

F-Response Universal Manual

2.0.1.11

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

Contents

Terminology	4
Examiner	4
Subject	4
Target.....	4
Supported Platforms	4
Overview	4
Appliance	5
Configuring the Appliance.....	5
Local Authentication	6
Active Directory Authentication	7
Basic Authentication	7
Advanced Authentication.....	7
Testing LDAP Configuration	8
Configuring Logging	9
Configuring Mission System	9
Complete Summary of all F-Response Universal Configuration File Options.....	10
Stopping, Starting, and Restarting F-Response Universal Appliance Software	11
Powering down the Appliance	11
Updating the Appliance Software.....	11
Changing the root password	12
Updating the License file.....	12
Examiner Software - Linux & OS X	13
Supported Linux Distributions	13
Supported OS X Versions.....	13
Download	13
Linux Examiner Installation	13
Centos 6 and 7.....	13
Debian 8 and Ubuntu 14	13
OS X Examiner Installation	14
Examiner Syslog Setup	17
Restarting Syslog on OSX	17
Restarting Syslog on Linux.....	17
Linux and OSX Examiner Overview	17
F-Response Configuration Interface	17
F-Response Examiner Interface	17

F-Response Command Interface	17
General Usage Pattern	17
F-Response Configuration Interface	18
init command	19
add command	19
rem command	19
opt command	19
host command	20
fuse command	20
pwd command	20
chg command	21
backup command	21
F-Response Examiner Interface	21
status command	22
start command	22
stop command	22
restart command	22
F-Response Command Interface	22
hget and mget command	23
hset command	23
mnt and umnt command	24
term command	24
Examiner Software - Windows	25
Overview of the F-Response Universal Windows Console	25
Installing the F-Response Universal Windows Console	25
Configuring the F-Response Universal Console	26
Credentials Settings	26
Login/Logout of Appliance	27
Configuring Deployment Settings	27
Deploying F-Response Universal	29
Deploy Via Browser	29
Via Email	33
Via LAN/WAN	33
Scanning for and deploying to Subject Machines	36
Via MSI	36
Stopping the remote software	37

Working with Subjects	38
Listing Subjects	38
Filtering Subjects	38
Connected vs Resolved Targets and Subjects.....	38
Connecting to Targets	39
Target Devices	39
DiscoveryShares™	39
Physical Drives, Partitions, and Volumes	40
MemoryShares™	40
Mission System	41
Overview of the Mission System.....	41
Creating a Mission	41
Approval Process.....	42
Mission Status	44
Working with Active Missions	44
Mission Expiration/Deletion.....	44
Appendix A.....	46
Legal Notices	46
Trademarks	46
Statement of Rights	46
Disclaimer	46
Patents	46
Appendix B.....	47
Release History.....	47
Appendix C.	48
Master Software License Agreement	48

Terminology

The term “Appliance” refers to both the physical and virtual versions of the F-Response Universal product. The F-Response Universal terms “Examiner”, “Subject” and “Target” are used throughout this manual. The definitions for Examiner, Subject and Target used in this manual are as follows:

Examiner

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

Subject

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

Target

F-Response Universal Targets refer to individual devices, shares, and data sources presented by Subjects to Examiners as defined above.

Supported Platforms

The F-Response Universal client 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, and 10) both 32 and 64 bit

Linux (Most modern distributions, using glibc 2.3.5 or better)

Apple OSX (10.3+ for command line, 10.6+ for GUI)

Overview

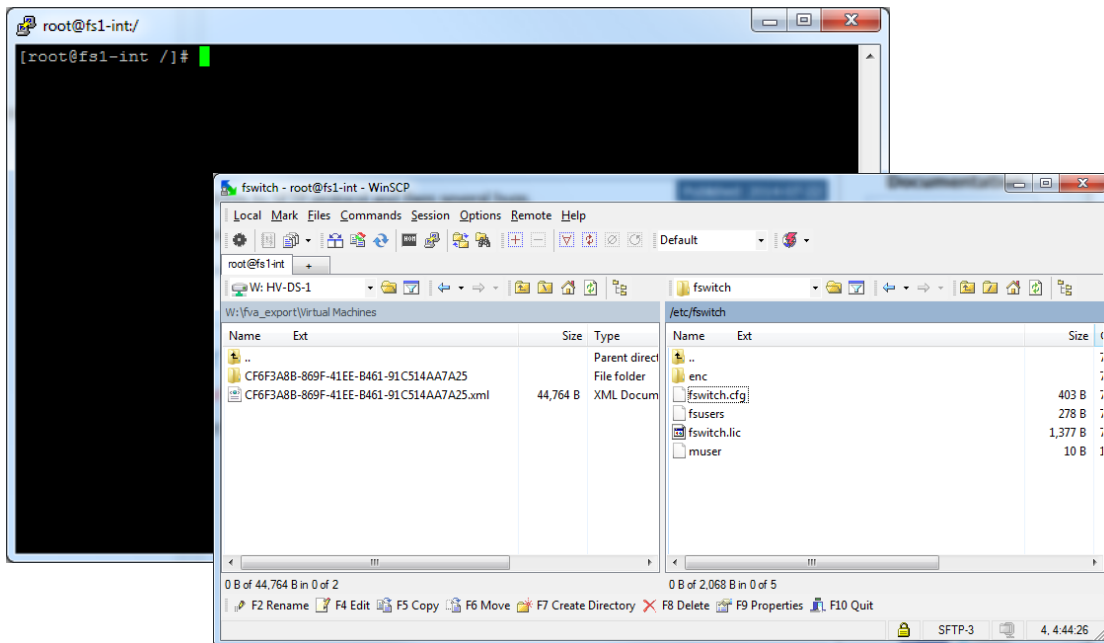
F-Response Universal is an appliance based product provided by F-Response which leverages our patent pending technology (“F-Switch”) to provide access to remote systems virtually anywhere in your network. F-Response Universal provides near instant access to Windows, Linux, and Apple OSX devices virtually regardless of the location provided they have network access. F-Response Universal is the onsite version of our cloud service offering, F-Response Now¹.

¹ <https://www.f-response.com/now>

Appliance

Configuring the Appliance

In this manual all configuration using the terminal will be done using the provided root account over a Windows SSH/SCP Session. A free Windows based SSH tool can be obtained via the Internet from www.putty.org, for SCP connections (File Copy) we recommend WinSCP, <http://winscp.net/eng/index.php>. All examples presented in this manual have been generated using Putty and WinSCP.



Local Authentication

F-Response Universal local authentication entails creating user accounts that reside within the F-Response Universal Appliance. These accounts require both a Username and Password and can be managed using the following command line tool. These commands must be run as “root” or using “sudo/su”.

Adding a Local User

```
/usr/sbin/fswitchadm adduser --username="USERNAME" --password="PASSWORD"
```

Removing a Local User

```
/usr/sbin/fswitchadm remuser --username="USERNAME"
```

Changing a password

```
/usr/sbin/fswitchadm setpass --username="USERNAME" --password="PASSWORD"
```

Listing all users

```
/usr/sbin/fswitchadm showusers
```

Active Directory Authentication

With Active Directory (LDAP) authentication enabled user accounts will not be needed on the F-Response Universal Appliance itself, rather the appliance will be configured to authenticate users directly against Active Directory based on group membership.

There are two options available when configuring LDAP Authentication for Active Directory, Basic, and Advanced. Basic Authentication requires all users be a member of the same domain. In our example that domain is “abcompany”, therefore all users would need to have “abcompany\<USERNAME>” accounts.

Advanced Authentication allows users in multiple domains to authenticate to the appliance provided a suitable domain controller is provided during the configuration.

Basic Authentication

The following information is necessary to configure the F-Response Universal appliance for Basic Active Directory Authentication:

1. A valid Active Directory Domain Controller providing LDAP or LDAP/SSL services (Will need hostname and port)
2. The Active Directory group whose membership controls access to the F-Response Universal Appliance
3. The LDAP Distinguished Name (DN) that completes the path to the aforementioned group

Armed with this information the following changes must be made to the F-Response Universal Configuration File (/etc/fswitch/fswitch.cfg).

In the following example our Active Directory Domain Controller is 10.1.1.22, and it is configured for LDAP/SSL on port 636. The user group we have configured is fresuniv_users and the full domain for the Active Directory is abccompany.local.

Using this information, update the following options in the /etc/fswitch/fswitch.cfg file:

```
{authtype,ldap} .
{ldap_server,"10.1.1.22"} .
{ldap_group,"CN=fresuniv_users,CN=Users"} .
{ldap_dn,"DC=abcompany,DC=local"} .
{ldap_ssl,true} .
{ldap_port,636} .
```

Advanced Authentication

The following information is necessary to configure the F-Response Universal appliance for Advanced Authentication:

1. Multiple valid Active Directory Domain Controllers (one for each domain needing access) providing LDAP or LDAP/SSL services (Will need hostname and port)
2. The Active Directory group whose membership controls access to the F-Response Universal Appliance
3. The LDAP Distinguished Name (DN) that completes the path to the aforementioned group

Armed with this information the following changes must be made to the F-Response Universal Configuration File (/etc/fswitch/fswitch.cfg).

In the following example we have two different users we would like to allow access from two different domains “chicago” and “tampa”. We have gathered the following information for each domain:

Domain:Chicago

Server:192.168.1.1

Port:636

SSL:Yes

Domain:Tampa

Server:192.168.2.1

Port:636

SSL:Yes

The user group we have configured is fresuniv_users and is defined in the “tampa” domain.

Using this information, update the following options in the /etc/fswitch/fswitch.cfg file:

```
{authtype,ldap}.
{ldap_server,"192.168.1.1"}.
{ldap_group,"CN=fresuniv_users,CN=Users,DC=chicago"}.
{ldap_dn,"DC=abcompany,DC=local"}.
{ldap_ssl,true}.
{ldap_port,636}.
{ldap_alternate_servers,[{"tampa",[{"server","192.168.2.1"}, {"port,636}, {"ssl,true}]}]}.
```

If we had multiple domains beyond the “tampa” domain we would add them on the same line as follows:

```
{ldap_alternate_servers,[{"tampa",[{"server","192.168.2.1"}, {"port,636}, {"ssl,true}]}], {"atlanta",[{"server","192.168.3.1"}, {"port,636}, {"ssl,true}]}]}.
```

Testing LDAP Configuration

In addition, the fswitchadm tool provided with the Universal appliance includes a “testldap” option that will use the information in the fswitch.cfg file (mentioned below) to test your ldap setup for accuracy.

Test LDAP Configuration

```
/usr/sbin/fswitchadm testldap --username="USERNAME" --domain="DOMAIN" --password="PASSWORD"
```

Configuring Logging

All F-Response Universal logs by default will be sent to Syslog on the F-Response Universal appliance. Alternatively, it is possible to configure the F-Response Universal Appliance Syslog service to leverage remote syslog servers. To enable logging to the remote syslog server, edit the `/etc/rsyslog.conf` file on the appliance with the following line:

For Remote Syslog Servers using TCP

```
*.* @@IP:PORT
```

For Remote Syslog Servers using UDP

```
*.*@IP:PORT
```

Where **IP** is the address of the syslog server, **PORT** is the port number for syslog communications, and the '@' symbol denotes whether the traffic is set to TCP or UDP (two '@@' symbols vs one '@' symbol).

Once the `rsyslog.conf` file has been updated and saved, restart the syslog service on the appliance with the following command:

```
service rsyslog restart
```

All logging will be redirected to the specified syslog server.

Configuring Mission System

The F-Response Universal Mission System requires access to an email (SMTP) server to send Mission Requests, Approvals, Denials, etc. In order to use the F-Response Universal Mission System the following information is needed:

1. A SMTP Server (IP and port)
2. Whether the SMTP Server is using SSL or not
3. Whether the SMTP Server is configured to require authentication or not
4. A username and password if authentication is required

Armed with this information the following changes must be made to the F-Response Universal Configuration File (`/etc/fswitch/fswitch.cfg`).

In the following example the SMTP Server is 10.1.1.33 and it is listening on TCP Port 587. It is not using SSL, however, SMTP authentication is still required. The username is `system` and the password is `system123`. The following configuration options in the `/etc/fswitch/fswitch.cfg` file are set to reflect these details:

```
{smtp_server,"10.1.1.33"}.  
{smtp_port,587}.  
{smtp_ssl,false}.  
{smtp_username,"system"}.  
{smtp_password,"system123"}.  
{smtp_auth,true}.  
{system,mission}.
```

Complete Summary of all F-Response Universal Configuration File Options

All configuration options reside within the F-Response Universal Configuration file (/etc/fswitch/fswitch.cfg). The following options exist in the configuration file.

{fswitch_port,80}.

F-Response Universal port controls the port the software will bind to on start, the value must be a valid port number that is not already in use by another service, the default port is 80.

{logtype,syslog}.

Logtype controls the logging model, currently the only logging option is syslog.

{authtype,ldap}.

Authtype specifies how F-Response Universal will authenticate Examiners, two options are currently available, local or ldap. "local" will use locally defined and created F-Response Universal Accounts, "ldap" will use the ldap_* settings defined below.

{verlevel,1}.

Verlevel indicates the version of the F-Switch protocol and will be incremented in future releases. This value should not be modified by the user.

{ldap_server,"xxx.xxx.xxx.xxx"}.

Ldap server is the Domain Controller, with LDAP Services enabled, that the appliance will attempt to communicate with to validate Examiner credentials and confirm group membership.

{ldap_group,"xxxxxxxxxxx"}.

Ldap group is the Active Directory group that Examiners must be a member of to successfully authenticate. Use any defined Active Directory group.

{ldap_dn,"DC=domaina,DC=companya,DC=local"}.

Ldap DN is the distinguished name for the domain in LDAP syntax. Ex. domaina.companya.local becomes "DC=domain,DC=companya,DC=local".

{ldap_ssl,true}.

Ldap SSL indicates whether the connection to the Domain Controller will be performed with SSL applied. Windows Domain Controllers do not have SSL enabled by default, it must be configured separately on the Domain Controller directly in order to use this option.

{ldap_port,636}.

Ldap port indicates the TCP port to use when connected to the Domain Controller.

{ldap_alternate_servers,[{"domaina", [{"server,"192.168.1.2"}, {"port,636}, {"ssl,true}]}]}.

{smtp_server,"xxx..."}.

SMTP Server is used by the Mission System when sending emails to approvers and examiners.

{smtp_port,587}.

SMTP Port indicates the TCP port to use when connecting to the SMTP Server.

{smtp_ssl,false}.

SMTP ssl defines whether SSL is required when communicating to the SMTP Server

```
{smtp_username,"xxxx@xxxx.xxx"}.
```

SMTP Username is used both if SMTP Authentication is required, or to provide the “From” address in the email messages as sent.

```
{smtp_password,"xxx"}.
```

SMTP Password should also be completed if the SMTP server requires authentication.

```
{smtp_auth,true}.
```

SMTP Auth indicates whether SMTP Authentication is required, valid options are true and false.

```
{system,mission}.
```

System indicates whether the appliance is in Mission Mode (mission) or Standard Mode (standard). If this option is changed a restart of the appliance should be performed.

```
{socket,inet | inet6 | both}.
```

Socket indicates which type of network socket the appliance software should bind and listen on. No socket option or “inet” will default bind to IPv4 only. “inet6” will bind to IPv6. “both” will bind to IPv4 and IPv6. Please note, enabling IPv6 support may require additional firewall changes to the iptables firewall on the appliance. Firewall configuration is outside the scope of this document.

Stopping, Starting, and Restarting F-Response Universal Appliance Software

The F-Response Universal Appliance software can be started, stopped, and restarted using the following command line options.

Starts the F-Response Universal Appliance Software

```
service fswitchbasic start
```

Stops the F-Response Universal Appliance Software

```
service fswitchbasic stop
```

Stops and Starts the F-Response Universal Appliance Software

```
service fswitchbasic restart
```

Powering down the Appliance

The appliance can be powered down using basic linux system power management commands, such as:

```
/sbin/shutdown -h now
```

Updating the Appliance Software

The F-Response Universal Appliance software packages are available directly from the F-Response Universal Internet based software repository and can be installed using the yum command line tool. Important note, updating F-Response Universal packages will not overwrite your existing configuration files.

```
yum update f-response-univ f-response-univ-clients
```

Changing the root password

The root account password can be changed at any time using the passwd command.

```
passwd root
```

Updating the License file

F-Response uses a subscription based licensing model. To update/activate the appliance, open the hyper link <http://<APPLIANCEIP>/activate> to obtain the activation code. Submit the activation code on the main F-Response website <https://www.f-response.com/univ-license/>

F-Response Appliance Licensing

Appliance Activation Code

```
D9wjBaVowSFyRkYAsG0DNYe29rpNR1UNtKO541umNH8=
```

replace it with the new file.

Once the activation code has been submitted to F-response and the processing has been completed, a license file will be emailed.

To update the license on the appliance itself, the new file will need to be copied to the /etc/fswitch directory (F-Response recommends using the tool WinSCP to accomplish this task). If a license file exists in this directory, delete it and

Examiner Software - Linux & OS X

The Linux and OS X examiner consist of three command line interfaces that are used to interact with the F-Response Universal appliance. First, the configuration interface (**fs_cfg**) manages user authentication and host connection information, i.e. such as username, password, host name, and port. Second, the examiner interface (**fs_exa**) starts, stops, and restarts connection to and from the appliance. Lastly, the command interface (**fs_cmd**) enables users to mount, unmount, terminate, and list missions, subjects, and targets on the connected appliance.

Supported Linux Distributions

Centos 6 - x86_64 - f-response-exa-centos6-VERSION.x86_64.rpm
Centos 7 - x86_64 - f-response-exa-centos7- VERSION.x86_64.rpm
Debian 8 - x86_64 - f-response-exa-debian8- VERSION.x86_64.deb
Ubuntu 14 - x86_64 - f-response-exa-ubuntu14- VERSION.x86_64.deb (compatible with SANS SIFT Kit)

Supported OS X Versions

OS X 10.8 Mountain Lion - x86_64 - f-response-exa-osx10.8-VERSION.x86_64.pkg
OS X 10.9 Mavericks - x86_64 - f-response-exa-osx10.9-VERSION.x86_64.pkg
OS X 10.10 Yosemite - x86_64 - f-response-exa-osx10.10-VERSION.x86_64.pkg

Download

The Linux and OSX packages are hosted on the appliance under the URL <http://<hostname>address/<univdl>>. F-Response Now users may access the Linux and OSX packages via <http://<hostname>address/<nowdl>>. Substitute the appliance's host name for <hostname> or IPv4 address for <address> and enter the URL into any browser to get to the download page.

Linux Examiner Installation

The Linux examiner must be install over command line using various package management tools.

Centos 6 and 7

The RPM can be install and uninstall using yum or rpm. Yum is the recommend method because yum automatically resolves missing dependencies, while rpm will not resolve missing dependencies.

Using yum to install the RPM

```
yum install f-response-exa-centos6-2.0.1.5.x86_64.rpm
```

Using rpm to install the RPM

```
rpm -i f-response-exa-centos6-2.0.1.5.x86_64.rpm
```

Using yum to remove the RPM installation

```
yum remove f-response-exa
```

Debian 8 and Ubuntu 14

The Debian package can be install and uninstall using dpkg and apt-get to resolve missing dependencies.

Using dpkg and apt-get to install the package

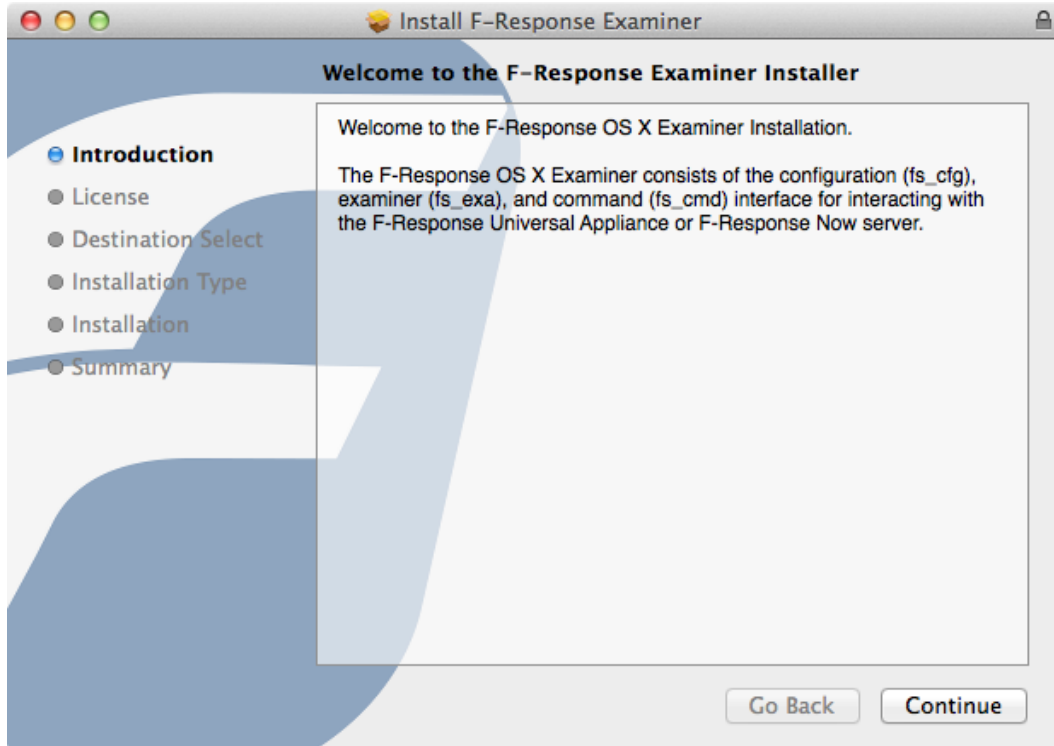
```
dpkg -i f-response-exa-debian8-2.0.1.5.x86_64.deb  
apt-get install -f
```

Using apt-get to remove the package

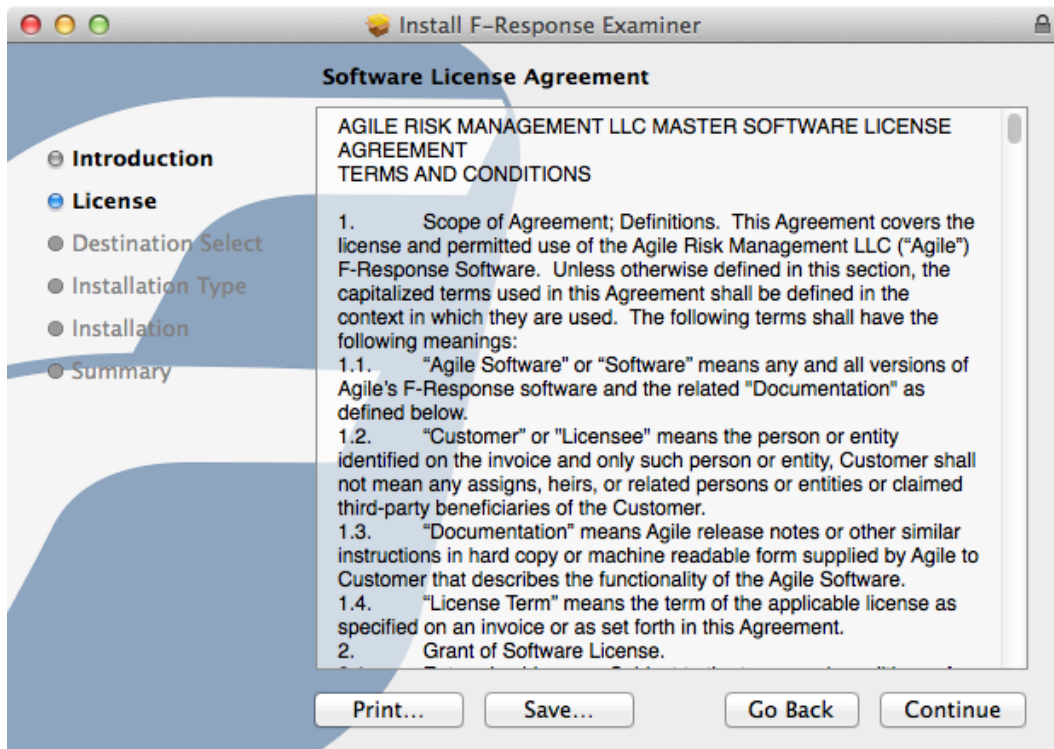
```
apt-get remove fresponseexa
```

OS X Examiner Installation

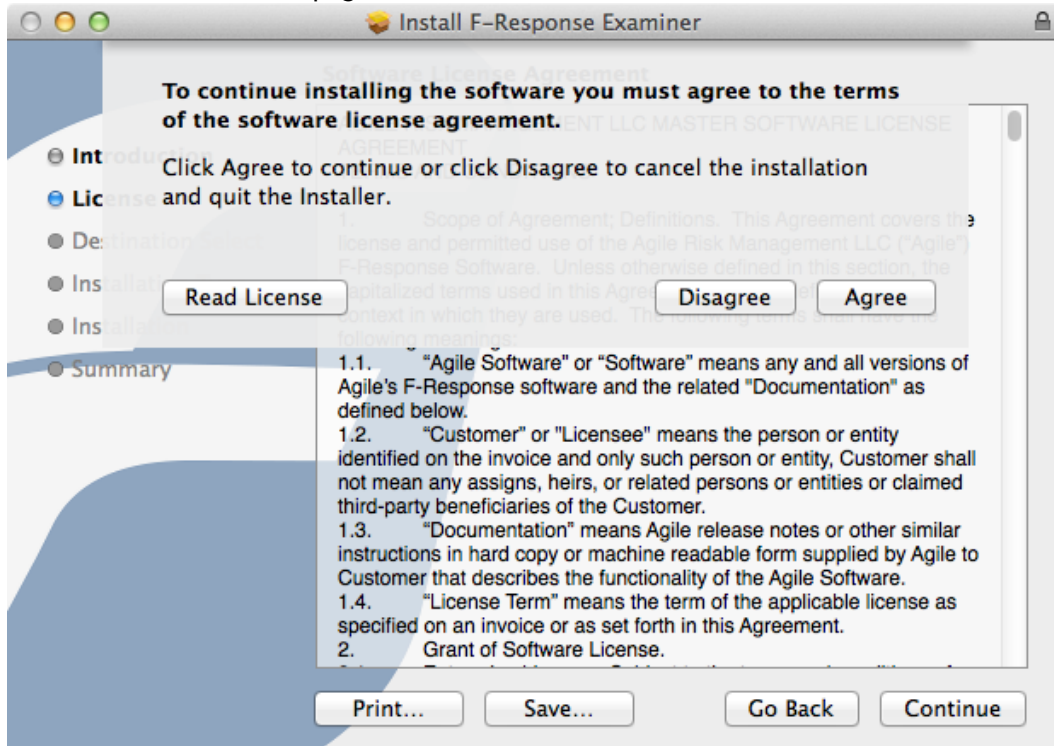
The OS X package installation is guided by an installation manager through the user-interface, which is consistent for OS X 8 to OS X 10.



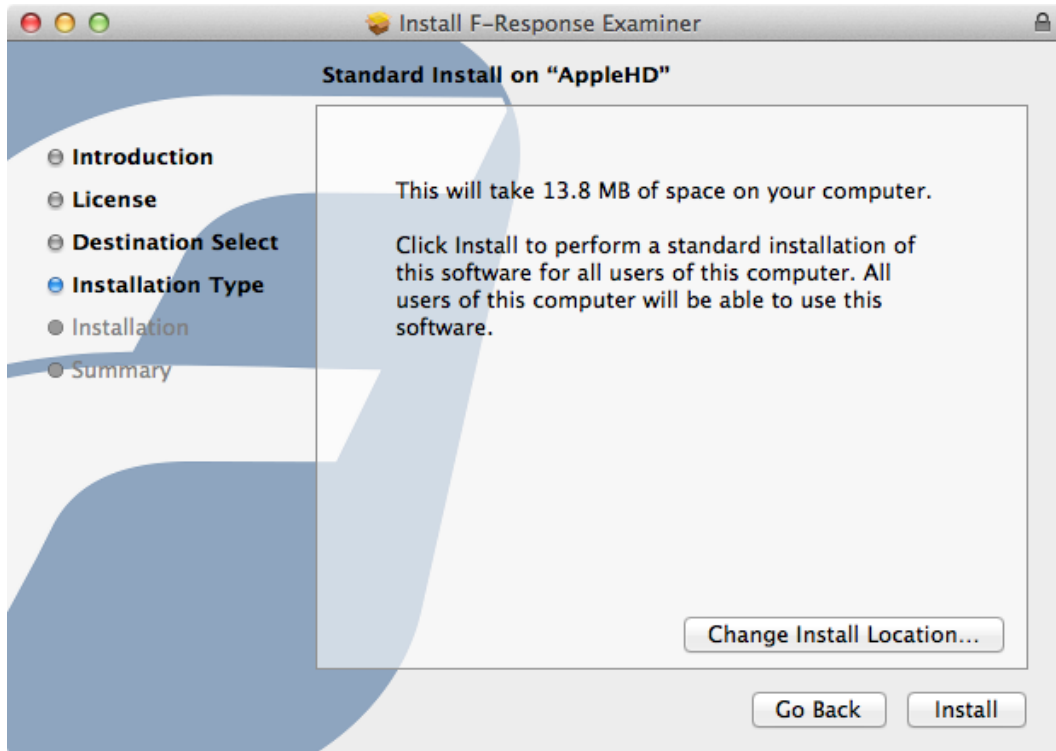
Click continue on introduction page.



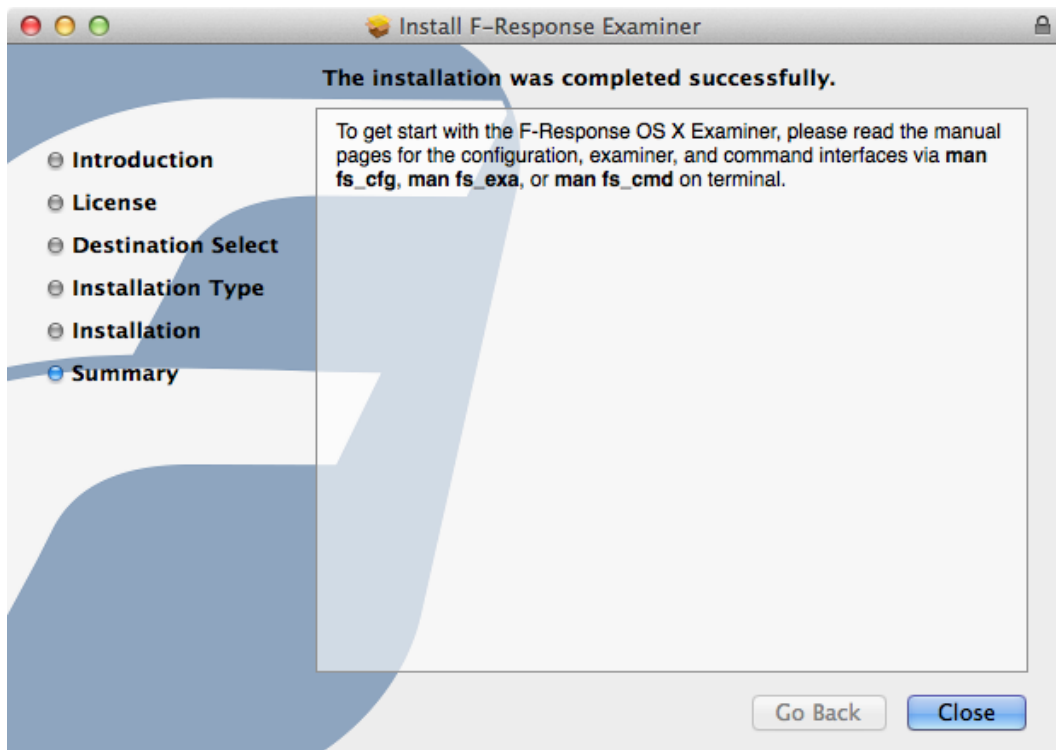
Click continue on license page.



Agree or disagree with the license.



Do not change the installation location and click install.



Click close to complete the installation. Also, check out the manual pages for each interface.

To uninstall the OSX package, run the following script:

```
pkgutil --forget com.fresponse.oexa
rm -f /usr/bin/fs_exa /usr/bin/fs_dae
rm -f /usr/bin/fs_cfg /usr/bin/fs_cmd
rm -f /etc/asl/com.fresponse.asl
rm -f /usr/share/man/man8/fs_exa.8
rm -f /usr/share/man/man8/fs_cmd.8
rm -f /usr/share/man/man8/fs_cfg.8
rm -rf /etc/fsnow
rm -rf /var/lib/fsnow
rm -rf /var/lib/fsnow-mnts
```

Examiner Syslog Setup

After installing the Linux and OSX examiner, a syslog configuration file is installed in a location dependent on the platform. To activate the syslog after installation, either restart your computer or syslog service. The default location of the examiner's log file is /var/log/fsnow.cfg on both Linux and OSX.

Restarting Syslog on OSX

```
sudo launchctl unload /System/Library/LaunchDaemons/com.apple.syslogd.plist
sudo launchctl load /System/Library/LaunchDaemons/com.apple.syslogd.plist
```

Restarting Syslog on Linux

```
service rsyslog restart
systemctl restart rsyslog
```

Linux and OSX Examiner Overview

The Linux and OSX examiner consist of three command line interfaces as follows.

F-Response Configuration Interface

The configuration interface support 8 commands for creating and backing up configuration files, adding or removing accounts, listing accounts and fuse options, and changing account or fuse settings; these 8 commands are **init**, **add**, **rem**, **opt**, **host**, **fuse**, **pwd**, and **chg**. An account is identify by username and hostname, where username is used to authenticate to the appliance specified by hostname.

F-Response Examiner Interface

The examiner interface supports 4 commands for starting, stopping, restarting, and displaying the accounts associated with each appliance; these 4 commands are **start**, **stop**, **restart**, and **status**. These commands are analogous to the **service** or **systemctl** commands.

F-Response Command Interface

The command interface supports 6 commands for mounting, unmounting, terminating, and displaying missions, subjects, and targets connected on an appliance; these 6 commands are **hget**, **hset**, **mget**, **mnt**, **umnt**, and **term**.

General Usage Pattern

1. Add an account and appliance to the default configuration file.

```
fs_cfg add loki@192.168.1.82:80 -m ~/Desktop
```

2. Connect to appliance and authenticate using account.

```
fs_exa start -a 192.168.1.82
```

3. Set the default appliance.

```
fs_cmd hset -a 192.168.1.82
```

4. Get a list of missions, subjects, and targets.

```
fs_cmd hget
```

5. Mount a target by either device id or subject and target name.

```
fs_cmd mnt -d KSNp+bXFBGcAAQ  
fs_cmd mnt -s win7-dev-mobile -t DiscoveryShare-C
```

6. Perform analysis on mounted target.

```
ls ~/Desktop/win7-dev-mobile/DiscoveryShare-C
```

7. Get a list of mounted missions, subjects, and targets.

```
fs_cmd mget
```

8. Unmount a target by either device id or subject and target name.

```
fs_cmd umnt -d KSNp+bXFBGcAAQ  
fs_cmd umnt -s win7-dev-mobile -t DiscoveryShare-C
```

9. Disconnect a subject from the appliance.

```
fs_cmd term -s win7-dev-mobile
```

10. Disconnect from appliance.

```
fs_exa stop -a 192.168.1.82
```

11. Reference the unix manual pages, which is identical to this manual.

```
man fs_cfg  
man fs_exa  
man fs_cmd
```

F-Response Configuration Interface

The configuration interface supports the following 8 commands:

- **init** - create an empty configuration file
- **add** - add an account and appliance
- **rem** - remove an account and appliance
- **opt** - change the values for fuse settings
- **host** - display the host list
- **fuse** - display the fuses option
- **pwd** - change a local account password on the appliance
- **chg** - change the values for account settings
- **backup** - create a back up of a configuration file

The configuration interface manages the accounts and fuse options in a configuration file. By default, the configuration file is located in `/etc/fsnow/fsnow.cfg`, but other configuration files may be specified with the `-c`, `--config` option.

While the configuration file may be modified directly using any text editor, directly modifying the configuration file may lead to invalid values or improper syntax. Therefore, it is recommended to use the configuration interface to back up and modify configuration files.

init command

An empty configuration file is created using **fs_cfg init**, where the **-o, --output <path>** option specifies the path to write the empty configuration file and the **-e, --cache <path>** option specifies the default cache path of the configuration file.

Creating an empty configuration file:

```
loki@localhost# fs_cfg init -o /etc/fsnow/fsnow.cfg -e /var/lib/fsnow
fs_cfg: new configuration file created on path '/etc/fsnow/fsnow.cfg'.
```

add command

A new account is added to a configuration file using **fs_cfg add <user>@<host>:<port>** or **fs_cfg add <domain>\\<user>@<host>:<port>** syntax, where **-c, --config <path>** specifies the configuration file to store the account, **-m, --mount <path>** specifies the default mount path, **-l, --ldap** indicates the new account is an LDAP account, and **-p, --password <password>** to specify the password on command line without being prompted.

Adding an appliance with a local account:

```
loki@localhost# fs_cfg add loki@192.168.1.82:80 -m ~/Desktop
Enter password: ***
Re-enter password: ***
fs_cfg: new appliance 192.168.1.82:80 add to appliance list.
```

Adding an appliance with a LDAP account

```
loki@localhost# fs_cfg add WINDOMAIN\\loki@192.168.1.82:80 -m ~/Desktop --
ldap
Enter password: ***
Re-enter password: ***
fs_cfg: new appliance 192.168.1.82:80 add to appliance list.
```

rem command

An account can be removed from a configuration file using **fs_cfg rem**, where **-c, --config <path>** specifies the configuration file containing the account and **-a, --appliance <name>** specifies the appliance associated with the account to remove.

Removing an account:

```
loki@localhost# fs_cfg rem -a 192.168.1.82
fs_cfg: removed appliance 192.168.1.82 from appliance list.
```

opt command

The fuse options can be configured using **fs_cfg opt <option>=<value>** or **fs_cfg opt <option>:<value>** syntax, where **-c, --config <path>** specifies the configuration file containing the fuse options. A single or multiple options may be specified by separating each option-value pair by whitespace.

The following options are supported:

- **default_permissions=boolean** - enable root access only

- allow_other=boolean - enable root and all users access
- allow_root=boolean - enable root and mounting user access
- max_read=integer - maximum number of bytes per read request
- max_background=integer - maximum number of request queued

The following values for each type:

- boolean = 'true' or 'false'
- integer = 32-bit signed integer

Setting a single option:

```
loki@localhost# fs_cfg opt max_read=524288
fs_cfg: max_read set to 524288.
fs_cfg: update fuse option list.
```

Setting multiple options:

```
loki@localhost# fs_cfg opt allow_root=false default_permissions=false
fs_cfg: allow_root set to false.
fs_cfg: default_permissions set to false.
fs_cfg: update fuse option list.
```

host command

Print a list of accounts by using `fs_cfg host`, where `-c,--config <path>` specifies the configuration file containing the accounts.

Print a list of accounts:

```
loki@localhost# fs_cfg host
user  host      port  mount          auth
loki  192.168.1.82  80    /var/lib/fsnow-mnts  local
```

fuse command

Print a list of fuse options by using `fs_cfg fuse`, where `-c,--config <path>` specifies the configuration file containing the fuse options.

Print a list of fuse options:

```
loki@localhost# fs_cfg fuse
option                value
default_permissions  true
allow_other           false
allow_root            false
auto_cache            false
max_read              524288
async_read            true
sync_read             false
max_background        5
```

pwd command

The `fs_cfg pwd` command is used to change a local account password on a specific appliance, where `-c,--config <path>` specifies the configuration file containing the account, `-a,--appliance <name>` specifies the appliance, and `-p,--password <password>` to specify the password on command line without being prompted.

Changing a local account password:

```
loki@localhost# fs_cfg pwd -a 192.168.1.82
Enter password: ***
Re-enter password: ***
fs_cfg: successfully changed password.
```

chg command

An account can be modified using `fs_cfg chg <field>=<string>` or `fs_cfg chg <field>:<string>` syntax, where `-c,--config <path>` specifies the configuration file containing the account. A single or multiple fields may be specified by separating each field-value pair by whitespace.

The following fields are supported:

- `host` - appliance's host name or IP address
- `port` - appliance's port
- `local_user` - local account username
- `local_pass` - local account password
- `ldap_user` - LDAP account name
- `ldap_pass` - LDAP account password
- `mount` - default mount path

Setting a single field:

```
loki@localhost# fs_cfg chg local_user=tricky -a 192.168.1.82
fs_cfg: local_user set to tricky.
fs_cfg: update '192.168.1.82' record.
```

Setting multiple fields:

```
loki@localhost# fs_cfg chg local_user=loki port=80 -a 192.168.1.82
fs_cfg: local_user set to loki.
fs_cfg: port set to 80.
fs_cfg: update '192.168.1.82' record.
```

backup command

The `fs_cfg backup` command is used to copy an existing configuration file, where `-c,--config <path>` specifies the configuration file to be backed up and `-o,--output <path>` specifies the path of the new configuration file.

Backing up a configuration file:

```
loki@localhost# fs_cfg backup -c /etc/fsnow/fsnow.cfg -o
/etc/fsnow/fsnow.cfg.back
fs_cfg: copied /etc/fsnow/fsnow.cfg to /etc/fsnow/fsnow.cfg.back.
```

F-Response Examiner Interface

The examiner interface supports the following 4 commands:

- `status` - print a list of account status
- `start` - connect to appliance
- `stop` - disconnect from appliance
- `restart` - disconnect or connect to appliance

The examiner interface manages the connectivity of multiple appliances. By default, the examiner interface manages the appliances in the default configuration file located in `/etc/fsnow/fsnow.cfg`. However, any configuration file created and managed by the configuration interface can be used with the examiner interface, which can be specified with the `-c,--config <path>` option.

It is very important to understand that all connected appliances keep their resources in the cache path, which is where the examiner and command interface will search for resource when managing or interacting with a specific appliance. Therefore, the examiner and command interface should be supplied with the same cache directory and configuration file consistently.

status command

Use the **fs_exa status** command to print the status of every appliance.

Print the status of every appliance:

```
loki@localhost# fs_exa status
user  host      port  mount          auth  status
loki  192.168.1.82  80    /var/lib/fsnow-mnts  local  disconnected
```

start command

Use the **fs_exa start** command to establish a connection to an appliance, where **-c,--config <path>** specifies the configuration file containing an account for the appliance, **-e,--cache <path>** specifies where to create the cache resources, and **-a,--appliance <name>** specifies the appliance to connect to. By default, the **fs_exa start** command connects to every appliance if the **-a,--appliance <name>** is not specified.

Connect to an appliance:

```
loki@localhost# fs_exa start -a 192.168.1.82
fs_exa: connected to appliance '192.168.1.82:80'.
```

stop command

Use the **fs_exa stop** command to disconnect from an appliance, where **-c,--config <path>** specifies the configuration file containing an account for the appliance, **-e,--cache <path>** specifies where the cache resources are, and **-a,--appliance <name>** specifies the appliance to disconnect from. By default, the **fs_exa stop** command disconnects from every appliance and every target mounted from that appliance if the **-a,--appliance <name>** is not specified.

Disconnect from an appliance:

```
loki@localhost# fs_exa stop -a 192.168.1.82
fs_exa: disconnected from appliance '192.168.1.82:80'.
```

restart command

The **fs_exa restart** command calls the **fs_exa stop** and **fs_exa start** command in sequence, therefore all the flags that applied to **fs_exa stop** and **fs_exa start** can be applied to **fs_exa restart**.

Restart a connection from and to an appliance:

```
loki@localhost# fs_exa restart -a 192.168.1.82
fs_exa: disconnected from appliance '192.168.1.82:80'.
fs_exa: connected to appliance '192.168.1.82:80'.
```

F-Response Command Interface

The command interface supports the following 6 commands:

1. **hget** - print a list of missions, subjects, and targets
2. **mget** - print a list of mounted missions, subjects, and targets
3. **hset** - set the default host
4. **mnt** - mount a target by device id or subject and target name

5. **umnt** - unmount a target by device id or subject and target name
6. **term** - disconnect a subject from the appliance by subject name

The command interface interacts with multiple connected appliances. By default, the command interface interacts with the appliances in the default configuration file located in `/etc/fsnow/fsnow.cfg`. However, any configuration file created and managed by the configuration interface can be used with the command interface, which can be specified with the `-c,--config <path>` option.

hget and mget command

The `fs_cmd hget` command prints a list of missions, subjects, and targets, where the `-a,--appliance <name>` specifies an appliance. By default, `fs_cmd hget` command prints a list of missions, subjects, and targets from all connected appliances in the default configuration file located in `/etc/fsnow/fsnow.cfg`. And the `fs_cmd hget` command will display either standard or mission format based on the mode of the appliance.

Standard Mode CSV Format

`<state>`, `<device-id>`, `<host-name>`, `<subject-name>`, `<target-name>`, `<mount-path>`

Mission Mode CSV Format

`<state>`, `<device-id>`, `<host-name>`, `<subject-name>`, `<target-name>`, `<mount-path>`, `<mission-id>`, `<mission-name>`

Print and filter missions, subjects, and targets by row:

```
loki@localhost# fs_cmd hget | grep Volume
2,nvlt7nLMeK0AAg,"192.168.1.82","win7-dev-mobile","Volume-C-61338mb",".../fsnow-mnts"
2,nvlt7nLMeK0ABA,"192.168.1.82","win7-dev-mobile","Volume-F-32765mb",".../fsnow-mnts"
2,nvlt7nLMeK0ABg,"192.168.1.82","win7-dev-mobile","Volume-H-5117mb",".../fsnow-mnts"
```

Print and filter missions, subjects, and targets by row and column:

```
loki@localhost# fs_cmd hget | cut -d, -f3-6 | grep Disk-0
"192.168.1.82","win7-dev-mobile","Disk-0-Part-1-Unused-1mb","/var/lib/fsnow-mnts"
"192.168.1.82","win7-dev-mobile","Disk-0-Part-2-Active-100mb","/var/lib/fsnow-mnts"
"192.168.1.82","win7-dev-mobile","Disk-0-Part-3-Active-61338mb","/var/lib/fsnow-mnts"
"192.168.1.82","win7-dev-mobile","Disk-0-Part-4-Unused-1mb","/var/lib/fsnow-mnts"
"192.168.1.82","win7-dev-mobile","Disk-0-61440mb","/var/lib/fsnow-mnts"
```

The `fs_cmd mget` command prints only missions, subjects, and targets that are mounted, but produce the same formatted output as `fs_cmd hget` and can be passed a `-a,--appliance <name>` option.

The output of `fs_cmd hget` and `mget` can be pipe to various UNIX utilities available on Linux and OS X, such as `cut`, `grep`, and `awk`, to filter the output. The `cut` utility can filter by column, `grep` utility can filter by row, and piping to both can filter by column and row. Any high level scripting language, such as Python, can easily parse the output and build a higher level interface on top of the command interface.

hset command

By setting the default appliance with the `fs_cmd hset` command, where `-a,--appliance <name>` specifies the appliance, the `-a,--appliance <name>` option can be omitted from the `fs_cmd mnt`, `umnt`, and `term` command.

Set the default appliance:

```
loki@localhost# fs_cmd hset -a 192.168.1.82
fs_cmd: default appliance set to '192.168.1.82'.
```

mnt and umnt command

A target can be mounted using the `fs_cmd mnt` command and unmounted using the `fs_cmd umnt` command, where `-d,--dev <id>` specifies the device id, `-s,--subject <name>` specifies the subject name, `-t,--target <name>` specifies the target name, `-m,--mount <path>` specifies the mount point, `-a,--appliance <name>` specifies the appliance, and `-c,--config <path>` specifies the configuration file containing the account for the appliance. By default, the `fs_cmd mnt` reads the default configuration file located in `/etc/fsnow/fsnow.cfg` and use the default appliance set by `fs_cmd hset` command.

Mounting a target by device id

```
loki@localhost# fs_cmd mnt -d KSNp+bXFBGcAAQ -a 192.168.1.82
fs_cmd: connected to appliance '192.168.1.82:80'.
fs_cmd: mounted target 'DiscoveryShare-C' on subject 'win7-dev-mobile'.
fs_cmd: mounted on path '/var/lib/fsnow-mnts/win7-dev-mobile/DiscoveryShare-C'.
```

Unmounting a target by device id

```
loki@localhost# fs_cmd umnt -d KSNp+bXFBGcAAQ -a 192.168.1.82
fs_cmd: unmounted target DiscoveryShare-C on subject win7-dev-mobile.
```

Mounting a target by subject and target name

```
loki@localhost# fs_cmd mnt -s win7-dev-mobile -t DiscoveryShare-C -a
192.168.1.82
fs_cmd: connected to appliance '192.168.1.82:80'.
fs_cmd: mounted target 'DiscoveryShare-C' on subject 'win7-dev-mobile'.
fs_cmd: mounted on path '/var/lib/fsnow-mnts/win7-dev-mobile/DiscoveryShare-C'.
```

Unmounting a target by subject and target name

```
loki@localhost# fs_cmd umnt -s win7-dev-mobile -t DiscoveryShare-C -a
192.168.1.82
fs_cmd: unmounted target DiscoveryShare-C on subject win7-dev-mobile.
```

term command

Use `fs_cmd term` to disconnect a subject from the appliance, `-s,--subject <name>` and `-d,--dev <id>` specifies the subject, `-a,--appliance <name>` specifies the appliance, and `-c,--config <path>` specifies the configuration file containing the account for the appliance. By default, the `fs_cmd term` reads the default configuration file located in `/etc/fsnow/fsnow.cfg` and use the default appliance set by `fs_cmd hset` command.

Terminating a subject by device id

```
loki@localhost# fs_cmd term -d KSNp+bXFBGcAAQ -a 192.168.1.82
fs_cmd: terminated 'win7-dev-mobile' on '192.168.1.82:80'.
```

Terminating a subject by subject name

```
loki@localhost# fs_cmd term -s win7-dev-mobile -a 192.168.1.82
fs_cmd: terminated 'win7-dev-mobile' on '192.168.1.82:80'.
```

Examiner Software - Windows

Overview of the F-Response Universal Windows Console

The F-Response Universal Windows Console provides direct access to the F-Response Universal Appliance(s) enabling connections to remote subject machines. The F-Response Universal Windows Console must be installed on any and all examiner computers looking to access F-Response Universal.

Installing the F-Response Universal Windows Console

The F-Response Universal Windows Console software is available directly from the F-Response Universal appliance itself. Use the following link to download and install the F-Response Universal Windows Console:

<http://<APPLIANCE> HOSTNAME OR IP> /univdl>

F-Response Universal Installer Downloads

Installer

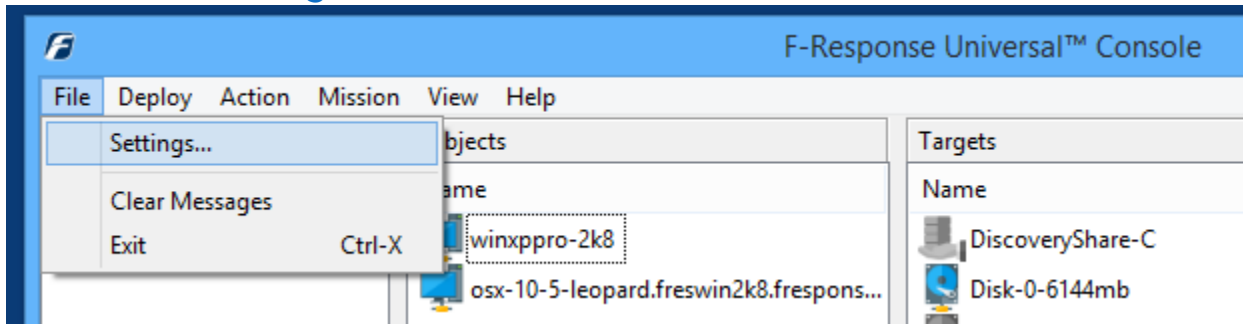
Software Installers (2)

Name	Download
F-Response Universal Software Installer for Windows	Link
F-Response Universal Software Installer for Linux	Link

After a successful installation the F-Response Universal Software will be available from the Start Menu. Select the **F-Response Universal Console** to begin.

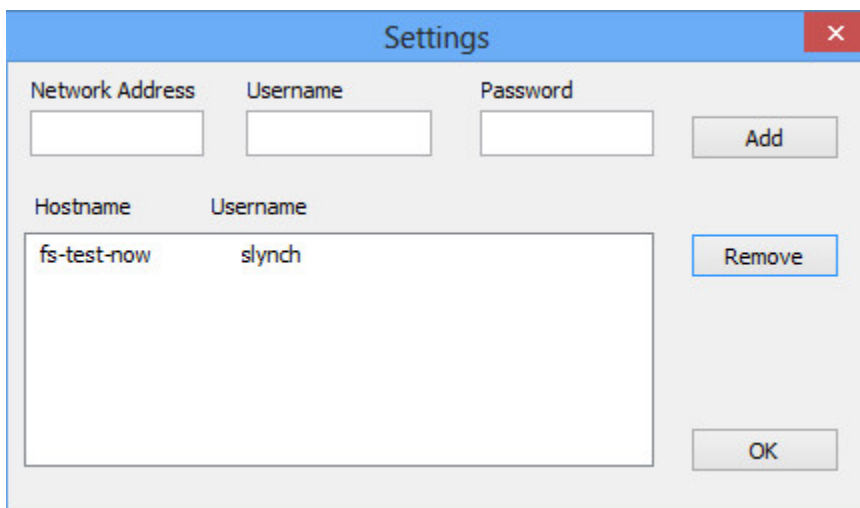
Configuring the F-Response Universal Console

Credentials Settings



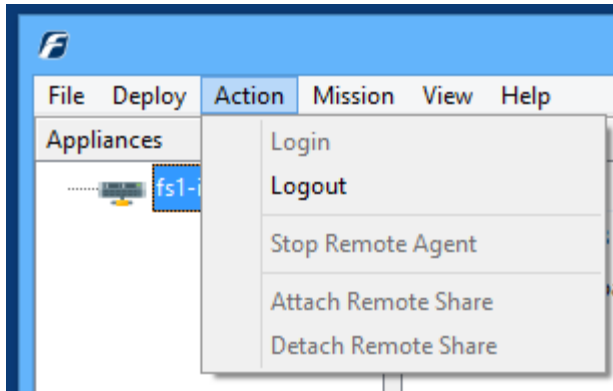
Once loaded the F-Response Universal Console File Menu contains the Settings command, this command will open the Settings dialog and allow you to configure one or more F-Response Universal Appliance accounts.

Here the credentials can be entered and saved for each appliance in the environment. Enter the appliance hostname or IP address, account, and password, then click **Add** to add the credential for each appliance to appear in the console.





The F-Response Universal appliances will appear in the main console window.

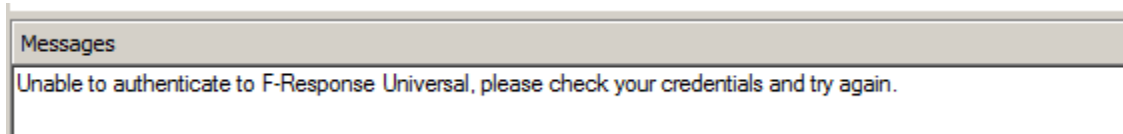
Login/Logout of Appliance



Double click on the individual appliance or highlight it and choose the Action->Login/Logout menu command to authenticate to the appliance.

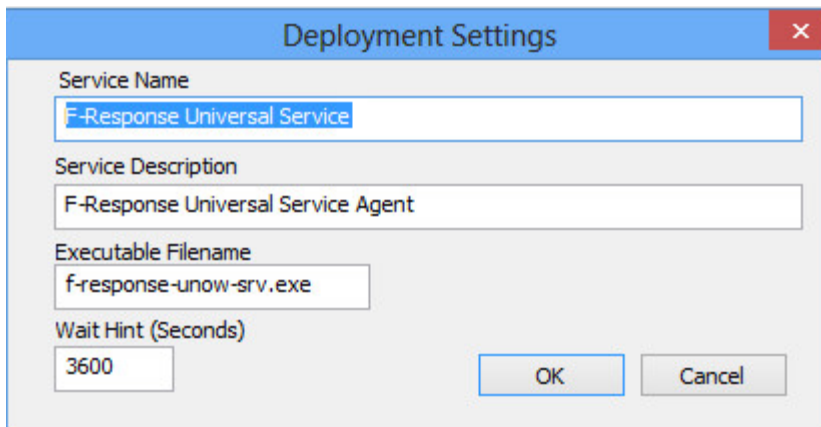
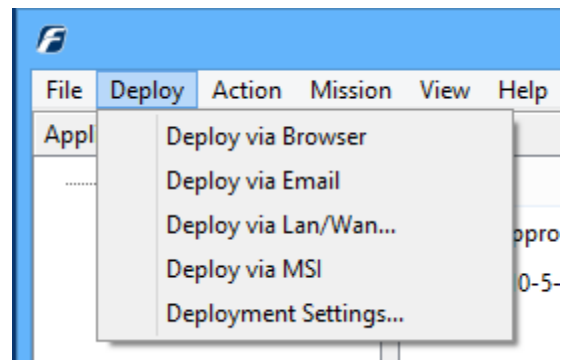
Successful authentication will change the appliance icon from a grey appliance icon 

to a color appliance icon . Un-successful authentication will raise the messages panel indicating further information.



Configuring Deployment Settings

Click the Deploy->Deployment Settings... menu option to access the deployment settings for the subject software.



The four fields presented here will be populated with default information that can be customized as needed for the environment. Note this is the information that will appear in the services panel of the subject machine.

Service Name: F-Response Universal software will run as a service on the subject machine. The service name can be left at

the default or renamed to anything other than an existing Windows service name.

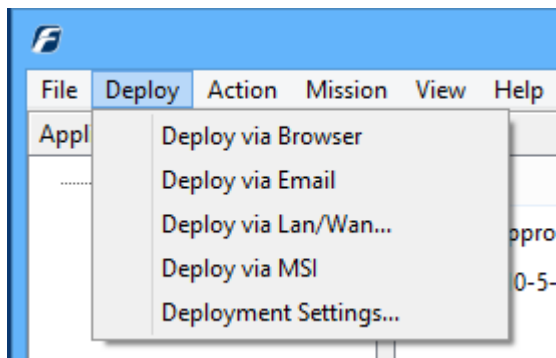
Service Description: provides the option for further details about the F-Response Universal Service.

Executable Filename: The service executable can be renamed as well.

Wait Hint(Seconds): Is the time the subject will wait before checking into the F-Response Universal Appliance should it lose connectivity. The default is one hour (3600 seconds).

Deploying F-Response Universal

F-Response Universal software can be deployed to remote target systems a number of ways, including via Browser, Email, LAN/WAN, or MSI. The browser and email methods are non-covert (a GUI will appear on the subject), while the LAN/WAN and MSI allow for covert connection.



Deploy Via Browser

The first deployment option on the list, **Deploy via Browser**, will provide a link to the subject (client) software for various operating systems². Individual software links or the link to the F-Response Client Downloads page can be provided to remote subjects directly.

F-Response Client Downloads

Clients

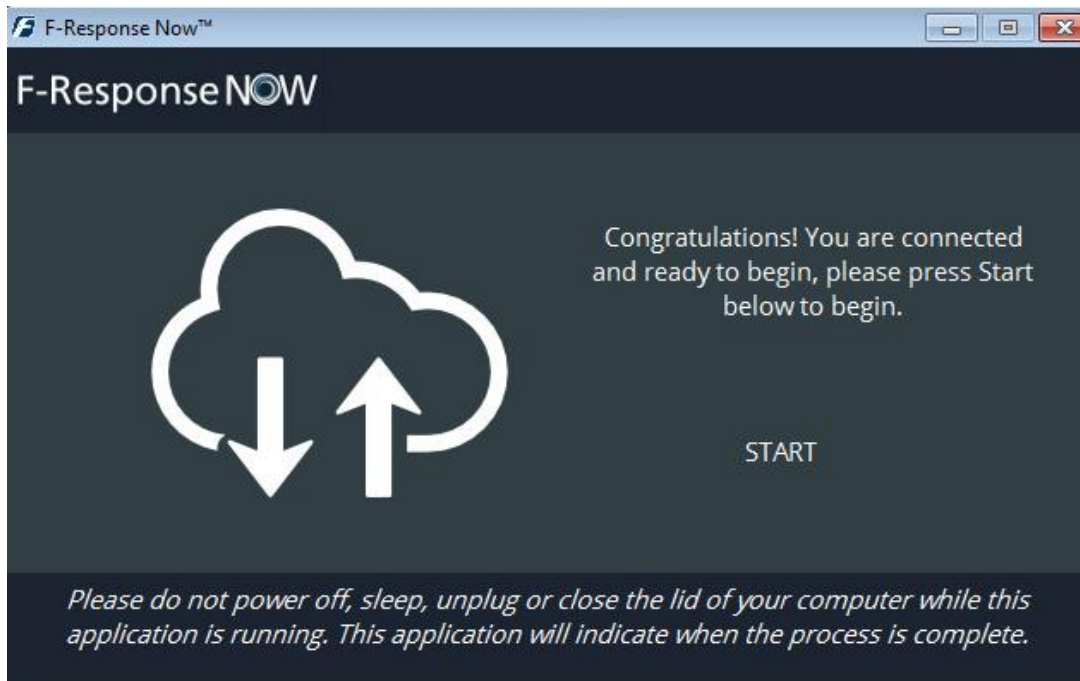
Client Executables (5)

Name	Download
F-Response Windows GUI Client RECOMMENDED	Link
F-Response Apple OSX Client	Link
F-Response Apple OSX Command Line Client	Link
F-Response Linux 64bit Client	Link
F-Response Linux 32bit Client	Link

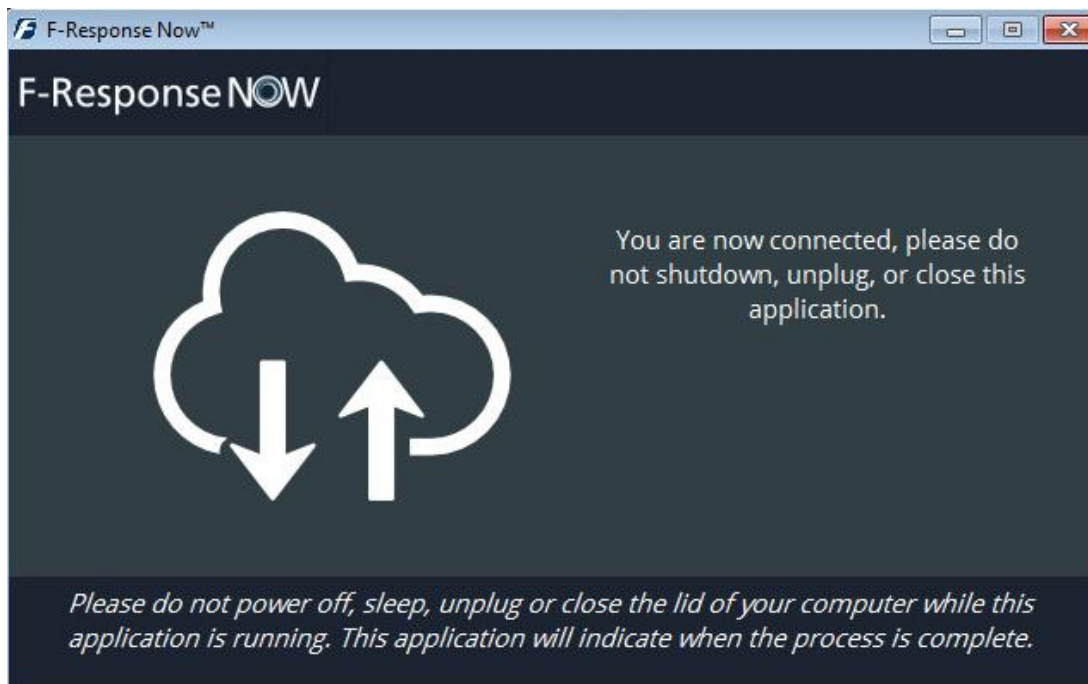
² Note if the appliance is in mission mode, a mission must be created for the subject(s) prior executing the subject software from the Downloads page.

Windows Subjects

Download the Windows subject software from the link on the Downloads page. The executable must be run with administrative rights to access the subject machine's resources. Double click on the executable and the F-Response GUI window will appear:



Click the start link in the window and the GUI will show the software as connected to the Appliance:

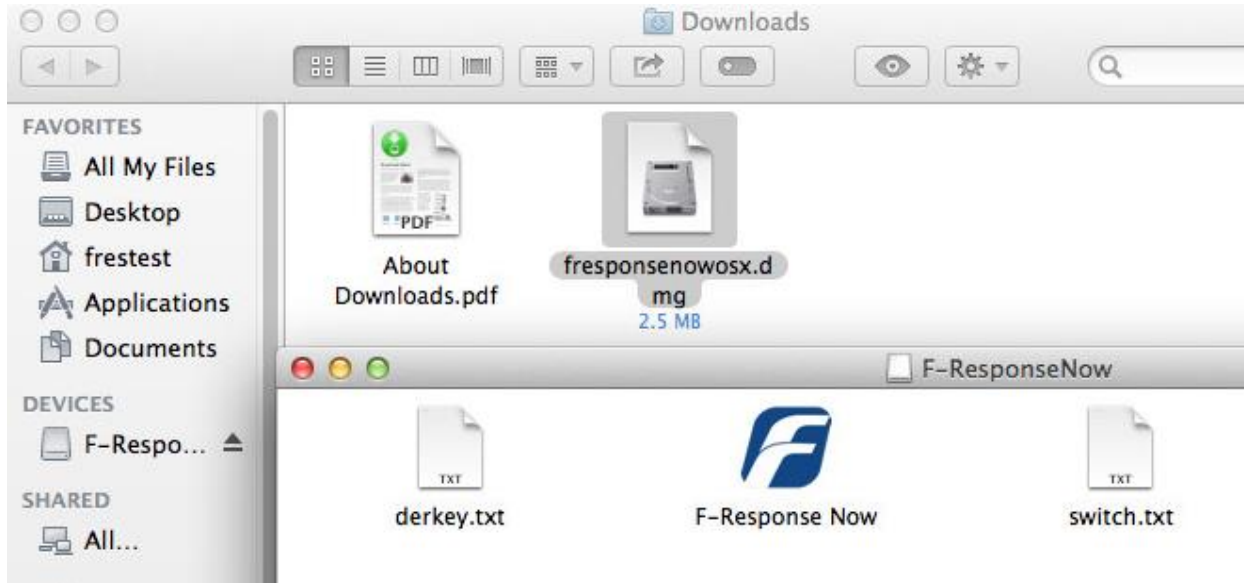


The subject should now be visible in the F-Response Universal console on the examiner machine.

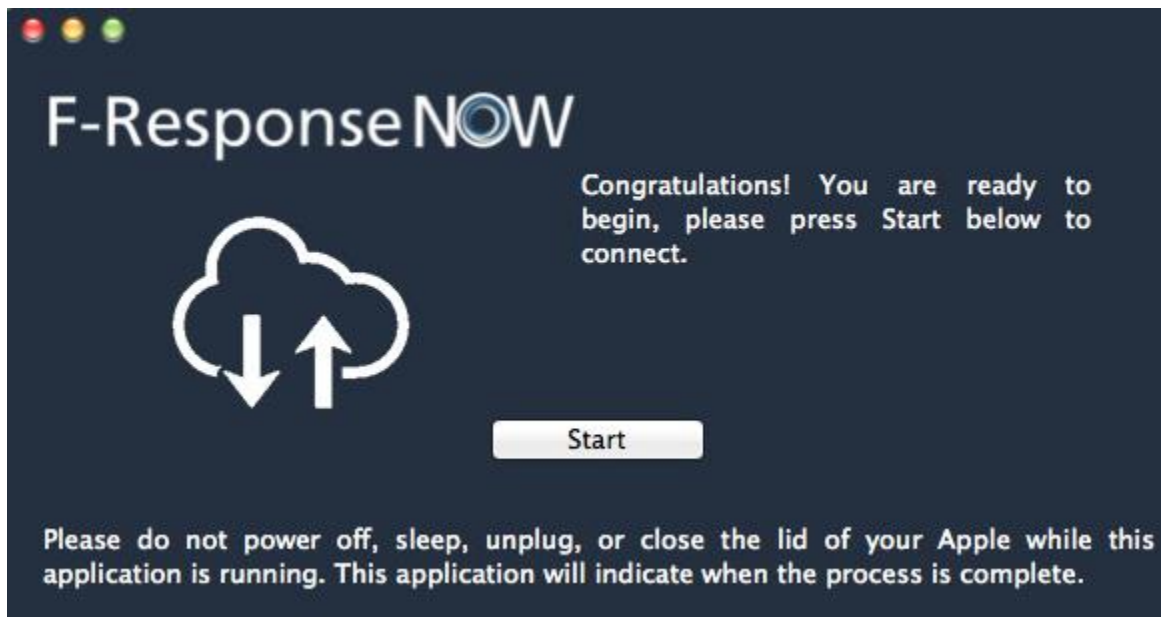
Apple Subjects

The Downloads page contains a link for the Apple OSX subject executable. Use the following steps to download and execute the software on the Apple OSX machine.

Download the OSX client and open the Downloads folder. Double click on the frespsenowosx.dmg file and it will mount as a drive.



Right-click on the F-Response Now icon and choose Open (Note: double-clicking will not work). Choose Open when presented with the identity warning. The F-Response client software will appear:



Click the start button and enter the password to start the software on the client:



The software will start on the Apple subject and appear in the examiner console:



The subject should now be visible in the console on the examiner machine.

Alternatively, command line version of the software can be downloaded and executed from a terminal session on the Apple subject.

Open the Terminal in Apple OSX, use the Finder->Applications->Utilities->Terminal to get started.

1. Use curl or a similar tool to download the appropriate executable, the 'JO' option will copy the subject executable with the relevant information for the appliance:
`curl -JO http://<YOUR APPLIANCE>/dl?file=frespsenowosxcmd`
2. Mark the file as an executable
`chmod +x frespsenowosxcmd<relevantapplianceinfo>`
3. Execute the software as admin using sudo
`sudo ./frespsenowosxcmd<relevantapplianceinfo>`

See the example below for downloading and executing the Apple OSX command line version of F-Switch.

```

tmp — frespnsenowosxc — 80x24
sh-3.2# curl -JO http://fs-test-univ/dl?file=frespnsenowosxcmd
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 1038k  100 1038k    0     0 2322k    0  --:--:--  --:--:--  --:--:-- 2323k
curl: Saved to filename 'frespnsenowosxcmd_fs-test-univ_80_968ee6e520'
sh-3.2# chmod +x frespnsenowosxcmd_fs-test-univ_80_968ee6e520
sh-3.2# sudo ./frespnsenowosxcmd_fs-test-univ_80_968ee6e520
F-Response Universal/Now Client (Apple OS X),(Version 1.0.73.9) Started.

```

Linux Subjects

The Downloads page contains links for both 64 and 32 bit Linux (x86 and x64) subject executables. Use the following syntax to execute the software on the Linux machine:

1. Use wget or a similar tool to download the appropriate executable:
wget -O frespnsenow-lin http://<YOUR APPLIANCE >/dl?file=frespnsenowlin
2. Mark the file as executable:
chmod +x frespnsenowlin
3. Execute the software as root (either as root directly or using “su” or “sudo”):
./F-Response Universal-lin -s <YOUR APPLIANCE>

See the example below for downloading the x64 version of F-Response Universal to a remote x64 bit Linux machine.

```

root@lin64-ubuntu14:/tmp# wget -O frespnsenow-lin64 http://fs-test-univ/dl?file=frespnsenowlin64
--2014-11-14 16:41:56-- http://fs-test-univ/dl?file=frespnsenowlin64
Resolving fs-test-univ (fs-test-univ)... 192.168.1.224
Connecting to fs-test-univ (fs-test-univ):192.168.1.224:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 242796 (237K) [Application/octet-stream]
Saving to: 'frespnsenow-lin64'

100%[=====>] 242,796  --.-K/s  in 0.004s

2014-11-14 16:41:56 (56.6 MB/s) - 'frespnsenow-lin64' saved [242796/242796]

root@lin64-ubuntu14:/tmp# chmod +x frespnsenow-lin64
root@lin64-ubuntu14:/tmp# ./frespnsenow-lin64 -s fs-test-univ -w60
F-Response Universal/Now Client (Linux),(Version 1.0.73.9) Started.
-

```

Via Email

F-Response Universal can also be deployed via email by simply emailing the client download link to the remote user. The Deploy->Deploy via Email button does this for you by generating a sample email with the appropriate link using your registered email client. The client can then be instructed to follow the same steps for [Deploy Via Browser](#)

Via LAN/WAN

F-Response Universal also has the ability to deploy to subject machines directly over the LAN/WAN in the environment. Select Deploy->Deploy via LAN/WAN from the menu to view the dialog for pushing F-

Response Universal subject software over the network. There are 3 sections here: **Deployment Credentials**, **Scan for Machines**, and **Scan Results**.

The screenshot shows a window titled "Deploy via LAN/WAN" with a close button in the top right corner. The window is divided into four main sections:

- Deployment Credentials:** Contains the text "In order to deploy F-Response Universal to remote machines you must have valid credentials, use this button to add or remove credentials." and a button labeled "Configure Credentials".
- Scan for Machines:** Contains the instruction "Input a comma separated list of IP addresses and or machine names to be scanned (ex. MACHINE1, MACHINE2, 192.168.1.1)" and a large text input field. A "Start Scan" button is located to the right of the input field.
- Scan Results:** Features a table with three columns: "Hostname", "Platform", and "Status". Below the table is a large text area. To the right of this area are two buttons: "Install/Start F-Response" and "Stop/Uninstall F-Response".
- Errors:** Contains a large text input field for logging errors. An "OK" button is located at the bottom right of the window.

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 **User name** (with administrator level privileges), **Domain** (if local account leave blank), and **Password**. Click **Add Credential** to add it to the stack.

Deploy via LAN/WAN Credentials Configure

Windows Domain/Network Credentials

Username	Domain(Optional)	Password

Add

Username	Domain (Optional)
frestest	FRES...

Remove

Unix Credentials

User Account

User

Root

Assume Root

Password

User Password

Root Password

SSH Key File

Browse

Username	UserType	Auth Type	Assume Root
root	R	P	
frestest	U	P	sudo

Add

Remove

OK Cancel

Apple/Linux

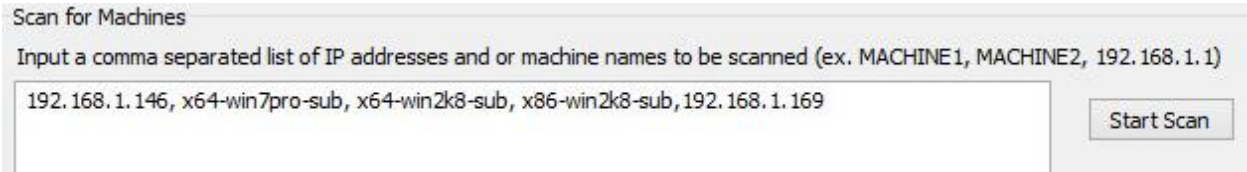
Under **Unix Credentials** credentials can be added for Apple OSX, and Linux subjects.

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, simple select root under **User Account**, check **Root Password** and enter the password. Click **Add Credential** for each account entered to add them to the stack.

Multiple accounts can be added if needed and the credentials are held for the duration of the F-Response Universal Console session. Click **Ok** in the lower right corner once all the necessary credentials have been entered.

Scanning for and deploying to Subject Machines

The **Scan for Machines** field allows for the input of a comma separated list of hostnames or IP addresses. Enter the list of subject machines to be deployed to and press **Start Scan** to the right of the text box.



Scan for Machines

Input a comma separated list of IP addresses and or machine names to be scanned (ex. MACHINE1, MACHINE2, 192.168.1.1)

192.168.1.146, x64-win7pro-sub, x64-win2k8-sub, x86-win2k8-sub, 192.168.1.169

Start Scan

The results will appear in the **Scan Results** box below:



Scan Results

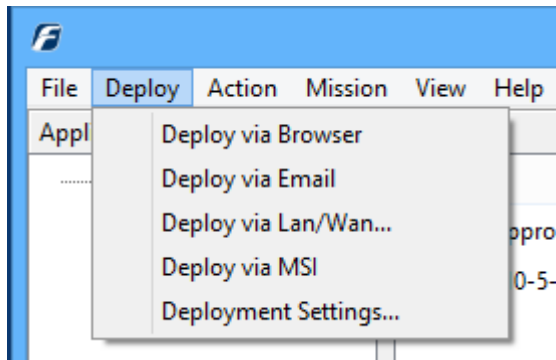
Hostname	Platform	Status
x64-win2k8-sub	Windows	Started
x64-win7pro-sub	Windows	Available
192.168.1.146	Apple OSX	Available

Install/Start F-Response

Stop/Uninstall F-Response

To install the F-Response Universal software on the subject machine, click on the hostname of the machine to highlight it, then select **Install/Start F-Response** on the right. After a short moment, in the **F-Response Software Status** column, the status of the machine will change to **Installed** and then **Started** showing it is connected to the F-Response Universal Appliance.

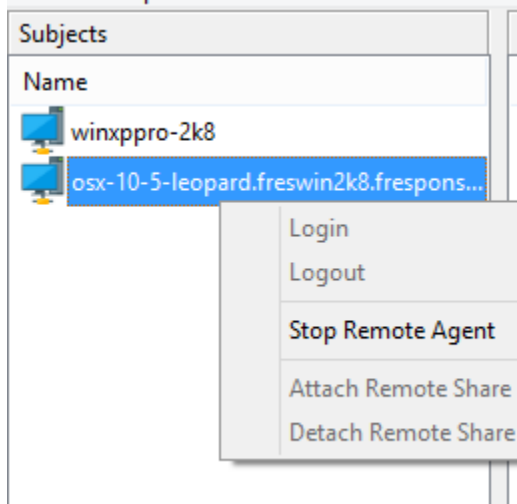
Via MSI



F-Response Universal offers the option to create a 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 very simple. Configure the [deployment settings](#) under Deploy->Deployment Settings. Once this is complete, click the Deploy->Deploy via MSI menu command and provide the location where the newly created MSI should be saved.

Stopping the remote software

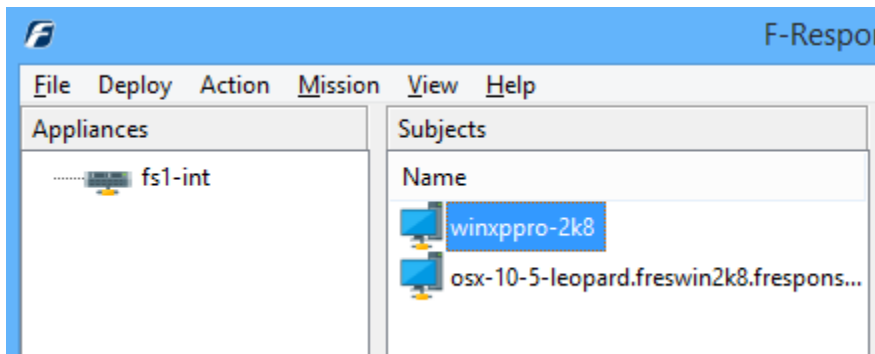


When finished using F-Response Universal on one or more subject machines, there are multiple ways to remove or stop the software on the remote machine. If the software was deployed using the LAN/WAN or MSI deployment options it should be stopped and removed using that same option. If the software was started manually by a remote user via the [Deploy via Browser](#) or [Email](#) option it can be stopped using the Action menu option Stop Remote Agent.

Working with Subjects

Listing Subjects

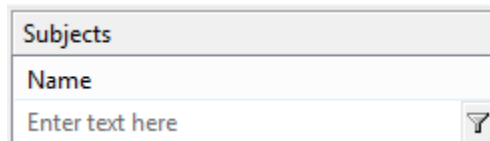
After starting the F-Response Universal software on one or more remote subjects the subjects will appear in the F-Response Universal Console as seen below.



Selecting any individual subject will populate the Targets window with available targets for that subject. Additional information on individual target types and authenticating to them is available in the "Connecting To Targets" section of this manual.

Filtering Subjects

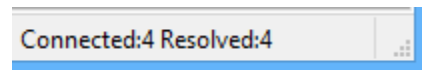
Using the "View->Filter" menu option you can enable a drop down filter over top of the Subjects listing. This filter view will allow the user to selectively reduce the overall number of visual Subjects using basic filtering ("Ex. z* would show all the Subjects starting with z").



Filtering can be unapplied at any time by simply turning off the filter view using the View menu.

Connected vs Resolved Targets and Subjects




Connecting to an F-Response Universal appliance triggers a background resolution process. This process will begin resolving and caching Subject machines and their Targets. As resolution updates the bottom right Status bar pain will contain additional details on the number of machines resolved vs connected. Keep in mind that not all Targets may be available until the resolution is complete.











Connecting to Targets

Target Devices

Each remote machine has the ability to display different targets based on the machine itself. The following list identifies the available Target types, where they are available, and what they represent:




- **DiscoveryShares™** 
 - DiscoveryShares™ allow F-Response Universal users to access a remote machine's files and folders completely read-only with no file locking, whether they be Windows, Linux, or Apple OSX. DiscoveryShares™ offer a great way for both technical and non-technical users to access a remote machine's files and folders.
- **Physical Drives, Partitions, and Volumes** 
 - F-Response Universal appliances provide a complete SCSI Adapter for presenting remote physical disk(s) as full, read-only SCSI devices.
- **MemoryShares™** 
 - MemoryShares™ provide live physical memory access to remote Windows subject physical memory as a live file, suitable for imaging and analysis with virtually any incident response product.











Targets	
Name	
	DiscoveryShare-C
	Disk-0-6144mb
	Disk-0-Part-1-Unused-0mb
	Disk-0-Part-2-Active-6134mb
	Disk-0-Part-3-Unused-9mb
	Disk-1-1024mb
	MemoryShare-384mb
	Volume-C-6134mb

DiscoveryShares™

Double click on the DiscoveryShare™ to access the files and folder on the remote subject. All activity is write protected by default.



The remote Apple OSX System files and folders can then be reviewed forensic or eDiscovery tools or simply using Windows Explorer natively.

Targets		
Name		Mount Point
	DiscoveryShare-AppleHD-/dev/rdisk0s2	\\.\E:\
	Disk-rdisk0-40960mb	
	Disk-rdisk0-Part-1-Unused-0mb	

Name ^
 .fsevents
 .HFS+ Private Directory Data
 .Spotlight-V100
 .Trashes
 .vol
 ^^^HFS+ Private Data
 Applications
 bin
 cores
 dev

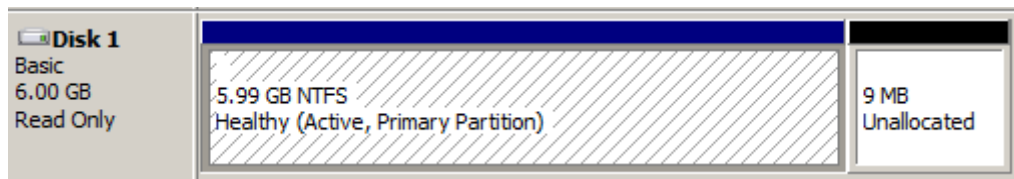
Physical Drives, Partitions, and Volumes

Double click on a physical device for the remote system. Once attached access to the full physical device is completely read-only. The attached drive is a full physical SCSI device in the context of the examiner machine. Individual partitions can also be connected separately using the Disk-X-Part-X Targets. Individual partitions will be shown as DOS drive letters.

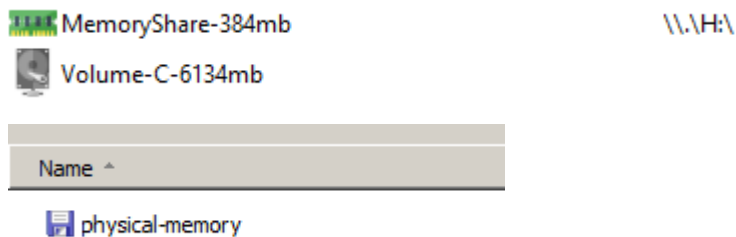
Targets	
Name	Mount Point
 DiscoveryShare-C	
 Disk-0-6144mb	\\.\PhysicalDrive1

MemoryShares™

Double click on the MemoryShare™ for a Windows system. Once attached, access to the complete



physical memory of the remote machine is presented via a “live file” on the share. This live file represents the physical memory of the remote machine in real-time and is not a snapshot or point in time image. Furthermore this image file can be readily opened and analyzed in applications like Volatility³ for real time analysis.



³ <http://code.google.com/p/volatility/>

Mission System

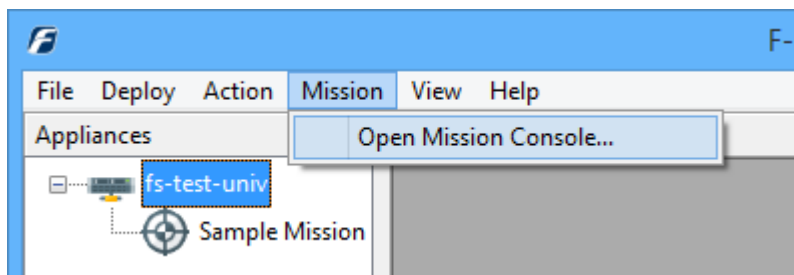
Overview of the Mission System

F-Response Universal offers the option of additional security controls by enabling the patent-pending Mission System, allowing for provisioning and de-provisioning access to F-Response Universal resources and capabilities. To enable the Mission System, enable the option in the F-Response Universal Configuration file (/etc/fswitch/fswitch.cfg).

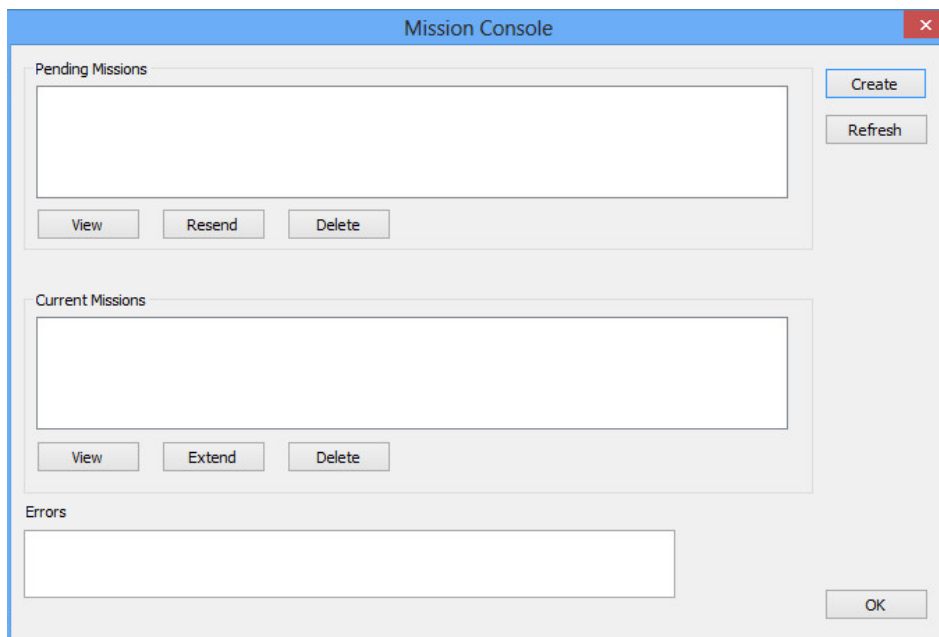
Access to subject machines is controlled by requests and approvals through email to an 'Approver'. Once the Approver verifies access is permitted to the requested subject machines, the examiner can then access and perform the required functions.

Creating a Mission

Please note that once a Mission is created it cannot be altered. If additional examiners or subject machines need to be added later the mission can be deleted and a new mission created or an additional mission can be created with the new information.



To add a new mission, highlight the appliance and click the Mission->Open Mission Console... command. If this command is disabled it means the Mission System has not been enabled on that appliance. The Mission Console dialog will open.



When clicking the Mission Console the screen will show the current and pending missions. To create a new mission, click the Create button option in the top right corner. The **Create New Mission** window will open:

First, create a name for the mission and enter it into the **Name** field. The Mission length is a minimum of one day and the length of time needed for the assignment is set in the **End Date** field.

The **Approver** field is critical as this should contain the email address of the individual in the organization responsible for allowing access to the specific client machine(s) listed in the mission request. The **Creator** Email address can be the current examiner creating the request, or another examiner who has been assigned to the mission task.

By default the current examiner logged into the system is added to the **Examiners** field. If additional examiners are part of this assignment they can be added here separated by commas. In the **Subjects** field, enter the list of subject machines by hostname, again, separated by commas.

Lastly, there is the option to add notes in the **Notes** field to further

explain the Mission request. Click Create in the lower right corner to create the mission and send the request for approval

Approval Process

The new mission will be listed in the **Pending Missions** section. There are options that allow for a review of the mission details (**View Mission**), a reminder of the request for approval (**Resend Mission**), and the ability to delete the mission completely.

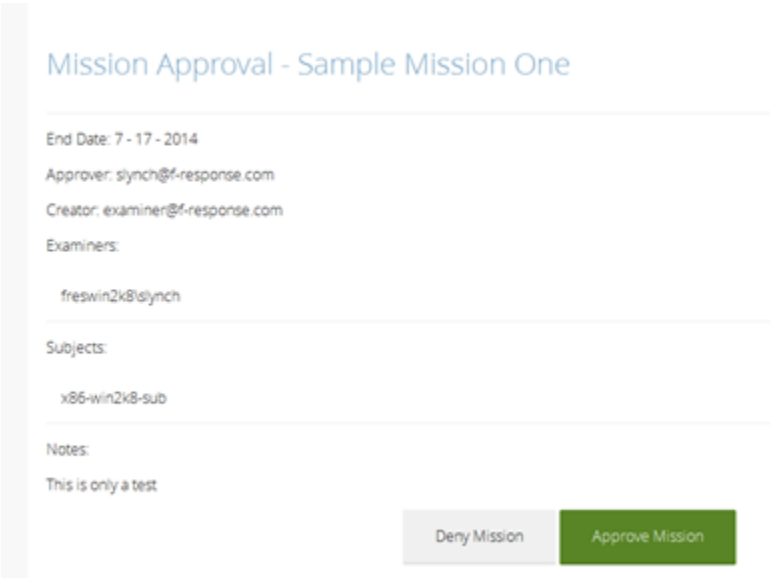
The approver will receive an email detailing the mission request with a link to approve or deny the requested mission:

freswin2k8\examiner has created the following mission, please review the mission and approve or deny the it via the link below.

Mission Name: Sample Mission One
Examiners: freswin2k8\examiner
Subjects: x86-win2k8-sub
Notes: This is only a test

https://fs2-int/mission?msid=677726&op=decision_view&token=677833

Clicking the hyperlink in the email will open a webpage on the switch and allow the approver to deny or approve the mission. Selecting either option will return an “operation completed” message and the approver can close the webpage.



Once the mission has been approved (or denied), the requesting examiner will receive a message notification of the action taken. If the mission is approved, the examiner can click the Refresh Missions link in the top right corner and the mission will appear under the Current Missions section indicating it is now active and will appear in the F-Response Universal Console.

Mission Status

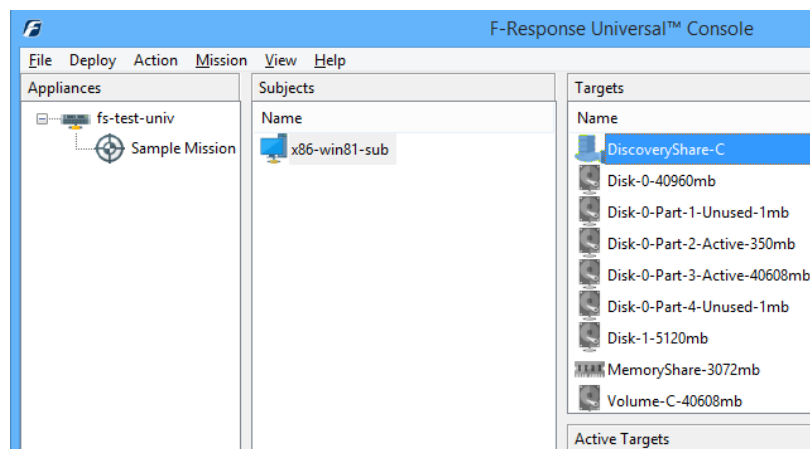
Once the mission has been approved it will move to the **Current Missions** portion of the window. If the mission console is open and the Approver grants access yet the mission does not appear in the **Current Missions** section of the screen, simply click the **Refresh** button.

There are options in the Current Missions sections to allow for a detailed review of the mission (**View Mission**), the ability to **Extend** the Mission request, or to **Delete** the mission completely.

The **Extend Mission** option will send a notice to the Approver letting them know the additional time that will be needed to complete the mission. Note when a mission expires it is not terminated. However, the Approver will receive a message letting them know the mission is still active. If an extension is sent the Approver will receive notification of the new date and receive another message if the new expiration date is reached.

Working with Active Missions

Approved missions will appear in the main console. Provided the requested subjects have the F-Response Universal client software installed on them, they will appear under the mission as they check into the system. How frequently subjects will check into the switch and appear in the mission is determined by the Wait Hint as configured in [Deploy->Deployment Settings....](#)



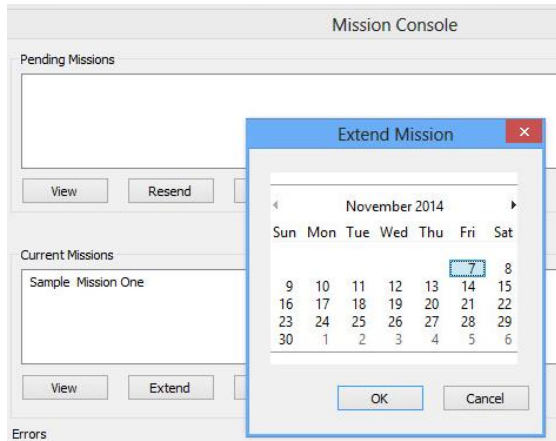
Once the subject machines appear under the Mission, double click on a machine to obtain a list of potential targets.

Mission Expiration/Deletion

A mission will remain active until deleted by the Examiner in the Mission Console. The Approver will receive a message notification that the mission has reached its allotted time but is still active. The Examiner has the option to extend the date and trigger a new notification to the Approver, but the expiration will not affect the open mission.

If additional subjects need to be added to an investigation, an additional mission must be created for these subjects or the mission deleted and recreated with all the pertinent subjects. Subjects cannot be added to a mission once created.

To Extend a mission, highlight the mission in the Mission Console and click the Extend button to choose the new expiration date:



A new email notification will be sent to the Approver.

To delete the mission completely, simply highlight the mission in the Mission Console and click Delete. A notification will be sent to the approver

Appendix A.

Legal Notices

Copyright © 2015 Agile Risk Management, LLC. All rights reserved.

This document is protected by copyright with all rights reserved.

Trademarks

F-Response, DiscoveryShare, MemoryShare, and F-Switch are trademarks 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; and other Patents Pending.

Appendix B.

Release History

2.0.1.11 -> Updated F-Response Universal deployment processes to handle the recent changes in Apple OSX El Capitan. Additional minor user interface corrections.

2.0.1.6 -> Updated F-Response Universal User Interfaces (Now and Universal) for more efficient usage. Additional icons, grids, and layout to provide for an easier user experience. Modifications to the LDAP authentication system allowing for more diverse Domain authentication scenarios. Additional Examiner software packages for Apple OSX and Linux. Minor adjustments to the Mission System to address ipv6 address differences. Modifications to the F-Response Universal Subject software for Windows to reduce potential for hibernation and sleep while actively mounted.

1.0.75.7 -> Corrected issues with remote DiscoveryShare name content filtering. Upgraded the F-Response F-Switch SCSI Adapter to address a timing issue during drive attach/detach operations. Added a complete LDAP configuration testing tool to address issues with properly configuring LDAP authentication. Added additional options in configuration to handle IPv4/IPv6 socket binding.

1.0.75.6 -> Addressed issues with remote DiscoveryShare content that violates Windows naming conventions. Modified the physical drive numbering detection model. Improved LDAP authentication model to better handle complex LDAP configurations.

1.0.75.5 -> Updated F-Response Universal and Now clients to better detect spurious memory reservations, address internal drive and volume access authentication inconsistencies. Updated F-Response Universal and Now appliance software to improve LDAP/Active Directory integration, better handle systems with modified tcp ports. Updated F-Response Univ/Now Linux examiner to reduce 3rd party dependencies and streamline configuration. Libconfig dropped in favor of Lua style configuration and additional build platform included, Centos 7. Updated Android apk build to improve performance based on internal testing and user feedback. Windows F-Response Univ/Now console improvements for stability.

1.0.75.4 -> Updated F-Response F-Switch SCSI driver to revision 4. Improved stability and performance in high speed IO operations. Modified worker process to improve stability and memory consumption in high speed IO operations.

1.0.75.3 -> Modifications to the internal F-Response Univ/Now architecture to improve data transmission speed and performance.

1.0.75.2 -> Modifications to the examiner driver stack to improve performance, stability, and reduce potential for device timeout.

1.0.75.1 -> Modifications to subject executables to include dynamic reconnection to Univ/Now, additional keep-alive improvements to long haul network links, read timeouts and stability updates.

1.0.74.8 -> Modifications to address worker process loading in non-standard operating environments.

Initial Release -> 1.0.74.7

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.

=====

Copyright (c) 1998-2011 The OpenSSL Project. 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.
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.

Copyright © 2006 Alistair Crooks. 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.
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 Huguin <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.