Your Mission: Connect to a remote Apple target(s) disk using F-Response Consultant Edition.

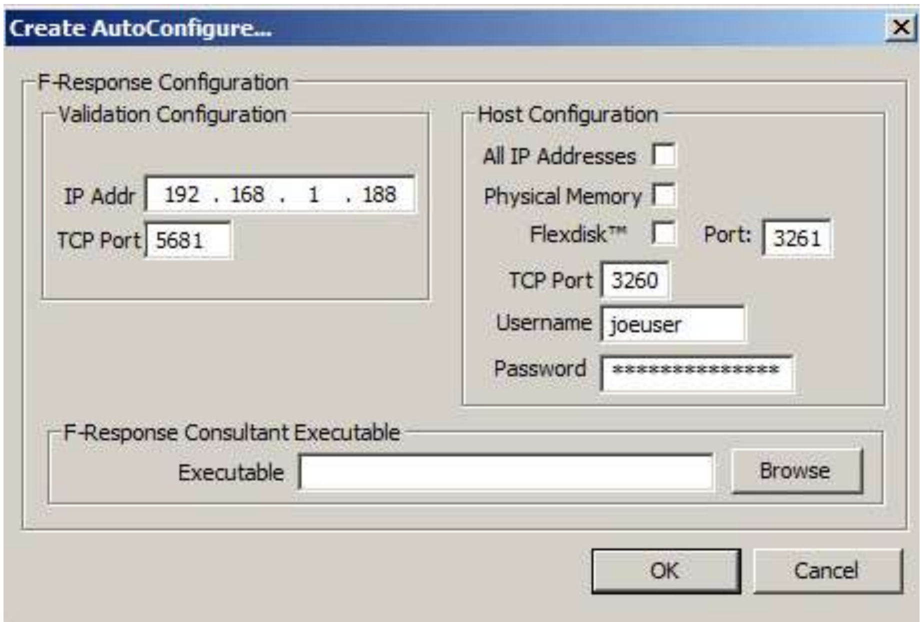
Note: This guide assumes you have installed F-Response Consultant Edition, your F-Response licensing dongle is plugged into your analyst machine, the F-Response License Manager Monitor is installed and running, and the F-Response Consultant Connector (FCC) has been started. Remote Login (SSH) should be enabled on the Apple target(s). For more information, please reference the F-Response User Manual, or the F-Response Consultant Edition Training Video on the F-Response Website.

F-response 3.09.06 supports the following Apple OSX Platforms: 10.3, 10.4, 10.5, 10.6, 10.7 Universal Binary.

Step 1: Create a Bundle

First we'll need to create an auto-config bundle to deploy to the Apple target machine using the F-Response Consultant Connector.

Choose File – Create Autoconfigure and the Automatic Configuration window will appear:



IP Addr 192 . 168 . 1 . 188
TCP Port 5681

All IP Addresses ☐
Physical Memory ☐
Flexdisk™ ☐ Port: 3261
TCP Port 3260
Username joeuser
Password ***************

Executable

Under Validation Configuration, verify the IP address of your analyst machine (where the F-Response license dongle is plugged in and the Licensing Manager is running) and leave the default port at 5681.

Next, under Host Configuration, Create an F-Response username and password. You can make it anything you would like. Again, leave the default port at 3260.

There are three check box options here as well. None of them are really applicable to what we are looking to accomplish here, so they can be ignored. Click OK to save the resulting autoconfiguration file (fresponse.ini).

Lastly, we'll need to choose the F-Response Consultant executable "f-response-ce". If you installed F-Response with the default settings this file can be found in the Program Files\F-Response\F-Response Consultant Edition directory.

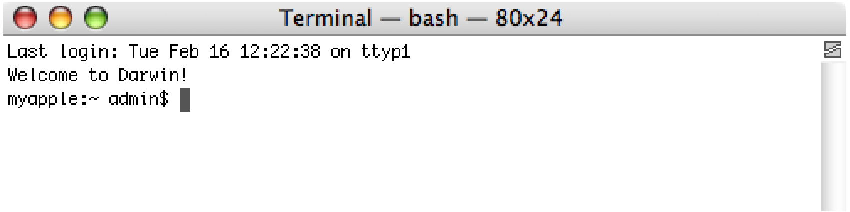
Step 2: Distribute the bundle

Once you have finished creating the fresponse.ini file, you'll want to couple it with the Apple' f-response-ce-e-osx' executable (also located in the default directory for F-Response Consultant Edition, see above) and make it available to your Apple target machine(s). You can do this however you would like by copying both files to a CD, USB thumb drive or network share as an example of some the most common options.

Step 3: Fire it up!

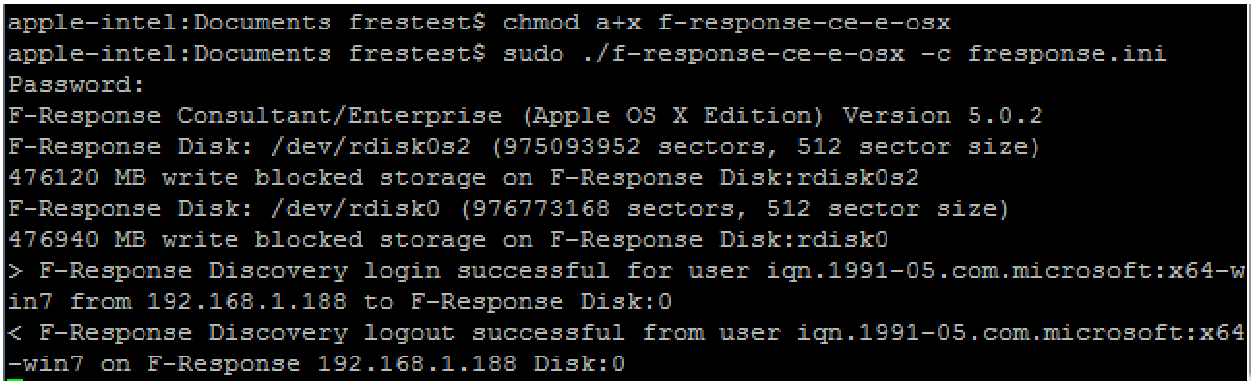
Once the files are available to the target Apple machine(s), open the terminal application. If you are unfamiliar with OSX, you can find the terminal application in the utilities folder or by typing 'terminal' into the Finder.

The terminal application will look similar to the following:



```
Last login: Tue Feb 16 12:22:38 on ttyp1
Welcome to Darwin!
myapple:~ admin$
```

Next, we'll need to locate our F-Response files from step 2 and start the f-response target code.



```
apple-intel:Documents frestest$ chmod a+x f-response-ce-e-osx
apple-intel:Documents frestest$ sudo ./f-response-ce-e-osx -c fresponse.ini
Password:
F-Response Consultant/Enterprise (Apple OS X Edition) Version 5.0.2
F-Response Disk: /dev/rdisk0s2 (975093952 sectors, 512 sector size)
476120 MB write blocked storage on F-Response Disk:rdisk0s2
F-Response Disk: /dev/rdisk0 (976773168 sectors, 512 sector size)
476940 MB write blocked storage on F-Response Disk:rdisk0
> F-Response Discovery login successful for user iqn.1991-05.com.microsoft:x64-w
in7 from 192.168.1.188 to F-Response Disk:0
< F-Response Discovery logout successful from user iqn.1991-05.com.microsoft:x64
-win7 on F-Response 192.168.1.188 Disk:0
```

The exact structure of this command may vary depending on where the files are located. In this example they were copied to the Documents directory and executed from there. Because they were copied locally, the file needs to be defined as an executable, which is done by the command:

chmod a+x f-response-ce-e-osx

followed by the command:

sudo ./f-response-ce-e-osx –c ./fresponse.ini

To start the F-Response target code.

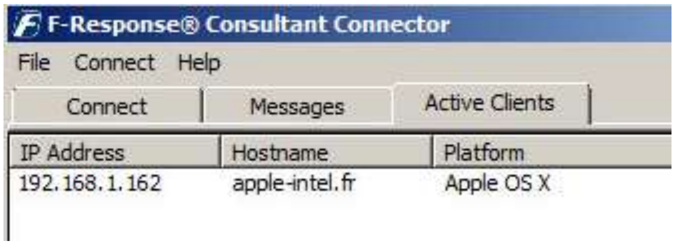
The "sudo" or "SuperUser Do" command gives us the temporary administrator privileges we need to run the F-Response target code. You will be prompted to enter the password for your user account (the same account you used to log into your Apple machine) to complete the command. F-Response will then run and use the bundled information contained in the fresponse.ini file to locate the licensing server (your analyst machine).

Once your analyst machine has been successfully located, F-Response will list each available write-blocked target on the machine. These targets can then be seen on your analyst machine in the F-Response Consultant Connector.

Repeat Steps 2 and 3 for each Apple target machine you would like to view in the FCC on your analyst machine.

Step 4: Viewing your Target Disk(s)

In the FCC on your analyst machine, look at the active clients tab for a list of Apple target machines.

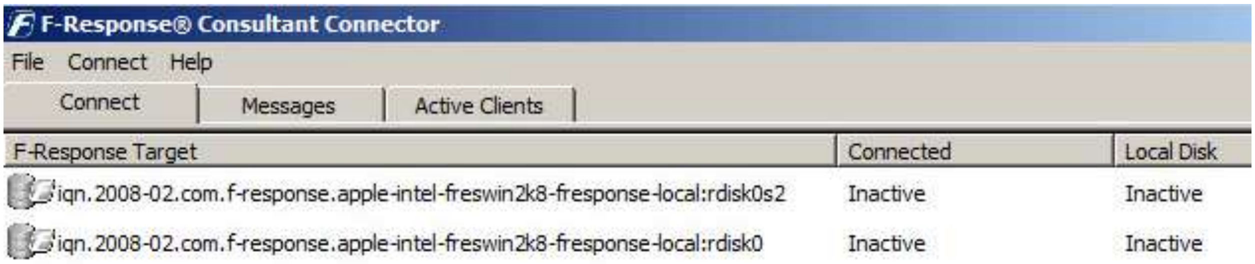


IP Address	Hostname	Platform
192.168.1.162	apple-intel.fr	Apple OS X

Here we can find potential target disks on the Apple targets by highlighting the machine(s) 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.

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.



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.apple-intel-freswin2k8-fresponse-local:rdisk0s2	Inactive	Inactive
iqn.2008-02.com.f-response.apple-intel-freswin2k8-fresponse-local:rdisk0	Inactive	Inactive

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).

<u>Understanding F-Response Disk Naming</u>

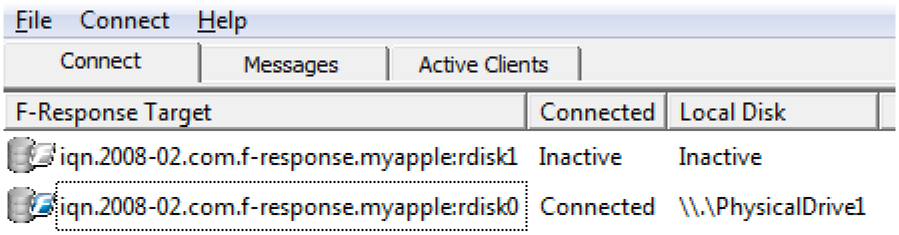
F-Response uses the following naming convention for target disks:

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 Apple 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", Apple identifies hard disks using the format "rdisk#". The 'x' portion is a number, starting with zero, representing the physical drive. For example:



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.myapple:rdisk1	Inactive	Inactive
iqn.2008-02.com.f-response.myapple:rdisk0	Connected	\\.\PhysicalDrive1

The first target in this list is on the target machine named 'myapple', and we can tell by the last piece of the name, "rdisk1", this is the second physical disk as seen by the O/S, in this case it is the USB drive we used for the F-Response target code so we are not interested in analyzing this drive. The second target in this list is on the same machine, but represents the first physical disk as shown by the last portion of the naming convention, "rdisk0".

Troubleshooting

F-Response says I'm connected to the remote disk, yet I cannot see it in Explorer? *Correct, while your Windows analysis machine can only read FAT and NTFS, Apple most likely is using the one of the Apple standard HFS+ file system formats. To view the disk you will need use one of your third party tools.*

When I try to start F-Response on the target I get an error telling me it could not connect to Validation server? *Check your license manager is bound to the correct local IP address on your analyst machine. You may also check inside the fresponse.ini file to see the IP address matches your F-Response license manager.*

When I try to execute the "sudo" command and enter my password I get "Access Denied", why? *In the Apple OS environment your account can be either a user account or an admin account. Make sure your user account is set as an admin account and try executing sudo again.*

I have no password assigned for my user account, so what do I type when sudo asks for a password? You *will need to define a password for your user account before sudo will be able to function correctly. You may also need to confirm your user account is an admin account.*

F-Response Consultant Edition works well, but I'd like to know if there's a way to hide the deployment or perhaps access it in a more covert manner. Does such an option exist? *F-Response Consultant Edition was not designed with covert deployment in mind. For more covert deployment and access options see F-Response Enterprise Edition.*