F-Response Mission Guide
Connecting to Windows target(s) using F-Response Enterprise Edition
Rev 2.0
April 2, 2013

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 Enterprise Edition.

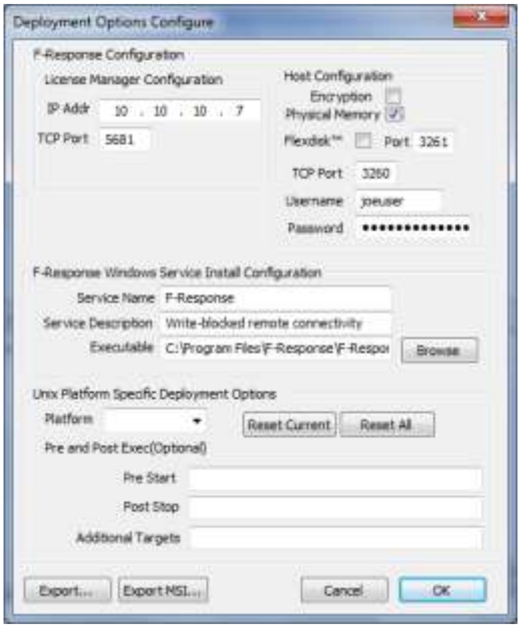
Note: This guide assumes you have installed F-Response Enterprise Edition, your F-Response licensing dongle is plugged into your analyst machine, the F-Response License Manager Monitor is installed and running, and the F-Response Enterprise Management Console (FEMC) has been started. For more information, please reference the F-Response User Manual, or the F-Response Enterprise Edition Video on the F-Response Website.

F-Response EE supports Windows 2000, 2003, XP, Vista, 2008, 7, 8 (32 & 64 Bit).

Step 1: Ready the Console!

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.


Deployment Options Configure

F-Response Configuration

License Manager Configuration
IP Addr 10 . 10 . 10 . 7
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
Service Description Write-blocked remote connectivity
Executable C:\Program Files\F-Response\F-Respor

Unix Platform Specific Deployment Options
Platform
Pre and Post Exec(Optional)
Pre Start
Post Stop
Additional Targets

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 areas.

Under Host configuration, enter a username and password for F-Response to use while communicating with your Windows target machine(s). You can make it anything you would like. Leave the TCP port default at 3260. Although not part of our objective, it's worth noting that Physical Memory can be captured and presented as a local disk for Windows machines by selecting the physical memory check box here.

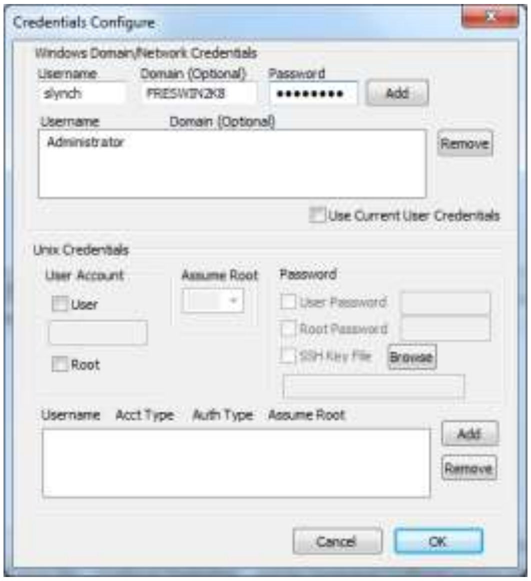
Under F-Response Windows Service Install Configuration you will need to enter in a Service Name and Description (your choice entirely) and select the Windows version of F-Response as the Executable. If you installed F-Response with the standard defaults you can browse to the C:\Program Files\F-Response\F-Response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

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, can be ignored as we are not concerned with Unix targets for our mission.

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

Under the **Windows Domain/Network Credentials** section of the window you can enter the user name and password for a local account on the target machine, or a domain account by specifying the domain along with the user name and password.



Username: slynch
Domain (Optional): FRESWIN2K8
Password: •••••••••

Username: Administrator

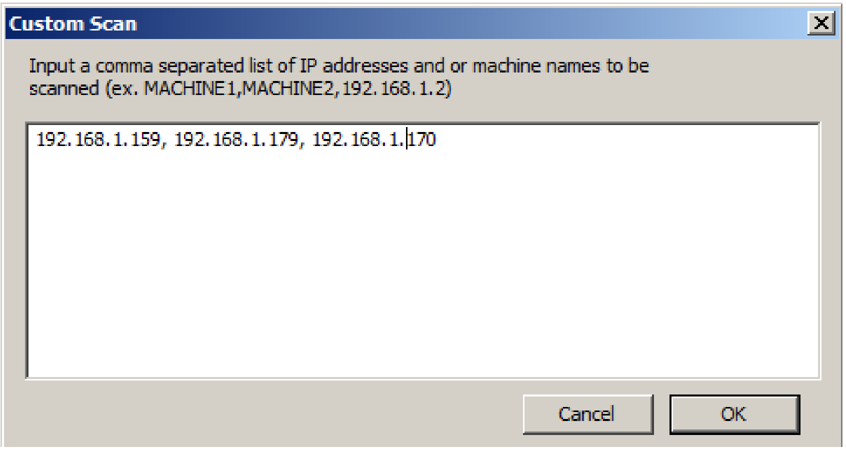
Click the **Add** button and the information is added to the list of credentials F-Response will use to access the Windows target machines (choosing targets will be explained in step 3 of this document).

Additionally, there is the option to bypass the list of credentials and use the account you are currently logged into your analyst laptop with by checking the Use Current User Credentials box.

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

Step 2: Scan for target Windows machines

In the FEMC there are several ways to scan for your Windows 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)

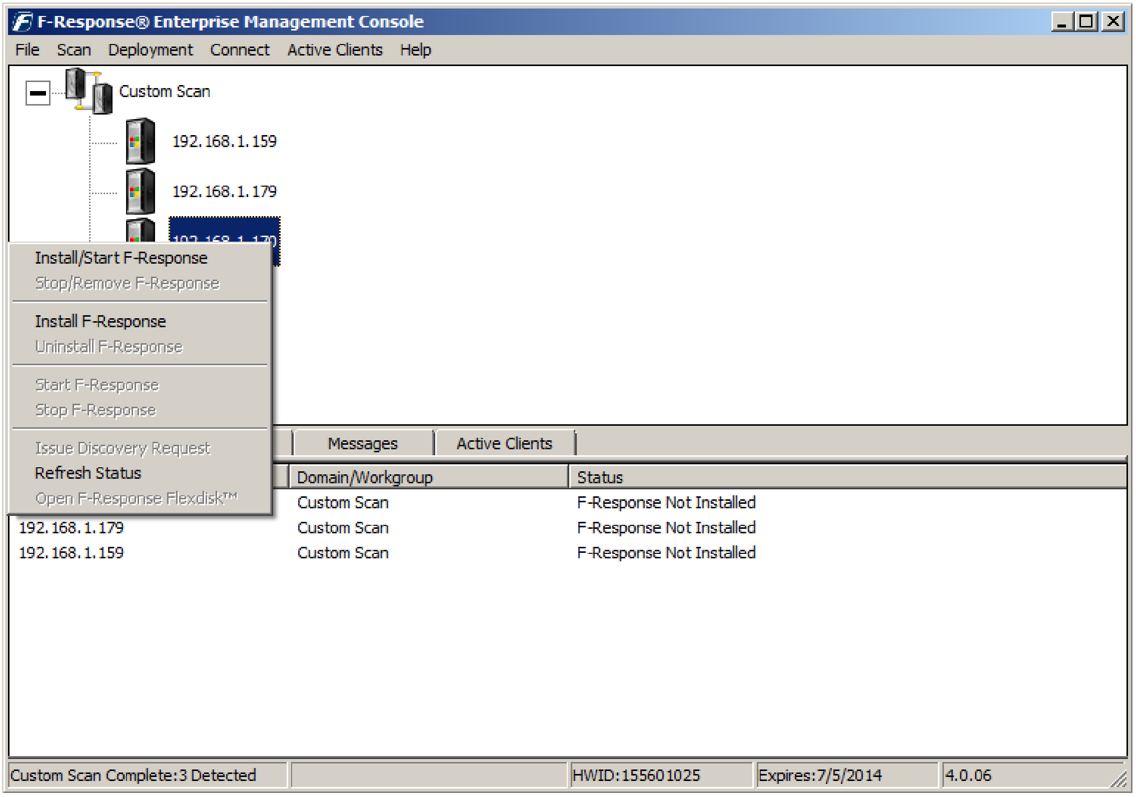
192.168.1.159, 192.168.1.179, 192.168.1.170

In the FEMC choose **Custom Scan** from the **Scan** menu, enter your Windows 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

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

F-Response can be deployed, started, and a discovery request issued in one step by using **the Install/Start F-Response** option. Choose a Windows target machine from the **Custom Scan** list, highlight and right click on it, then select **Install/Start F-Response**.



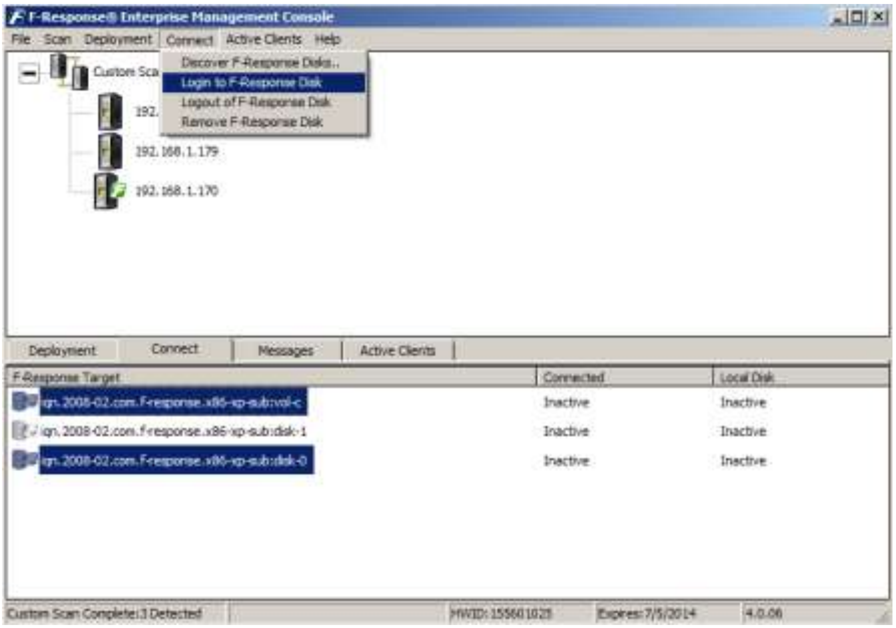
	Domain/Workgroup	Status
	Custom Scan	F-Response Not Installed
192.168.1.179	Custom Scan	F-Response Not Installed
192.168.1.159	Custom Scan	F-Response Not Installed

The F-Response Badge will turn green indicating F-Response is now running on the target machine. If you have several Windows 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 Windows 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 remote disk(s).

Click the **Connect** tab in the lower portion of the window to see the list of potential targets on the remote machines where F-Response is installed and running.



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.x86-xp-sub:vol-c	Inactive	Inactive
iqn.2008-02.com.f-response.x86-xp-sub:disk-1	Inactive	Inactive
iqn.2008-02.com.f-response.x86-xp-sub:disk-0	Inactive	Inactive

Custom Scan Complete:3 Detected HWID: 155601025 Expires:7/5/2014 4.0.06

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).

Understanding F-Response Disk Naming

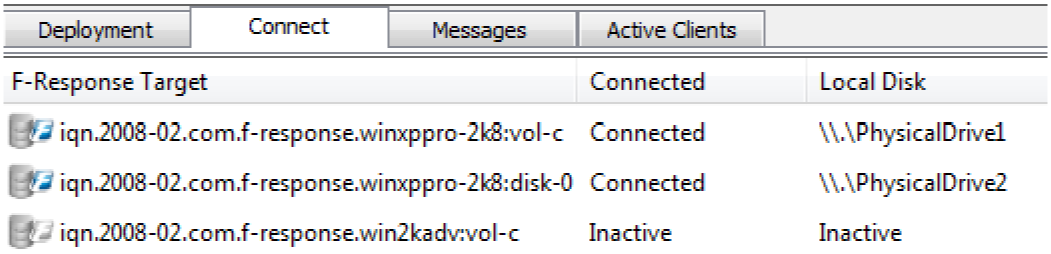
F-Response uses the following naming convention for target disks:

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:



F-Response Target	Connected	Local Disk
iqn.2008-02.com.f-response.winxppro-2k8:vol-c	Connected	\\.\PhysicalDrive1
iqn.2008-02.com.f-response.winxppro-2k8:disk-0	Connected	\\.\PhysicalDrive2
iqn.2008-02.com.f-response.win2kadv:vol-c	Inactive	Inactive

The first target in this list is on the target machine named 'winxppro-2k8', and we can tell by the last piece of the name this is the logical volume 'C' 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). The third and last target in this list we are not currently connected to, but can tell by the naming convention it is volume C on the machine named 'win2kadv'.

Troubleshooting

My Windows 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 am unable to connect to the remote F-Response Windows target, it just shows up with a question mark. *Check the Messages tab. It's possible the credentials are configured incorrectly.*

I can deploy F-Response, but when I try to start it I get an error telling me it could not connect to Validation server? *Check if your license manager is bound to the correct local IP address on your analyst machine.*

When I attempt to deploy F-Response using the FEMC I cannot, even though I have valid credentials? *This is typically the case when attempting to connect to Windows machines not part of a Domain.*

Your target machine is most likely a Windows XP machine not running in "Classic" mode for credential authentication. To switch the target machine to Classic you must open the Local Security Policy Administration Tool under Control Panel, Administrative Tools. You will then select Local Policies->Security Options and change the value of "Network Access: Sharing and Security Model for Local Accounts" to "Classic – Local Users authenticate as themselves". This is only necessary in when using the FEMC to deploy F-Response to computers not part of a Windows Domain.

If the target machine is a Windows 7, Vista, or newer Windows OS and not joined to a Domain (ie. Workgroup Member) then a key will need to be added to the registry of the target machine. You can manually create and add it the registry by following these steps:

To create your registry key, copy the following information into Notepad:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

“LocalAccountTokenFilterPolicy”=dword:00000001
```

Save this file as LocalAccountTokenFilterPolicy.reg*, and then copy it to your target machine. Double click this file on the target machine to populate the registry with this key.*

To remove follow the same steps as above this time with the following information:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

“LocalAccountTokenFilterPolicy”=dword:00000000
```

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).*