to copy these files to either a network share, a usb disk, or some other portable media such that they can be transported to and executed on the target machine.

Once on the target machine simply double click to execute the Consultant edition executable.

The executable should automatically configure and validate, at this point simply press "Start" to begin the Consultant edition program on the target computer.



Step 3: Issue Discovery Request

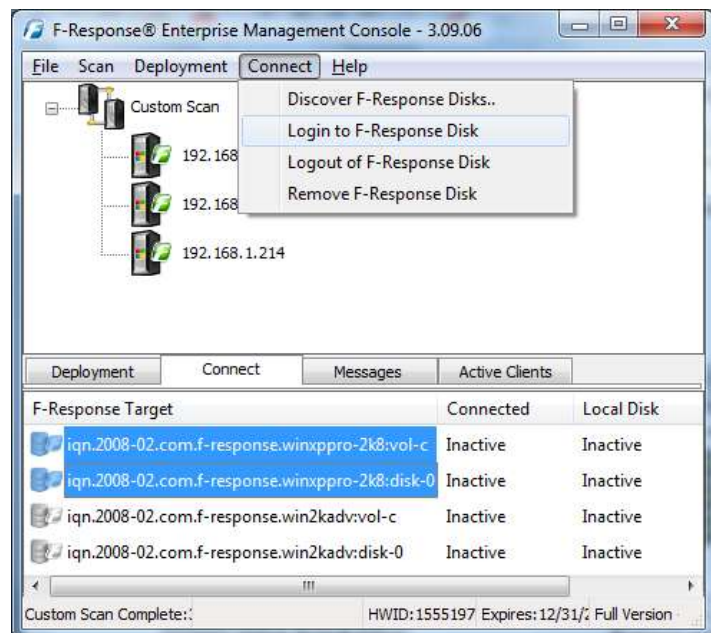
Return to your F-Response Enterprise Management Console (FEMC) and select the Active Clients tab. On this tab you should now see your target Consultant edition machine, select it, right click, and select "Issue Discovery Request" from the drop-down context menu.

Deployment	Connect	Messages	Active Clients
IP Address	Hostname	Platform	
192.168.1.24	ANALYST	Windows 7	

Step 4: Connect to disk(s) on your Windows target(s)

The results of your discovery request will be listed under the Connect tab. Here you can pick what disk(s) to connect to by highlighting and choosing Login to F-Response Disk from the Connect drop down or right click menus.

Once you log into the target disk the F-Response badge icon will change from gray to blue and the Connected status column will show as Connected.



Step 5: Fire up the tool of your choice!

F-Response is a vendor neutral product. Once F-Response presents the remote target disk as a write blocked local connection, we step out of your way so that you can select the right tool to get your job done. At this point, you can reach into your toolbox and apply the tool of your choice to the target disk(s).

Understanding F-Response Disk Naming




F-Response uses the following naming convention for target disks:

iqn.2008-02.com.f-response.HOSTNAME.O/S disk name

We are only concerned with the "HOSTNAME.O/S disk name" portion of the name.

HOSTNAME is the name of your Windows target machine. If you only know the IP address a quick glance back at the Active Clients tab will help you tie the hostname to the address.

For the "O/S disk name," F-Response can access both remote physical disks and the logical volumes on those disks. Windows identifies hard disks using the format "disk-#". The 'x' portion is a number, starting with zero, representing the physical drive. Windows identifies logical volumes in the format "vol-*", where "*" is a letter corresponding to a volume on the remote physical disk. For example:

Deployment	Connect	Messages	Active Clients	
F-Response Target		Connected		Local Disk
 iqn.2008-02.com.f-response.winxppro-2k8:vol-c	Connected			\\.\PhysicalDrive1
 iqn.2008-02.com.f-response.winxppro-2k8:disk-0	Connected			\\.\PhysicalDrive2
 iqn.2008-02.com.f-response.win2kadv:vol-c	Inactive			Inactive

The first target in this list is on the target machine named 'winxppro-2k8', and we can tell by the last piece of the name this is the logical volume 'C' on that machine. The second target in this list is on the same machine, but represents the entire physical disk (and any logical volumes it may contain) as shown by the last portion of the naming convention (disk-0). The third and last target in this list we are not currently connected to, but can tell by the naming convention it is volume C on the machine named 'win2kadv'.

Troubleshooting

If you are having issues not covered in this guide. Please don't hesitate to contact us directly either on the web (www.f-response.com) or via email (support@f-response.com).