F-Response Manual

8.0.0.57

Provides a complete breakdown of leveraging F-Response to perform expert remote e-discovery, computer forensics, and incident response.

Contents

Terminology

The following terminology will be used throughout this manual.

EXAMINER

F-Response Examiner refers to the applications used to connect to remote Subjects and Providers to attach devices and shares.

SUBJECT

F-Response Subject refers to the applications used to present remote devices, drives, memory and shares to Examiners as defined above.

PROVIDER

Provider refers to the supported 3rd party Cloud Services providers that F-Response is able to connect to and present data from.

TARGET

Targets refer to individual devices, shares, and data sources presented by Subjects or Providers to Examiners as defined above.

PHYSICAL DEVICE

Physical Device refers to the F-Response connected subject's remote physical disks and logical volumes presented as locally attached physical disks.

PHYSICAL IMAGE

Physical Image refers to an Expert Witness (EWF) formatted full device acquisition. Physical Images will include the allocated and unallocated content of the physical device. Physical images can only be performed against Physical Devices.

LIVE FILE DEVICE

Live File Device refers to the F-Response connected subject's remote physical disks and logical volumes presented as locally attached live raw files (Linux and OSX Examiner Platforms Only).

Overview

F-Response is a software product which leverages our patented and patent pending technology to provide access to remote drives, memory, volumes, and 3rd party cloud storage.

Supported Platforms

Subject

The F-Response Subject executables are designed to provide all or a subset of the available target types on the following operating systems:

Microsoft Windows (XP, 2003, Vista, 2008, 7, 2008r2, 2012, 8, 2012r2, 10, 2016) both 32 and 64 bit
Linux (Most modern distributions)
Apple OSX (10.6+, note: SIP must be disabled in 10.13+)

Examiner

The F-Response Examiner executables and management tools provide access to F-Response Subjects and Targets on the following supported operating systems:

Microsoft Windows (8,10) both 32 and 64 bit
Linux (Most modern distributions)
Apple OSX (10.8+)

Provider

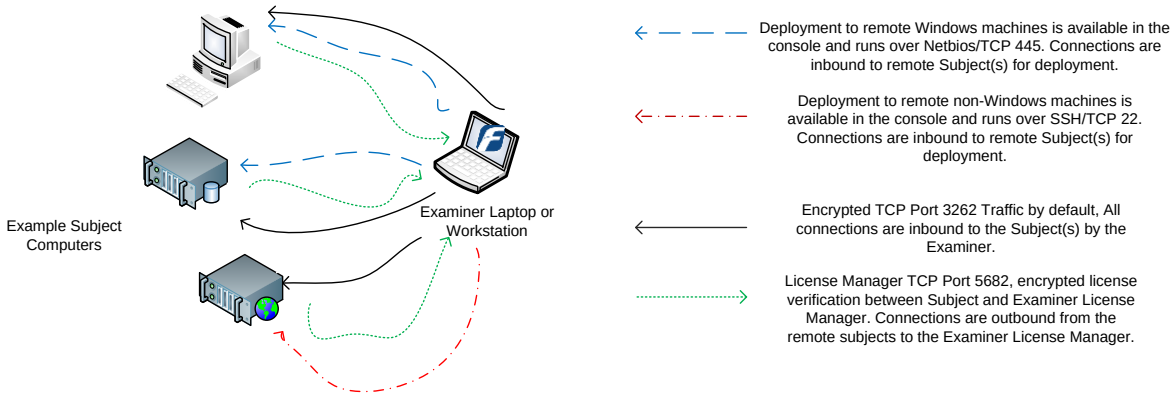
The F-Response Management Console supports the following 3rd party Cloud Storage and Local Storage Providers:

Amazon Simple Storage Service (S3)
Box.com
Box.com for Business
Dropbox
Dropbox for Business
GSuite
Google Drive for Consumers
Google Mail (OAuthv2)
Office 365 OneDrive for Business
OneDrive for Consumers

Technical Architecture

The following overview summarizes the F-Response technical architecture sufficient to implement F-Response in your environment.

Network Ports and Overview



Internal Windows Software Architecture

The Windows F-Response Examiner uses a web RPC service to provide connections to remote data sources and provide imaging services. The service is considered critical infrastructure and must be installed and running to use the F-Response Management Console or F-Response Control Panel Applet:

- F-Response Web RPC Service

Please make sure the service is started prior to contacting support.

Internal Unix Software Architecture

The Unix F-Response Examiner uses a set of command line tools and worker processes to provide connections to remove devices. The following command line tools are considered critical infrastructure and must be installed on the examiner's machine.

- fr_lm
- fr_exa
- fr_ace
- fr_ssh (Optional, necessary for deploying to Unix machines.)
- fr_win (Optional, necessary for deploying to Windows machines.)

While functional on their own, the command line tools are also used by a provided graphical interface.

Licensing

F-Response software uses one or more hardware dongles to enforce the licensing model depending on the version selected. The following list indicates the version and how licensing is managed.

Enterprise, Consultant + Covert, Consultant

These versions of F-Response use a single hardware dongle that functions as a USB human interface device (HID). This device is inserted in the examiner machine, or in another machine on the network functioning as the License Manager. This dongle must remain inserted always.

TACTICAL

This version of F-Response provides two license dongles that function as a pair. Each dongle is a USB Storage device. The dongle marked “TACTICAL Subject” is to be inserted in the Subject computer, the dongle marked “TACTICAL Examiner” is to be inserted in the Examiner computer. These dongles must remain inserted in both computers throughout the operation to maintain a consistent connection. For Cloud Service access, only the “TACTICAL Examiner” dongle is required and must be in the Examiner machine throughout the connection.

Field Kit

This version of F-Response uses a single hardware dongle that functions as a USB human interface device (HID). This device must reside in the Subject computer in order to execute the F-Response software on the Subject machine.

Windows

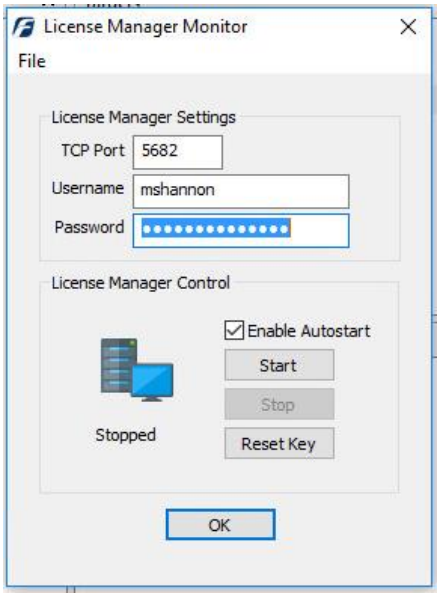
License Manager

Using the F-Response License Manager Software (Enterprise, Consultant + Covert, Consultant)

To validate your license (F-Response Dongle) from remote computers running F-Response Enterprise, Consultant + Covert, or Consultant Edition, you must have your dongle physically connected to your analysis machine and the F-Response License Manager must be started.

The first time the F-Response License Manager (F-Response LM) software is executed it will display a System Tray icon indicating the License Manager server is not started.

System Tray Icon indicating the F-Response License Manager is not running



F-Response License Manager Monitor, Main Window

The representation above shows a running F-Response License Manager Monitor. Details of the information in the Network tab fields are as follows:

TCP PORT

Local machine TCP port currently listening for incoming F-Response Enterprise/Consultant Edition License Validation requests.

USERNAME

The F-Response specific username[3] used to control access to F-Response Subjects.

PASSWORD

The F-Response specific password used to control access to F-Response Subjects.

Operation

START

Starts the License Manager Server.

STOP

Stops the License Manager Server.

RESET KEY

Since the License Manager Server is responsible for priming the unique encryption parameters for the subjects it is possible some organizations will want to reset this key information from time to time. Stop the License Manager Server and use this button to reset the key parameters.

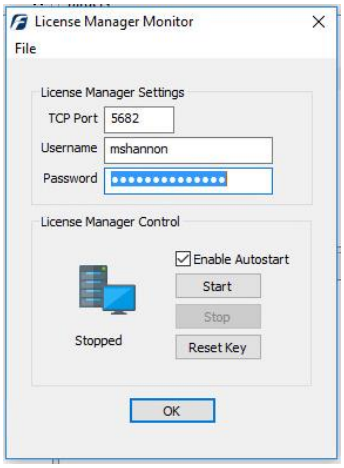
ENABLE AUTO START

Checking this box sets the License Manager Server to automatically start when the local computer boots.

3 The versions of F-Response prior to version 7 had the username and password for F-Response in the Management Console.

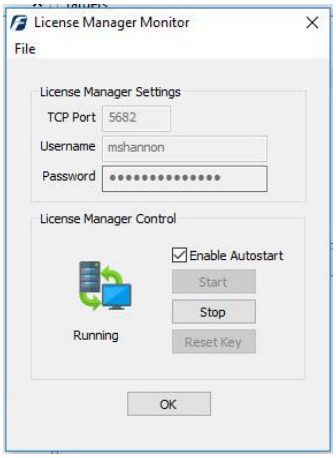
Starting the F-Response License Manager

Before you can begin using F-Response Enterprise, Consultant + Covert, and/or Consultant Edition you must Start the F-Response License Manager service. Right click on the F-Response License Manager icon and choose Open LM Configuration in the System Tray to bring up the License Manager Monitor console.



F-Response License Manager Monitor console, Main Window

Start the F-Response License Manager service by pressing the Start button. Your F-Response dongle must be inserted prior to starting the License Manager server.

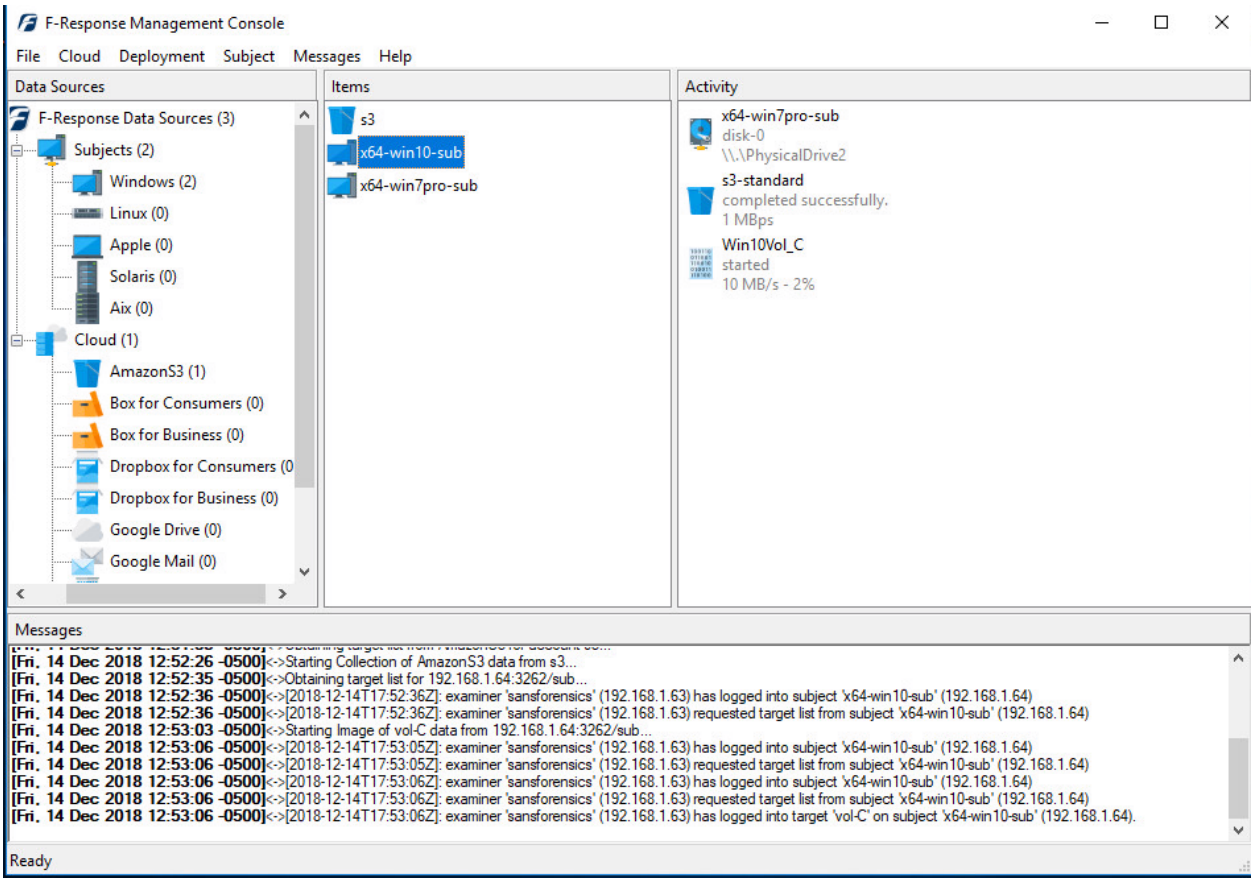


F-Response License Manager running and waiting for licensing requests.

The F-Response License Manager is now running and waiting for licensing requests. The License Manager automatically creates Windows Firewall exceptions for the service application, however if you are using other firewall products you many need to add exceptions as necessary.

F-Response Management Console

Starting with F-Response version 7 each separate F-Response application has now been merged into a single F-Response Management Console. This console gives TACTICAL and above F-Response users the ability to access remote subjects, cloud providers, and create an image from a single location and through a consistent interface.



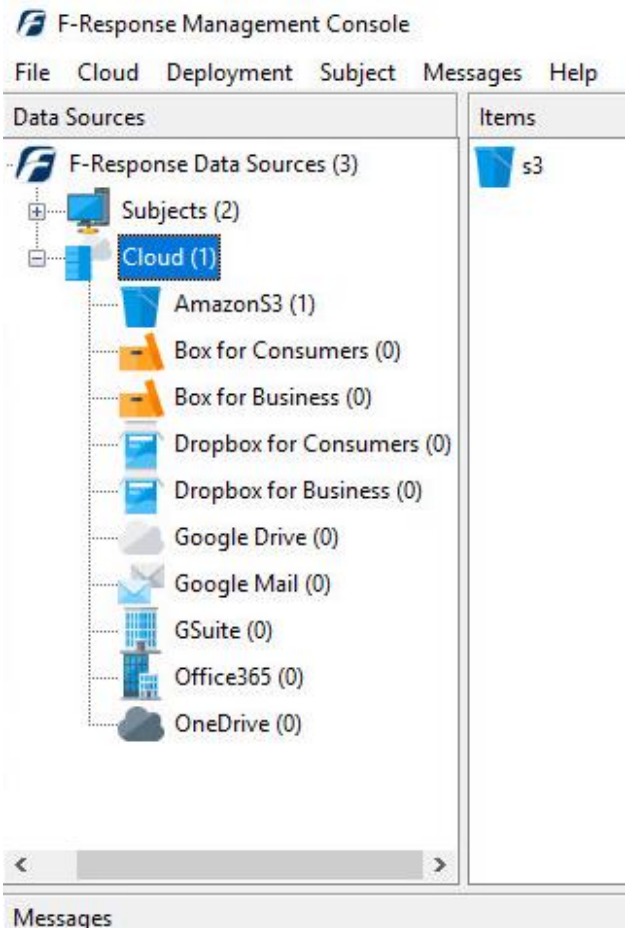
The F-Response Management Console

Providers

Using the Management Console to collect Cloud data

Disclaimer: F-Response provides access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources are by their very nature volatile. F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection.

The F-Response Management Console offers the ability to perform cloud provider data collections to either Virtual Hard Disk (VHD) or Native Directory locations. All supported providers (which varies by F-Response License) are visible in the Data Sources pane. Configuring access to these providers varies greatly by provider, therefore for the most accurate information see the appropriate Mission Guide[4] on the F-Response Website.

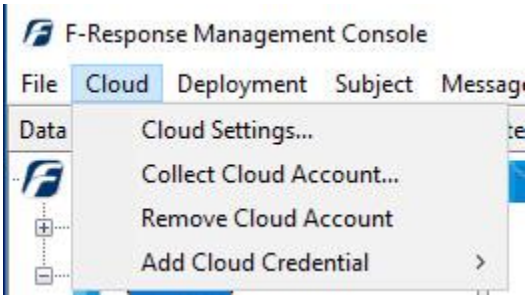


F-Response Cloud Providers

4 Mission Guides are specific training documents available for a wide array of topics on the F-Response Website at https://www.f-response.com/support/missionguides

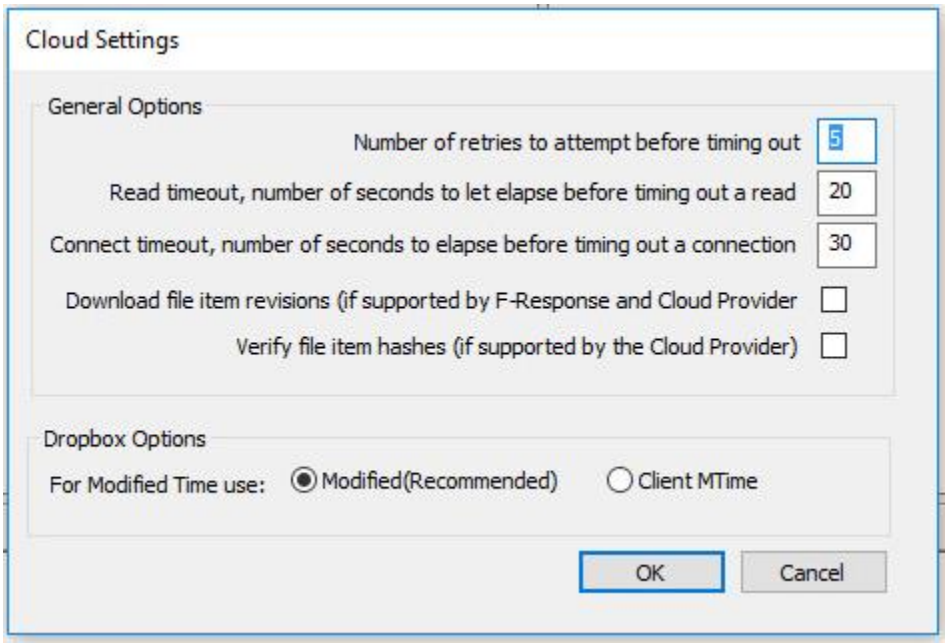
Configuring Cloud Settings

The Cloud menu gives us the ability to access Cloud Settings and Credentials. Using the Cloud Settings we can configure both provider specific and application wide settings for communicating with cloud and 3rd party data providers.



Cloud Menu

There are many options that can be configured for communicating with Cloud Providers, these options include:



Cloud Provider Settings

NUMBER OF RETRIES TO ATTEMPT BEFORE TIMING OUT

Setting this number instructs the software to attempt this many web operations before giving up on the request.

READ TIMEOUT, NUMBER OF SECONDS TO ELASPE BEFORE TIMING OUT A READ

Setting this number instructs the software to wait this many seconds before timing out a read attempt.

CONNECT TIMEOUT, NUMBER OF SECODS TO ELAPSE BEFORE TIMING OUT A CONNECTION

Setting this number instructs the software to wait this many seconds before timing out a connection attempt.

DOWNLOAD FILE ITEM REVISIONS (IF SUPPORTED BY F-RESPONSE AND CLOUD PROVIDER)

Some cloud providers store multiple revisions of a given item. If this option is enabled and both F-Response and the provider support revisions, multiple file revisions (where accessible) will be downloaded.

VERIFY FILE ITEM HASHES (IF SUPPORTED BY THE CLOUD PROVIDER)

If this option is enabled and the cloud provider provides file item hashes, F-Response will verify the file items against the hashes immediately after downloading them.

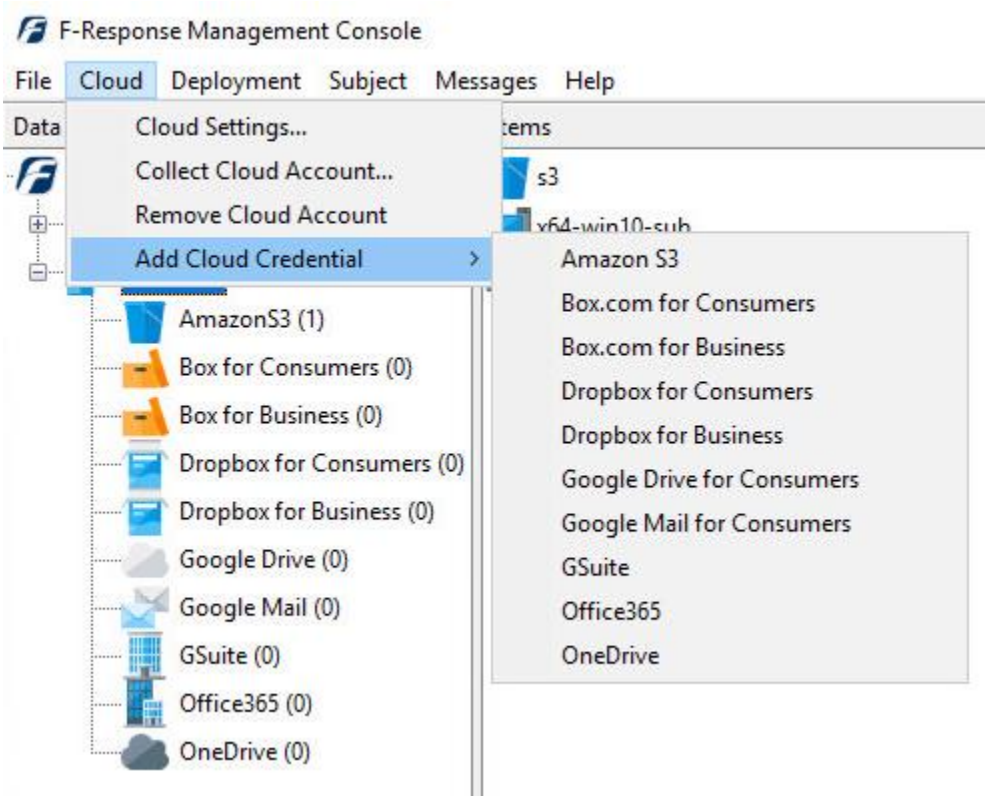
Dropbox Options

FOR MODIFIED TIME USE:

Dropbox provides two different times that can be used as Modified Time for a given file. By default, the software uses the Modified time as provided by the Dropbox Servers. Alternatively, it is possible to use the Client MTime, a non- verified time that is assigned to the files when they are modified by a Dropbox Client tool. The Client MTime is not verified by Dropbox.

Configuring Cloud Credentials

Before you can connect to Cloud services you must first input valid credentials. While the credentials necessary vary by Cloud Provider, all credentials must be input using one of the Configure Credentials dialog boxes.

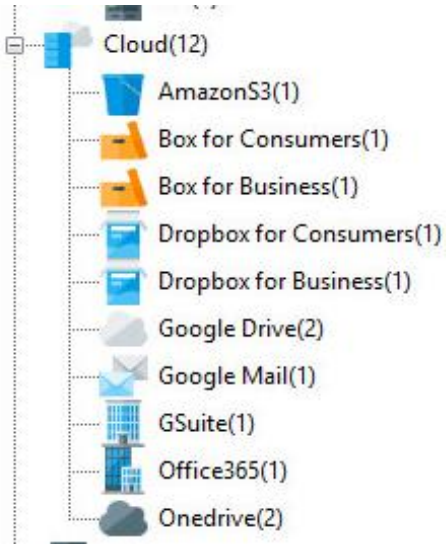


Provider Credentials

As the credential location and process for acquiring those credentials changes frequently for almost all providers, including each one in this manual would quickly become obsolete. Please refer to the specific Mission Guide on the F-Response Website for details on provider you are attempting to access. F-Response Mission Guides are available at https://www.f-response.com/support/missionguides

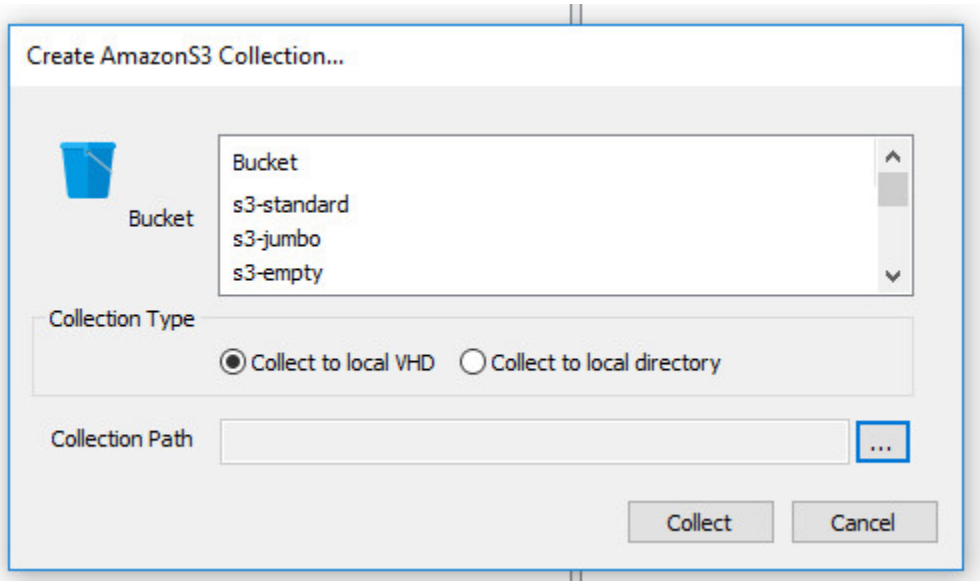
Collecting a Cloud Account

After successfully adding one or more cloud accounts you will find them visible in the Data Sources tree view under the specific provider.



Select an individual Cloud provider to populate the Items panel with accounts

Double clicking on an individual account will trigger a dialog for collection of that account, more details on specific dialogs by provider are available in the individual provider Mission Guides on our website.



Creating a Collection…

Subjects – Exporting and Deploying

Using the Management Console to deploy and/or connect to remote Subjects

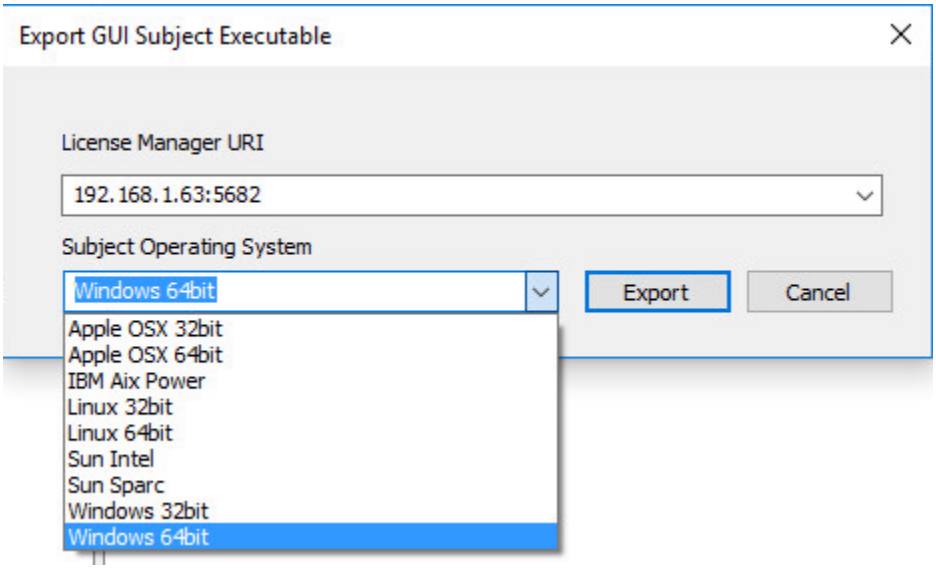
The F-Response Management Console provides options for connecting to remote subjects for all versions of F-Response (TACTICAL, Consultant, Consultant + Covert, Enterprise). Field Kit customers will want to use the F-Response Control Panel Applet for connecting to remote machines.

Customers using F-Response Consultant edition and above have the option to export unique preconfigured subject executables for different platforms. These exported subjects reduce some of the configuration complexity and allow for easier operation.

Customers using F-Response Consultant + Covert and Enterprise have the option to export unique preconfigured subject executables for different platforms as well as the option to deploy those customized subject executables to remote machines with the proper credentials.

Export GUI Subject executable (Consultant, Consultant + Covert, and Enterprise)

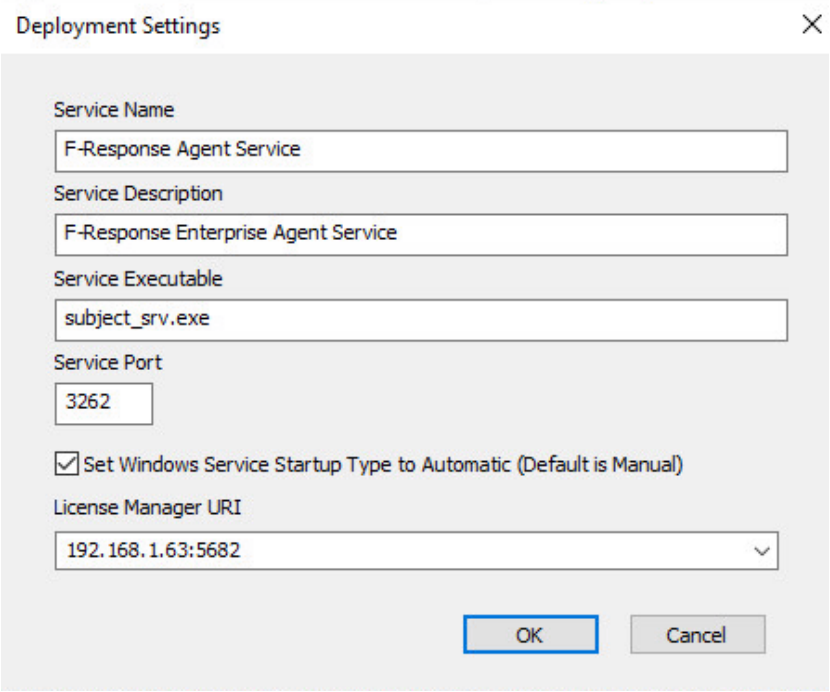
F-Response Consultant edition and above users also have the option of exporting individual subject executables pre-configured for usage. Using the Export GUI Subject executable window, you'll be able to select both the License Manager URI (where the subject should go to check its license), and the Platform of the executable you wish to export.



Export GUI Subject Executable Window

Deployment Settings

Prior to beginning any deployment operations, you should review the Deployment Settings. Please refer to the guidelines below for configuring the deployment settings.



Deployment Settings Dialog

SERVICE NAME

This is the name the F-Response Subject service will be installed as on the remote computer(s). This name is completely user selectable. Please do NOT use the name of an existing service as they may conflict.

SERVICE DESCRIPTION

Description value that will be assigned to the F-Response Subject service when installed on the remote computer(s). This description is completely optional.

SERVICE EXECUTABLE

This is the executable name that will be assigned when the Subject software is deployed.

SERVICE PORT

This is the TCP port the F-Response Subject service will listen on.

SET STARTUP TYPE

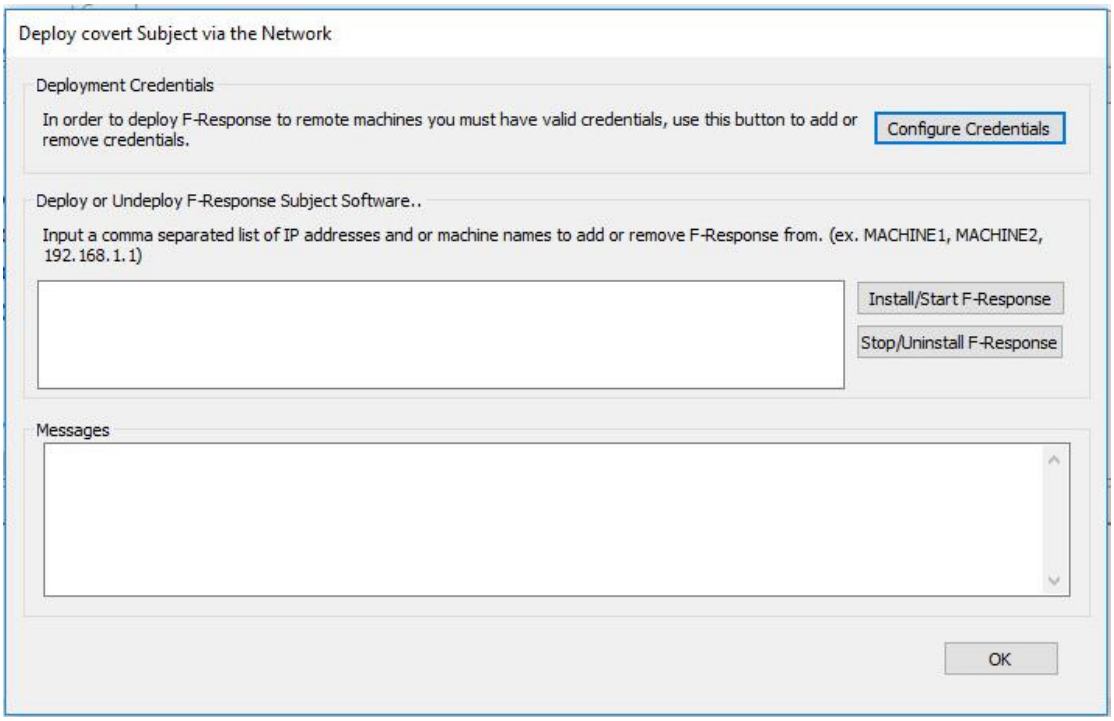
If this option is enabled the service will be set to start on install.

LICENSE MANAGER URI

This is the IP and Port of the F-Response License Manager that the Subject will be configured to communicate with.

Deploy covert Subject via the Network

Select Deployment->Deploy covert Subject via the Network from the menu to view the dialog for pushing F-Response Subject software over the network. There are 3 sections here: **Deployment Credentials**, **Scan for Machines**, and **Scan Results**.



Deployment Dialog

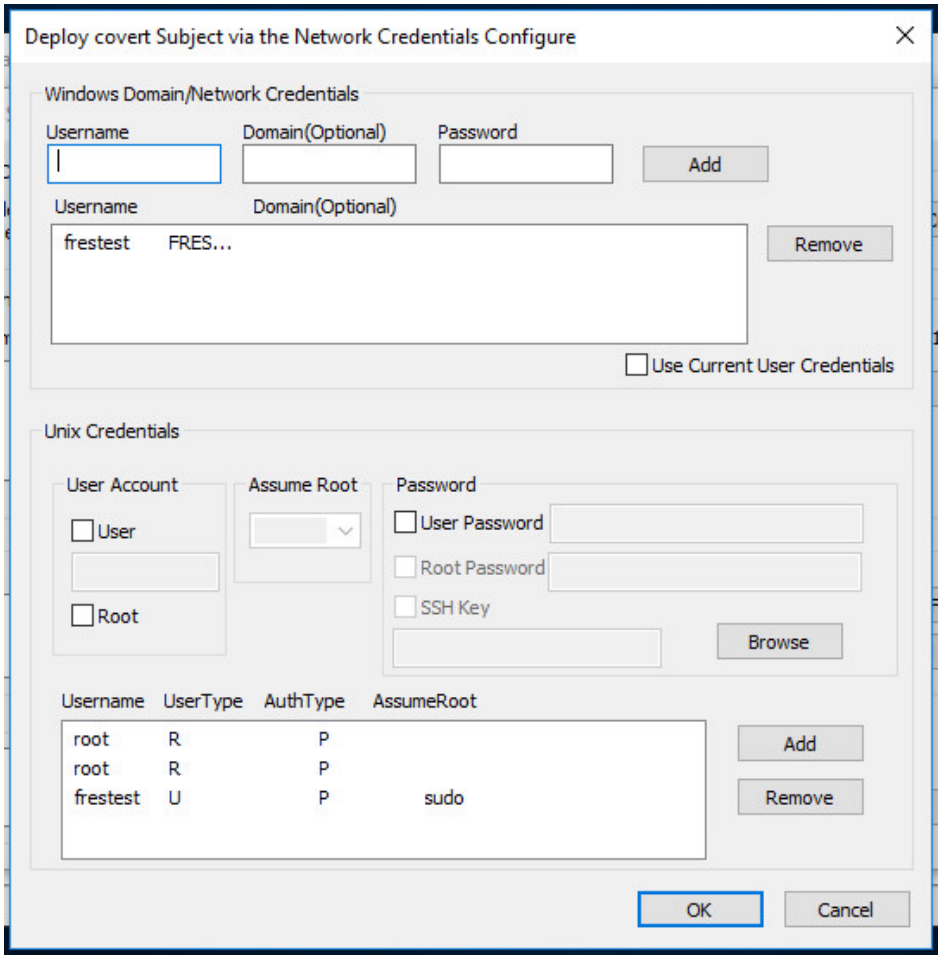
The first step to deploy over the network is to click the Configure Credentials button in the top right corner and the Configure Credentials window will open.

Configure Credentials

Here credentials can be set up for both Windows (the top section of the window) and Non-Windows platforms (the lower portion).

Windows

Under **Windows Credentials**, enter the **Username** (with administrator level privileges), **Domain** (if local account leave this value blank), and **Password**. Click **Add** to add the credential to the stack.



Deployment Credentials Dialog

Apple/Linux

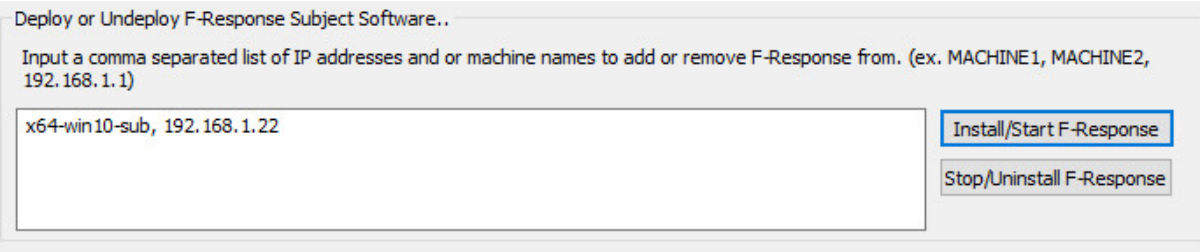
Under **Unix Credentials, C**redentials can be added for supported Non-Windows Platforms.

Under **User Account** check **User** and enter the User name. The user account must have elevated privileges to install and run the subject software so select **su** or **sudo** from the drop down list under **Assume Root**. Next check **User Password** and enter the password for the account. Alternatively, if using the root account, simply select **Root** under **User Account**, check **Root Password** and enter the password. Click **Add** for each account entered to add them to the stack.

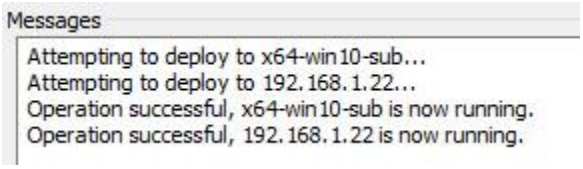
Multiple accounts can be added if needed. Click **Ok** in the lower right corner once all the necessary credentials have been entered.

Scanning for and deploying to Subject Machines

After adding at least one credential you will be able to use the Deploy or Undeploy box to add one or more comma delineated hostnames or IP addresses. Once you've added them you must press the Install/Start F-Response button to begin the scanning and deployment process.



The results will appear below in the Messages section of the dialog. Provided your credentials were successful and the machine was available on the network you should see the following response. If not, please check your credentials and try again.

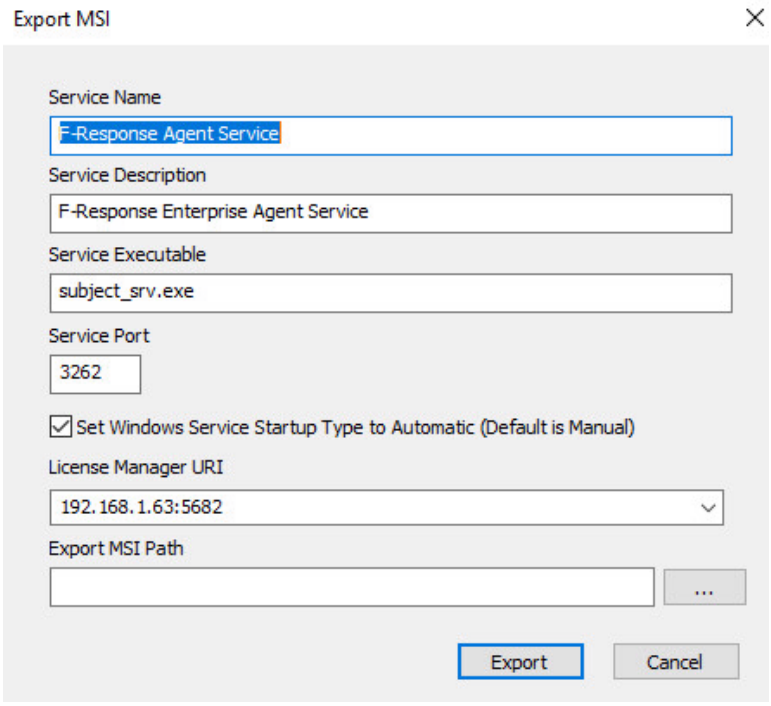


Click OK to return to the main window of the F-Response Management Console.

Export covert Microsoft Software Installer

F-Response Consultant + Covert and Enterprise also offers the option under the Deployment menu to create a Microsoft Software Installer (MSI) which can then be distributed throughout the environment using an alternative software distribution method such as Group Policy in Active Directory, Microsoft System Center Configuration Manager (SCCM), or various other software deployment tools.

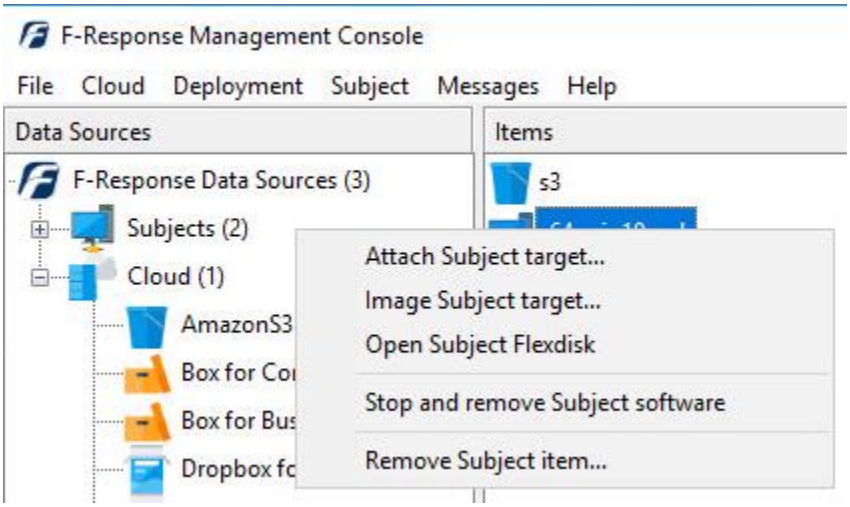
The process to create an MSI is straight forward, simply modify any of the settings specific to the environment as necessary (i.e. changing the Service Name, or Description, etc.). After which use the "…" button to select a location to save the exported MSI.



Export Microsoft Software Installer Window

Stopping the remote software

When finished using F-Response on one or more subject machines, there are multiple ways to remove or stop the software on the remote machine. It can be removed directly by using the "Stop and Remove Subject Software" option, or through the Deployment process covered earlier.



Stop and Remove F-Response Menu

Command Line Subject Options for Manual Deployment

The F-Response Main Console provides multiple deployment options, however in some instances the Enterprise or Consultant + Covert software must be deployed using another means. In this instance it is possible to configure and install the Enterprise or Consultant + Covert service natively on the local machine using the following command line arguments:

To Add the Service with all required arguments:

-a “SERVICE NAME” -> Sets the Service Name and adds the new service.

-k DONGLENUMBER -> Sets the dongle # for the license manager.

-s LICENSEMANAGERURI -> Sets the License Manager URI, IP:Port.

-l LOCALPORT -> Sets the local port F-Response should listen on.

There are two subject executables available:

subject_srv.exe ->for 32 bit systems

subject_srv-x64.exe ->for 64 bit systems

Example of adding the “Test Service” on a 64 bit local machine.

“subject_srv-x64.exe -a “Test Service” -k 155520212 -s 192.168.1.1:5682 -l 3262”

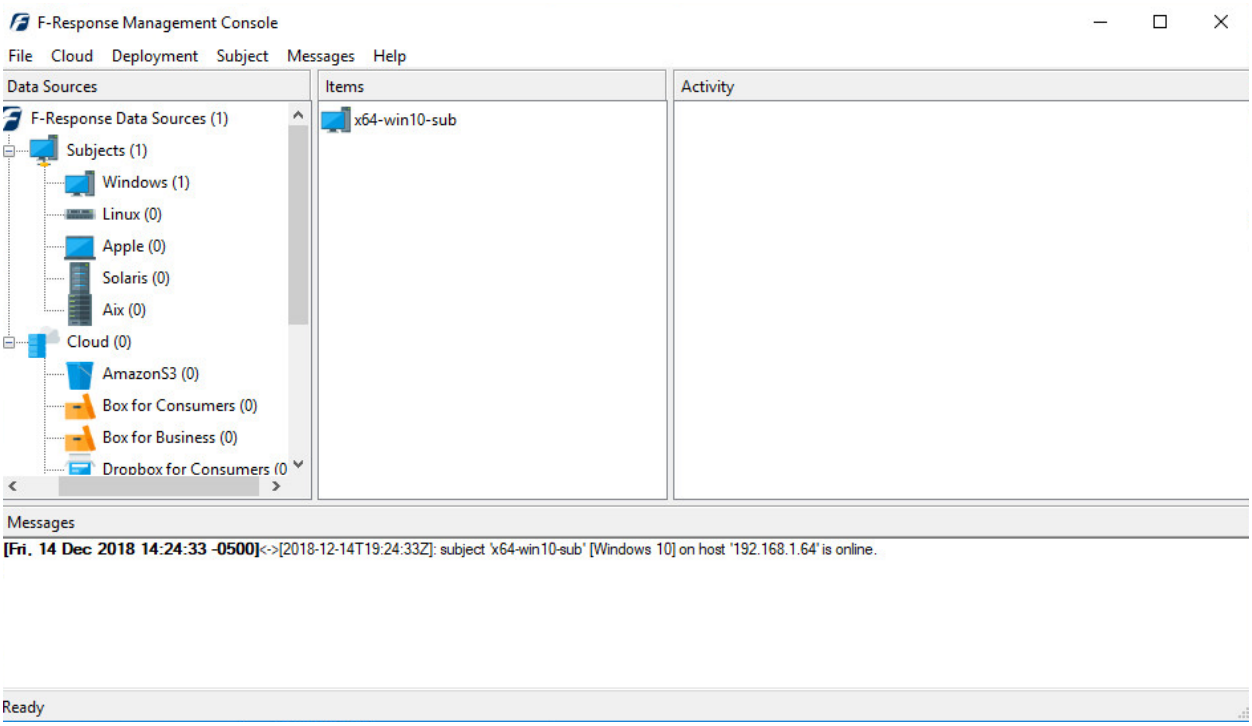
To Remove the Service:

-r “SERVICE NAME” -> Removes the service by name.

Subjects – Working with Subjects

Listing License Managed Subjects

After starting the F-Response software on one or more remote subjects any subjects configured to use your local license manager will appear in the F-Response Management Console as seen below[5].

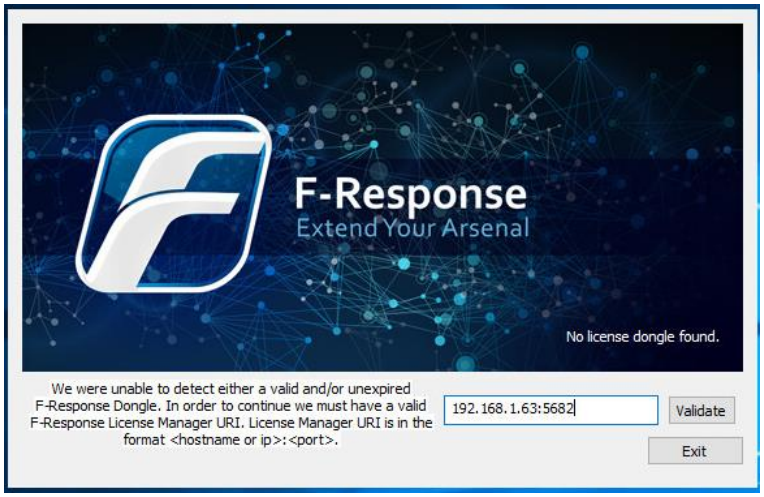


Subjects currently connected to the local license manager

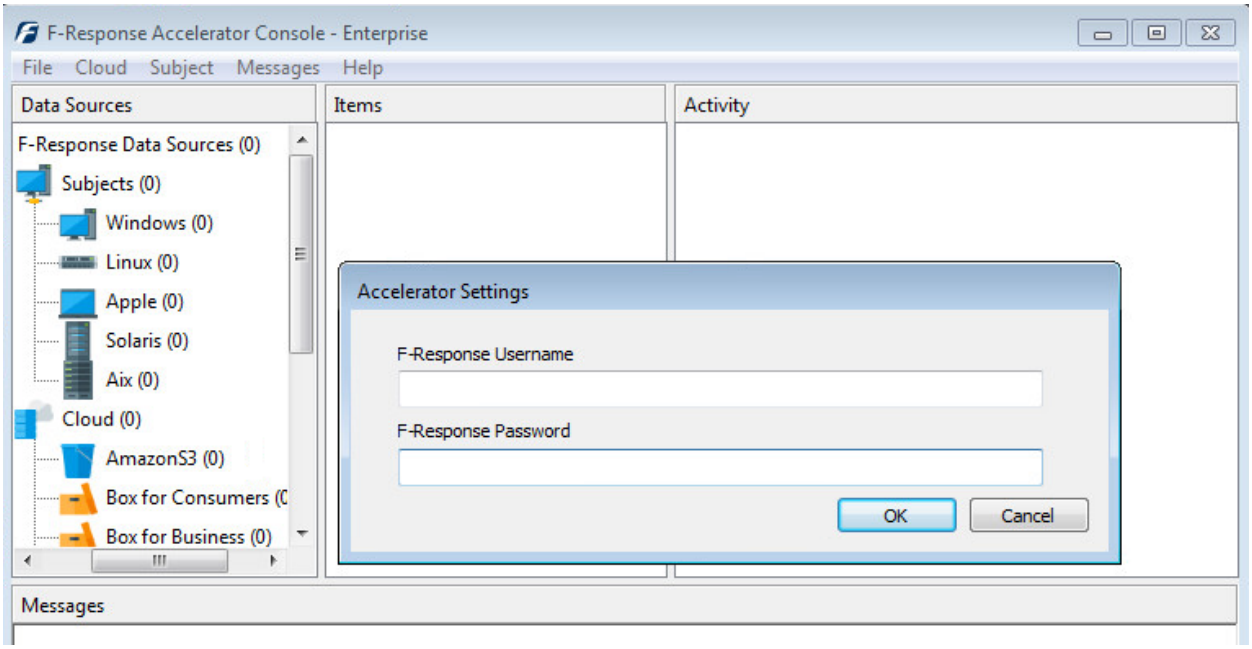
5 In prior versions of F-Response this would be equivalent to the "Active Clients" panel.

Adding Accelerator Subjects

When running the F-Response Management Console on a machine without a local license dongle, providing the location of a license dongle on the network opens the F-Response Accelerator version of the Management Console. In this mode you can add remote subjects directly using their URI.

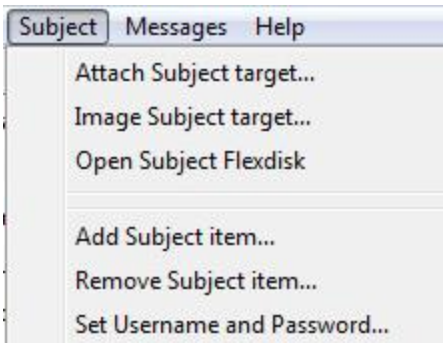


Dialog prompting the location of a valid license manager



F-Response "Accelerator" Console

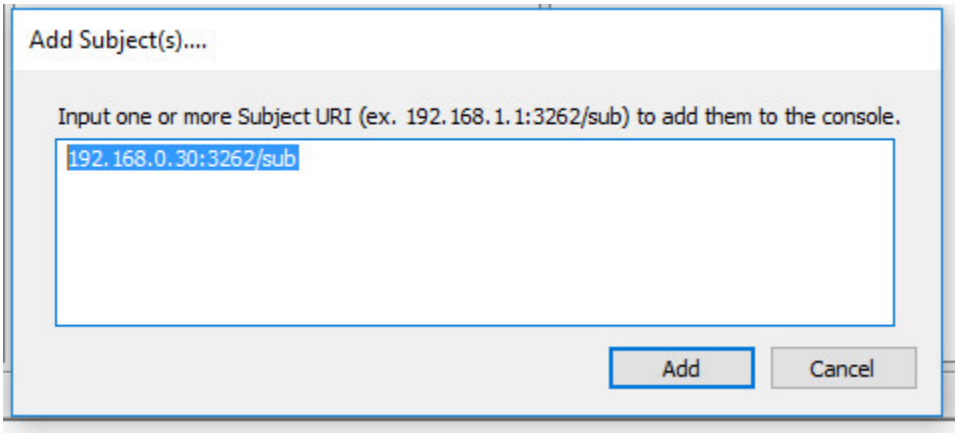
The first step to using the F-Response Management Console in "Accelerator" mode to connect to remote deployed and running instances of F-Response is to make sure the F-Response Username and Password value has been set. You will find those settings under Subject->Set Username and Password…



Accelerator Settings Menu

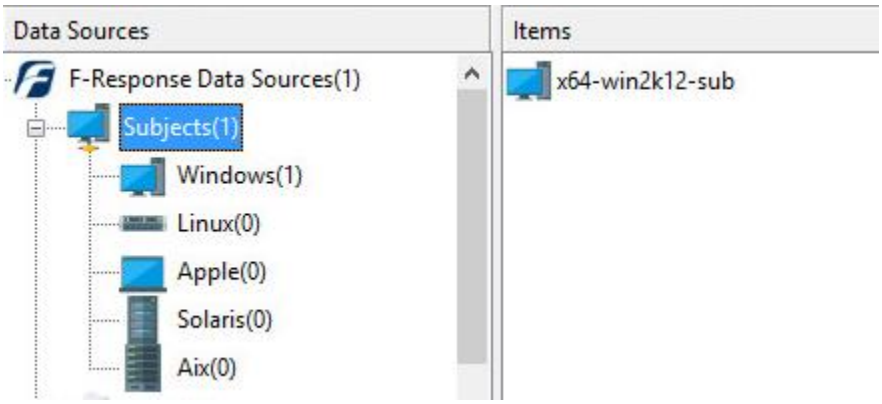
Here the credentials entered should match those set up on the examiner machine with the license dongle attached, as entered in the License Manager Monitor

Next you can add one or more Subjects by inputting their full URI on into the Add Accelerator Subjects dialog.



Add Accelerator Subjects Dialog

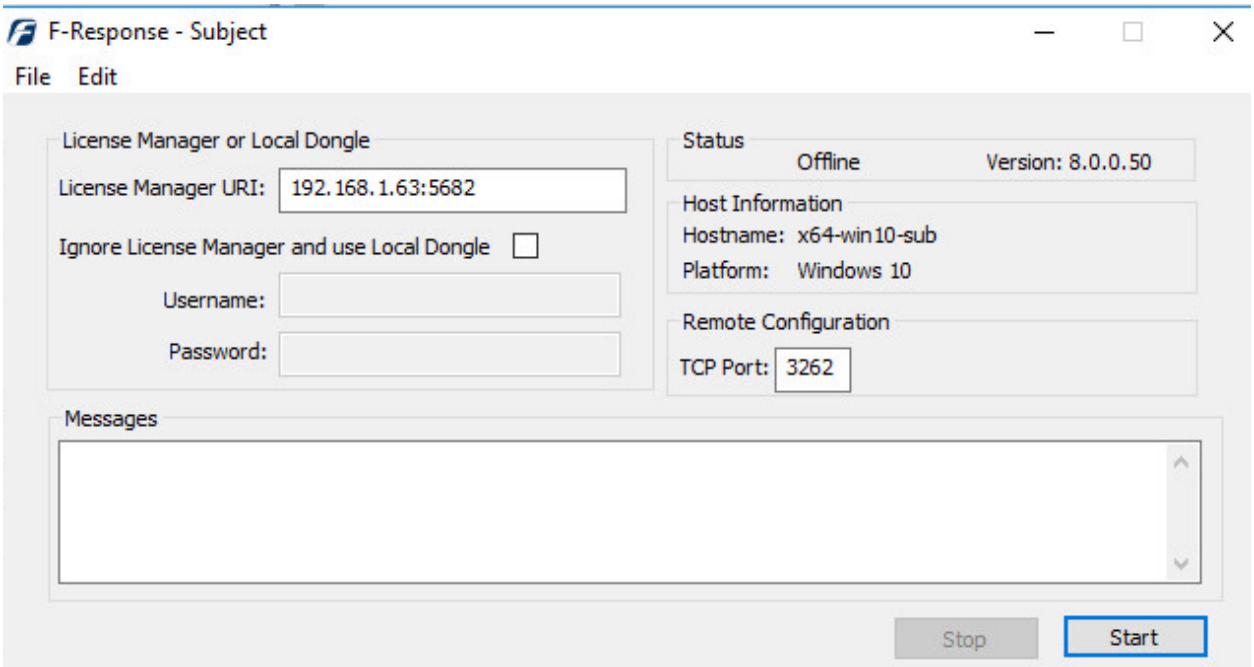
Provided the username and password configured earlier are correct and there were no issues communicating with the remote subjects you should see icons for them appear in the Data Sources panel.



Accelerator Panel showing multiple subjects

Consultant and Field Kit Subject

F-Response Field Kit and Consultant edition use the same graphical subject software on remote machines. The following outlines the steps necessary to configure and use the graphical subject software.



LICENSE MANAGER URI

This is the URI necessary for locating the license manager.

IGNORE LICENSE MANAGER AND USE LOCAL DONGLE

This option will set the executable in Field Kit mode and will not attempt to contact a remote license manager.

USERNAME

In Field Kit mode the selected Username must be input in this field.

PASSWORD

In Field Kit mode the selected Password must be input in this field.

TCP PORT

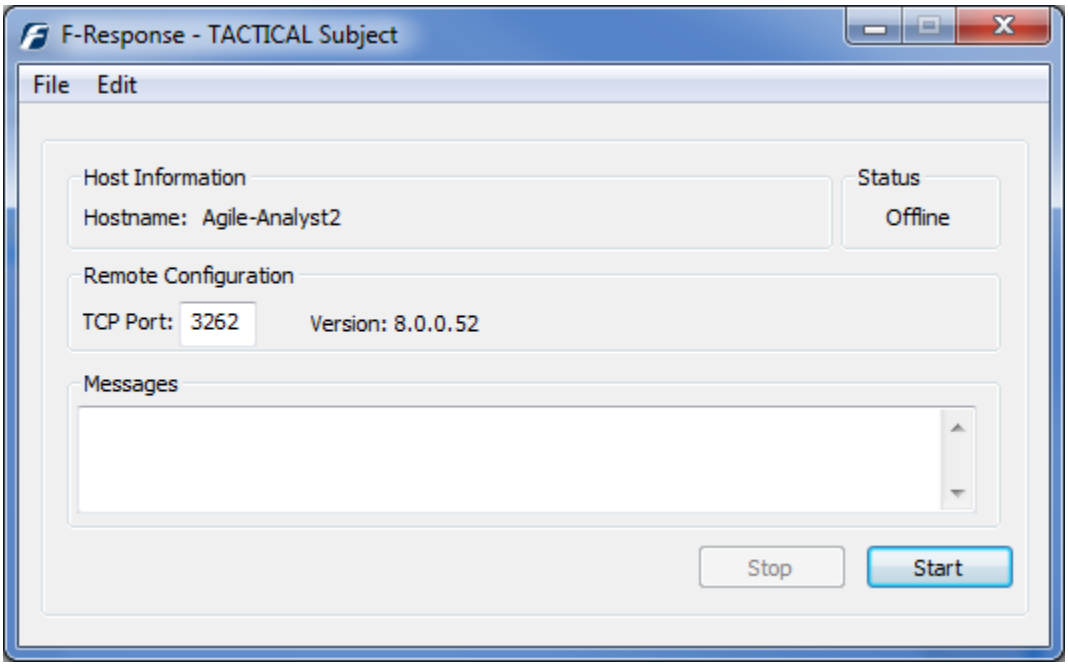
This is the TCP port the F-Response Subject service will listen on.

MESSAGES

Any errors or output will be presented here.

TACTICAL Subject

F-Response TACTICAL edition use a graphical subject software on remote machines. The following outlines the steps necessary to configure and use the graphical subject software.



TCP PORT

This is the TCP port the F-Response Subject service will listen on.

MESSAGES

Any errors or output will be presented here.

Non-Windows Subjects

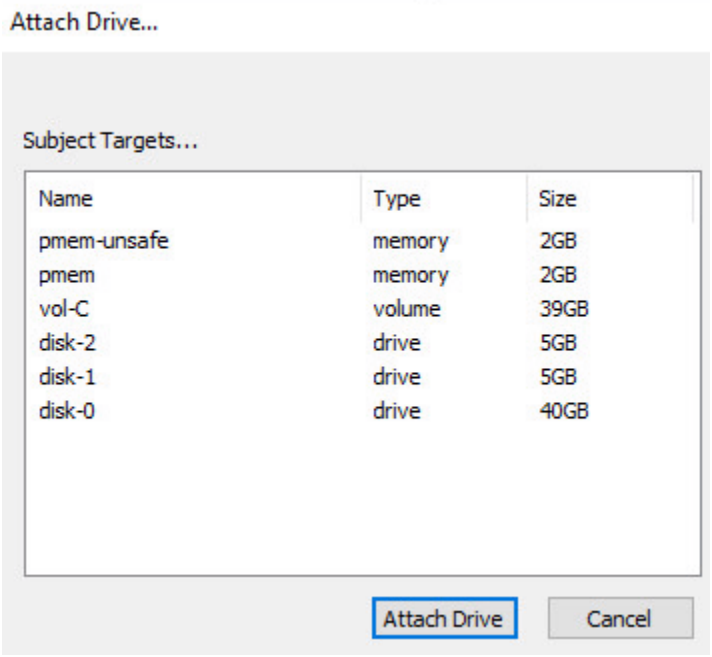
All Non-Windows F-Response Subjects are command line based and can be found in your installation folder, or deployed/exported using the mechanisms defined earlier in this manual. The following command line options are the same regardless of Non-Windows Platform.

```
F-Response <PLATFORM> Subject <VERSION> Consultant Edition
Copyright F-Response, All Rights Reserved
-h                    ; print help message
-s  <port=3262>       ; subject tcp port
-m  <host>:<port=5682> ; license manager server
Thank you for using F-Response.

F-Response <PLATFORM> Subject <VERSION> Field Kit Edition
Copyright F-Response, All Rights Reserved
-h                    ; print help message
-s  <port=3262>       ; subject tcp port
-u  <username>        ; username
-p  <password>        ; password
Thank you for using F-Response.
```

Subject Targets

F-Response will present the resources on the remote subject computers as Subject Targets.



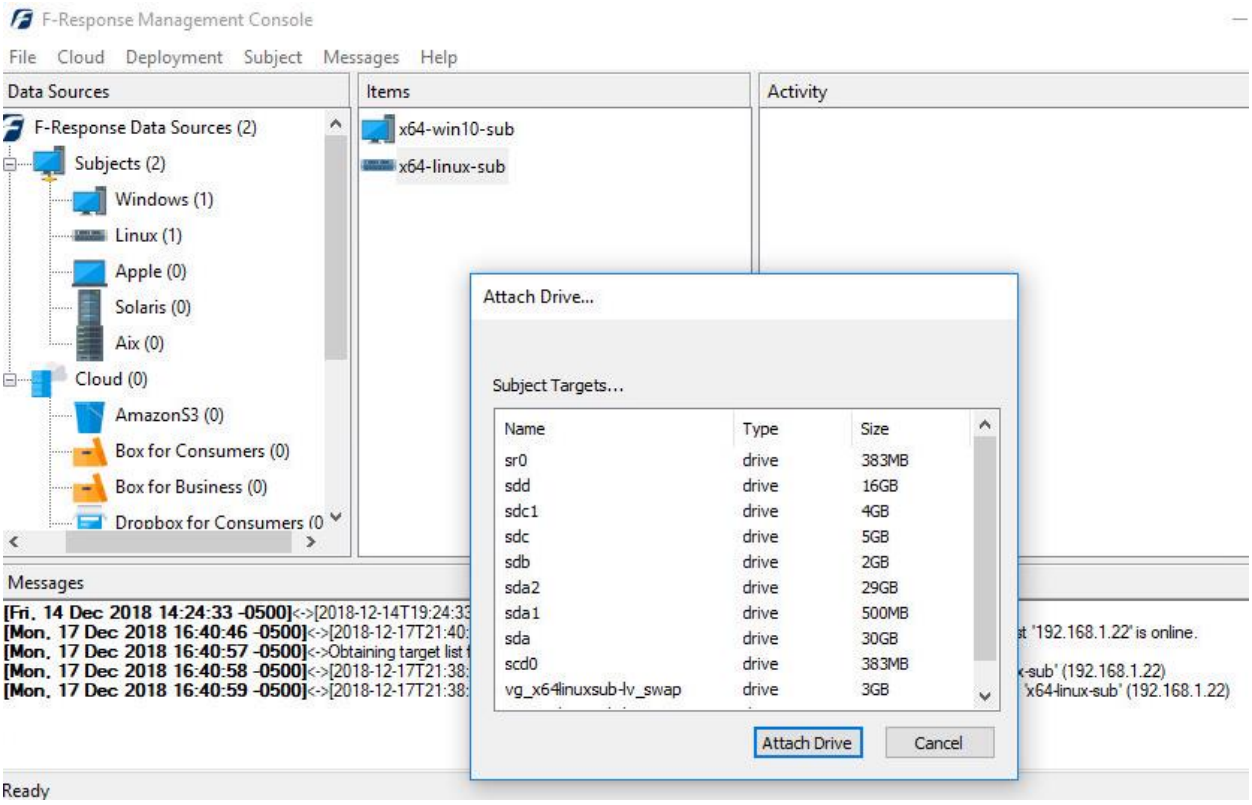
You'll find options for physical disks attached to the remote machine (disk-x), the logical volumes and partitions (Vol-C, sda1, sda2), and, in the case of Windows subject computers, physical memory. Physical memory is available in two formats: pmem and pmem-unsafe.

Note pmem is normal standard access to remote physical memory that works through an overlay and skips device allocated or restricted areas of memory as set by the operation system. This is the preferred method of accessing remote memory.

F-Response now also offers a pmem-unsafe option which will attempt to read all memory on the remote subject regardless of restriction. Please consider this puts you at risk of crashing the remote system so proceed with this knowledge.

Attaching Drives

After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Double-Click on any subject to open a dialog for attaching a subject disk, or use the Subject menu for attaching a disk or starting a direct image of one or more subject targets.



Subject and Targets

Active Targets

Imaging

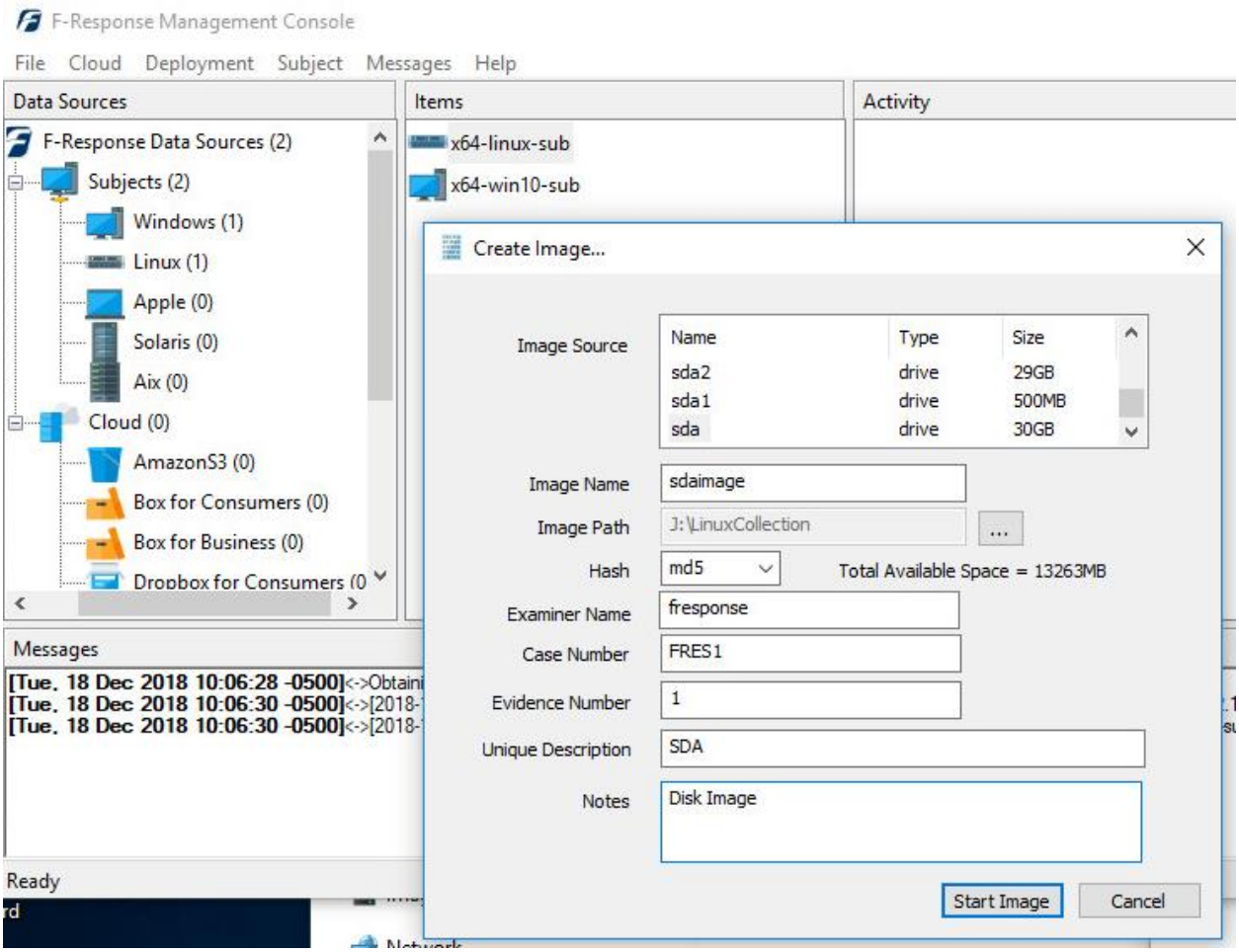
Overview

The F-Response Management Console provides a simple and straightforward mechanism for creating images of F-Response devices and targets. This imaging capability is completely optional however, since F-Response devices are vendor neutral you are welcome to use whatever imaging or analysis tools you would like.

Direct Physical Image

Creating a Direct Image from the Console

After successfully deploying F-Response to one or more remote machines you should be able to see those machines by selecting Subjects or a specific platform in the Data Sources panel. The subject entries will appear in the Items panel. Right click on any subject and select Image Subject Target menu option to commence a direct image of one or more subject targets.

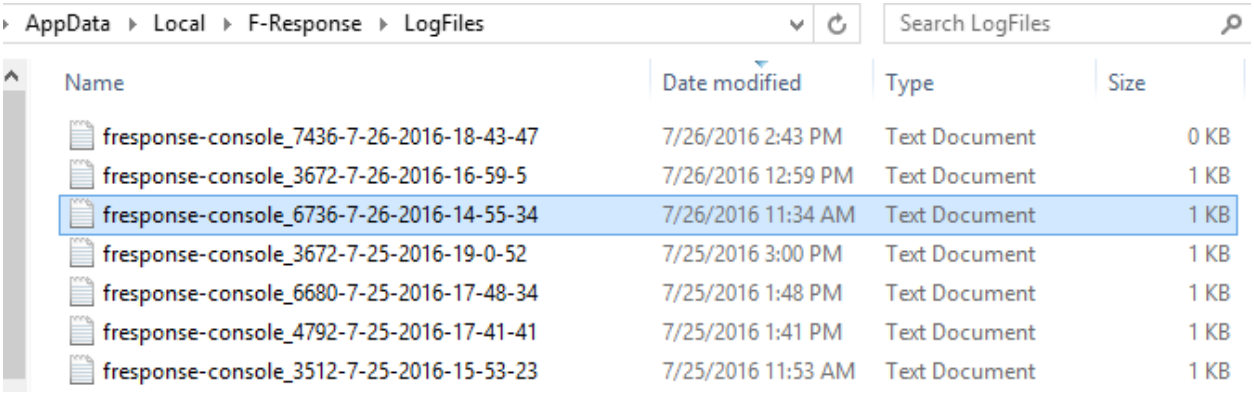


Start Imaging Process…

Active Images

Messages

The Management Console retains a Messages Panel showing all the textual messages, errors or otherwise returned by running F-Response operations. These logs are displayed on the screen and stored in text files generated for each execution of the F-Response Management Console. By default these log files are stored in the Examiner's profile directory under AppData\Local\F-Response\LogFiles.

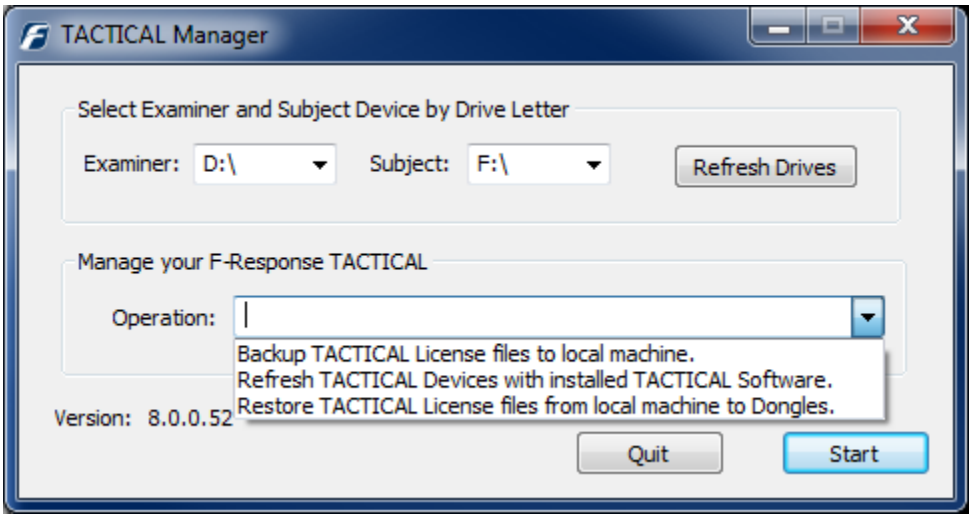


Profile directory showing messages log files

The name of the log file is based on the process identifier of the console when it was opened and the date and time of that opening.

Managing F-Response TACTICAL

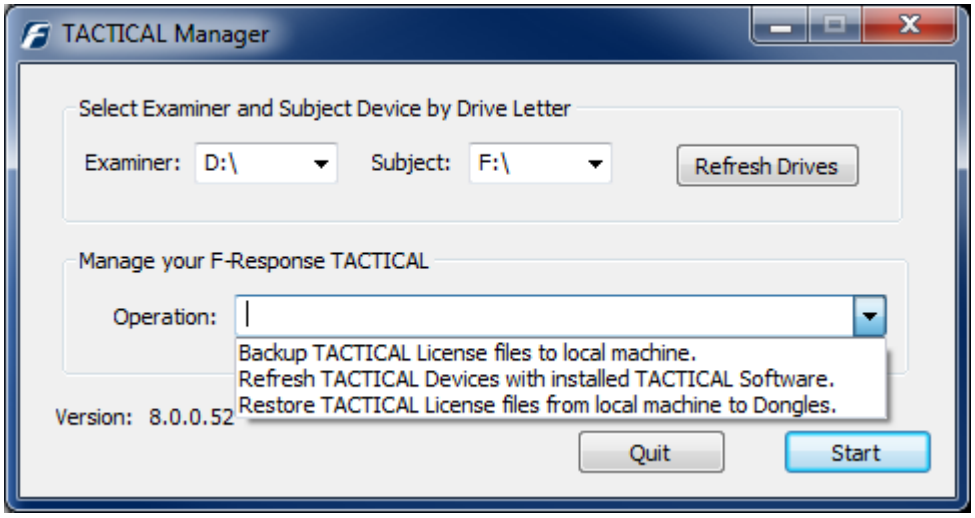
Backing up your F-Response TACTICAL Licenses



F-Response TACTICAL Manager "Backup TACTICAL Licenses"

We recommend using the F-Response TACTICAL Manager to backup your F-Response TACTICAL License files to your Analyst or Investigator's computer prior to using F-Response TACTICAL for the first time. Insert both F-Response TACTICAL Fobs into your computer and select the appropriate drive letter for the Examiner and Subject device. If the drive letter is not listed, press "Refresh Drives" to re-populate the drop down listing of available devices. Press Start to begin the backup operation. TACTICAL License files are stored in C:\Program Files\F-Responsev7\F-Response TACTICAL\Tactical License Backup

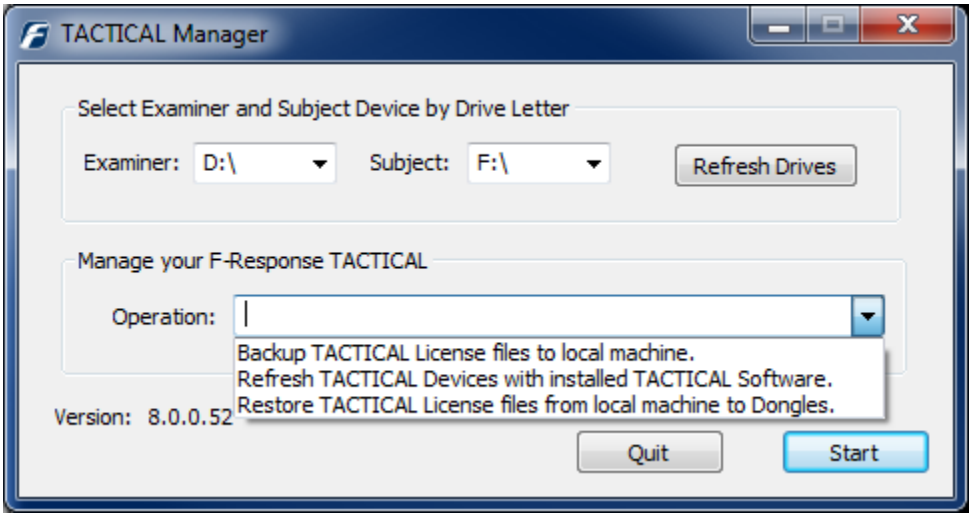
Refreshing the F-Response TACTICAL Software



F-Response TACTICAL Manager "Refresh TACTICAL Devices…"

Should the F-Response TACTICAL software ever be accidentally deleted, or if you have downloaded and installed a new version of F-Response TACTICAL, it will be necessary to update and restore the software to your F-Response TACTICAL Fobs. Insert both F-Response TACTICAL Fobs into your computer and select the appropriate drive letter for the Examiner and Subject device. If the drive letter is not listed, press "Refresh Drives" to re-populate the drop down listing of available devices. Press Start to begin the Restore/Update operation.

Restoring your F-Response TACTICAL Licenses

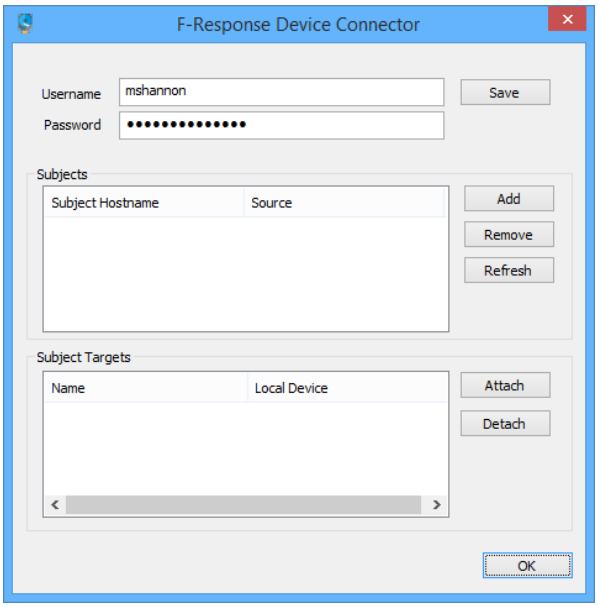


F-Response TACTICAL Manager "Restore TACTICAL Licenses…"

Should the F-Response TACTICAL licenses ever be accidentally deleted, or if you have downloaded and copied new license files to your computer, it will be necessary to update and restore the licenses to your F-Response TACTICAL Fobs. Insert both F-Response TACTICAL Fobs into your computer and select the appropriate drive letter for the Examiner and Subject device. If the drive letter is not listed, press "Refresh Drives" to re-populate the drop down listing of available devices. Press Start to begin the Restore/Update operation.

F-Response Device Connector Applet

The F-Response Device Connector Applet is a secondary mechanism for interacting with F-Response Devices (Subject presented targets), listing and attaching/detaching them. The F-Response Device Connector is available via the Control Panel on your Examiner machine after installing F-Response.



USERNAME

F-Response Username designated for accessing remote F-Response Subjects.

PASSWORD

F-Response Password designated for accessing remote F-Response Subjects.

ADD

Add a new remote Subject by URI, Ex. HOSTNAME:PORT or IP:PORT.

REMOVE

Select and remove an existing F-Response Subject.

REFRESH

Refresh the list of Subject Targets for the selected Subject.

ATTACH

Select and attach a Subject Target.

DETACH

Select and detach a Subject Target.

Unix[7]

Installation and Configuration

All Unix versions of F-Response require installation. The following commands outline the installation, post install configuration, and uninstall process.

Installing RPM (.rpm)

```
# yum install fresponse.x86_64.rpm
```

Installing Debian (.deb)

```
# dpkg -i fresponse.x86_64.deb
# apt-get install -f
```

Installing Apple Disk Image (.dmg)

```
$ hdiutil attach fresponse.x86_64.dmg
$ sudo installer -pkg /Volumes/fresponse7/fresponse.x86_64.pkg  -target /
$ sudo cp -R /Volumes/fresponse7/fresponse-console.app/ /Applications/fresponse-console.app/
$ sudo cp -R /Volumes/fresponse7/fresponse-accelerator.app/ /Applications/fresponse-
accelerator.app/
$ hdiutil detach /Volumes/fresponse7
```

Installing RPM (.rpm) for deployment tools (Linux Only)

```
# yum install fresponsewin.centos6.x86_64.rpm
```

Installing Debian (.deb) for deployment tools (Linux Only)

```
# dpkg -i fresponsewin.ubuntu14.x86_64.deb
# apt-get install -f
```

Uninstallation

Uninstalling RPM (.rpm)

```
# yum remove fresponse
```

Uninstalling Debian (.deb)

```
# apt-get remove fresponse
```

Uninstalling Apple Disk Image (.dmg)

```
$ sudo fr_uninstall.sh
```

Uninstalling RPM (.rpm) for deployment tools (Linux Only)

```
# yum remove fresponsewin
```

Uninstalling Debian (.deb) for deployment tools (Linux Only)

```
# apt-get remove fresponsewin
```

[7] For the sake of this document Unix encompasses the following F-Response Examiner platforms: Linux and Apple OSX.

Post Installation

Updating /var/lib/f-response

The F-Response directory is installed as /var/lib/f-response with permissions enabled for all users. However, for additional security we recommend changing the ownership and permissions to allow access to an individual user or group only.

```
$ sudo chown -R USERNAME:USERNAME /var/lib/f-response
$ sudo chmod -R og-rwx /var/lib/f-response
```

Updating fusermount – Linux Only

The examiner and accelerator use `fusermount` to mount and unmount F-Response Live File Devices. We recommend confirming the user account used in the preceding step has read and execute permissions on fusermount.

```
$ whereis fusermount
fusermount: /bin/fusermount /usr/bin/fusermount
$ sudo chmod o+rx /bin/fusermount /usr/bin/fusermount
```

Updating /etc/fuse.conf – Linux Only

The examiner and accelerator use `fusermount` which reads /etc/fuse.conf. We recommend confirming the user account used in the preceding steps has read permissions on the /etc/fuse.conf file. In addition, /etc/fuse.conf must have a single line with the value, **user_allow_other**, to enable non-root users to use `fusermount`.

```
$ sudo chmod o+r /etc/fuse.conf
```

Reloading udev rules – Linux Only

The /etc/udev/rules.d/99-fresponse.rules file is installed with the license manager to grant access to the license dongle for non-root users. However, the rules must be reloaded by running `udevadm` or restarting the system.

```
$ sudo udevadm control --reload-rules
$ sudo udevadm trigger
```

Updating $PATH

The license manager, examiner, and accelerator are installed on /usr/bin for Linux and /usr/local/bin for Mac OS X.

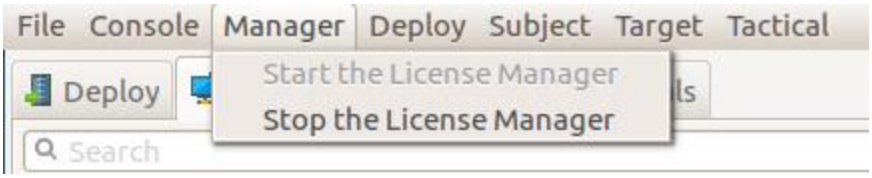
```
$ export PATH=$PATH:/usr/bin
$ export PATH=$PATH:/usr/local/bin
```

License Manager

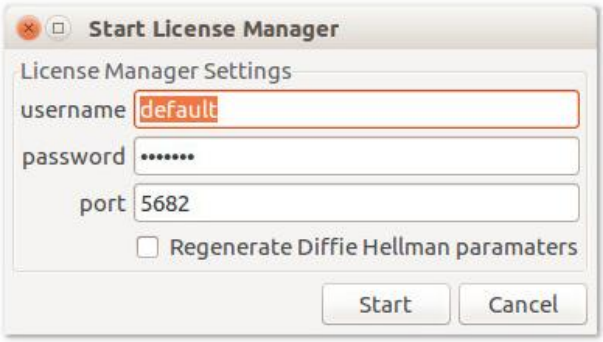
Using the F-Response Management Console

To validate your license (F-Response Dongle) from remote computers running F-Response Enterprise, Consultant + Covert, or Consultant Edition, you must have your dongle physically connected to your analysis machine and the F-Response License Manager must be started.

The F-Response License Manager interface is part of the Management Console.



Use the Manager Menu to Start and Stop the License Manager



Configure the License Manager with an arbitrary Username and Password that you can remember. This credential will be used to access F-Response on remote machines.

Using the License Manager Command Line Interface

The license manager interface implements a set of functions for managing the license manager server, which provides license verification and examiner authentication services for subjects and subject directory services for examiners.

start

The start command starts the license manager server. By default, the license manager server runs in the foreground and listens on port 5682. The -d or --daemon option can be specified to run the license manager server in the background and the --port argument can be specified to listen on a different port.

```
$ fr_lm start --port 5682 --daemon
F-Response Linux License Manager x.x.x.x
Copyright F-Response, All Rights Reserved
License manager process pid ... 5809.
License manager pid file path ... /var/lib/f-response/manager/pid.
Unikey hardware identifer ... 155710303
Unikey license type ... enterprise
Unikey expiration date ... 2018-08-02T00:00:00Z
License manager is online and running in  the background.
Exclude -d,--daemon on command line to run in foreground.
```

stop

The stop command stops the license manager server.

```
$ fr_lm stop
F-Response Linux License Manager x.x.x.x
Copyright F-Response, All Rights Reserved
Signal sigterm to license manager process -- 5809
Waiting for license manager ..  success
```

status

The status command prints the status of the license manager server. If the -j or --json option is specified, then the output is encoded in JSON.

```
$ fr_lm status --json
{
    "date": "2018-08-02T00:00:00Z",
    "expire": "1317764160000000000",
    "hid": "155710303",
    "license": "enterprise",
    "password": "U6kyPw3REZQqjO2LEOAT9g==",
    "port": "5682",
    "username": "default"
}
```

set

The set command sets the username and password of the license manager server, which is stored in /var/lib/f-response/config.

```
$ fr_lm set -u default -p default
F-Response Linux License Manager x.x.x.x
Copyright F-Response, All Rights Reserved
Updated /var/lib/f-response/config.
```

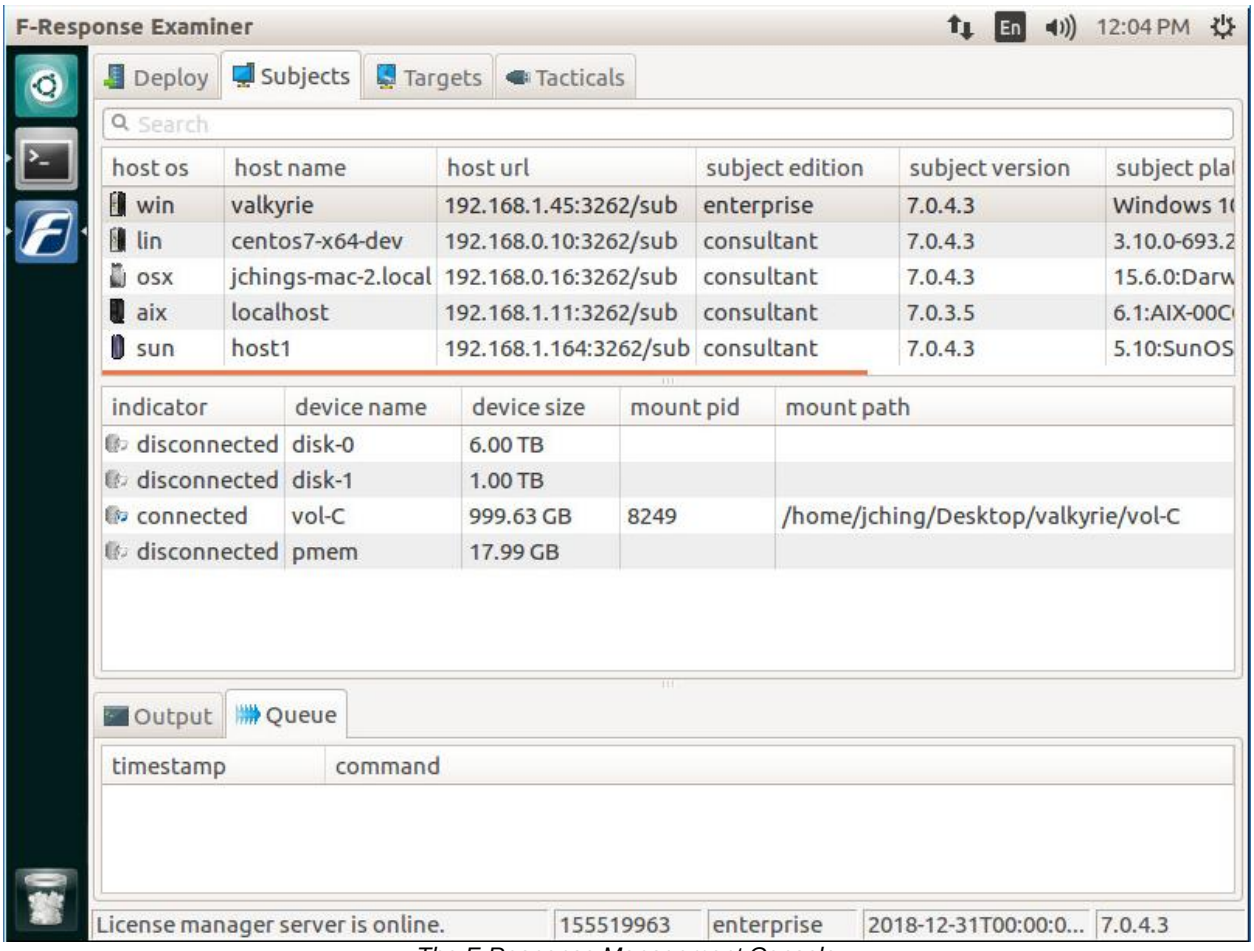
dhparam

The dhparam command generates Diffie Hellman parameters, which is encoded and written to /var/lib/f-response/dh.der.

```
$ fr_lm dhparam
F-Response Linux License Manager x.x.x.x
Copyright F-Response, All Rights Reserved
Please wait while the 1024-bit prime is being generated.
Successfully generated a 1024-bit prime using 2-generator.
Generated 1024-bit prime and 2-generator is encoded in DER format.
Diffie Hellman paramaters written to /var/lib/f-response/dh.der.
```

F-Response Management Console

Starting with F-Response version 7 each separate F-Response application has now been merged into a single F-Response Management Console. This console gives F-Response users the ability to access remote subjects from a single location and through a consistent interface.



The F-Response Management Console

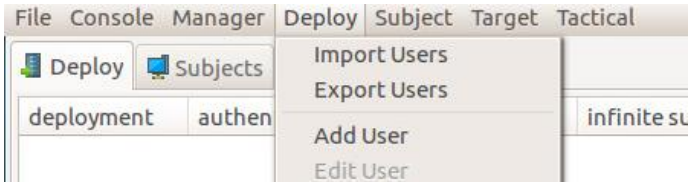
Subjects – Deploying using the Management Console

Using the Management Console to deploy and/or connect to remote Subjects

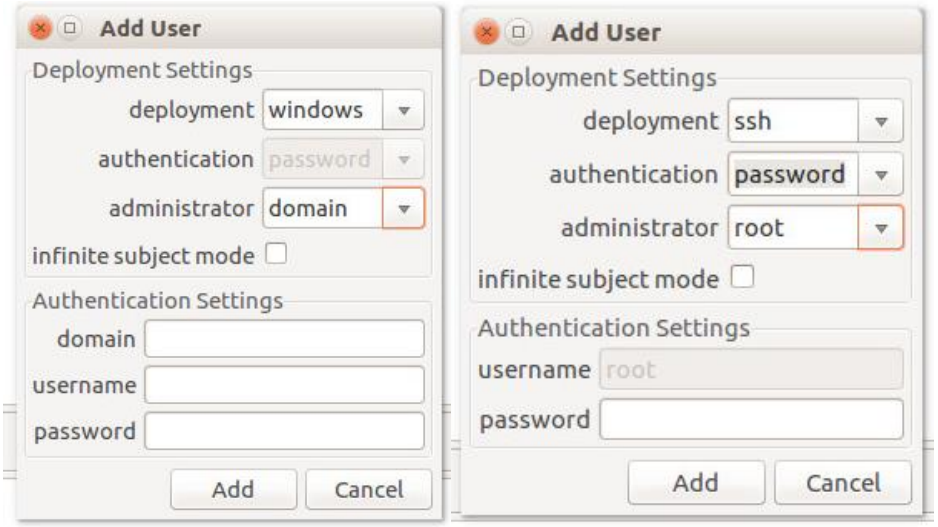
Customers using F-Response Consultant + Covert and Enterprise have the option to deploy customized subject executables to remote machines with the proper credentials.

Deploy covert Subject via the Network

Select Deploy->Add User to begin the deployment process. When prompted add one or more user accounts to access remote machines.



Add User Menu Option



Add User Dialog

Adding Windows Deployment User(s)

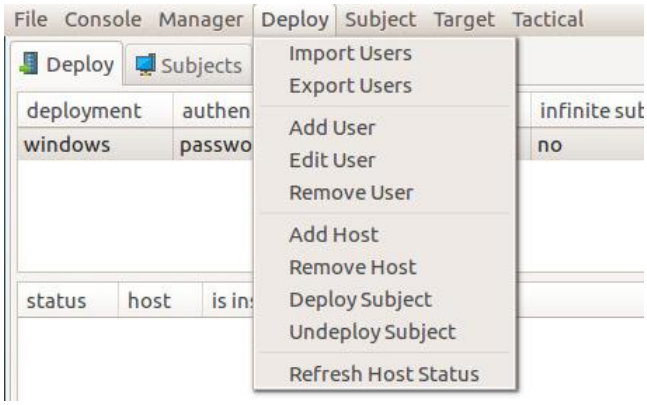
Use the “administrator” drop down to select either domain based credentials, or local machine credentials, then populate the username, password, and domain if selected. Press Add to add the user account to the console.

Adding Unix Deployment User(s)

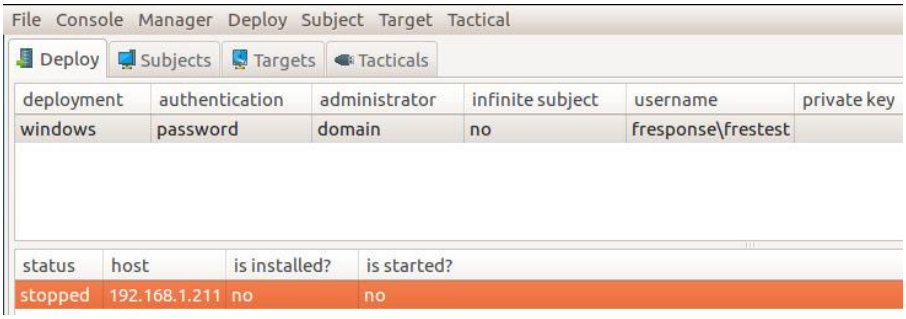
Use the “administrator” drop down to select root, sudo, or su for administrative rights and populate the username and password fields as appropriate.

Adding Hosts

Select a User and use the Add Host menu to input a list of remote hosts to deploy to using that user's account.



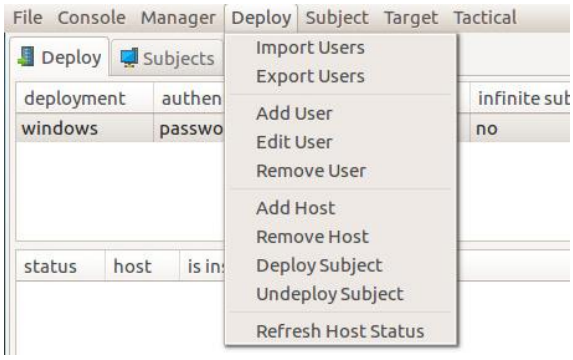
Add Host Menu Item



Newly added host for User frestest

Deploying the Subject Software

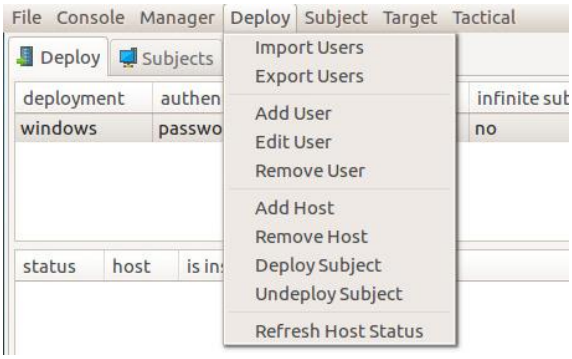
Use the Deploy->Deploy Subject menu item to select one or more hosts to deploy the F-Response Subject software to.



Deploy Subject Menu Item

Un-deploying Subject Software

Use the Deploy->Undeploy Subject menu item to select one or more hosts to remove the F-Response Subject software from.



Undeploy Subject Menu Item

Subjects – Deploying using the Command Line

Unix Deployment Interface

The Unix deployment interface implements a set of functions for installing and uninstalling the subject executable and starting and stopping the subject server on remote Unix machines. The remote computer must have a SSH server running and the user account must be either the root user or any user that can escalate privileges via `su` or `sudo`.

Authentication

The SSH deployment interface supports key and password authentication. To authenticate with a key, the -k argument with the private key path and -u argument with the username must be specified. And if the private key is password-protected, then the -w argument with the private key password must be specified. To authenticate with a password, the -u argument with the username and the -p argument with the password must be specified. If the password is not specified, then the controlling terminal will be prompted to enter a password.

```
$ fr_ssh -k ~/.ssh/id_rsa -u root -s <subject> <command>
```

```
$ fr_ssh -u root -p secret -s <subject> <command>
```

install

The install command uploads the subject executable to the remote computer. The install command selects a subject executable based on the remote computer's architecture and platform, then searches for the temporary directory, e.g. /tmp and /usr/tmp. After selecting a subject executable and finding the temporary directory, the subject executable is secure copied to the temporary directory on the remote computer.

```
$ fr_ssh -s 192.168.1.110 -u root -p secret install
F-Response Linux SSH Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Detected '155710303' license dongle with 'enterprise' license.
Detected superuser 'root'.
Connected to 192.168.1.110 on port 22.
Completed session handshake and key exchange.
Authenticated as root via password.
Detected 'linux' kernel and 'x86_64' platform.
Set source path to /var/lib/f-response/deploy/sub-lin-x86_64-consultant.
Set remote path to /tmp/fr_sub.
Uploading  0.00%        0 /  1322736 | /var/lib/f-response/deploy/sub-lin-x86_64-consultant
…
Uploading 50.80%   672000 /  1322736 | /var/lib/f-response/deploy/sub-lin-x86_64-consultant
…
Uploading 99.19%  1312000 /  1322736 | /var/lib/f-response/deploy/sub-lin-x86_64-consultant
Installed /tmp/fr_sub.
```

uninstall

The uninstall command removes the subject executable from the remote computer. If the subject executable exists in a temporary directory, then the subject is unlinked over SFTP.

```
$ fr_ssh -s 192.168.1.110 -u root -p secret uninstall
F-Response Linux SSH Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Detected '155710303' license dongle with 'enterprise' license.
Detected superuser 'root'.
```

```
Connected to 192.168.1.110 on port 22.
Completed session handshake and key exchange.
Authenticated as root via password.
Set remote path to /tmp/fr_sub.
Uninstalled /tmp/fr_sub.
```

start

The start command starts the subject server on the remote computer. The --manager argument specifies the license manager server, the --port argument specifies the subject server's listening port, and the --infinite option runs the subject server in infinite mode. By default, the license manager server is determined automatically, the subject server listens on port 3262, and the subject server runs in normal mode.

```
$ fr_ssh -s 192.168.1.110 -u root -k ~/.ssh/id_rsa start
F-Response Linux Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Set license manager ipv4 address to 192.168.1.110
Detected '155710303' license dongle with 'enterprise' license.
Detected superuser 'root'.
Connected to 192.168.1.110 on port 22.
Completed session handshake and key exchange.
Authenticated as root via /home/jching/.ssh/id_rsa.
Started subject executable '/tmp/fr_sub -m 192.168.1.110:5682/lm -k 155710303 -v -d -s 3262'.
Querying subject status -- 0 attempt.
Successfully queried subject status.
```

stop

The stop command stops the subject server on the remote computer. The --port argument specifies the listening port of the subject server. By default, the listening port is 3262.

```
$ fr_ssh -s 192.168.1.110 -u root -k ~/.ssh/id_rsa stop
F-Response Linux Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Detected '155710303' license dongle with 'enterprise' license.
F-Response Linux Examiner 7.0.4.1 Accelerator Edition
Copyright F-Response, All Rights Reserved
Cached subject file at /var/lib/f-response/cache/526911ba-6fee-4fa2-9007-bed26e50c24b/subject.
Cached targets file at /var/lib/f-response/cache/526911ba-6fee-4fa2-9007-bed26e50c24b/targets.
Subject 192.168.1.110:3262/sub received shutdown signal.
Uncached subject file at /var/lib/f-response/cache/526911ba-6fee-4fa2-9007-
bed26e50c24b/subject.
Uncached targets file at /var/lib/f-response/cache/526911ba-6fee-4fa2-9007-
bed26e50c24b/targets.
Stopped subject process on 192.168.1.110:22/ssh.
```

status

The status command checks that status of the subject executable and server.

```
$ fr_ssh -s 192.168.1.110 -u root -k ~/.ssh/id_rsa status
F-Response Linux Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Detected '155710303' license dongle with 'enterprise' license.
Detected superuser 'root'.
Connected to 192.168.1.110 on port 22.
Completed session handshake and key exchange.
Authenticated as root via /home/jching/.ssh/id_rsa.
Subject executable '/tmp/fr_sub' is installed.
Subject process '/tmp/fr_sub' is not running.
```

Windows Deployment Interface

The Windows deployment interface implements a set of functions for installing and uninstalling the subject executable and starting and stopping the subject service on remote Windows machines. For computers that are not in a domain, the UAC remote restriction on Window Vista or later must be disable. And the firewall must be configured to allow in-bound connections over port 445. Finally, the domain or local user account must have administrative privileges on the remote computer.

Authentication

The Windows deployment interface supports password authentication. The -u argument specifies the domain and username separated by two backslashes, e.g. fresponse\\frestest, or without the domain and only the username, e.g. frestest. And the -p argument specifies the password. If the -p argument is not specified, then the controlling terminal will be prompted to enter a password.

```
$ fr_win -u fresponse\\jching -p secret -s <subject> <command>
```

```
$ fr_win -u jching -p secret -s <subject> <command>
```

install

The install command uploads the subject executable to the remote computer. The install command connects to the administrative share for the disk volume C or a temporary share on the C:\ path. After connecting to a share on the C:\, the subject executable is uploaded to C:\Windows over SMB.

```
$ fr_win -s 192.168.1.45 -u fresponse\\frestest -p secret install
F-Response Linux Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Detected '155710303' license dongle with 'enterprise' license.
Detected windows 10.0.
Set share path to smb://192.168.1.45/C$/Windows.
Set source path to /var/lib/f-response/deploy/sub-win-i386-service.exe.
Set remote path to smb://192.168.1.45/C$/Windows/sub-win-i386-service.exe.
Uploading  0.00%        0 /  1169328 | /var/lib/f-response/deploy/sub-win-i386-service.exe
…

Uploading 50.44%   589824 /  1169328 | /var/lib/f-response/deploy/sub-win-i386-service.exe
…
Uploading 98.08%  1146880 /  1169328 | /var/lib/f-response/deploy/sub-win-i386-service.exe
Installed smb://192.168.1.45/C$/Windows/sub-win-i386-service.exe.
```

uninstall

The uninstall command removes the subject executable from the remote computer. If the subject executable exists in the C:\Windows directory, then the subject executable is removed over SMB.

```
$ fr_win -s 192.168.1.45 -u fresponse\\frestest -p secret uninstall
F-Response Linux Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Detected '155710303' license dongle with 'enterprise' license.
Detected windows 10.0.
Set share path to smb://192.168.1.45/C$/Windows.
Set remote path to smb://192.168.1.45/C$/Windows/sub-win-i386-service.exe.
Uninstalled smb://192.168.1.45/C$/Windows/sub-win-i386-service.exe.
```

start

The start command creates and starts the subject service on the remote computer. The --manager argument specifies the license manager server, the --port argument specifies the subject server's

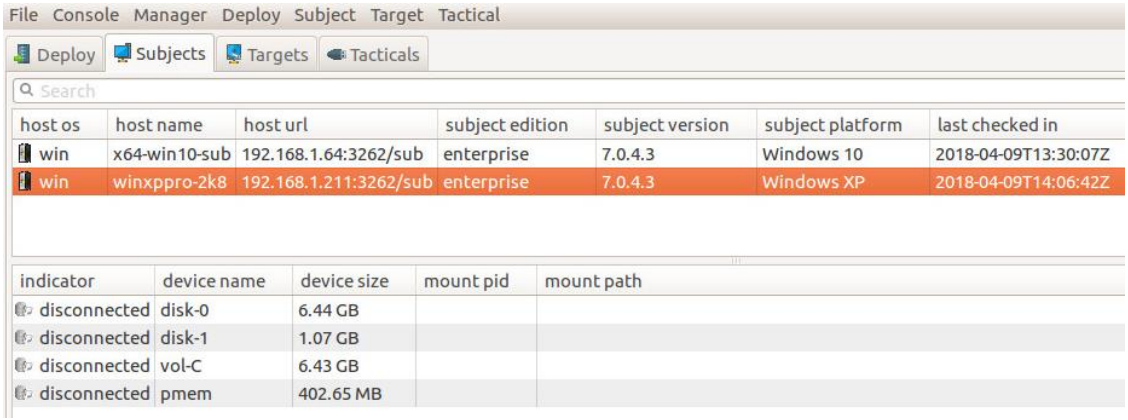
listening port, the --infinite option runs the subject server in infinite mode, the --autostart option starts the service on login after a reboot, and the --name argument specifies the service name of the subject service. By default, the license manager server is determined automatically, the subject server listens on port 3262, the subject server runs in normal mode, the subject service does not autostart, and the service name is “F-Response Subject”.

```
$ fr_win -s 192.168.1.45 -u fresponse\\frestest -p secret start
F-Response Linux Deployment 7.0.4.1
Copyright F-Response, All Rights Reserved
Set license manager ipv4 address to 192.168.1.110
Detected '155710303' license dongle with 'enterprise' license.
no talloc stackframe at ../source3/libsmb/cliconnect.c:3200, leaking memory
C:\Windows\sub-win-i386-service.exe -s "192.168.1.110:5682" -l "3262" -v "F-Response Subject" -
k "155710303".
Created subject service 'F-Response Subject'.
Started subject service 'F-Response Subject'.
Checking subject service 'F-Response Subject' status -- start pending.
Checking subject service 'F-Response Subject' status -- running.
```

Subjects – Working with Subjects using the Management Console

Listing License Managed Subjects

After starting the F-Response software on one or more remote subjects any subjects configured to use your local license manager will appear in the F-Response Management Console



Subjects currently connected to the local license manager

Selecting an individual subject from the Subjects tab will populate the targets list below.

Mounting Targets

Use the Subject->Mount Target menu item to select and mount one or more F-Response Subject Targets on your examiner machine as Live Device Files. See the section on "Using F-Response Live Device Files" for more information.

Subject Menu

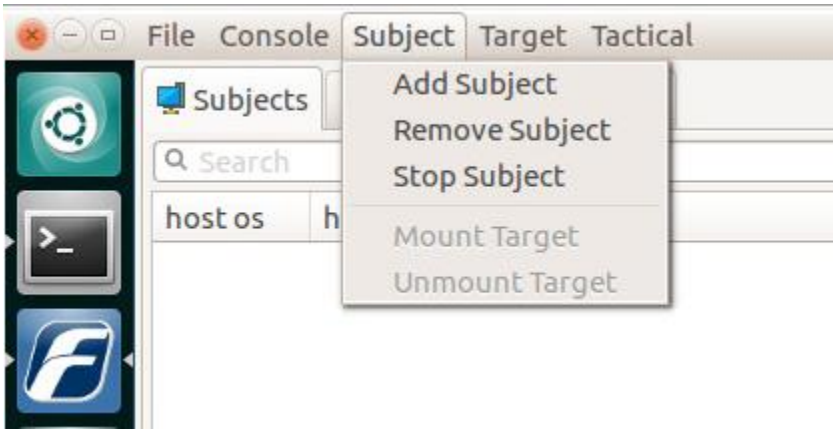
Unmounting Targets

Use the Subject->Unmount Target menu item to select and unmount one or more F-Response Subject Targets.

Subject Menu

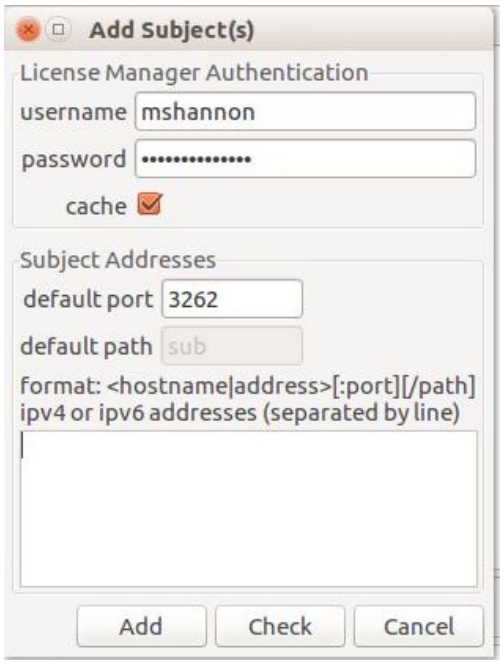
Adding Accelerator Subjects

When running the F-Response Accelerator on a machine without a local license dongle you can add remote subjects directly using their URI.



F-Response "Accelerator" Console

The first step to using the F-Response Accelerator Console to connect to remote deployed and running instances of F-Response is to make sure the F-Response Username and Password value has been set.



License Manager Authentication

Here the credentials entered should match those set up on the examiner machine with the license dongle attached, as entered in the License Manager. Next you can add one or more F-Response Subjects by inputting their full URI on into the text input at the bottom of the dialog.

Provided the username and password configured earlier are correct and there were no issues communicating with the remote subjects you should see icons for them appear in the Subjects panel.

Subjects – Working with Subjects using the Command Line

The F-Response Linux Examiner also includes a complete set of command line tools for enumerating and connecting to remote subjects and targets.

Examiner Interface

The examiner interface implements a set of functions for mounting and unmounting targets, stopping subjects, and printing the subject and target list.

cache

The cache command prints the subject list in CSV format. If the -s or --subject argument is specified, then the target list of the subject is printed in CSV format. And if the -j or --json option is specified, then the subject or target list is printed in JSON format.

```
$ fr_exa cache
name,platform,url,version
"centos6-x64-dev","2.6.32-642.3.1.el6.x86_64:Linux-x86_64","192.168.1.110:3262/sub","7.0.4.1"
```

```
$ fr_exa cache -s centos6-x64-dev
name,block_size,block_count,pid,mount_path
"vg_centos6x64dev-lv_root","512","29171712","0",""
"vg_centos6x64dev-lv_swap","512","3350528","0",""
"sda","512","33554432","0",""
"sda1","512","1024000","0",""
"sda2","512","32528384","0",""
"sdb","512","4194304","0",""
"sdc","512","83886080","0",""
"sdc1","512","83875302","0",""
"sdd","512","15482880","0",""
"sdd1","512","15474816","0",""
"sde","512","15482880","0",""
"sde1","512","15474816","0",""
```

mount

The mount command creates a target file on the mount path. The target file represents a device on the subject, i.e. reading from the target file is equivalent to reading from the device on the subject.

The subject, target, and mount path argument must be specified. The -s or --subject argument specifies the IPv4 address, IPv6 address, or resolvable hostname and the listening port of the subject, e.g. 192.168.1.1.110:3262 or centos6-x64-dev:3262. The -t or --target argument specifies the name of the target. And the -m or --mount argument specifies the mount path.

By default, the mount command runs in the foreground. If the -d or --daemon option is specified, then the mount command runs in the background.

```
$ fr_exa mount --subject centos6-x64-dev --target sda --mount ~/mnt --daemon
F-Response Linux Examiner 7.0.4.1
Copyright F-Response, All Rights Reserved
Connected to subject 192.168.1.110:3262/sub.
Connected to target sda.
Exported target on /home/frestest/mnt/centos6-x64-dev/sda.
Examiner worker is online and running in the background.
Exclude -d, --daemon on command line to run in foreground.
```

active

The active command prints the active target list in CSV format. If the -j or --json option is specified, then the active target list is printed in JSON format.

```
$ fr_exa active --json
{
    "subjects": [
        {
```

```
            "address": "192.168.1.110",
            "hostname": "centos6-x64-dev",
            "module": "consultant",
            "path": "/sub",
            "platform": "2.6.32-642.3.1.el6.x86_64:Linux-x86_64",
            "port": "3262",
            "seconds": "131533406930000000",
            "subject_type": "lin",
            "targets": [
                {
                    "block_count": "33554432",
                    "block_size": 512,
                    "id": 2,
                    "mount_path": "/home/jching/mnt/centos6-x64-dev/sda",
                    "name": "sda",
                    "pid": "3242",
                    "type": 1
                }
            ],
            "time": "2017-10-24T17:44:53Z",
            "uuid": "90b190b7-bfc8-4cde-9258-5b535c643aa6",
            "version": "7.0.4.1"
        }
    ]
}
```


umount

The umount command removes the target file.

```
$ fr_exa umount --subject centos6-x64-dev --target sda
F-Response Linux Examiner x.x.x.x
Copyright F-Response, All Rights Reserved
Founded subject centos6-x64-dev.
Founded target sda.
Successfully unmounted /home/frestest/mnt/centos6-x64-dev/sda.
```

stop

The stop command stops the subject server or service.

```
$ fr_exa stop --subject centos6-x64-dev
F-Response Linux Examiner x.x.x.x
Copyright F-Response, All Rights Reserved
Subject 192.168.1.110:3262/sub received shutdown signal.
```

Using F-Response Live Device Files

The examiner and accelerator export a live device file that represents a raw device on the subject. The following examples cover how to mount the live device file as a loopback device and process it with multiple open source tools.

Mounting the target file on a loopback device

You must have an attached device to make use of the SIFT workstation provided filesystem and partition table support. Since the target file is not an attached device it must be mounted as a loopback device.

```
$ fr_exa mount -s 192.168.1.45 -t vol-C -m . -d
F-Response Linux Examiner 7.0.4.1
Copyright F-Response, All Rights Reserved
Connected to subject 192.168.1.45:3262/sub.
Connected to target vol-C.
Exported target on /home/frestest/valkyrie/vol-C.
Examiner worker is online and running in  the background.
Exclude -d,--daemon on command line to run in foreground.
```

```
$ sudo losetup /dev/loop0 /home/frestest/valkyrie/vol-C/vol-C
```

```
$ sudo losetup -a
/dev/loop0: [0041]:2 (/home/frestest/valkyrie/vol-C/vol-C)
```

Mounting an NTFS filesystem from a loopback device

```
$ sudo mount -o ro /dev/loop0 mnt
```

```
$ ls -l mnt
total 29621533
drwxrwxrwx 1 root root           0 Jun 14 14:37 AMD
-rwxrwxrwx 1 root root           1 Oct 30  2015 BOOTNXT
drwxrwxrwx 1 root root        4096 Sep 11  2015 eclipse
-rwxrwxrwx 1 root root 12883050496 Aug 15 15:17 hiberfil.sys
drwxrwxrwx 1 root root           0 Jun 14 18:22 inetpub
-rwxrwxrwx 1 root root      904704 Dec  2  2006 msdia80.dll
-rwxrwxrwx 1 root root 17179869184 Aug 15 15:17 pagefile.sys
drwxrwxrwx 1 root root           0 Mar 18 21:03 PerfLogs
drwxrwxrwx 1 root root        4096 Aug 10 20:25 Perl64
drwxrwxrwx 1 root root        8192 Jul 19 16:54 ProgramData
drwxrwxrwx 1 root root       20480 Aug 16 13:41 Program Files
drwxrwxrwx 1 root root       20480 Aug 10 20:37 Program Files (x86)
drwxrwxrwx 1 root root        4096 Oct  7  2015 Python26
drwxrwxrwx 1 root root        4096 Aug 15  2016 Python27
drwxrwxrwx 1 root root           0 Jun 14 15:31 Recovery
drwxrwxrwx 1 root root        4096 Mar 25 13:43 $Recycle.Bin
-rwxrwxrwx 1 root root   268435456 Aug 15 15:17 swapfile.sys
drwxrwxrwx 1 root root        8192 Aug 18 15:46 System Volume Information
drwxrwxrwx 1 root root        4096 Jun 14 14:52 Users
drwxrwxrwx 1 root root       49152 Feb 11  2015 websymbols
drwxrwxrwx 1 root root       28672 Aug 10 17:35 Windows
```

Running Sleuthkit utilities on the device file

The `fls` utility prints the list of inodes and the `icat` utility writes the file content to stdout. In this example, `fls` is used to list the inodes of the root of a NTFS filesystem and the `icat` is used to retrieve the $MFT.

```
$ fls /dev/loop0
…
r/r 4-128-4:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
```

```
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
d/d 57-144-5:   $Recycle.Bin
r/r 9-144-17:   $Secure:$SDH
r/r 9-144-16:   $Secure:$SII
r/r 9-128-19:   $Secure:$SDS
r/r 10-128-1:   $UpCase
r/r 10-128-4:   $UpCase:$Info
r/r 3-128-3:    $Volume
…
```

```
$ icat /dev/loop0 0-128-1 > MFT
```

Running Volatility commands on the target file

In this example, a Windows 10 host is running the subject service and the physical memory target, i.e. pmem, is mounted and analyzed by Volatility[8] to obtain a list of running processes. Note that physical memory is only supported on Windows.

```
$ fr_exa mount -m . -s valkyrie -t pmem -d
F-Response Linux Examiner 7.0.4.1
Copyright F-Response, All Rights Reserved
Connected to subject 192.168.1.45:3262/sub.
Connected to target pmem.
Exported target on /home/jching/Desktop/valkyrie/pmem.
Examiner worker is online and running in  the background.
Exclude -d,--daemon on command line to run in foreground.
```

```
$ python /usr/bin/vol.py --profile Win10x64_14393 -f /home/jching/Desktop/valkyrie/pmem/pmem
pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ -----------
------------------- ------------------------------
0xffffcf877a020678                            4      0 22...0        0 ------      0 6171-06-10
06:11:23 UTC+0000
0xffffcf877d953038 p??}????smss.exe         456      0 21...4        0 ------      0 6235-10-10
07:30:54 UTC+0000
0xffffcf877e0bc7b8 ??"}????csrss.ex         560      0 21...0        0 ------      0 6236-08-31
02:15:52 UTC+0000
0xffffcf877dec97b8                          668      0 21...4        0 ------      0 6692-05-05
19:05:23 UTC+0000
…
```

Mounting the target file as a raw disk image (OSX)

The target file can be attached as a raw disk image using `hdiutil` and mounted as a filesystem using `diskutil`. In the example below, a windows 10 host with a VHD disk containing a FAT filesystem is mounted with the examiner.

```
$ fr_exa mount -s valkyrie -t disk-2 -m . -d
F-Response OSX Examiner x.x.x.x
Copyright F-Response, All Rights Reserved
Connected to subject 192.168.1.45:3262/sub.
Connected to target disk-2.
Exported target on /Users/frestest/Desktop/valkyrie/disk-2.
Examiner worker is online and running in  the background.
Exclude -d,--daemon on command line to run in foreground.
```

```
$ sudo hdiutil attach -imagekey diskimage-class=CRawDiskImage -nomount
/Users/frestest/Desktop/valkyrie/disk-2/disk-2
/dev/disk5              FDisk_partition_scheme
```

[8] http://www.volatilityfoundation.org/

```
/dev/disk5s1            Windows_FAT_16
```

```
$ sudo diskutil mount readOnly -mountPoint mnt /dev/disk5s1
Volume TESTVHD2GB on /dev/disk5s1 mounted
```

```
$ ls -l mnt
total 64
drwxrwxrwx  1 frestest  staff  32768 Aug 24 11:15 System Volume Information
```

```
$ sudo diskutil umount mnt
Volume TESTVHD2GB on disk5s1 unmounted
```

```
$ sudo hdiutil detach /dev/disk5
"disk5" unmounted.
"disk5" ejected.
```

```
$ fr_exa umount -s valkyrie -t disk-2
F-Response OSX Examiner x.x.x.x
Copyright F-Response, All Rights Reserved
Founded subject valkyrie.
Founded target disk-2.
Unmount successful for /Users/frestest/Desktop/valkyrie/disk-2
Successfully unmounted /Users/frestest/Desktop/valkyrie/disk-2.
```

Flexdisk™ API

Getting Started

Access to the Flexdisk™ API is available from any platform capable of issuing HTTPS URL based web queries, including all mobile device platforms. Accessing the Flexdisk™ is very simple, it was designed to be straight forward and universally accessible from most web friendly programming environments.

API Overview

The F-Response Flexdisk™ API consists of two main parts, flexd and hscsi.

/flexd?	/hscsi?
Explore, Read, Extract Provides access to file system structures and meta data.	**Read** Provides read access to physical device (memory) raw data.

Authentication

Access to the Flexdisk™ is protected using standard HTTP Basic Authentication over SSL. All web queries are authenticated using this model.

Data Encoding

Unless otherwise indicated the Flexdisk™ API makes use of the Javascript Object Notation (JSON) data encoding format. JSON is well documented in the industry and there are numerous libraries capable of manipulating JSON encoded content. More details on JSON and consuming JSON in your applications is available at http://www.json.org/.

Flexdisk™ Web Request and Response Values

Flexdisk™ Web Query Request Arguments

Request	Meaning	Values	Notes
tgt	Target	vol-C, rdisk0	Indicates the target name as provided by the main Flexdisk™ handler.
enc	Encoding	json, csv, html	Instructs the Flexdisk™ handler to return the output in one of three potential encoding formats, JSON, CSV, or HTML. Default is HTML unless otherwise configured
node	File or Directory Node value	<numeric>	Indicates the desired node by numeric value.
type	Response value type	data, meta, read	Indicates the desired value type, data for accessing the entire file, meta for file metadata, or read for reading from a select location within a file.
name	File or Directory Name	<text>	Indicates the name of the file or directory requested.
offset	File Offset to start at	<numeric>	Valid only for Read Operations (type=read), value in bytes.
len	Length of file content to obtain	<numeric>	Valid only for Read Operations (type=read), value in bytes.

Flexdisk™ Web Query Response Values (JSON Encoded Responses Only)

Response	Meaning	Values	Notes
name	Name of the object returned	<text>	Indicates the name of the returned object, depending on usage it may be a file, directory, or a disk/device.
type	Type of object returned	<text>	Indicates the type of the returned object. Examples include “ntfs” for file system type, or dir for directory node type.
uri	URL used to access the specific object	<url>	Provides a URL to access the object (data or explore) depending on the object.
node	Node value	<numeric>	Numeric identifier for a given object.
sectorsize	Size of a single sector	<numeric>	Indicates the Sector Size of a target device.
volsize	Size of the device	<numeric>	Indicates the size of the target device.
atime	Access Time	<unix time>	Indicates the last access time in unix time.
atime_hires	Access Time	<win32 time>	Indicates the last access time in win32 time, where available.
ctime	Change Time	<unix time>	Indicates the changed time on Ext2/3/4 and the Entry Modified Time on NTFS.
ctime_hires	Change Time	<win32 time>	Indicates the changed time on Ext2/3/4 and the Entry Modified Time on NTFS in win32 time.
crtime	Create Time	<unix time>	Indicates the Created time on FAT and NTFS.
crtime_hires	Create Time	<win32 time>	Indicates the Created time on FAT and NTFS in win32 time.
mtime	Modified Time	<unix time>	Indicates the Modified time on Ext2/3/4, the written time on FAT, and the File Modified Time on NTFS.
mtime_hires	Modified Time	<win32 time>	Indicates the Modified time on Ext2/3/4, the written time on FAT, and the File Modified Time on NTFS in Win32 time.
bkuptime	Backup Time (OSX)	<unix time>	Indicates the Backup time on HFS.

dtime	Deleted Time (Linux)	<unix time>	Indicates the Deleted time on Ext2/3.
host	Hostname	<text>	Hostname of the target machine.
date	Date	<datetime>	Date/Time of the completed query response.

Flexdisk™ Sample Queries

Obtain a listing of all Flexdisks™ on the target computer (JSON encoded)

Sample Request (Python): https://<host>:<port>/flexd?enc=json

```
import json
import requests
requests.packages.urllib3.disable_warnings()

credential = requests.auth.HTTPBasicAuth('default', 'default')
url = 'https://192.168.1.110:3262/flexd?enc=json'
request = requests.get(url, auth = credential, verify = False)
print json.dumps(request.json(), sort_keys=True, indent=4, separators=(',', ': '))
```

Sample Response:

```
{
    "response": {
        "contents": [
            {
                "name": "vg_centos6x64dev-lv_root",
                "sectorsize": "512",
                "type": "ext4",
                "uri": "https://192.168.1.110:3262/flexd?tgt=vg_centos6x64dev-
lv_root&enc=json",
                "volsize": "14935916544"
            },
            {
                "name": "sda1",
                "sectorsize": "512",
                "type": "ext4",
                "uri": "https://192.168.1.110:3262/flexd?tgt=sda1&enc=json",
                "volsize": "524288000"
            }
        ],
        "date": "Thu, 10 Aug 2017 10:02:12 (EDT)",
        "host": "192.168.1.110:3262"
    }
}
```

Obtain a listing of the content for the root of a provided Flexdisk™ (JSON encoded)

Sample Request (Python): https://<host>:<port>/flexd?enc=json&tgt=<target>

```
import json
import requests
requests.packages.urllib3.disable_warnings()

credential = requests.auth.HTTPBasicAuth('default', 'default')
url = 'https://192.168.1.110:3262/flexd?enc=json&tgt=vg_centos6x64dev-lv_root'
request = requests.get(url, auth = credential, verify = False)
print json.dumps(request.json(), sort_keys=True, indent=4, separators=(',', ': '))
```

Sample Response:

```
{
```

```
   "response" : {
       "host": "192.168.1.110:3262",
       "date": "Fri, 11 Aug 2017 09:58:52 (EDT)",
       "contents": [
           …
           {
              "name": "dev",
              "size": "4096",
              "type": "dir",
              "state": "alloc",
              "uri": "https://192.168.1.110:3262/flexd?tgt=vg_centos6x64dev-
lv_root&node=260609&enc=json&name=dev",
              "node": "260609",
              "atime":"1470333601",
              "atime_hires":"1311480728179999945",
              "ctime":"1470333601",
              "ctime_hires":"1311480728279999943",
              "crtime":"1470333601",
              "crtime_hires":"1311480728179999945",
              "mtime":"1470333601",
              "mtime_hires":"1311480728179999945",
              "bkuptime":"0",
              "dtime":"0"
           }
           …
       ]
   }
}
```

Extract a given allocated or unallocated file based on the node.

Sample Request (Python):

https://<host>:<port>/flexd?type=data&tgt=<target>&node=<node>&name=<filename>

```
import json
import requests
import Crypto.Hash.MD5
requests.packages.urllib3.disable_warnings()

# create https session (keepalive)
with requests.Session() as session:
    credential = requests.auth.HTTPBasicAuth('default', 'default')

    # node and file paramaters are
    # obtain via directory request
    host = '192.168.1.110:3262'
    target = 'vg_centos6x64dev-lv_root'
    node = 393680
    file = 'sub-lin-x86_64-consultant'
    url = 'https://{0}/flexd?type=data&tgt={1}&node={2}&name={3}'.format(host, target, node,
file)

    md5 = Crypto.Hash.MD5.new()

    # md5 the file  using a
    # buffer size of 524288
    offset = 0
    length = 4321409
    stream = session.get(url, auth = credential, verify = False, stream = True)
    for buffer in stream.iter_content(chunk_size = 524288):
        md5.update(buffer)
        offset = offset + len(buffer)
        length = length - len(buffer)
        print '{0:3.2f}%\r'.format(100 * (float(offset) / (offset + length))),
    print '{0}'.format(md5.hexdigest())
```

Sample Response:

A stream of file content (chunk encoding) from specified node.

Obtain a listing of the content for a given directory node of selected Flexdisk™ (JSON encoded)

Sample Request (Python): https://<host>:<port>/flexd?enc=json&tgt=<target>&node=<node>

```
import json
import requests
requests.packages.urllib3.disable_warnings()

credential = requests.auth.HTTPBasicAuth('default', 'default')
target = 'vg_centos6x64dev-lv_root'
node = 260610
directory = 'root'
url = 'https://192.168.1.110:3262/flexd?enc=json&tgt={0}&node={1}&name={2}'.format(target,
node, directory)
request = requests.get(url, auth = credential, verify = False)
print json.dumps(request.json(), sort_keys=True, indent=4, separators=(',', ': '))
```

Sample Response:

```
{
    "response": {
        "contents": [
            {
                "atime": "1502370970",
                "atime_hires": "131468446104637471",
                "bkuptime": "0",
                "crtime": "1471015743",
                "crtime_hires": "131154893760015088",
                "ctime": "1480707734",
                "ctime_hires": "131251814300892295",
                "dtime": "0",
                "ext": "sh",
                "mtime": "1480707633",
                "mtime_hires": "0",
                "name": "sync.sh",
                "node": "273085",
                "size": "380",
                "state": "alloc",
                "type": "file",
                "uri": "https://192.168.1.110:3262/flexd?tgt=vg_centos6x64dev-
lv_root&node=273085&type=data&name=sync.sh"
            }
        ],
        "date": "Fri, 11 Aug 2017 10:37:39 (EDT)",
        "host": "192.168.1.110:3262"
    }
}
```

Read from a given location in a file node.

Sample Request (Python):

```
import json
import requests
import Crypto.Hash.MD5
requests.packages.urllib3.disable_warnings()

# create https session (keepalive)
with requests.Session() as session:
    credential = requests.auth.HTTPBasicAuth('default', 'default')

    # node and file paramaters are
```

```
    # obtain via directory request
    host = '192.168.1.110:3262'
    target = 'vg_centos6x64dev-lv_root'
    node = 393680
    file = 'sub-lin-x86_64-consultant'

    md5 = Crypto.Hash.MD5.new()

    # md5 the file  using a
    # buffer size of 524288
    offset = 0
    length = 4321409
    while 0 < length:
        url = 'https://{0}/flexd?type=data&tgt={1}&node={2}&name={3}&offset={4}' \
        '&len={5}'.format(host, target, node, file, offset, min(524288, length))
        buffer = session.get(url, auth = credential, verify = False, stream = False).content

        md5.update(buffer)
        offset = offset + len(buffer)
        length = length - len(buffer)
        print '{0:3.2f}%\r'.format(100 * (float(offset) / (offset + length))),
    print '{0}'.format(md5.hexdigest())
```

Sample Response:

A block of file content from specified node[9].

[9] We recommended streaming the file content versus issuing a separate HTTPS requests for each block of data

hSCSI™ Web Request and Response Values

hSCSI™ Web Query Request Arguments

Request	Meaning	Values	Notes
tgt	Target	fdisk-0	Indicates the target name as provided by the main hSCSI™ handler.
offset	File Offset to start at	<numeric>	Valid only for Read Operations (type=read), value in blocks.
len	Length of file content to obtain	<numeric>	Valid only for Read Operations (type=read), value is number of blocks. Total size may not be larger than 65535 bytes (Ex. 1 Block = 512 bytes, max read is 126 blocks)

hSCSI™ Web Query Response Values (JSON Encoded Responses Only)

Response	Meaning	Values	Notes
name	Name of the object returned	<text>	Indicates the name of the returned object, depending on usage it may be a file, directory, or a disk/device.
type	Type of object returned	<text>	Indicates the type of the returned object. Examples include disk, pmem, etc.
uri	URL used to access the specific object	<url>	Provides a URL to access the object (data or explore) depending on the object.
blocksz	Size of a single sector	<numeric>	Indicates the block size (sector size) of a target hSCSI™ device.
blockc	Count of sectors	<numeric>	Indicates the total block(sector) count.
disksize	Size of the disk in bytes	<unix time>	Indicates the total device size in bytes.
host	Hostname	<text>	Hostname of the target machine.
date	Date	<datetime>	Date/Time of the completed query response.

hSCSI™ Sample Queries

Obtain a listing of all hSCSI™ targets on the target computer (JSON encoded)

Sample Request (Python): https://<host>:<port>/hscsi?

```
import json
import requests
requests.packages.urllib3.disable_warnings()

credential = requests.auth.HTTPBasicAuth('default', 'default')
url = 'https://192.168.1.110:3262/hscsi?'
request = requests.get(url, auth = credential, verify = False)
print json.dumps(request.json(), sort_keys=True, indent=4, separators=(',', ': '))
```

Sample Response:

```
{
    "response": {
        "contents": [
            {
                "blockc": "33554432",
                "blocksz": "512",
                "disksize": "17179869184",
                "name": "sda",
                "type": "physical",
                "uri": "https://192.168.1.110:3262/hscsi?tgt=sda"
            },
```

```
            {
                "blockc": "1024000",
                "blocksz": "512",
                "disksize": "524288000",
                "name": "sda1",
                "type": "physical",
                "uri": "https://192.168.1.110:3262/hscsi?tgt=sda1"
            },
            {
                "blockc": "32528384",
                "blocksz": "512",
                "disksize": "16654532608",
                "name": "sda2",
                "type": "physical",
                "uri": "https://192.168.1.110:3262/hscsi?tgt=sda2"
            }
        ],
        "date": "Fri, 11 Aug 2017 11:17:37 (EDT)",
        "host": "192.168.1.110:3262"
    }
}
```


Read from a given location in a hSCSI™ target

Sample Request (Python): https://<host>:<port>/hscsi?tgt=<target>&offset=<offset>&len=<length>

```
import json
import requests
import Crypto.Hash.MD5
requests.packages.urllib3.disable_warnings()

# create https session (keepalive)
with requests.Session() as session:
    credential = requests.auth.HTTPBasicAuth('default', 'default')

    # node and file paramaters are
    # obtain via directory request
    host = '192.168.1.110:3262'
    target = 'sda1'

    md5 = Crypto.Hash.MD5.new()

    # md5 the file  using a
    # buffer size of 524288
    offset = 0
    length = 524288000
    while 0 < length:
        url = 'https://{0}/hscsi?tgt={1}&offset={2}&len={3}' \
        .format(host, target, offset / 512, min(524288 / 512, length / 512))
        buffer = session.get(url, auth = credential, verify = False, stream = False).content
        if len(buffer) <= 0:
            break

        md5.update(buffer)
        offset = offset + len(buffer)
        length = length - len(buffer)
        print '{0:3.2f}%\r'.format(100 * (float(offset) / (offset + length))),
    print '{0}'.format(md5.hexdigest())
```

Sample Response:

A block of data from specified target.

Appendix A.

Legal Notices

Trademarks

F-Response is a trademark of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC's IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.

Patents

F-Response is covered by United States Patent Numbers: 8,171,108; 7,899,882; 9,037,630; 9,148,418, and other Patents Pending.

Appendix B.

Release History

F-Response 8.0.1.X contains the following new features and enhancements:

Changes affecting all versions

- New F-Response release

F-Response 7.0.4.4 contains the following new features and enhancements:

Changes affecting Enterprise, Consultant + Covert, Consultant Edition, and TACTICAL

- Improved NTFS volume shrink during VHD/E01 virtual image creation.
- Improved handling of > 2TB devices.
- Generates a single e01 file for physical images.
- Corrected Accelerator menu and window title to better reflect usage.
- Moved comprehensive logs to the system32\LogFiles directory by process.
- Corrected issue with event logs for subject access and operation notification.
- Improved Linux Examiner graphical user interface and command line tools.
- Corrected Windows Export UI to account for all available interfaces.
- Fixed a menu issue with the F-Response Accelerator for Consultant + Covert.
- Corrected TACTICAL Subject for Windows to properly handle Windows XP.

F-Response 7.0.3.1 contains the following new features and enhancements:

Changes affecting Enterprise, Consultant + Covert, Consultant Edition, and TACTICAL

- Additional error messages for failed MSI exports and Provider drive attach operations.
- Corrected issue with IMAP not offering full drive attachment.
- Moved crashfiles and/or bad input error logs from the user's profile to the system TEMP directory.
- Corrected TACTICAL license backup and restore process in cases where folder paths don't exist.
- Improved handling of cloud accounts with filenames too large to be displayed.
- Updated manual with additional Linux and OSX examiner command line tool details.
- Implemented SSH and windows deployment interfaces for Linux.
- Modified F-Response Linux Examiner JSON output to improve key-value readability.
- Network settings to improve stability on busy and idle connections.
- Improved version requirements for F-Response Linux Examiner system dependencies.
- Updated man pages and manual for Linux and Mac OS X.

Appendix C.

Master Software License Agreement

AGILE RISK MANAGEMENT LLC MASTER SOFTWARE LICENSE AGREEMENT

TERMS AND CONDITIONS

1. Scope of Agreement; Definitions. This Agreement covers the license and permitted use of the Agile Risk Management LLC ("Agile") F-Response Software. Unless otherwise defined in this section, the capitalized terms used in this Agreement shall be defined in the context in which they are used. The following terms shall have the following meanings:

1.1. "Agile Software" or "Software" means any and all versions of Agile's F-Response software and the related "Documentation" as defined below.

1.2. "Customer" or "Licensee" means the person or entity identified on the invoice and only such person or entity, Customer shall not mean any assigns, heirs, or related persons or entities or claimed third-party beneficiaries of the Customer.

1.3. "Documentation" means Agile release notes or other similar instructions in hard copy or machine readable form supplied by Agile to Customer that describes the functionality of the Agile Software.

1.4. "License Term" means the term of the applicable license as specified on an invoice or as set forth in this Agreement.

2. Grant of Software License.

2.1. Enterprise License. Subject to the terms and conditions of this Agreement only, Agile grants Customer a non-exclusive, non-transferable license to install the Agile Software and to use the Agile Software during the License Term, in object code form only.

2.2. Third Party Software. Customer acknowledges that the Agile Software may include or require the use of software programs created by third parties, and the Customer acknowledges that its use of such third party software programs shall be governed exclusively by the third party's applicable license agreement.

3. Software License Restrictions.

3.1. No Reverse Engineering; Other Restrictions. Customer shall not, directly or indirectly: (i) sell, license, sublicense, lease, redistribute or transfer any Agile Software; (ii) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, or distribute any Agile Software; (iii) rent or lease any rights in any Agile Software in any form to any entity; (iv) remove, alter or obscure any proprietary notice, labels or marks on any Agile Software. Customer is responsible for all use of the Software and for compliance with this Agreement and any applicable third party software license agreement.

3.2. Intellectual Property. Agile retains all title, patent, copyright and other intellectual proprietary rights in, and ownership of, the Agile Software regardless of the type of access or media upon which the original or any copy may be recorded or fixed. Unless otherwise expressly stated herein, this Agreement does not transfer to Customer any title, or other ownership right or interest in any Agile Software. Customer does not acquire any rights, express or implied, other than those expressly granted in this Agreement.

4. Ordering & Fulfillment. Unless otherwise set forth in an Agile-generated Estimate pricing is set forth on the F-Response website and is subject to change at any time. Each order shall be subject to Agile's reasonable acceptance. Unless otherwise set forth in an Agile generated Estimate. Delivery terms are FOB Agile's shipping point.

5. Payments. Customer agrees to pay amounts invoiced by Agile for the license granted under this Agreement. If any authority imposes a duty, tax or similar levy (other than taxes based on Agile's income), Customer agrees to pay, or to promptly reimburse Agile for, all such amounts. Unless otherwise indicated in an invoice, all Agile invoices are payable thirty (30) days from the date of the invoice. Agile reserves the right to charge and Customer agrees to pay Agile for every unauthorized copy or unauthorized year an amount equal to the cost per copy, per year, per computer, or per user, whichever is greater, as a late payment fee in the event Customer fails to remit payments when due or Customer otherwise violates the payment provisions of this Agreement. In addition to any other rights set forth in this Agreement, Agile may suspend performance or withhold fulfilling new Customer orders in the event Customer has failed to timely remit payment for outstanding and past due invoices.

6. Confidentiality.

6.1. Definition. "Confidential Information" means: (a) any non-public technical or business information of a party, including without limitation any information relating to a party's techniques, algorithms, software, know-how, current and future products and services, research, engineering, vulnerabilities, designs, financial information, procurement requirements, manufacturing, customer lists, business forecasts, marketing plans and information; (b) any other information of a party that is disclosed in writing and is conspicuously designated as "Confidential" at the time of disclosure or that is disclosed orally and is identified as "Confidential" at the time of disclosure; or (c) the specific terms and conditions of this Agreement.

6.2. Exclusions. Confidential Information shall not include information which: (i) is or becomes generally known to the public through no fault or breach of this Agreement by the receiving Party; (ii) the receiving Party can demonstrate by written evidence was rightfully in the receiving Party's possession at the time of disclosure, without an obligation of confidentiality; (iii) is independently developed by the receiving Party without use of or access to the disclosing Party's Confidential Information or otherwise in breach of this Agreement; (iv) the receiving Party rightfully obtains from a third party not under a duty of confidentiality and without restriction on use or disclosure, or (v) is required to be disclosed pursuant to, or by, any applicable laws, rules, regulatory authority, court order or other legal process to do so, provided that the Receiving Party shall, promptly upon learning that such disclosure is required, give written notice of such disclosure to the Disclosing Party.

6.3. Obligations. Each Party shall maintain in confidence all Confidential Information of the disclosing Party that is delivered to the receiving Party and will not use such Confidential Information except as expressly permitted herein. Each Party will take all reasonable measures to maintain the confidentiality of such Confidential Information, but in no event less than the measures it uses to protect its own Confidential Information. Each Party will limit the disclosure of such Confidential Information to those of its employees with a bona fide need to access such Confidential Information in order to exercise its rights and obligations under this Agreement provided that all such employees are bound by a written non-disclosure agreement that contains restrictions at least as protective as those set forth herein.

6.4. Injunctive Relief. Each Party understands and agrees that the other Party will suffer irreparable harm in the event that the receiving Party of Confidential Information breaches any of its obligations under this section and that monetary damages will be inadequate to compensate the non-breaching Party. In the event of a breach or threatened breach of any of the provisions of this section, the non-breaching Party, in addition to and not in limitation of any other rights, remedies or damages available to it at law or in equity, shall be entitled to a temporary restraining order, preliminary

injunction and/or permanent injunction in order to prevent or to restrain any such breach by the other Party.

7. DISCLAIMER OF WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AGILE AND ITS SUPPLIERS PROVIDE THE SOFTWARE AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, DUTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, OF ACCURACY OR COMPLETENESS OF RESPONSES, OF RESULTS, OF WORKMANLIKE EFFORT, OF LACK OF VIRUSES, AND OF LACK OF NEGLIGENCE, ALL WITH REGARD TO THE SOFTWARE, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.

8. Limitations and Exclusions.

8.1. Limitation of Liability and Remedies. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES IN CONTRACT OR ANY OTHER THEORY IN LAW OR IN EQUITY), THE ENTIRE LIABILITY OF EITHER PARTY AND WITH RESPECT TO AGILE, ANY OF ITS SUPPLIERS, UNDER ANY PROVISION OF THIS AGREEMENT AND THE EXCLUSIVE REMEDY HEREUNDER SHALL BE LIMITED TO THREE TIMES THE TOTAL AMOUNT PAID BY CUSTOMER FOR THE LICENSE; PROVIDED, HOWEVER THAT THIS LIMITATION DOES NOT APPLY TO ANY OF THE FOLLOWING: (A) A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT; OR (B) ANY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT BY A PARTY. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

8.2. Exclusion of Incidental, Consequential and Certain Other Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY, AND WITH RESPECT TO AGILE, ITS SUPPLIERS, BE LIABLE TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF AGILE OR ANY SUPPLIER, AND EVEN IF AGILE OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, DAMAGES (INCLUDING WITHOUT LIMITATION, LIABILITIES RELATED TO A LOSS OF USE, PROFITS, GOODWILL OR SAVINGS OR A LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA), WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED IN ADVANCE OR AWARE OF THE POSSIBILITY OF ANY SUCH LOSS OR DAMAGE. THE FOREGOING LIMITATIONS OF LIABILITY WILL NOT APPLY TO ANY OF THE FOLLOWING: (A) A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT; OR (B) ANY GROSS NEGLIGENCE OR WILLFUL MISCONDUCT BY A PARTY.

8.3. Indemnification. Licensor hereby agrees to indemnify, hold harmless and defend Licensee and any partner, principal, employee or agent thereof against all claims, liabilities, losses, expenses (including attorney's fees and legal expenses related to such defense), fines, penalties, taxes or damages (collectively "Liabilities") asserted by any third party where such Liabilities arise out of or result from: (1) any claim that the Software or Customer's use thereof violates any copyright, trademark, patent and/or any other intellectual property rights; (2) the negligence of Licensor in the course of providing any Services hereunder; or (3) the representations or warranties made by Licensor hereunder, or their breach. Licensee shall promptly notify Licensor of any third party claim and Licensor shall, at Licensee's option, conduct the defense in any such third party action arising as described herein at Licensor's sole expense and Licensee shall cooperate with such defense.

9. Verification.

9.1. Agile has the right to request Customer complete a self-audit questionnaire in a form provided by Agile. If an audit reveals unlicensed use of the Agile Software, Customer agrees to promptly order and pay for licenses to permit all past and ongoing usage.

10. Support Services

10.1. Rights and Obligations. This Agreement does not obligate Agile to provide any support services or to support any software provided as part of those services. If Agile does provide support services to you, use of any such support services is governed by the Agile policies and programs described in the user manual, in online documentation, on Agile's support webpage, or in other Agile-provided materials. Any software Agile may provide you as part of support services are governed by this Agreement, unless separate terms are provided.

10.2. Consent to Use of Data. You agree that Agile and its affiliates may collect and use technical information gathered as part of the support services provided to you, if any, related to the Software. Agile may use this information solely to improve our products or to provide customized services or technologies to you and will not disclose this information in a form that personally identifies you.

11. Miscellaneous.

11.1. Legal Compliance; Restricted Rights. Each Party agrees to comply with all applicable Laws. Without limiting the foregoing, Customer agrees to comply with all U.S. export Laws and applicable export Laws of its locality (if Customer is not located in the United States), and Customer agrees not to export any Software or other materials provided by Agile without first obtaining all required authorizations or licenses. In the event the Software is provided to the United States government it is provided with only "LIMITED RIGHTS" and "RESTRICTED RIGHTS" as defined in FAR 52.227-14 if the commercial terms are deemed not to apply.

11.2. Governing Law; Severability. This Agreement (including any addendum or amendment to this Agreement which is included with the Software) are the entire agreement between you and Agile relating to the Software and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the Software or any other subject matter covered by this Agreement. To the extent the terms of any Agile policies or programs for support services conflict with the terms of this Agreement, the terms of this Agreement shall control. This Agreement shall be governed by the laws of the State of Florida, USA, without regard to choice-of-law provisions. You and Agile agree to submit to the personal and exclusive jurisdiction of the Florida state court located in Tampa, Florida, and the United States District Court for the Middle District of Florida. If any provision of this Agreement is held to be illegal or unenforceable for any reason, then such provision shall be deemed to be restated so as to be enforceable to the maximum extent permissible under law, and the remainder of this Agreement shall remain in full force and effect. Customer and Agile agree that this Agreement shall not be governed by the U.N. Convention on Contracts for the International Sale of Goods.

11.3. Notices. Any notices under this Agreement will be personally delivered or sent by certified or registered mail, return receipt requested, or by nationally recognized overnight express courier, to the address specified herein or such other address as a Party may specify in writing. Such notices will be effective upon receipt, which may be shown by confirmation of delivery.

11.4. Assignment. Customer may not assign or otherwise transfer this Agreement without the Agile's prior written consent, which consent shall not be unreasonably withheld, conditioned or delayed. This Agreement shall be binding upon and inure to the benefit of the Parties' successors and permitted assigns, if any.

11.5. Force Majeure. Neither Party shall be liable for any delay or failure due to a force majeure event and other causes beyond its reasonable control. This provision shall not apply to any of Customer's payment obligations.

11.6. Redistribution Compliance.

(a) F-Response distributes software libraries developed by The Sleuth Kit ("TSK"). The license information and source code for TSK can be found at http://www.sleuthkit.org/. If any changes have been made by Agile to the TSK libraries distributed with the F-Response software, those changes can be found online at http://www.f-response.com/TSKinfo.

(b) A portion of the F-Response Software was derived using source code provided by multiple 3rd parties which requires the following notices be posted herein, and which applies only to the source code. F-Response code is distributed only in binary or object code form. F-Response source

code, and any revised 3rd party code contained within the F-Response source code, is not available for distribution. The name of 3rd parties included below are not being used to endorse or promote this product, nor is the name of the author being used to endorse or promote this product. This information is presented solely to comply with the required license agreements which require reproduction of the following copyright notice, list of conditions and disclaimer:

Copyright (c) 2009-2014 Petri Lehtinen <petri@digip.org>

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young
eay@cryptsoft.com). This product includes software written by Tim
Hudson (tjh@cryptsoft.com).

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

- Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2011-2014, Loïc Hoguin <essen@ninenines.eu>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright 2009-2011 Andrew Thompson <andrew@hijacked.us>. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE PROJECT ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2000-2010 Marc Alexander Lehmann <schmorp@schmorp.de>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

11.7. General. This Agreement, including its exhibits (all of which are incorporated herein), are collectively the Parties' complete agreement regarding its subject matter, superseding any prior oral or written communications. Amendments or changes to this Agreement must be in mutually executed writings to be effective. The Parties agree that, to the extent any Customer purchase or sales order contains terms or conditions that conflict with, or supplement, this Agreement, such terms and conditions shall be void and have no effect, and the provisions of this Agreement shall control. Unless otherwise expressly set forth in an exhibit that is executed by the Parties, this Agreement shall control in the event of any conflict with an exhibit. Sections 2, 3, 5, 7, 8, and 9, and all warranty disclaimers, use restrictions and provisions relating to Agile's intellectual property ownership, shall survive the termination or expiration of this Agreement. The Parties are independent contractors for all purposes under this Agreement.

11.8. Changes to this agreement. Agile will entertain changes to this agreement on a case by case basis. Changes to this Agreement may require that the Customer pay an additional administrative fee depending on the scope and complexity of the changes required by the Customer. The additional administrative fee, if any, must be paid before the license will be activated.