F-Response Mission Guide
Connecting to Apple target(s) using F-Response Enterprise
Rev 3.0
January 8, 2014

Email:support@f-response.com
Website:www.f-response.com

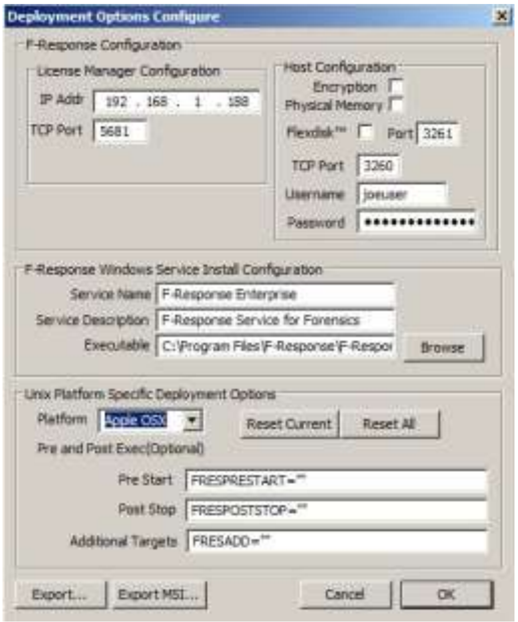
Phone: 1-800-317-5497

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

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. 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 Enterprise Edition Training Video on the F-Response Website.

F-Response supports deployment to Apple platforms via the F-Response Enterprise Management Console (FEMC). The easiest way to deploy the F-Response target code is by using the FEMC as demonstrated below.

Step 1: Ready the Console!


Deployment Options Configure

F-Response Configuration
License Manager Configuration
IP Addr 192 . 168 . 1 . 198
TCP Port 5681
Host Configuration
Encryption □
Physical Memory □
Flexdisk™ □ Port 3261
TCP Port 3260
Username joeuser
Password ••••••••••••••

F-Response Windows Service Install Configuration
Service Name F-Response Enterprise
Service Description F-Response Service for Forensics
Executable C:\Program Files\F-Response\F-Respo

Unix Platform Specific Deployment Options
Platform Apple OSX
Pre and Post Exec(Optional)
Pre Start FRESPRESTART=""
Post Stop FRESPOSTSTOP=""
Additional Targets FRESADD=""

Before using the FEMC some configuration is required. You will need to configure the Deployment Options Configure, and Credentials Configure windows. The details can be found in the F-Response Manual, but to accomplish our mission as quickly as possible here are some quick configuration suggestions:

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

Good news, some of the work here has already been done for you, and typically once you input this information you won't need to change it again. You'll only need to fill in the Host Configuration and Windows Service Install Configuration sections.

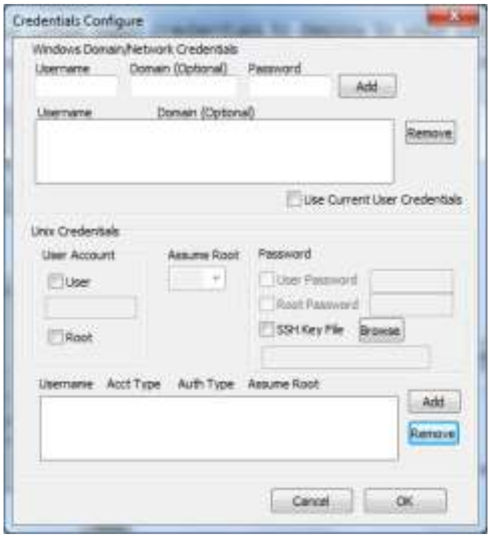
Under Host Configuration, enter a username and password for F-Response to use while communicating with your Apple target machine(s). You can make it anything you would like. Leave the TCP port default at 3260 and ignore the box for Physical Memory as this is not an option for Apple targets.

Under F-Response Windows Service Install Configuration you will need to enter in a Service Name and Description (your choice entirely) and select the Windows version of F-Response as the Executable. If you installed F-Response with the standard defaults you can browse to the C:\Program Files\F-Response\F-Response Enterprise Edition directory and choose the f-response-ent.exe file. This will unlock access to the scanning options in later steps.

The IP Address of your License Manager (your analyst machine's IP) and default port of 5681 will automatically populate under the Validation Configuration section.

The "Unix Platform Specific Deployment Options" portion of the window (the lower half) allows you to make temporary exceptions to the Apple firewall for your environment, run scripts, and set additional targets. The defaults provided here should be sufficient such that no action is needed unless you suspect the need to reset to the factory defaults. You can do this by selecting Apple OSX from the platform list and clicking the Reset Current button. Configuration of the firewall, scripts, and additional targets are beyond the scope of this mission guide.

Next you need to configure your Apple login credentials to deploy to your Apple target machine(s). In the FEMC go to File – Configure Credentials… and the Credentials Configure window will open:



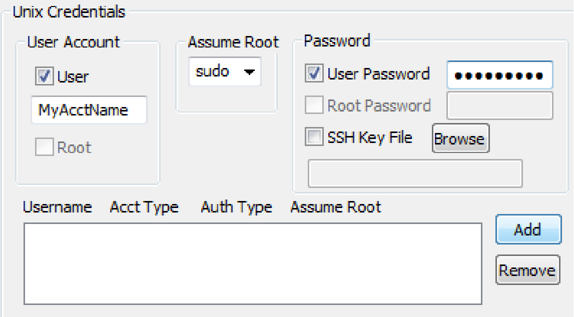
Here we are only concerned with the Unix Credentials, the lower half of the window.

F-Response uses SSH/SFTP to access Apple targets. Unix Credentials are covered in detail in Appendix E of the F-Response Manual, but here is a quick overview to accomplish your mission.

Generally there are two types of Apple accounts for our purposes: the all powerful administrator "root" account, and a general user account that can assume root privileges for a time.

The Root account on Apple machines is disabled by default so most likely this is not an option. Given the power of the Root account, it is more likely you will be using a general user account that will assume root privileges.

For Apple machines, we can accomplish this using Sudo. Sudo, or "SuperUser Do", is used to execute a command as the Root administrator.



☑ User
MyAcctName
□ Root
Assume Root: sudo
☑ User Password ●●●●●●●●●

To configure F-Response to deploy to your Apple target using sudo:

Check the box for User in the User Account section and enter your account name.

Choose sudo from the Assume Root drop down box.

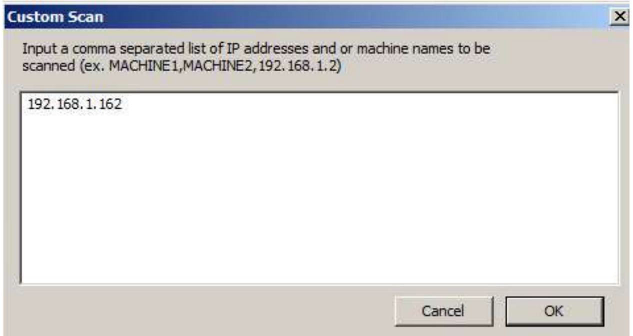
Check the box for both User Password and enter the password.

Click the Add button to add the account to the list of credentials for F-Response.

Once you have configured your deployment settings and login credentials you are ready to use F-Response to connect to your Apple target(s).

Step 2: Scan for target Apple machines

In the FEMC there are several ways to scan for your Apple target machine(s). For our purposes, we assume you already have a list of machines you would like to connect to so we are going to use the custom scan option.

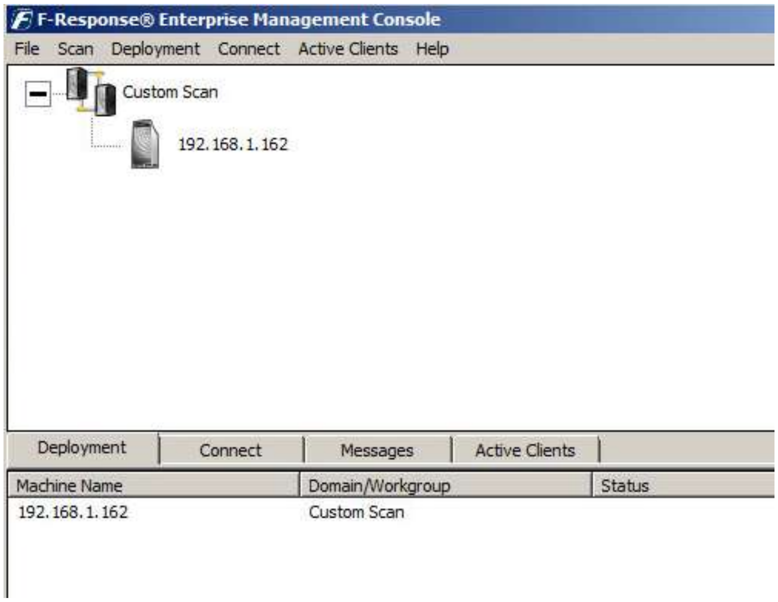


Input a comma separated list of IP addresses and or machine names to be scanned (ex. MACHINE1,MACHINE2,192.168.1.2)

192.168.1.162

In the FEMC choose Custom Scan from the Scan menu, enter your Apple machine name(s) or IP address each separated by a comma. This data is retained so you may need to clear out any old information first. Click OK to have F-Response start scanning.

Step 3: Deploy and start F-Response on your target



Machine Name	Domain/Workgroup	Status
192.168.1.162	Custom Scan	

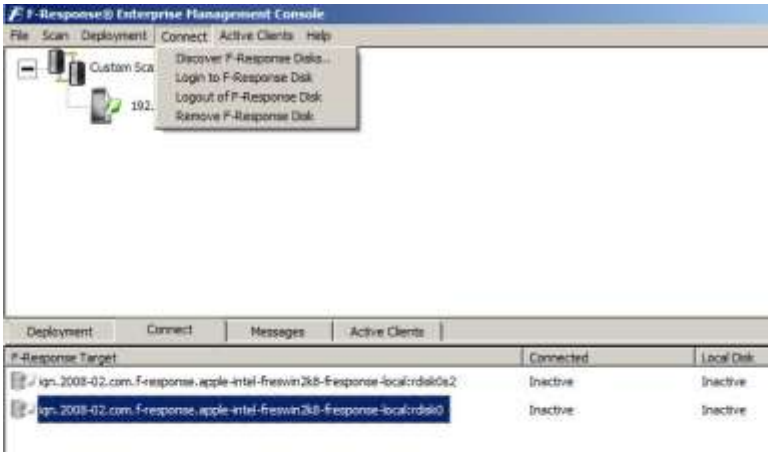
When the scan completes, Apple machines can be identified in the list by the F-Response Apple icon:

To deploy the F-Response target code to a Apple machine, highlight and right click on it then select Install/Start F-Response. The Install/Start option will Deploy, Start, and Discover target disks on the remote Apple machine in a single step.

The F-Response badge will appear in green indicating F-Response is now running on your target. If you have several Apple targets you need to install F-Response on, you can highlight them all under the deployment tab and choose Install/Start F-Response from the deployment drop down menu.

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

Once F-Response is installed and running on your target machines, as seen by the icons with green badges, you can find, connect, and open a write-blocked connection to the disk(s).



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

The list of potential targets 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). Good luck in your future mission.

Understanding F-Response Naming

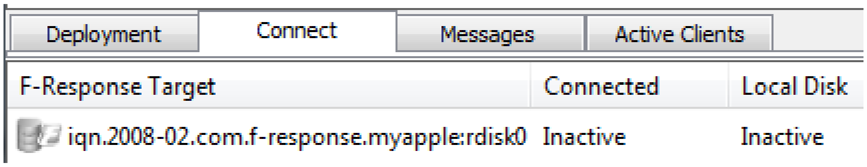
F-Response uses the following naming convention for target disks:

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 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 order the Apple O/S added the drive. For example:



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

This target is the first physical drive on the Apple machine named 'myapple'.

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.*

My Apple target shows in the scan list, yet it does not appear under the deployment tab? *You just need to refresh the full view by double-clicking the root of the scan tree.*

I can deploy F-Response to my target machines, but when I try to start it 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.*

I am unable to connect to the remote F-Response Apple target, it just shows up with a question mark. *Check the Messages tab. It's possible the credentials are configured incorrectly. Note that your Apple user account must have a password to use sudo and cannot be blank.*

F-Response is still telling me it is unable to connect to the remote target? *You may want to test your credentials without F-Response. Trying using a tool like PuTTy to connect to your target machine using SSH (remember SSH and SFTP must be enabled on the target machine).*