

Your Mission: Use the F-Response Accelerator to connect multiple analysts to multiple target disks.

Note: This guide assumes you already have a working knowledge of F-Response Enterprise Edition or F-Response Consultant Edition. Also, the F-Response licensing dongle is plugged into an analyst machine, the F-Response License Manager Monitor is installed and running, and either the F-Response Enterprise Management Console (FEMC) or F-Response Consultant Connector has been started. For more information, please reference the F-Response User Manual, or the Mission Guide for F-Response EE or CE available on the F-Response Website under support.

Scenario

Often there are several machines at a client site that require examination or imaging. Using F-Response Enterprise Edition or Consultant Edition in conjunction with the F-Response Accelerator, available hardware can be leveraged to connect several analyst machines to different target machines for use concurrently.

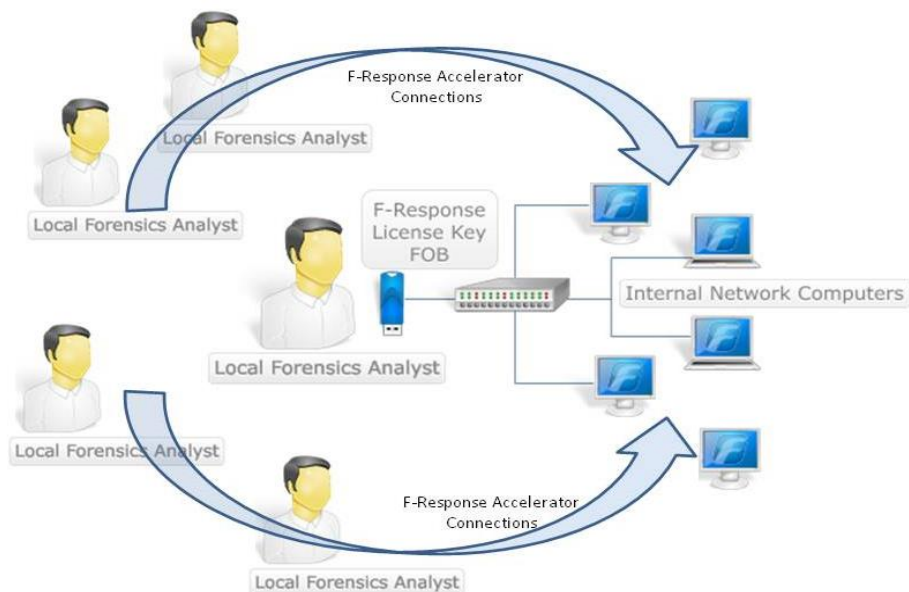
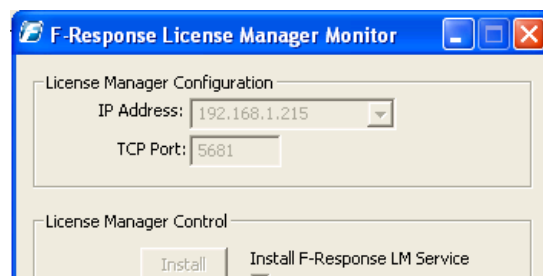
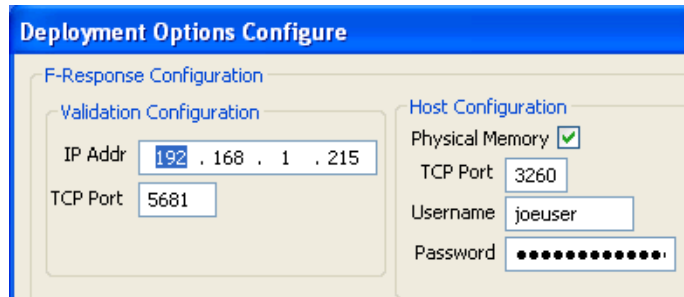


Diagram depicting multiple Accelerator connections accessing multiple target computers.

One computer will have the F-Response licensing dongle plugged in, F-Response License Manager Monitor (LMM) installed and running, and either the F-Response Enterprise Management Console (FEMC) or F-Response Consultant Connector (FCC) started. In addition you have already deployed F-Response CE or EE to your target machine(s).



F-Response License Manager Monitor, should be started and running on your CE or EE computer.

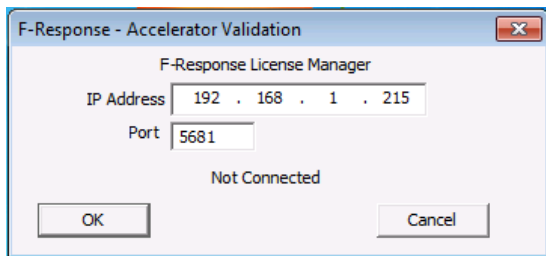


You will also need the following Host Configuration information: TCP Port, Username, and Password, as exemplified in the figure above.

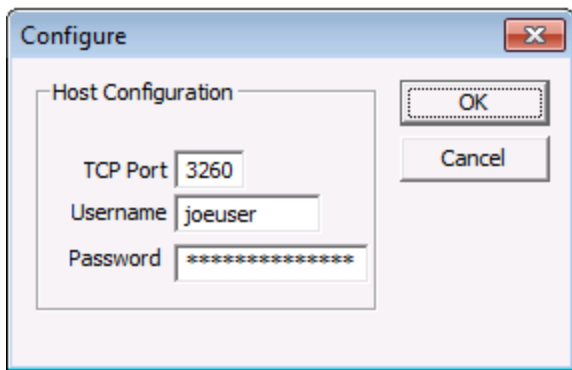
Step One: Prepare and Configure the Analyst Machines

Additional analyst computers can be configured using F-Response Accelerator. Install F-Response Enterprise or Consultant edition on each machine. Once the install is complete you can browse the F-Response directory to locate the F-Response Accelerator executable. If F-Response was installed with the default settings, the "f-response-accel.exe" executable can be found in C:\Program Files\F-Response\...

Start the Accelerator on each analyst machine. The Accelerator Validation window will appear and prompt you for the IP of the LMM running on the master analyst machine.



Again, the IP and port entered here should match the IP and port of the LMM running on the master analyst machine. After entering the IP and port of the licensing server, click OK in the Accelerator Validation window.

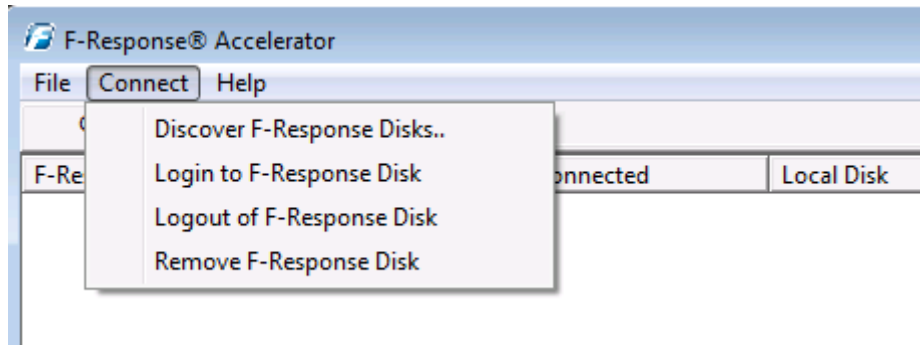


Next, click the File menu and select Configure. The Configure window will open where you can enter the F-Response username and password. The F-Response port, username and password should be identical to the information from either your FEMC Deployment Options or the FCC Configure/Quick Configure.

Click Okay after configuring your host information.

Step Two: Connect to F-Response Targets from Analyst Machines

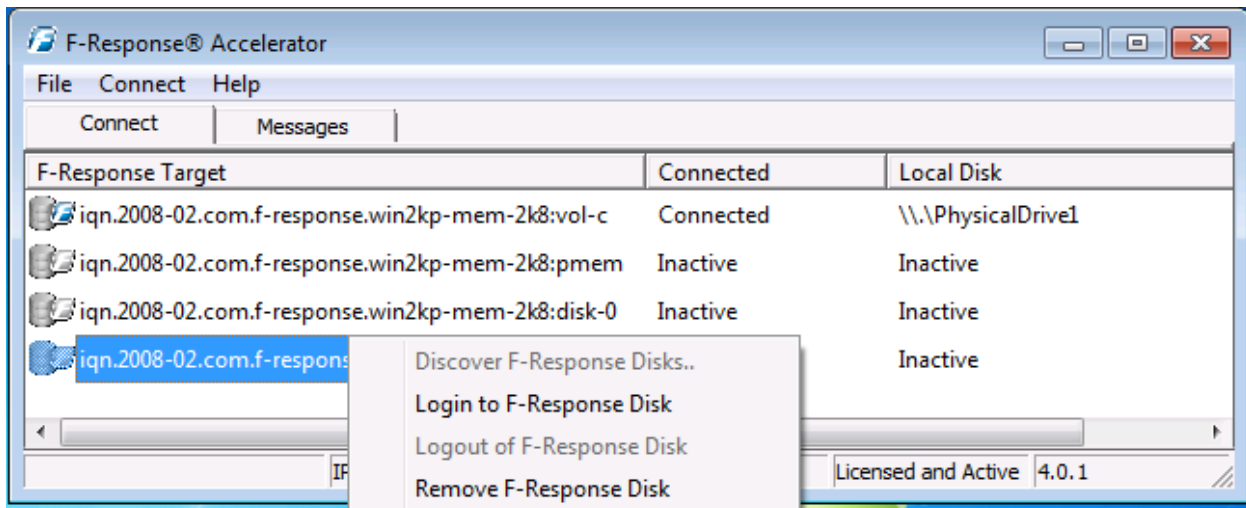
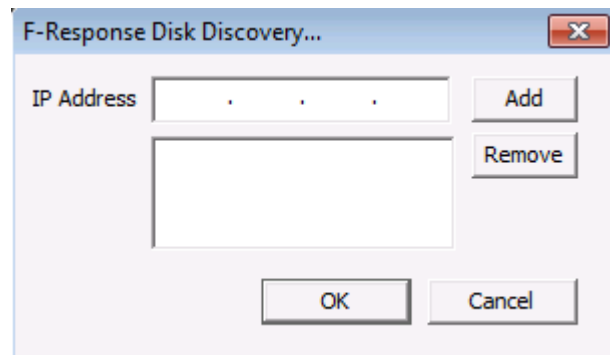
Click the connect menu option and select Discover F-Response Disks..



F-Response Accelerator, Connect->Discover F-Response Disks..

This menu option will open the Disk Discovery window. Here you can enter the IP address(es) of the target machine(s) you deployed to.

Once you have added the IP address(es) of your targets running F-Response, click OK and you will be presented with a list of physical disks and logical volumes (and physical memory for windows systems if it was selected) available to you on each target machine. 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.



F-Response Accelerator showing available target disks

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.

Repeat these steps for each Accelerator machine you wish to use in your collection or analysis.

Step Five: 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) for forensically sound imaging, examination, eDiscovery, data recovery, incident response, triage, or whatever the mission call for.