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

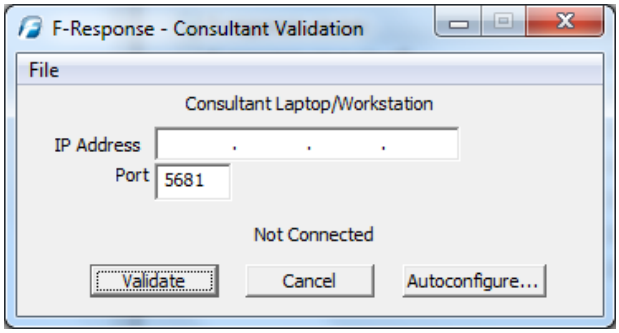
Your Mission: Connect to a remote Windows target(s) disk using F-Response Consultant Edition.

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. For more information, please reference the F-Response User Manual, or the F-Response Consultant Edition Training Video on the F-Response Website.

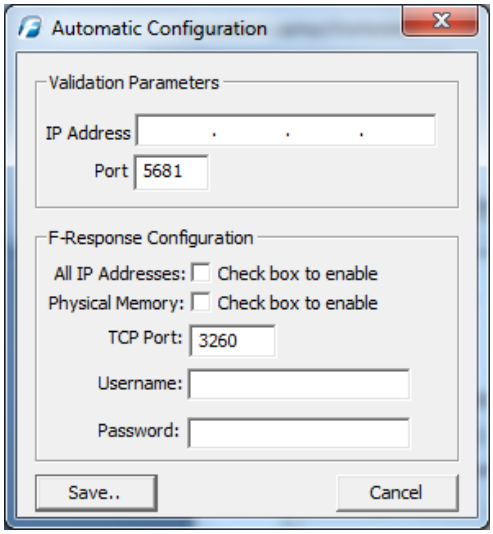
F-Response CE 3.09.08 supports Windows 2000, 2003, XP, Vista, 2008, 7 (32 & 64 Bit).

Step 1: Create a Bundle

There are a few ways to deploy F-Response to a Windows target machine(s), but for our mission we'll use the option to create an autoconfiguration bundle. If you've installed F-Response on your analyst machine using the standard default, the F-Response Windows target code is located in the C:\Program Files\F-Response\F-Response Consultant Edition directory. Start the f-response-ce.exe executable and the following window will appear:



Click the Autoconfigure… button and the Automatic Configuration window will appear:



Under Validation Parameters, enter 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 F-Response 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 two check box options here as well. You can check the All IP Addresses box if you wish to bind to all the IP addresses on the target machine (provided more than one exists). Also, although this is not our objective here, it's worth noting there is also an option to capture physical memory on Windows targets and have F-Response present it to you as a local hard disk by selecting the Physical Memory check box.

Click Save.. to save the resulting autoconfiguration file (fresponse.ini).

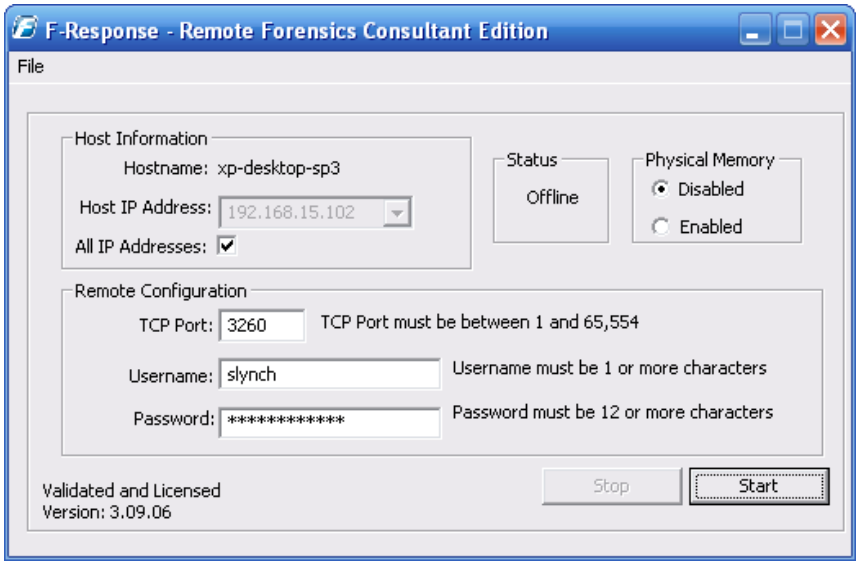
Email:support@f-response.com
Website:www.f-response.com
YahooIM:fresponse_s
Phone: 1-800-317-5497

Step 2: Distribute the bundle

Once you have finished creating the fresponse.ini file, you'll want to couple it with the f-response-ce.exe executable and make it available to your Windows 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 Windows machine start the f-response-ce executable. The executable will look for the licensing server (your analyst machine) and the following window will appear already populated with all the necessary details thanks to the bundle you already created.

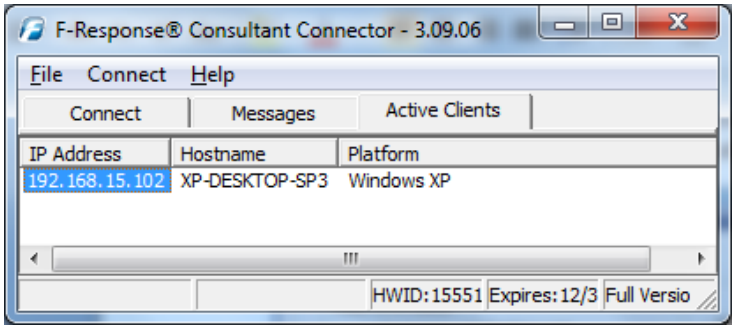


Click the start button and F-Response is good to go on your Windows Target. You have the option of hiding and un-hiding this window by using the Ctrl-Alt-F12 key combination.

Repeat Steps 2 and 3 for each Windows target machine you would like to view in the F-Response Consultant Connector on your analyst machine.

Step 4: Viewing your Target Disk(s)

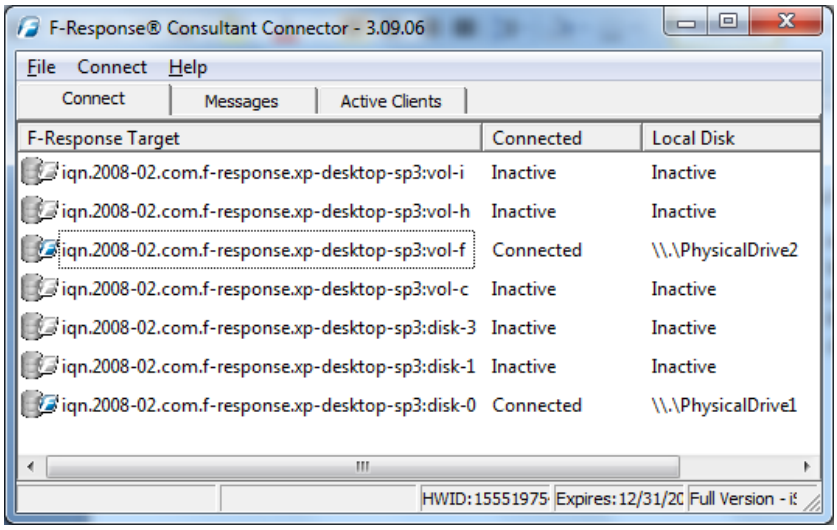
In the FCC on your analyst machine, look at the active clients tab for a list of windows target machines.



Here we can find potential target disks on the Windows 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.

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



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.

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

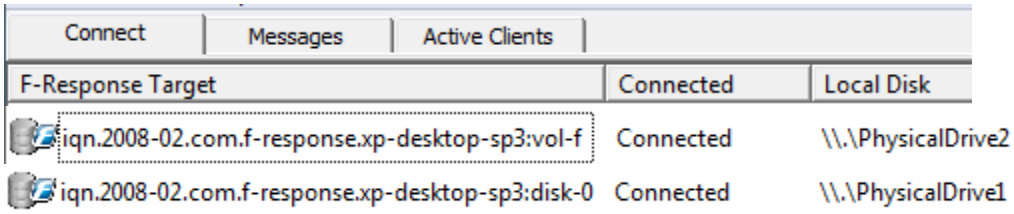
F-Response uses the following naming convention for target disks:

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:



The first target in this list is on the target machine named 'xp-desktop-sp3', and we can tell by the last piece of the name this is the logical volume 'f' 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".

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

Troubleshooting

When I "Issue Discovery Request" I don't see any Targets and in the Messages Panel it indicates Connection Error, what should I do? *F-Response Consultant Edition makes firewall exceptions for the Windows Firewall automatically, however if your target is running another firewall product you will need to make port exceptions (TCP 3260 default) or disable the firewall temporarily for the duration of the activity.*

Attempting the windows hide key sequence CTRL-ALT-F12 does not hide the window, in fact it appears to load another application's configuration panel. Is there anything I can do? *While effort was done to select a key sequence least likely to be in use on a system, it is possible that another application has already registered that key sequence. In this case you would need to stop that application and restart F-Response Consultant Edition to register the key sequence to F-Response.*

On Windows Vista I get an error message indicating "No Physical Disks Detected", what do I do? *Typically this is related to Windows Vista ,2008, and Win7 User Account Controls (UAC). The typical solution is to select the Consultant executable and right click selecting "Run as Administrator".*

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 we recommend F-Response Enterprise Edition.*

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), or via IM (YahooIM fresponse_s).*