F-Response Mission Guide
Using F-Response Consultant and the F-Response CD-ROM to connect to a target machine
Rev 3.0
March 24, 2010

Email:support@f-response.com

Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497

Your Mission: Connect to a target machine using F-Response Consultant Edition and the F-Response CD-ROM.

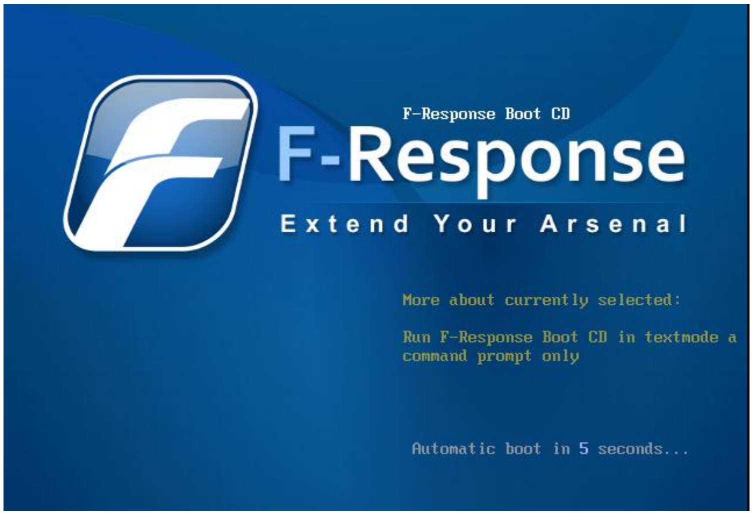
Note: This guide assumes you have downloaded and burned a copy of the F-Response CD-ROM iso image from the F-Response website. The F-Response licensing dongle is plugged into your analyst machine, the F-Response License Manager Monitor is installed and running, and the F-Response Consultant Connector (FCC) has been started. For more information on using Consultant Edition, please reference the F-Response User Manual, or the F-Response Consultant Edition Training Video on the F-Response Website.

The F-Response CD-ROM used in conjunction with F-Response Consultant Edition, is a great tool for analysis or acquisition of a target machine that should not be booted into the OS for possible altering of data on the target disk.

Step 1: Configure the Target Machine

To use the F-Response CD-ROM on your target machine, make sure it is configured to boot from CD-ROM. Check this by pressing F2 on most machines during the initial stage of the boot process and verify the boot order in the BIOS. If altering of data during boot is a concern, you may want to ensure it does not boot into the OS by temporarily physically disconnecting the hard drive cable while configuring the BIOS.

Once you are sure the target machine is configured to boot from CD, insert the F-Response CD-ROM and power on. During the CD-ROM boot process, you will be greeted with the F-Response screen:



More about currently selected:

Run F-Response Boot CD in textmode a command prompt only

Automatic boot in 5 seconds...

This tells us the target machine is successfully booting from the F-Response CD. Nothing will be changed or altered on this machine's hard drive(s). The screen will change to text and you will be presented with a login prompt once the boot process is complete.

```
The system is up and running now.
Login as “root” with password “toor”, both without quotes, lowercase.

If you have never used F-Response before, visit http://www.f-response.com and select Mission
Guides where you will find a mission guide for using this CDROM.

After you login you will use one of the following F-Response Applications:
f-response-ce-e-lin -> F-Response Consultant/Enterprise Edition
f-response-fk-lin -> F-Response Field Kit Edition (Requires locally attached dongle)
f-response-tacsub-lin -> F-Response TACTICAL (Requires locally attached TACTICAL Subject device)

When you are finished, use the “shutdown” or “reboot” command and wait for the computer to
reboot.
Be sure to remote the CDROM disc when complete.

Thanks and enjoy!      F-Response Management                                    March 2010
Frescd login: root
Password: ****

root@frescd23965:~# _
```

Here at the login prompt you will type “root” for the login then enter “toor” for the password (minus the “quotes”). Upon successful login, the end of the prompt will change to a pound sign (#).

Step 2: Start F-Response on the Target Machine

Now that the target machine is booted from the CD and you have successfully logged in, you can start the F-Response Target code. You may notice there are a few options for executing F-Response on this machine but this guide assumes you are running a licensed copy of F-Response Consultant Edition on your analyst machine.

To start F-Response on this machine we are going to use the f-response-ce-e-lin executable. You will need to create a username and password for F-Response to use, you can make it anything you like but make note of it because you will need it later when you configure your analyst machine. You will also need the IP address of the F-Response License Manager monitor (your analyst machine).

The syntax of the command to start F-Response on the target machine is:

./f-response-ce-e-lin –u username –p password –S IPoflicensingserver

For example, if we wanted to use a username of “joeuser” with a password of “remember1234” for F-Response and the IP of our license manager (analyst machine) is 192.168.15.111, we would type:

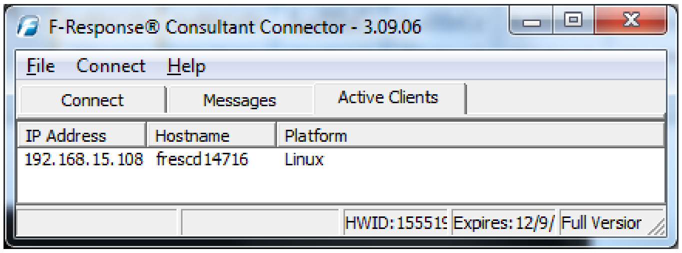
./f-response-ce-e-lin –u joeuser –p remember1234 –S 192.168.15.111 [ENTER]

```
root@frescd23965:~# ./f-response-ce-e-lin –u joeuser –p remember1234 –S 192.168.15.111
F-Response Consultant/Enterprise (Linux Edition) Version 3.09.06
F-Response Disk: /dev/hdc (29225 sectors, 2048 sector size)
57 MB write blocked storage on F-Response Disk:hdc
F-Response Disk: /dev/sda (16777216 sectors, 512 sector size)
8192 MB write blocked storage on F-Response Disk:sda
```

F-Response will start up and list available write-blocked disks on the target machine. We'll leave F-Response running here and return to the analyst machine.

Step 3: Configure and Connect to Target Disks

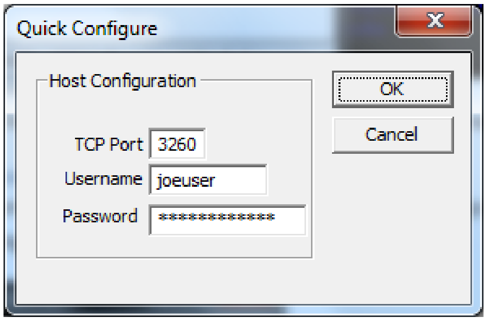
Once F-Response is started on our target machine, we can return to our analyst machine to configure and view the target disks using the F-Response Consultant Connector (FCC).



IP Address	Hostname	Platform
192.168.15.108	frescd14716	Linux

HWID:15551§ Expires:12/9/ Full Versior

First, we'll enter the username and password we created for F-Response in Step 2. Go to File – Quick Configure and the Quick Configure window will open:

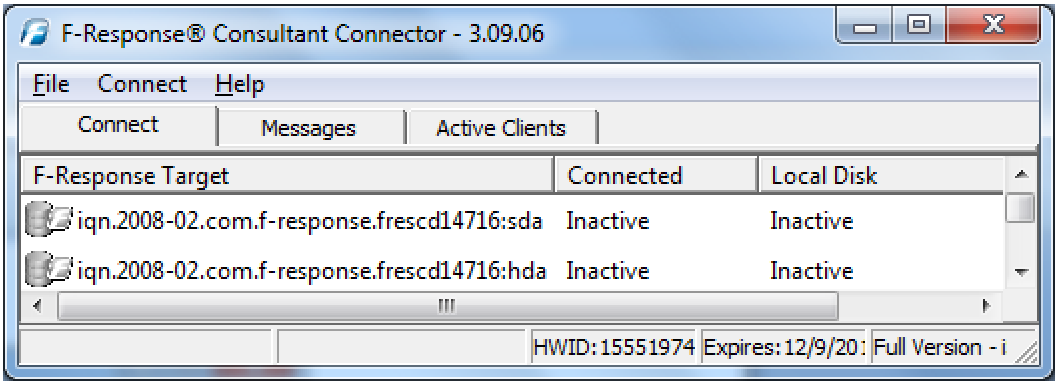


Host Configuration
TCP Port 3260
Username joeuser
Password *************

Leave the TCP Port at the default 3260 and enter the username and password you created. Click OK to return to the FCC.

If you look at the Active Clients tab in the FCC you will see your target machine listed. Here we can find potential target disks on the target machine by highlighting the machine and selecting Issue Discovery Request from the Connect drop down or right click menus.

Once you've issued a discovery request, move on over to the Connect tab to see the results.

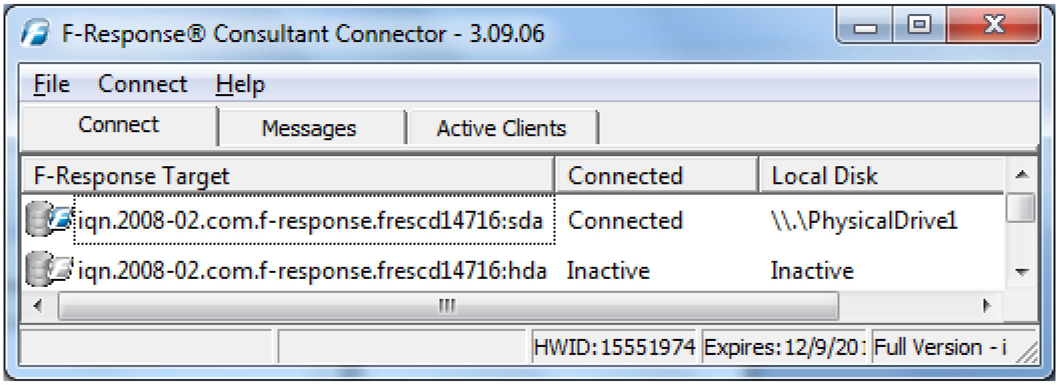


F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.frescd14716:sda	Inactive	Inactive
iqn.2008-02.com.f-response.frescd14716:hda	Inactive	Inactive

HWID:15551974 Expires:12/9/20: Full Version - i

Under the Connect tab 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. See "Understanding F-Response Disk Naming" below for more information on the disk naming convention.

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.



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.frescd14716:sda	Connected	\\.\PhysicalDrive1
iqn.2008-02.com.f-response.frescd14716:hda	Inactive	Inactive

HWID:15551974 Expires:12/9/20: Full Version - i

Step 4: 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).

Step 5: Clean up time.

Once you have completed using F-Response on the target machine, hold down the Ctrl key and press 'c' to stop f-response from running. Don't forget to remove the F-Response CD from the machine, then type 'shutdown' at the command prompt and press enter to power the machine back down.

Understanding F-Response Disk Naming

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

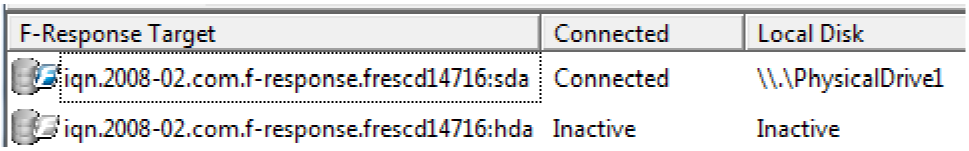
iqn.2008-02.com.f-response.frescdxxxx:disk name

"frescdxxxx" is the hostname of your target machine. The F-Response CD-ROM will identify the target machine as "frescdxxxxx" where xxxxx is a randomly generated number. If you have multiple targets running the F-Response CD and you know the IP addresses, a quick glance back at the Active Clients tab will help you tie the hostname to the address.

We are mainly concerned with the "disk name" portion of the name.

F-Response CD-ROM uses Linux to access the hard drive(s) of your target machine and will present the disk to you in a Linux naming format.

For the "disk name," Linux identifies hard disks using the format hdx or sdx. An "hd" prefix tells us this is a IDE or PATA disk and an "sd"prefix is used for SCSI, SATA, or USB drives. The 'x' portion is a letter, starting with 'a', representing the order the Linux O/S added the drive. For example:



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.frescd14716:sda	Connected	\\.\PhysicalDrive1
iqn.2008-02.com.f-response.frescd14716:hda	Inactive	Inactive

This first item in the list of target disks is the first SCSI,SATA,or USB drive on the target machine named "frescd14716" as seen by the F-Response CD-ROM. If the last part of the name said "sdb" or "sdc" it would be the second or third physical disk on the machine.

The second item in this list of target disks is the first IDE drive as we can see from the "hda" at the end of the name. Again, if the last part of the name read "hdb" or "hdc" this would indicate the second or third IDE drive as seen by F-Response CD-ROM. If you recall from Step 2, this drive was listed on the target machine as 57 MB in size, this helps us in identifying it as the CD-ROM drive containing the F-Response boot CD so it can be safely ignored.

Troubleshooting

The F-Response Boot CD does not appear to boot when I start my machine, why? *You most likely need to modify the BIOS of your machine to properly boot from CDROM first. The specific steps needed to do this vary by hardware provider, please contact your target machine's hardware provider for more details.*

Trying to start F-Response Consultant from the command line presents and error, why? *The most likely reason is incorrect command line flags and options. Be sure to read the command line flags carefully and try again, if you continue to have issues please contact support.*

The F-Response Boot CD does not appear to recognize my target machine's disk devices, any suggestions? *We have made every attempt to collect a large number of Linux kernel modules for different disk devices, however it's impossible to include every potential configuration. In this instance please contact support and provide them with additional information about the hardware present in your configuration and we'll do our best to find a way to help you get it recognized.*