F-Response Mission Guide
Manually deploying F-Response Enterprise Edition
Rev 2.0
March 19, 2013

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

Your Mission: Deploy F-Response Target code without the use of the F-Response Enterprise Management Console.

Note: This guide assumes you have downloaded and installed F-Response Enterprise Edition on your licensing server, the F-Response dongle is plugged in and the License Manager Monitor is running. It is also assumed F-Response is running in a Windows Domain based network and firewall rules allow for remote administration from the "worker" machines.

Overview

Given a situation where it is not possible for different Analysts to deploy and start the F-Response target code using the FEMC, you can create a configuration file on the licensing server, couple it with the F-Response executable, and make the files available to the Analysts for manual deployment and execution. Alternatively, F-Response also offers the option to create a MSI to distribute to the target machines by other means.

Step 1: Use the FEMC to create a configuration (ini) file.

In the FEMC on the Licensing Server go to File – Configure Options… and the Deployment Options Configure window will open.
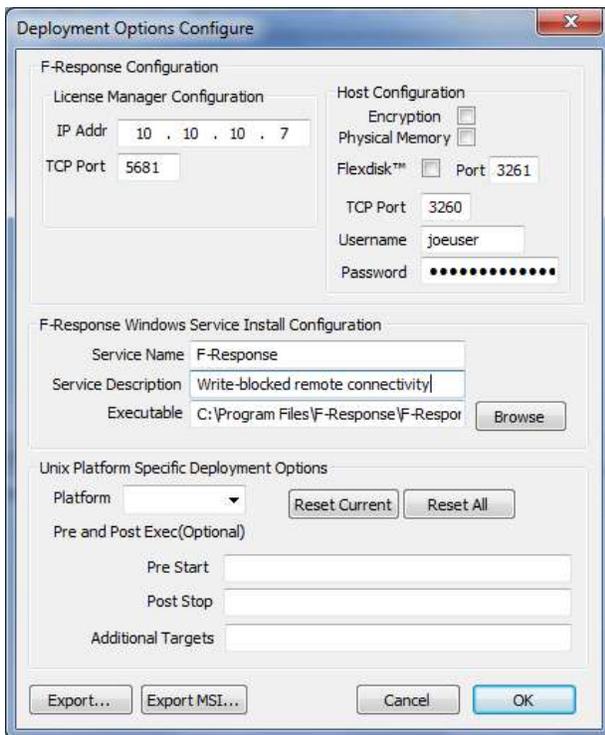
Good news, some of the work here has already been done for you, and typically once you input this information you won't need to change it again. You'll only need to fill in the Host Configuration and Windows Service Install Configuration areas.

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. It's also worth noting that Physical Memory can be captured and presented as a local disk for 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 Service 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 and the default port of 5681 will automatically populate under the Validation Configuration section.

F-Response Mission Guide   **Email**:support@f-response.com
Manually deploying F-Response Enterprise Edition   **Website**:www.f-response.com
Rev 2.0   **YahooIM**:fresponse_s
March 19, 2013   **Phone**: 1-800-317-5497

Click the Export button to create the configuration file and save the F-Response configuration file (f-response-ent.exe.ini). along with the executable to distribute to the target machine(s). In order to use the configuration file with F-Response as you've configured it you will need to make sure it has the exact same name as the executable with an additional ".ini" extension. For example:

"Ex. f-response-ent.exe would mean the ini must be f-response-ent.exe.ini"

Or

"Ex. secret-file.exe would mean the ini must be secret-file.exe.ini"

Step 2: Ready and distribute the configuration file and F-Response executable.

You can distribute the F-Response Target code and configuration file several ways (USB, CD-Rom, i.e.) but in an enterprise environment it probably easiest to use an administrative share for deployment. From the F-Response install directory, copy the **f-response-ent.exe** and the newly created **f-response.exe.ini** file to a share the Analysts have access to for distribution.

Once these files are available, the analysts can copy them to the target machines as needed. The configuration file can be used repeatedly provided the F-Response password or IP address of the licensing server does not change.

Step 3: Install PsTools on the Analyst machines and open a command line on the target.

On the Analyst machines, pstools should be installed and can be [downloaded here](#). PsExec is part of the PsTools suite and can be used to open a command line on the remote target machine. To open a shell on the target machine, on the analyst machine type:

Psexec.exe –u username \\HostnameorIP cmd

Where "username" is an account on the target machine, and "HostnameorIP" is the host name or IP address of the target machine.

Enter the password for the account with rights on the target machine when prompted.

The title bar will show you are now connected to the remote target machine and present you with a command prompt.

F-Response Mission Guide
Manually deploying F-Response Enterprise Edition
Rev 2.0
March 19, 2013

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

Step 4: Start F-Response on the Target machine(s).

Once you have a remote command prompt running, issue the following commands to start the F-Response target code.

Type **f-response-ent –a "Service Name"** where "ServiceName" is the name you want to assign to the F-Response service.

Then, start the F-response service on the target by typing **net start "Service Name"**
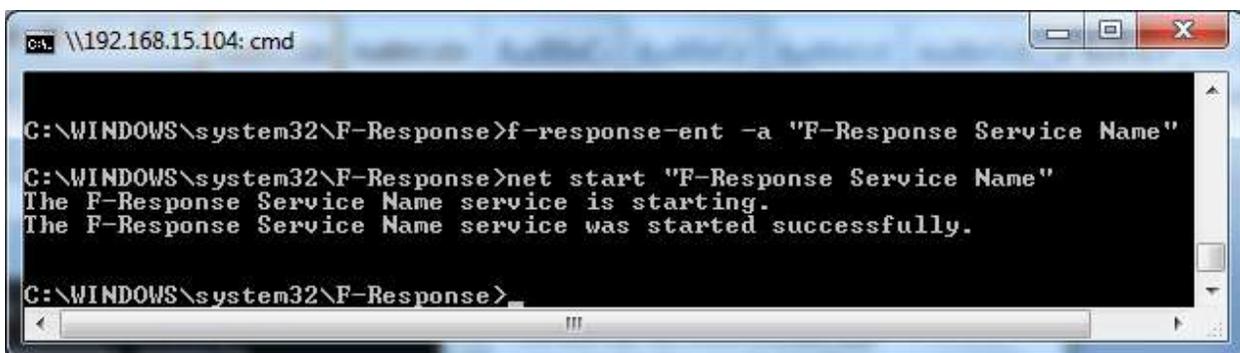
F-Response is now running on the target machine.