F-Response Collect Manual

8.7.1.33

Provides a complete breakdown of leveraging F-Response Collect to perform expert remote image collection.

Contents

Terminology

The term “Server” refers to the F-Response Collect Server software product. The F-Response Collect terms “Examiner” and “Subject” are used throughout this manual. The definitions for Examiner, Subject are as follows:

Examiner

F-Response Collect Examiner refers to the applications used to connect to the F-Response Collect Server and create collections as well as download completed images.

Subject

F-Response Collect Subject refers to the applications used to perform those collections.

Supported Platforms

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

Microsoft Windows (7, 2008r2, 2012, 8, 2012r2, 10, 11, 2016, 2019, 2022) both 32 and 64-bit

Redhat/Centos/Rocky Linux 7+ 64-bit

Apple (developed on OSX Ventura for filesystem and user directory collection, can be run on arm/M1/M2 and heritage Intel/x86/64)

The F-**Response Collect Examiner tools** can be installed and run on:

Microsoft Windows (10, 11, 2012, 2016, 2019, 2022)

The **F-Response Collect Server** can be run on:

Redhat/Centos Linux 7+ 64-bit

Redhat 8/9 64 bit

Windows (10, 11, 2012, 2016, 2019, 2022) 64-bit

Overview

F-Response Collect is a server-based product provided by F-Response which provides forensic image collection services of remote subjects across virtually any routable IP network. F-Response Collect allows for the continuous collection of fully recoverable images (disks, volumes, profiles, and custom content) regardless of geographic distance or mobility of remote subjects.

F-Response Collect Server

Hardware Requirements

The largest overall indicator of performance is the CPU cores (virtual or physical) dedicated to the server. More cores translate to more active data connections to the server.

Recommended hardware configuration:

- 4-8 Cores
- 4-8 Gigabytes of RAM
- n Gigabytes of Drive Storage (Storage space needs are based on imaging requirements)
- 1+ Gigabit Ethernet ports

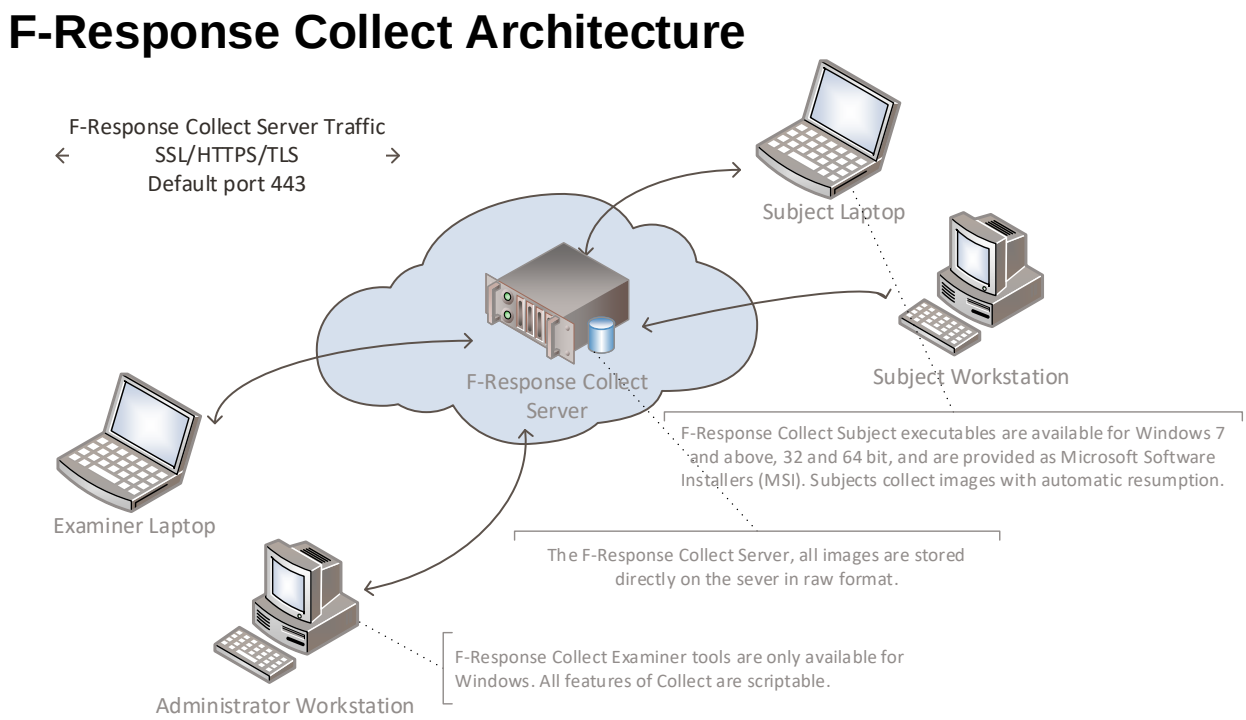
F-Response Collect Server License Validation

The F-Response Collect Server license is tied to the hardware of the server it is installed on and requires the IP and MAC address(es) are static/reserved for the machine. If you have unused network interfaces that might draw or generate a random address, you will want to disable those interfaces before continuing.

The F-Response Collect server must be able to contact license.f-response.com on TCP port 443 to maintain license validity. You may configure the proxy settings if your organization requires use of a proxy to connect to internet-based servers.

Architecture

F-Response Collect communication occurs over TCP Port 443(TLS/SSL/HTTPS) by default.



Basic Installation and Setup (Server) - Linux

You will find the latest server and examiner installation packages at https://www.f-response.com/support/downloads. To access this page, you will need your license number (Ex. 1999x). In addition, server configuration is done via the F-Response Configuration Tool that is installed as part of the F-Response Collect Examiner Windows installation package.

The F-Response Collect Server software is provided in RPM format for Centos/RedHat Enterprise Linux. If you are upgrading a current installation do not uninstall, simply run the new executable over the existing version to upgrade and keep your settings.

The full scope of installing and configuring a Centos/RedHat Enterprise server is beyond the scope of this document, but the following should be considered specific to F-Response Collect.

Collection Destination

Since F-Response Collect is used to collect forensic images, a sufficiently large storage destination on the server is a must. In addition, since the write speed must be reasonably high, we do not recommend quasi network storage solutions like SMB. Simply put, we recommend creating either a partition or attaching a disk, formatting it with a modern filesystem (Ext4, etc.), and creating a memorable mount point for that location. The examples herein use "/evidence" as the destination, but you are free to use whatever mount point you like provided it survives a reboot.

Network Hardware and Licensing

Be sure to make sure all active network interfaces either have a static network address configured or are set to use DHCP with a defined reservation. This will greatly reduce the chances for license invalidation post install.

Firewall(s)

F-Response Collect is going to bind to and listen on TCP port 443, as such, you will want to confirm there are no firewalls actively blocking traffic on that port. The proper configuration and management of firewalls is distribution specific and beyond the scope of this document.

Installing F-Response Collect

Note: All commands must be run with admin(root) privileges.

```
# rpm -Uvh F-Response-Collect-….rpm
```

Starting and Stopping F-Response Collect

Note: All commands must be run with admin(root) privileges.

```
# service frescollect start
```

```
# service frescollect stop
```

```
# service frescollect status
```

Basic Installation and Setup (Server) - Windows

You will find the latest server and examiner installation packages at https://www.f-response.com/support/downloads. To access this page, you will need your license number (Ex. 1999x). In addition, server configuration is done via the F-Response Configuration Tool that is installed as part of the F-Response Collect Examiner Windows installation package.

The F-Response Collect Server software is provided in an installer format for 64-bit Windows. If you are upgrading a current installation do not uninstall, simply run the new executable over the existing version to upgrade and keep your settings.

The full scope of installing and configuring Windows server is beyond the scope of this document, but the following should be considered specific to F-Response Collect.

Collection Destination

Since F-Response Collect is used to collect forensic images, a sufficiently large storage destination on the server is a must. In addition, since the write speed must be reasonably high, we do not recommend quasi network storage solutions like SMB. Simply put, we recommend creating either a partition or attaching a disk, formatting it with NTFS, and making it accessible under a drive letter. The examples herein use “e:\” as the destination, but you are free to use whatever drive letter you would like provided it is physical and persistent.

Network Hardware and Licensing

Be sure to make sure all active network interfaces either have a static network address configured or are set to use DHCP with a defined reservation. This will greatly reduce the chances for license invalidation post install.

In addition, run the following two commands in an administrator command prompt to disable typically unused interfaces that may interfere with licensing:

netsh interface isatap set state disabled
netsh interface teredo set state disabled

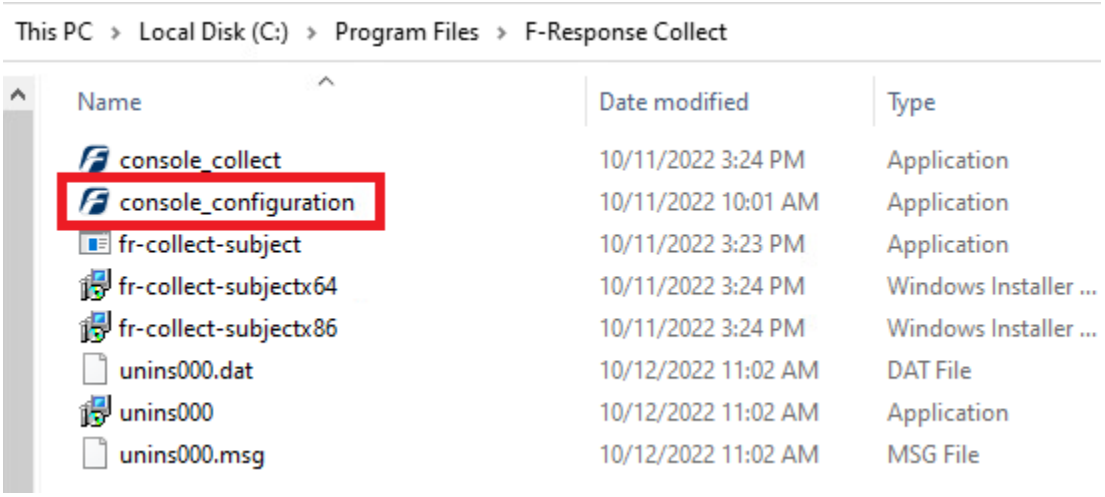
Firewall(s)

F-Response Collect is going to bind to and listen on TCP port 443, as such, you will want to confirm there are no firewalls actively blocking traffic on that port. The proper configuration and management of firewalls is Windows specific and beyond the scope of this document.

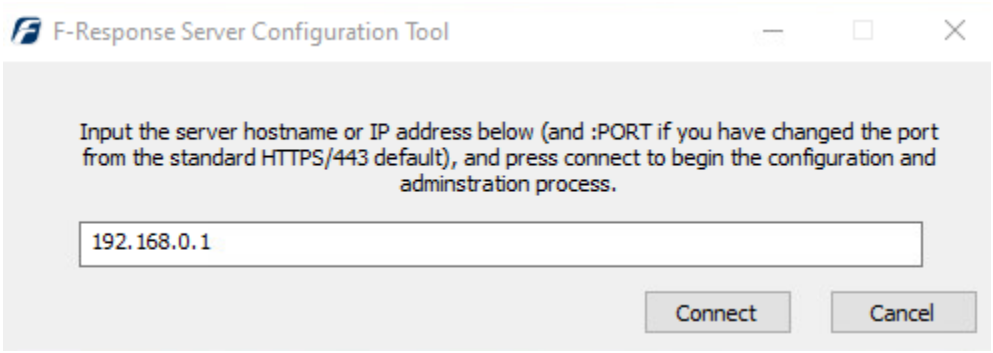
Getting started with F-Response Collect

Initial Configuration

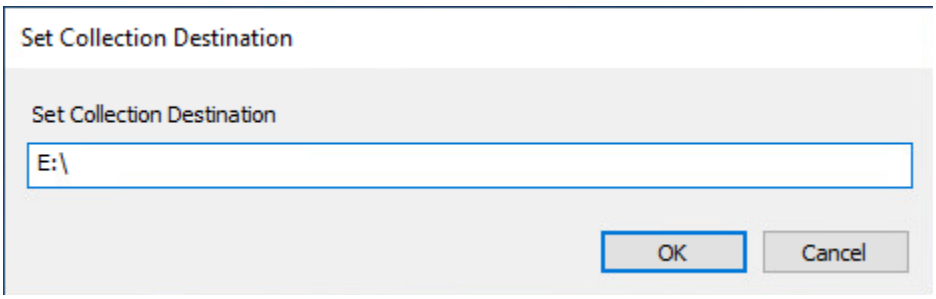
All configuration of the F-Response Collect Server is done through the F-Response Configuration Tool (console_configuration.exe) from an examiner computer. This tool is installed as part of the F-Response Collect Examiner installation package and will update the frescollect.cfg file on the server with the correct formatting for you.



The first step after executing the tool is to input either the hostname or IP address of the remote Collect Server. Since this is a new and unconfigured server, the Configuration Tool will step through a series of dialogs to configure the server for use.

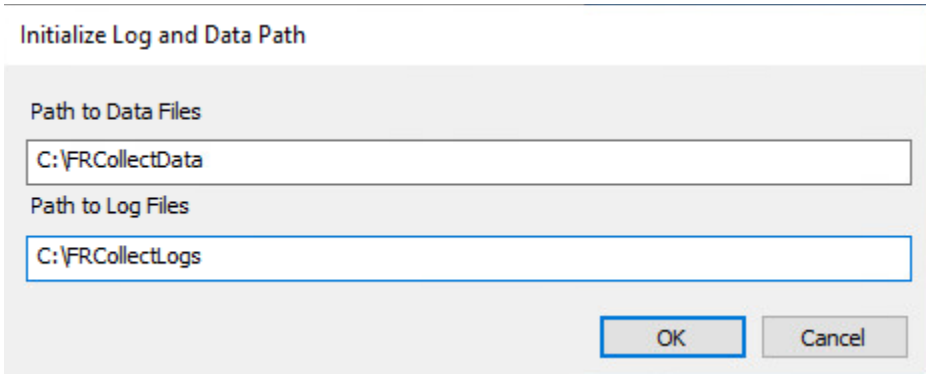


Next you will be prompted to enter a Collection Destination for image data collected on the Collect Server (the destination on the server where images will be saved). Consider the amount of data you will be collecting and choose a location with adequate storage space.

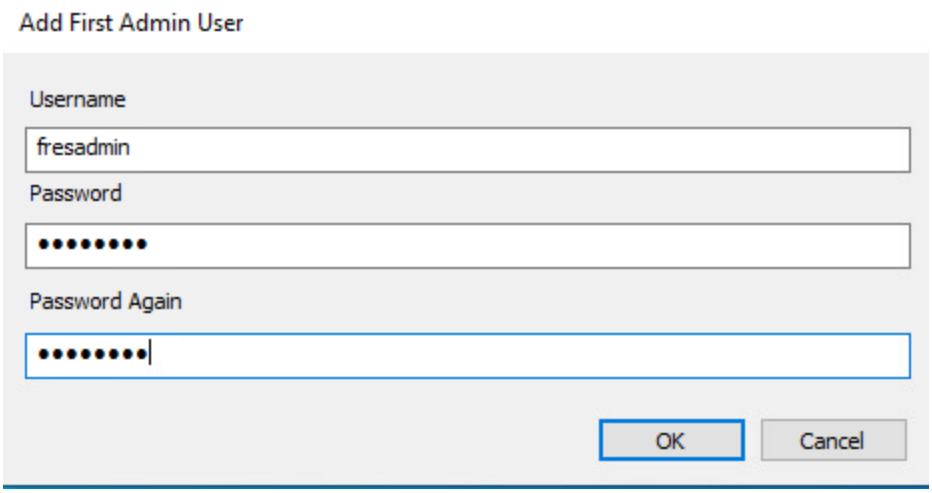


Type in the location for your collections and confirm by selecting the **OK** button. For Collect Server under Windows this would be the typical path with drive letter, For example **E:** or **E:\Evidence**.

The next prompt will be for your Data and Log folder locations. You can place these folders where you like but do not put them in the same location as your collections (from the previous step) or in the Program Files directory as Windows will sometimes enact UAC controls and cause problems. The Data folder contains operation data necessary to run the server. This includes user credentials, subjects, examiner, etc.

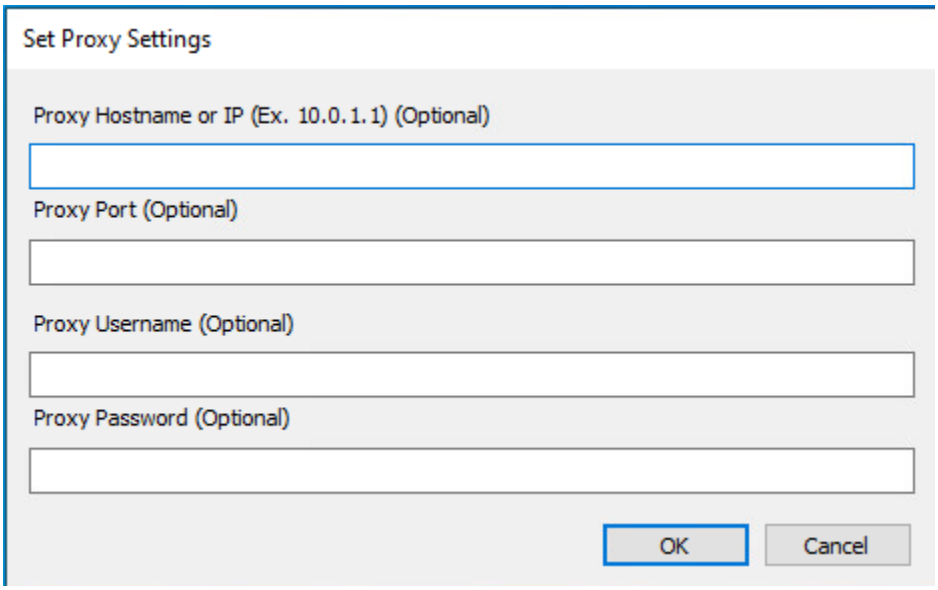


Next, you'll be prompted to create an administrator account.

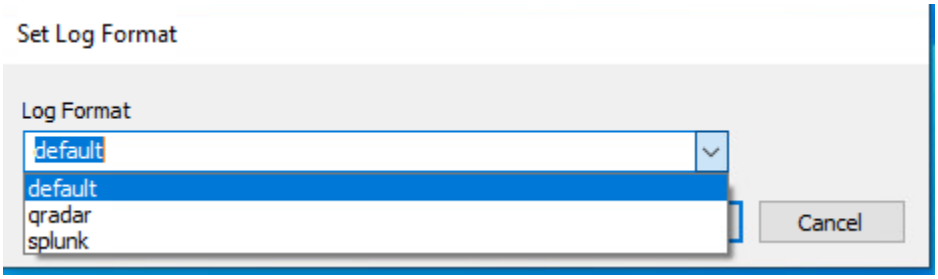


This is the administrator account you will use to login to the F-Response Collect Server initially and may be removed or changed later.

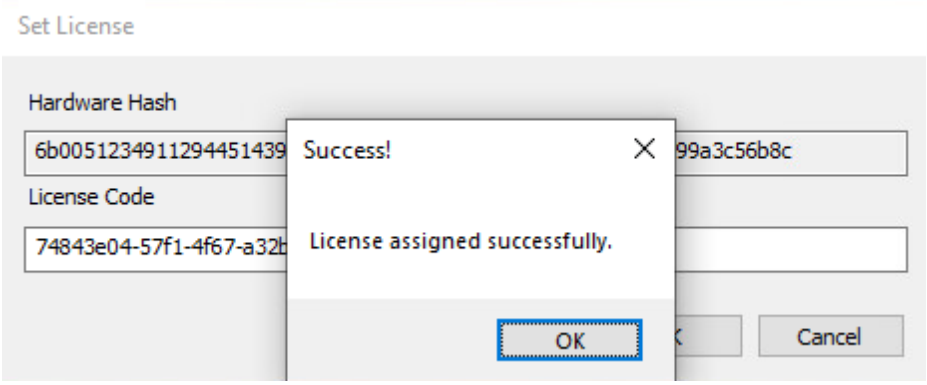
Once a valid account has been created, you will be prompted to input a proxy configuration (optional). This is necessary if your environment blocks the F-Response Collect server from accessing our internet facing licensing server(license.f-response.com) directly. If you do not need to input proxy information you may leave these fields blank and simply click the **OK** button.



Next, you will be asked what format you would like for log records. Please select the most appropriate format for your environment from the available drop-down options.

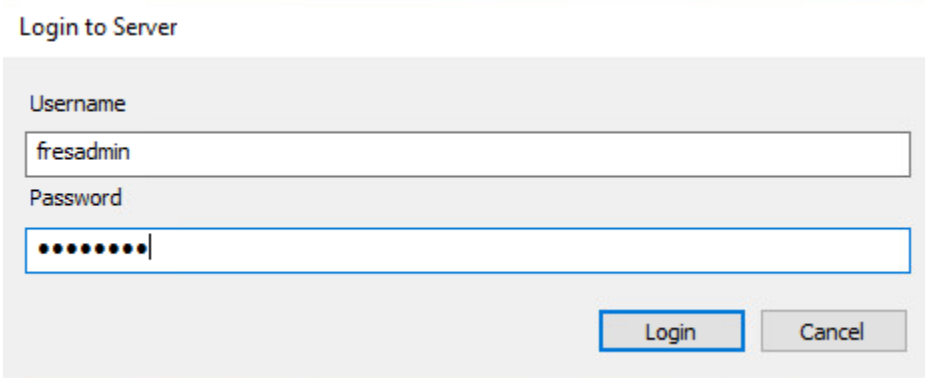


The next configuration item you will be prompted for is the license code as provided by F-Response. Do not share this code and be sure to save it in a secure location going forward. This code will be necessary should you ever need to reactivate your F-Response Collect server.



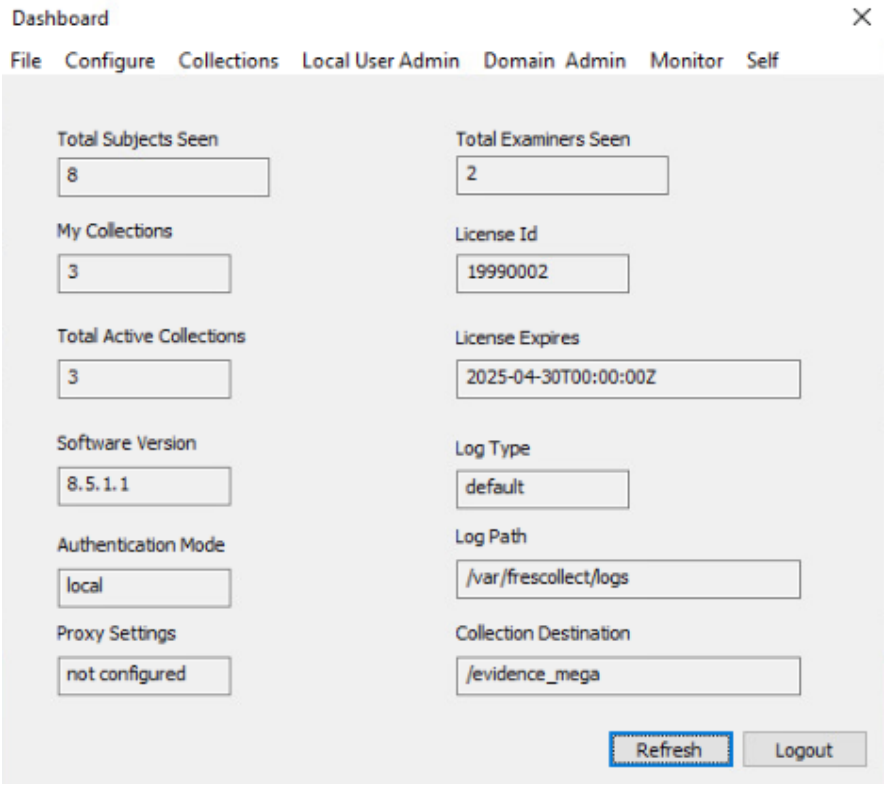
The hardware hash provided is a value generated by the Collect server based on the unique hardware configuration and should not be altered unless requested to by support. Paste in the license code and click OK to receive confirmation.

Provided everything worked correctly you should be greeted by an F-Response Collect login screen. Please use the initial user account created a few screens prior to login to the Server.



Upon successful login, you will see the F-Response Collect Dashboard which gives you an overview of the current state of your F-Response Collect server.

Dashboard



The dashboard gives you an initial overview of your Collect server. Here you can see:

Total Subjects Seen: The total number of subject computers that have been connected to the server.

Total Examiners Seen: The total number of examiner (or administrator) computers that have been connected to the server.

My Collections: Your total number of current active collections on the server.

License ID: The license number assigned to this server (needed for renewals and software downloads).

Total Active Collections: The total number of current active collections from all examiners and administrators.

License Expires: The date the license for the server will expire. (If a renewal has been paid and processed this field will update to the new date automatically once the current license expires.)

Software Version: The software version number currently running on the server.

Log Type: The current logging format (default is CSV).

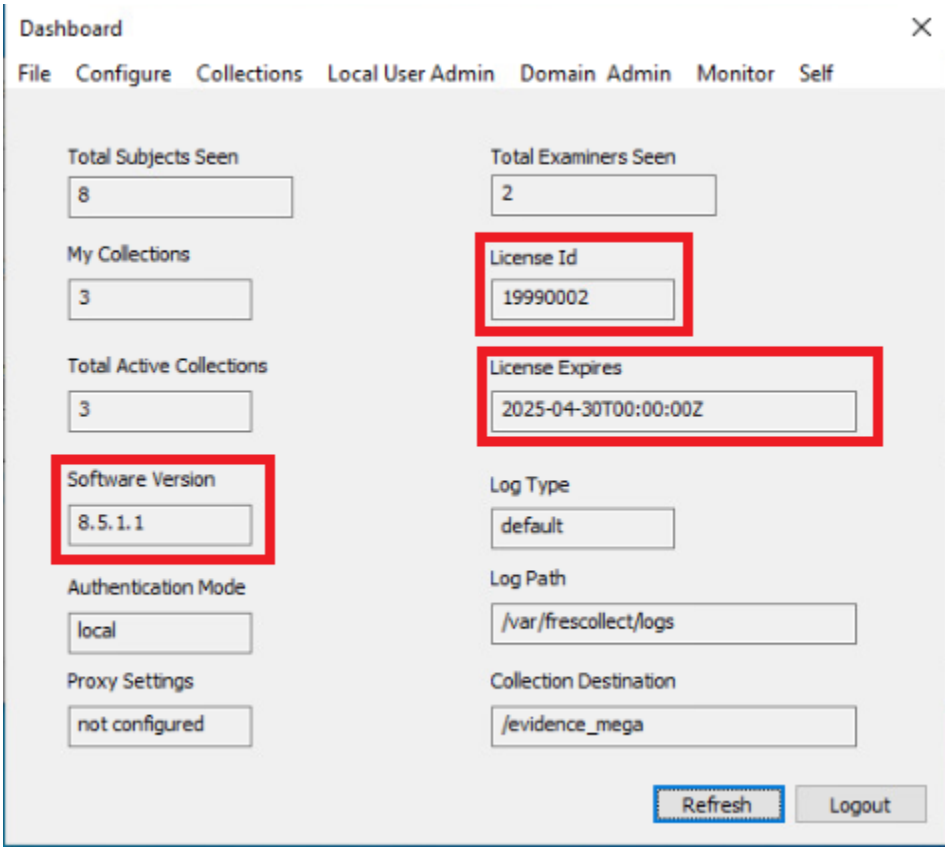
Authentication Mode: Authentication mode for the server can be set for Active Directory or local authentication.

Log Path: The location on the server where the logs are stored.

Proxy Settings: This field specifies if the server is configured to use a proxy for access to the F-Response licensing server.

Collection Destination: The location on the server where the image files will be stored.

Licensing/Software Updates



There are three important fields here to note for software and licensing: **Software Version, License Id,** and **License Expires**.

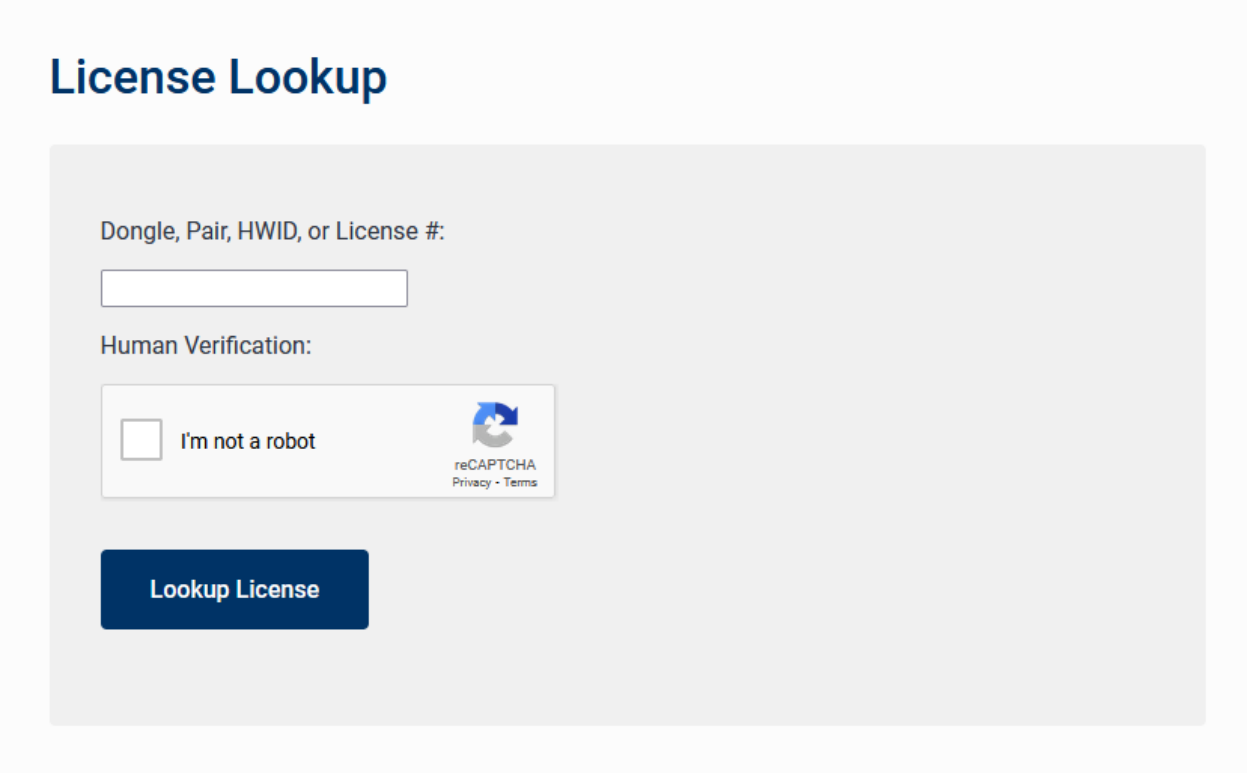
Software Version Number

The **Software Version** number of the Collect Server software you are running is provided on the Dashboard. Please make sure you are running the latest version of the software. There is no cost to upgrade to the latest version provided your license is not expired. There is nothing special required to upgrade the software to the new version—Do not uninstall the current software, just run the executable over the top to upgrade and keep all your settings.

The latest version of the software is always available from the download section of the F-Response website https://www.f-response.com/support/downloads. You will need your license ID number (below) to access the downloads.

License ID

The License ID number for your Collect server is visible on the Dashboard. This number can be entered into the downloads page https://www.f-response.com/support/downloads on the website to check for and obtain the latest version.



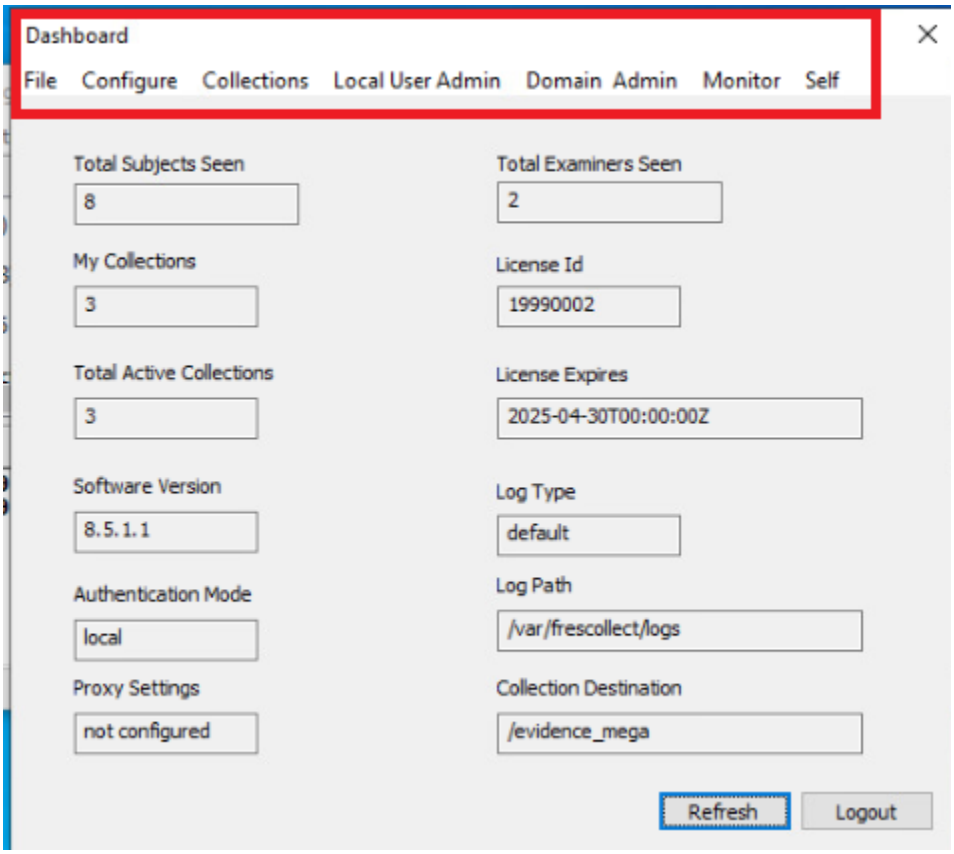
License Expiration

F-Response Collect is sold in 1- and 3-year license terms. The Collect software will cease to function on the expiration date shown on the dashboard. To renew F-Response Collect at the discounted renewal rate, the purchase must be made within 30 days post expiration.

To renew, go to the software renewals page on the F-Response website https://www.f-response.com/buyfresponse/software-renewals and complete the checkout process. Once the renewal is processed and the current license reaches expiration, the new license will automatically be downloaded and updated on the server.

Server Administration

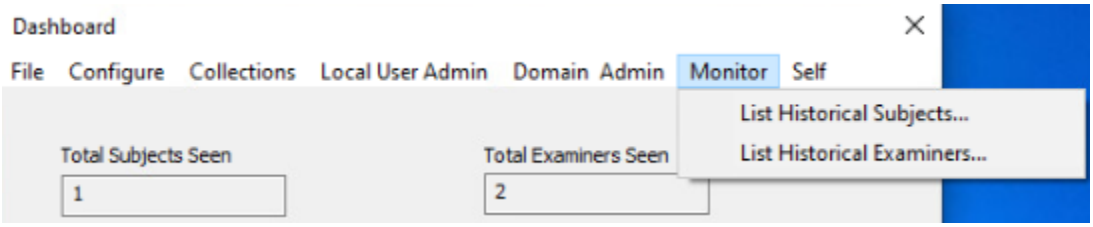
The Collect server can be configured using the drop-down menus along the top of the window.



Each of these options is covered below.

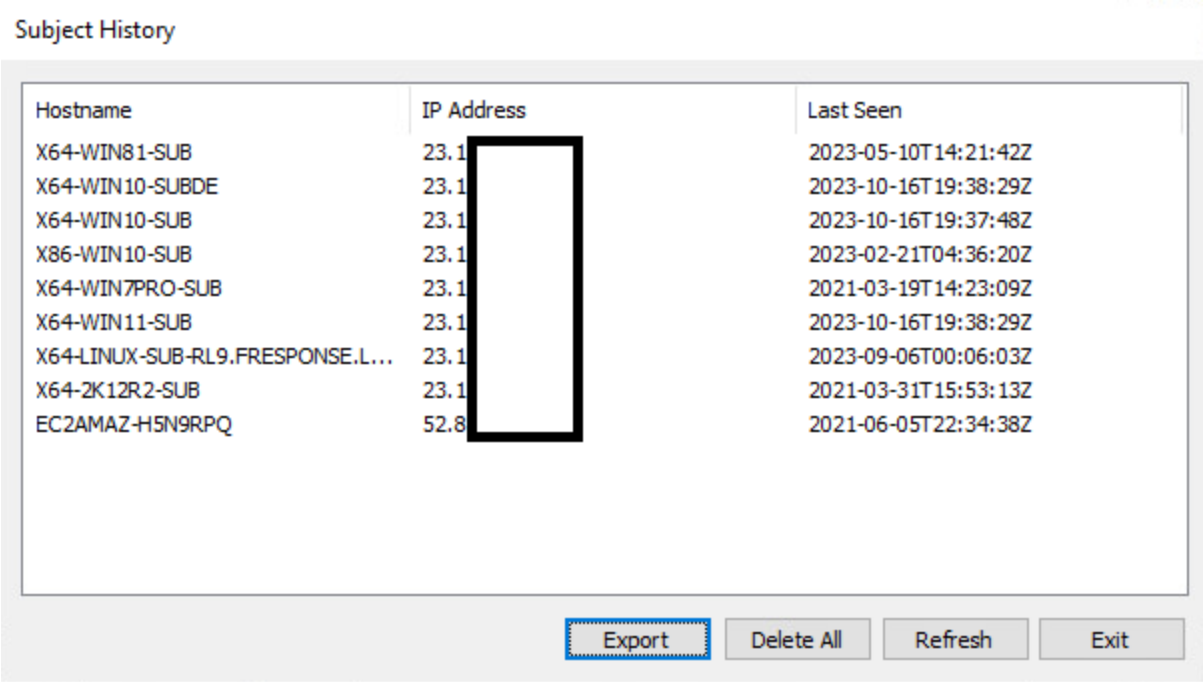
History

Further details on the **Total Subjects Seen** and **Total Examiners Seen** can be found by accessing the history on your server. Click on the **Monitor** drop down menu for the historical list of Examiner or Subject machines.



Subjects

Choose **List Historical Subjects…** from the **Monitor** menu to view subject computers that have checked into the server.

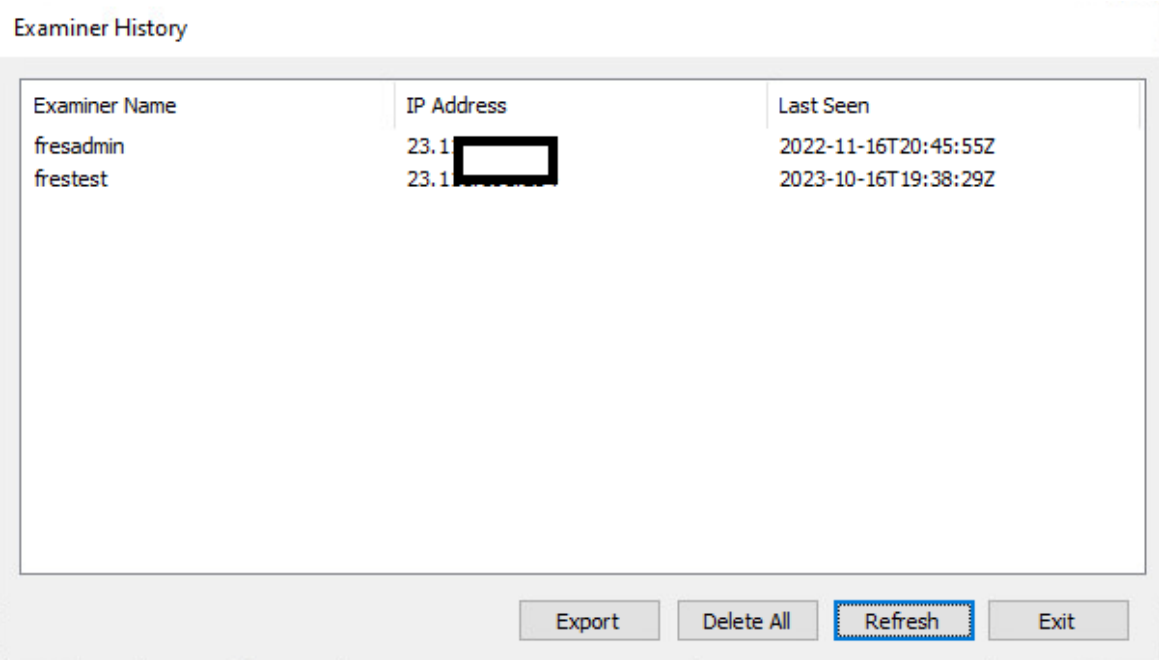


Here you can see the hostname and IP address of the subject, as well as the last time it checked in with the server. You can sort on any of the 3 columns depending on what you are looking for in the data. There is also an option to export the subject history to a csv file by clicking the Export button.

Lastly, you may choose to clear the Subject History completely. It is important to note this operation cannot be undone. After clearing, a new historical database will repopulate as subjects check-in with the server. To clear the subject history click the **Delete All** button.

Examiners

Choose **List Historical Examiners…** from the **Monitor** menu to view examiner computers that have checked into the server.



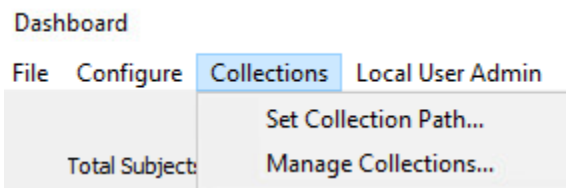
Here you can see the hostname and IP address of the examiner computer, and the last time the examiner logged into the server using the console. You can also sort on any of the 3 columns depending on what you are looking for in the data. There is also an option to export the examiner history to a csv file by clicking the Export button.

Lastly, you may choose to clear the Examiner History completely. It is important to note this operation cannot be undone. After clearing, a new historical database will repopulate as examiners login to the server using the management console. To clear the examiner history click the **Delete All** button.

Collections

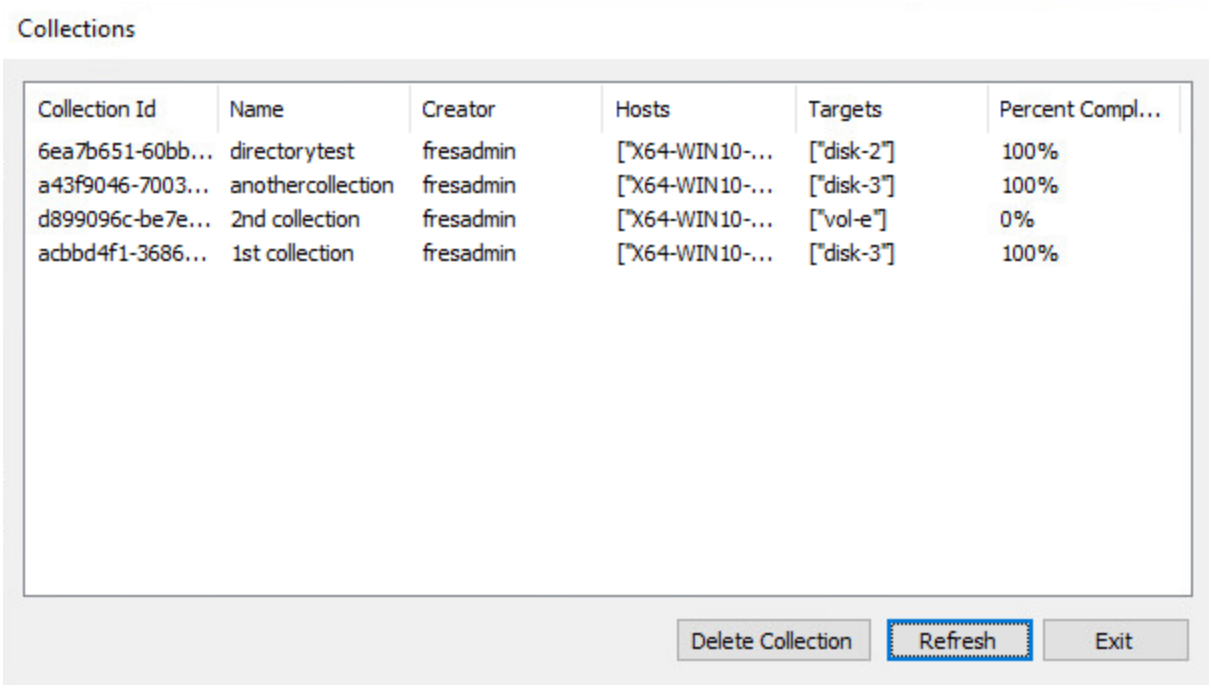
The dashboard will show the number of active collections for your login, as well as the total number of collections from all examiners/administrators on the server.

For more details about these collections, the Collections menu will allow you to change the collection path or view/manage your current collections. Both options are covered below.



Manage/View Collections

To view all the current active connections on the server, choose **Collections - Manage Collections…** from the Dashboard menu.



Here we can view the details for all current collections:

Collection Id: the unique identifier for the collection

Name: name of the collection entered by the examiner when it was created

Creator: The login of the examiner or administrator who created the collection.

Hosts: The list of remote subject computers within the collection.

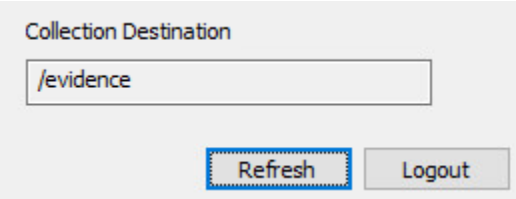
Targets: The remote system resource on the host to be imaged.

Percent Complete: The estimated completion of the collection (all hosts and targets).

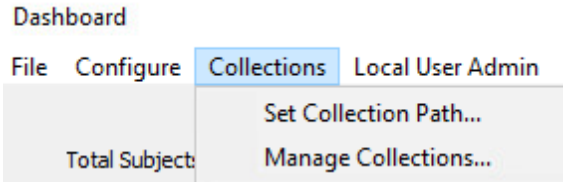
Collections no longer needed can be deleted from within the management console on the examiner computer but there is also an option here to remove a collection; simply highlight the collection and click the **Delete Collection** button to delete from the server. ***(CAUTION: This operation cannot be undone!)***

Collection Path

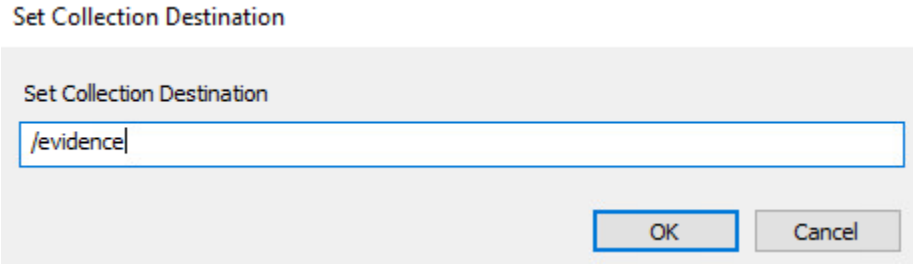
The location for images to be stored on the server as they are uploaded from the subjects is created when the server is first configured.



This path can be changed if needed by clicking the **Collections - Set Collection Path…** from the Dashboard menu.



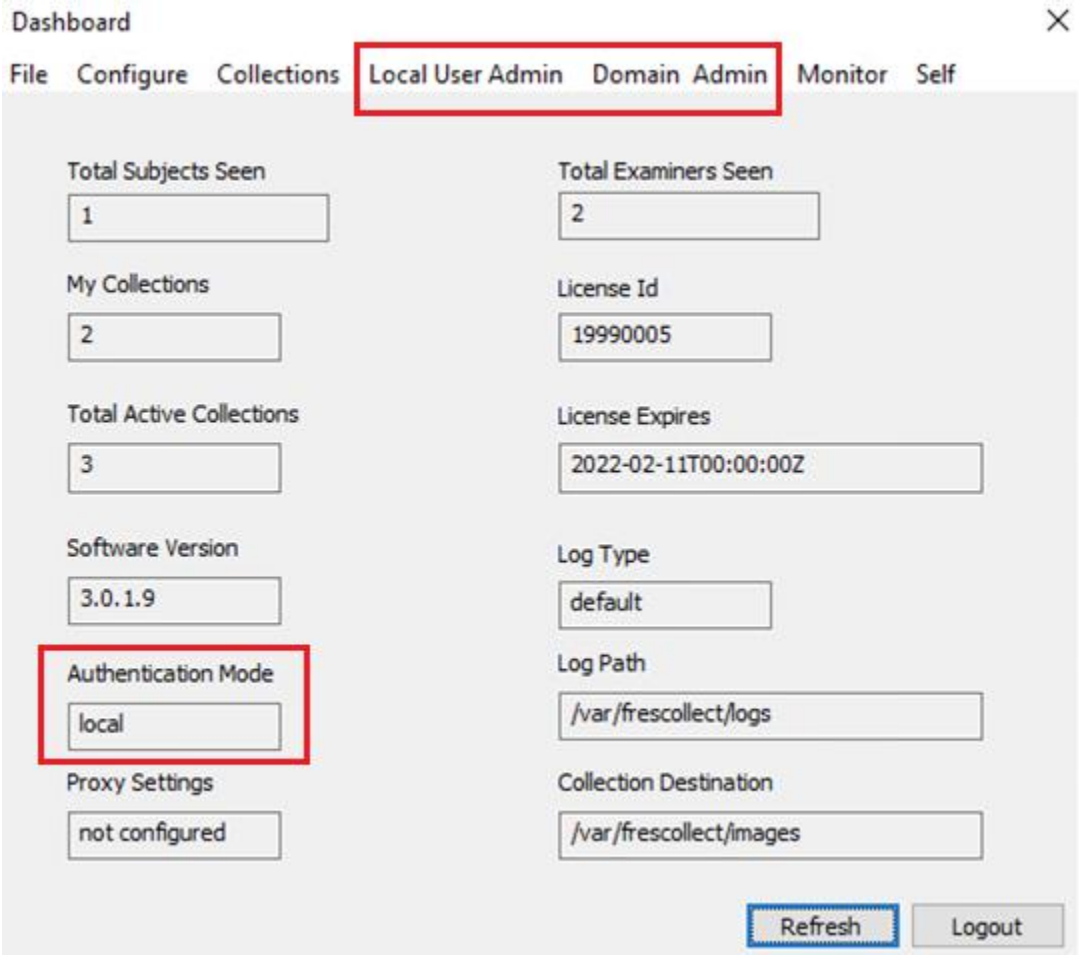
Note: The collection path cannot be changed unless there are no active collections. (i.e., the collection management window above must be completely empty).



Simply enter the new location for the collections to be stored (remember the Collect server is Linux based and requires a forward slash / to denote the directory location) and click **OK**.

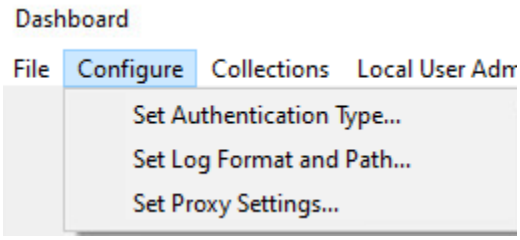
Authentication

The current authentication mode can be viewed on the Dashboard.



Authentication Type

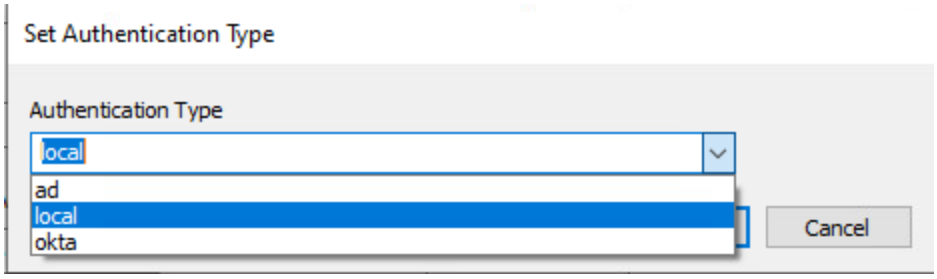
The F-Response Collect server can be set to **Local**, **Active Directory, or OKTA** Authentication.



Choose **Set Authentication Type…** from the **Configure** drop down menu.

Then simply choose the Authentication Type from the dropdown:

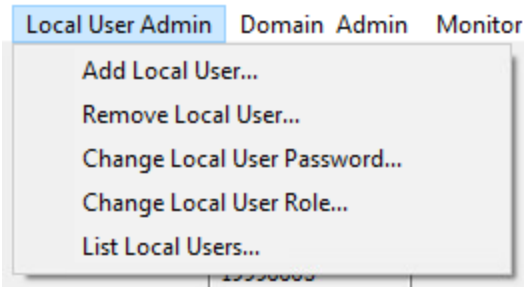
And click the OK button to set the server in the authentication mode needed.



Additional management for Local Users, Active Directory, and Okta are covered in those sections of this manual.

Managing Local User Accounts

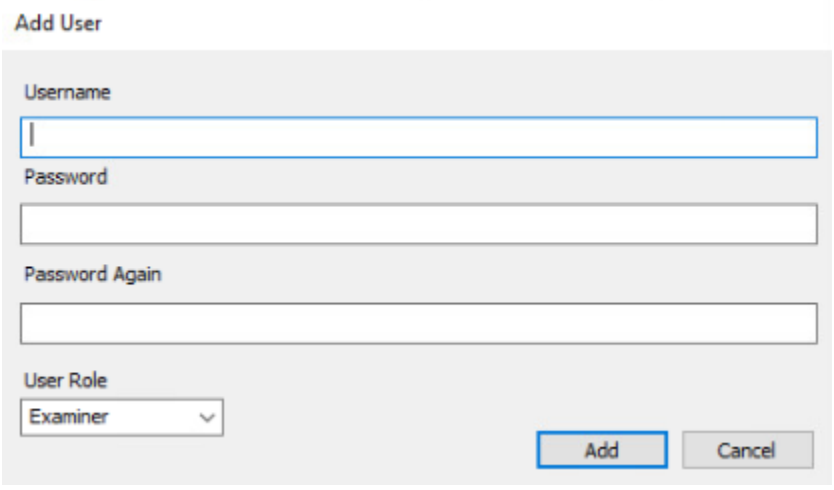
Local Accounts on the Collect server can be configured from the Dashboard under the **Local User Admin** drop down menu. **Note: Local accounts are only used if Active Directory Authentication is not enabled.**



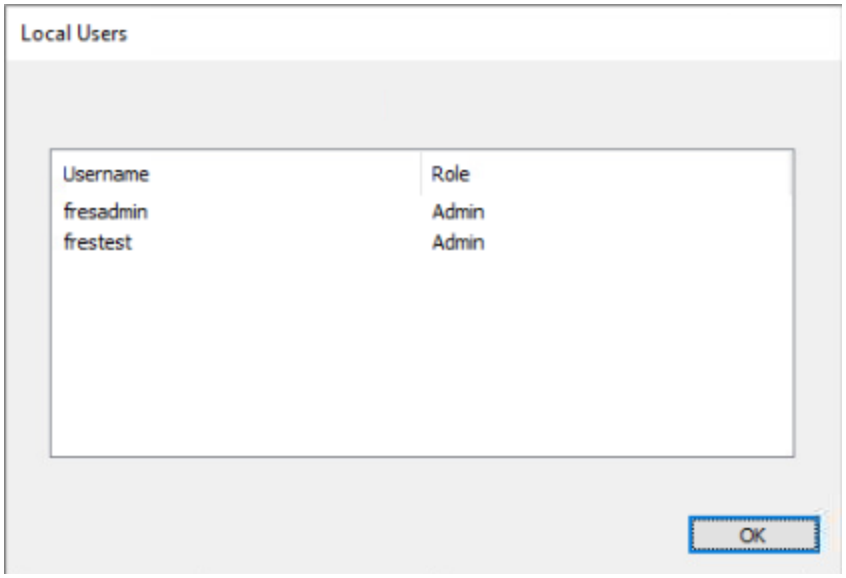
Here you have four options to manage user accounts on the Collect server. Details of each option are covered below.

Add a local user account

Click the **Add Local User…** from the drop-down under the Local User Admin menu on the Dashboard to add a new examiner or administrator to the Collect server.

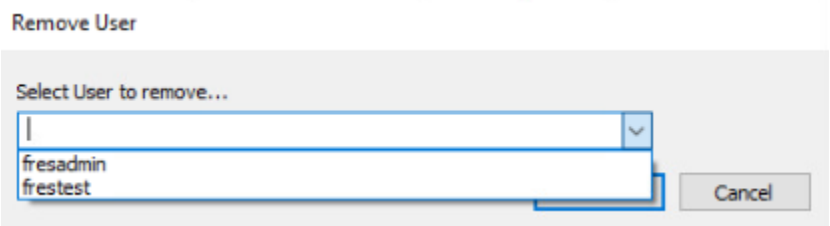


Simply enter the details and role information and click the **Add** button. The new user and their assigned role will appear in the **List Local Users…** from the **Local User Admin** drop-down menu.



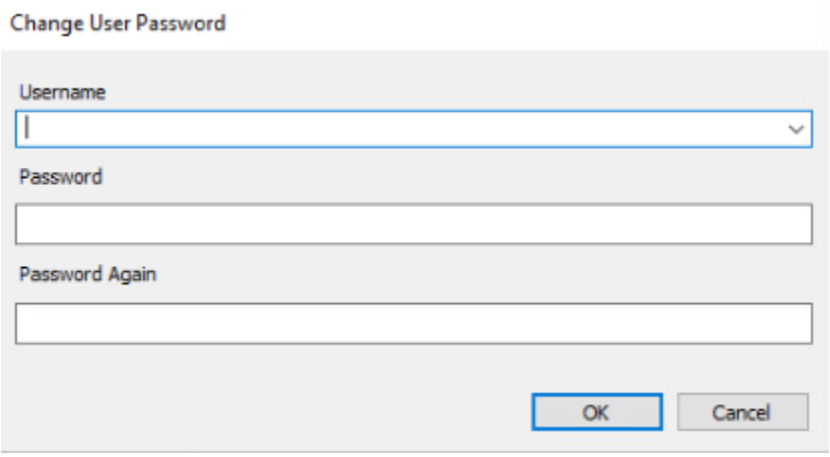
Remove a local user account

To remove a local user account from the server, select the **Remove User…** from the **Local User Admin** drop down menu, select the User from the drop-down list and click the **Remove** button.



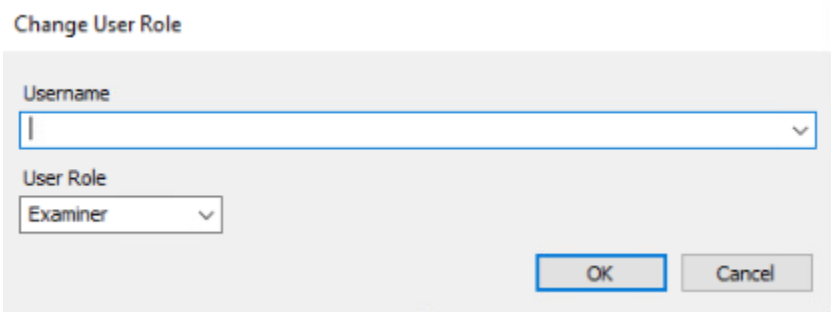
Changing a local user password

To change the password for a local user account, select the **Change User Password…** option from the **Local User Admin** drop down menu. Select the appropriate user account and enter the new password, then confirm by clicking the **OK** button.



Changing a local user role

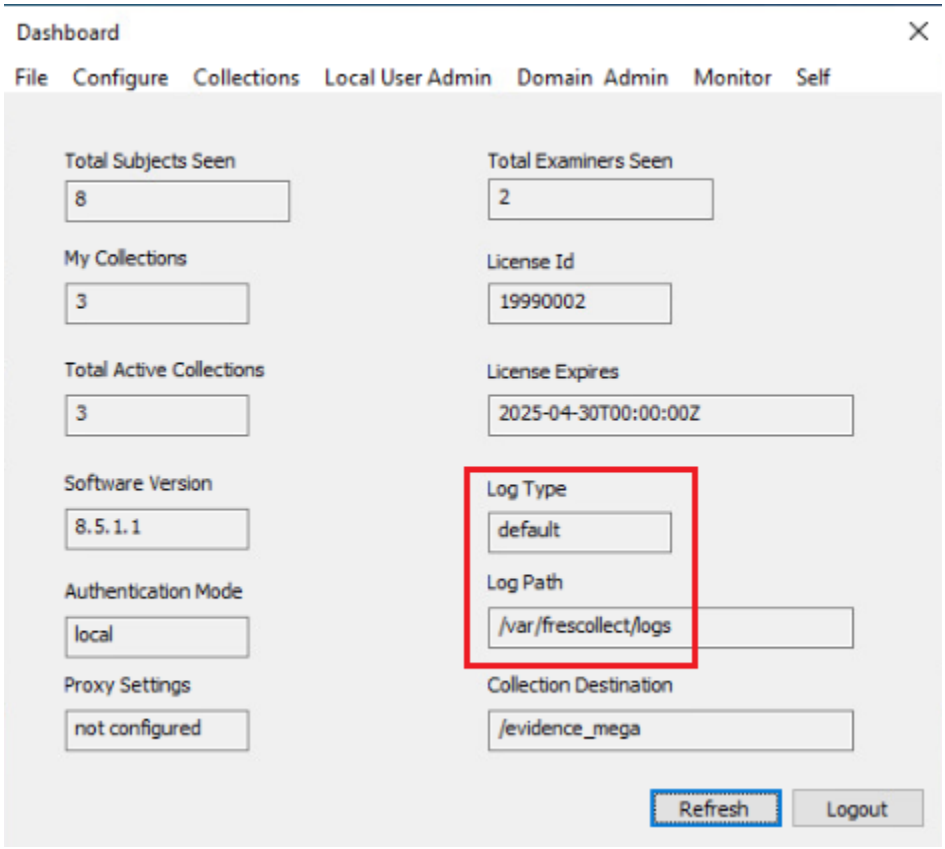
To change the role for a local user account, select the **Change User Role…** from the **Local User Admin** drop-down menu. Here you can select the User from the drop-down list and choose the role (*Examiner or Administrator).



The **Examiner** role allows for full use of F-Response Collect capabilities using the F-Response Collect Management Console, and view only permissions of the F-Response Collect Server Dashboard via the F-Response Server Configuration Tool (console_configuration.exe).

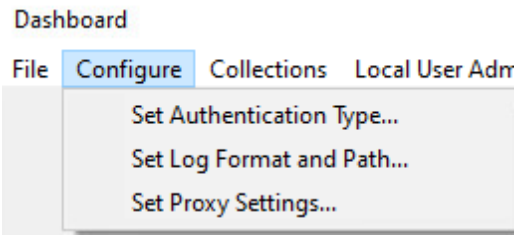
The **Administrator** role allows for full use of F-Response Collect capabilities using the F-Response Collect Management Console and full management of the F-Response Collect Server via the F-Response Server Configuration Tool (console_configuration.exe).

Logging

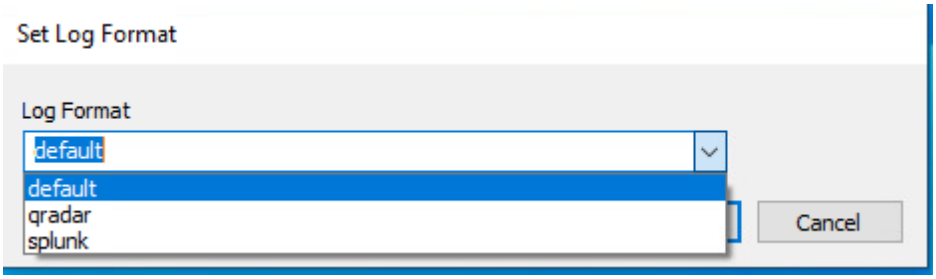


By default, the F-Response Collect Server will store logs in CSV format in the /var/frescollect/logs directory on the server. The server also offers the option to store logs in QRadar or Splunk format if needed.

To modify the log format or location, **choose Set Log Format and Path…** from the **Configure** drop down menu on the Dashboard.



This will allow you to choose the desired log format from the drop-down list. Select the required log type, modify or verify the Log Destination and click OK.



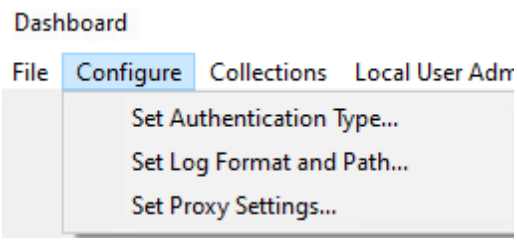
All F-Response Collect log entries share the same values:

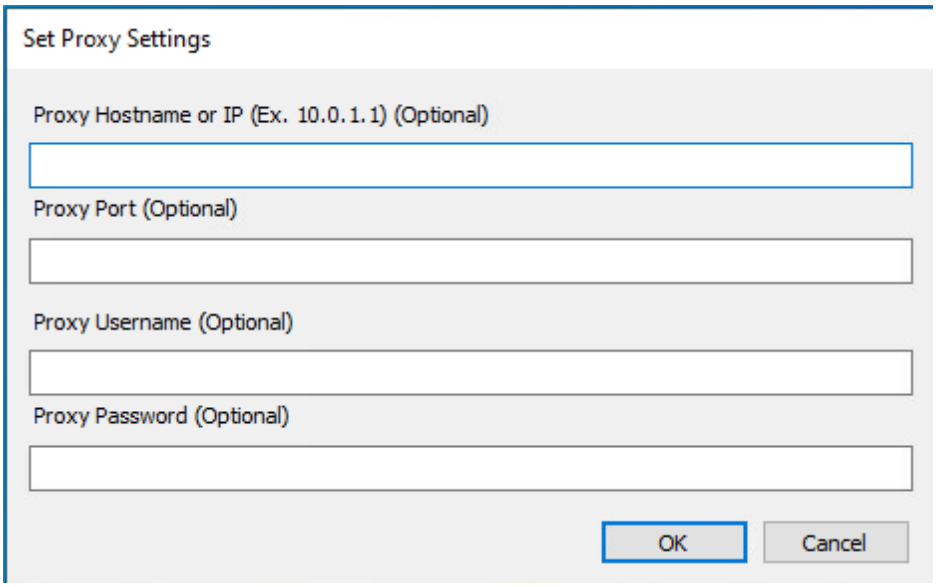
- Function:
  - Name of the subsystem involved.
- Username:
  - Where possible, includes the user, subject, or IP matching the event.
- Datetime:
  - Date and time when the event took place in UTC.
- Type:
  - Informational (info) or Error (error).
- Message:
  - Text based details.

For complete details on Log Formats, please see Log Formats in Appendix D

Proxy Settings

The Collect server can be configured to use a web proxy for accessing the remote license server at license.f-response.com under the **Configure** drop-down menu option from the Dashboard. Choose **Set Proxy Settings…** to open the configuration window.

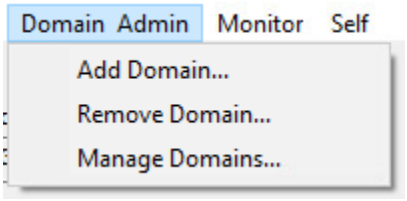




Here you can enter your proxy information (or clear the fields to remove the proxy) and click **OK** to confirm.

Active Directory Domain Configuration

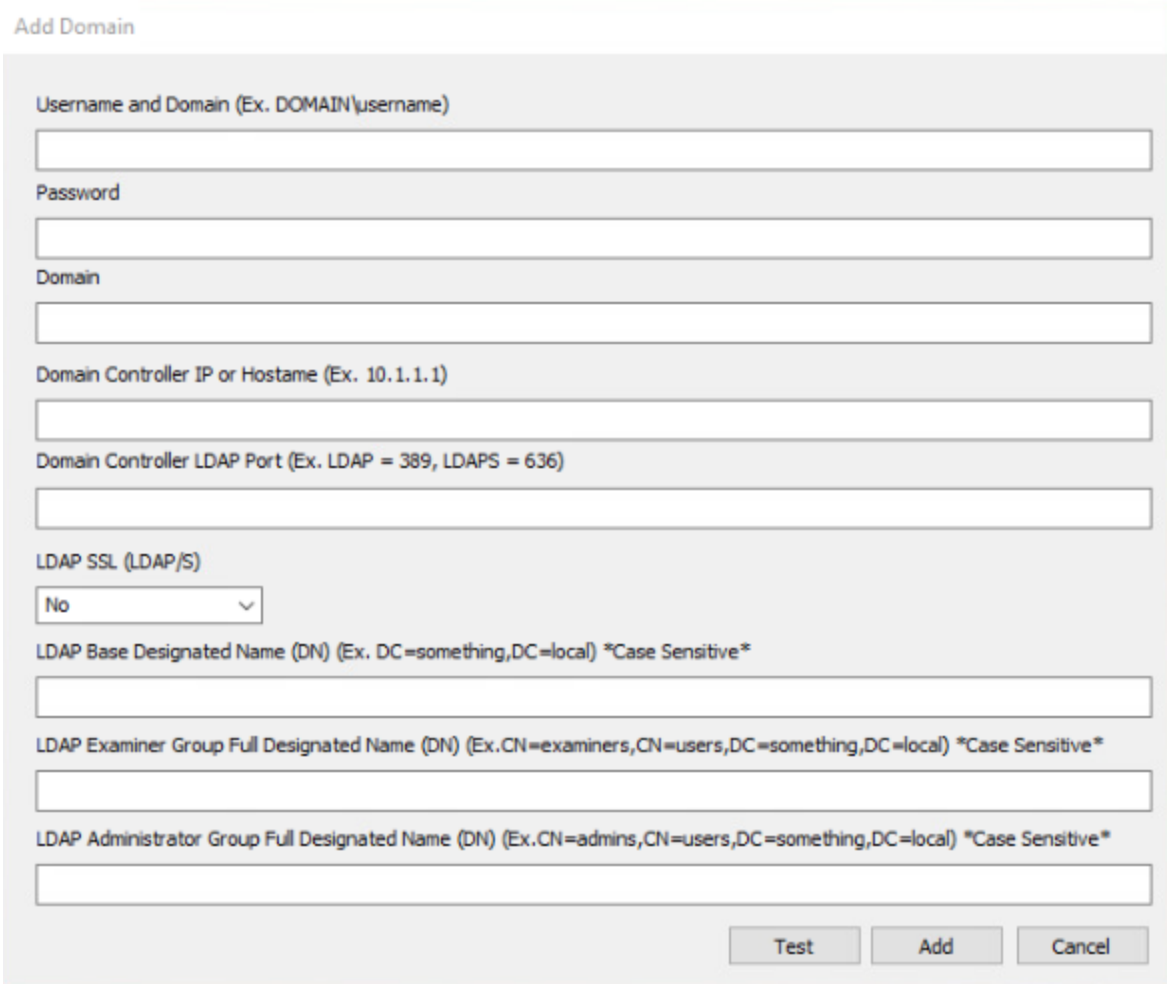
Adding your Active Directory domain



With Active Directory (LDAP) authentication enabled, local user accounts will no longer reside on the F-Response Collect server itself, rather the server will be configured to authenticate users directly against Active Directory based on group membership.

To configure the server with your Active Directory information, login to the dashboard and choose **Add Domain** from the Domain Admin drop down menu.

This will open the Add an Active Directory Authentication Domain window as pictured below.



Notice each field contains tips for how the data should be formatted. Once all the data is entered you can test everything is correct by clicking the **Test** button before committing by clicking the **Add** button.

- Username and Domain
  - A valid Active Directory account.
- Password
  - A valid Active Directory account password.
- Domain
  - Active Directory Domain you wish to add—must be the same one used for the Username and Domain above.
- Domain Controller IP or FQDN
  - The IP address or the Fully Qualified Domain Name of the Domain Controller (DC).
- Domain Controller LDAP Port
  - The TCP Port number LDAP runs on in your environment.
- LDAPS(With SSL Enabled)
  - If using LDAPS with SSL enabled select Yes from the drop-down.

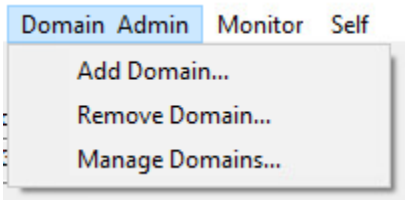
To configure F-Response Collect for Active Directory Authentication you will need two groups, one for Administrators and another for Examiners, along with the full LDAP name for each group. **Note: F-Response Collect does not support nested groups.**

- LDAP Base Designated Name (Case Sensitive, no spaces between commas)
    - The base name for the Active Directory Domain.
        - Ex. “DC=fresponse,DC=local”
- LDAP Admin Group Full Designated Name (Case Sensitive, no spaces between commas)
    - The full name for the Active Directory Domain group that contains F-Response Collect administrator users.
        - Ex. “CN=collectadmins,CN=Users,DC=fresponse,DC=local”
- LDAP Examiner Group Full Designated Name (Case Sensitive, no spaces between commas)
    - The full name for the Active Directory Domain group that contains F-Response Collect examiner users.
        - Ex. “CN=collectusers,CN=Users,DC=fresponse,DC=local”

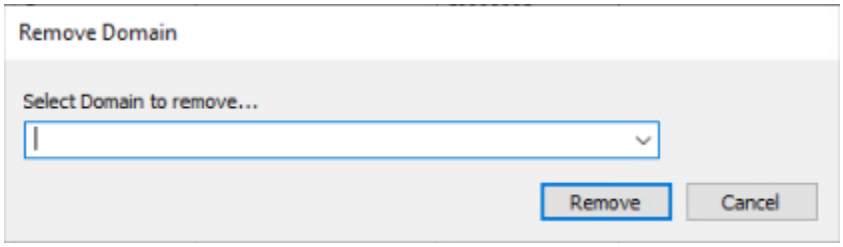
Note: Remember to set the Authentication Type to Active Directory to enable AD logins.

Removing your Active Directory Domain

To remove an active directory domain, login to the dashboard and choose **Remove Domain** from the Domain Admin drop down menu.

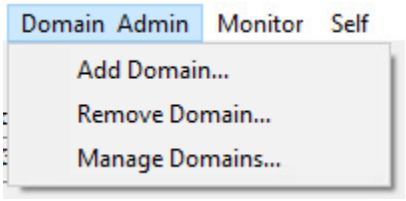


The Remove Active Directory Authentication Domain window will appear, simply choose the domain you wish to remove from the drop-down list and click the **Remove** button.



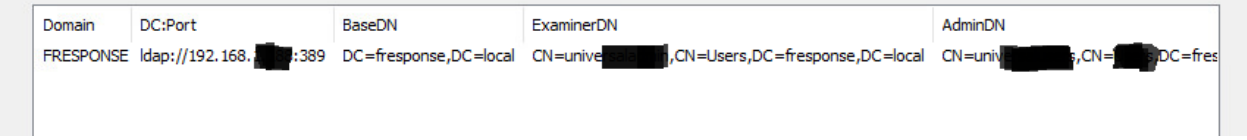
Manage Domains

To view the currently configured active directory domains, login to the dashboard and choose **Manage Domains…** from the Domain Admin drop-down menu.



The Domains window will appear, here you can view all the configuration details for each domain.

Domains



Domain	DC:Port	BaseDN	ExaminerDN	AdminDN
FRESPONSE	ldap://192.168.[redacted]:389	DC=fresponse,DC=local	CN=unive[redacted],CN=Users,DC=fresponse,DC=local	CN=uni[redacted],CN=[redacted]DC=fres

OKTA Configuration

Data Gathering

Note: If you are unfamiliar with how to setup an application or gather data settings from Okta, please see the guide on our website.

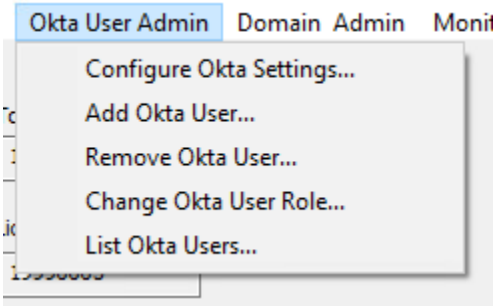
At a minimum, you will need 3 key pieces of data from your OKTA administrator to configure the F-Response Collect Server for OKTA authentication, they are:

1. **Client ID**
2. **Client Secret**
3. **OAuth Token URL**

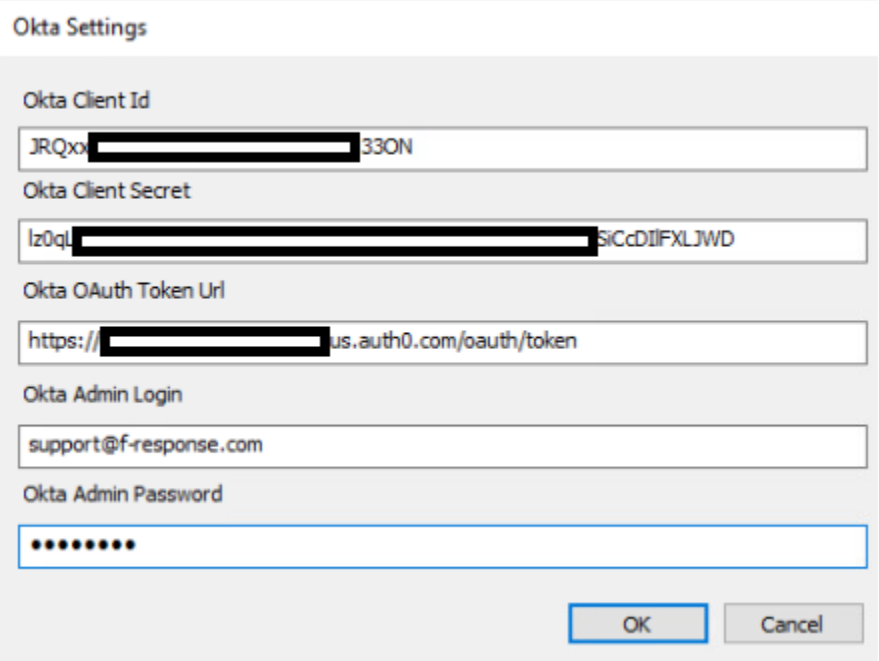
Additionally, if you would like to add additional F-Response Collect examiners/administrators you will also need the **Okta Username** and **User_id** for each.

Server Configuration/Enabling Okta Authentication

To configure the server with your Okta information, login to the dashboard and choose **Configure Okta Settings…** from the **Okta User Admin** drop down menu.



This will open the **Okta Settings** window as pictured below.

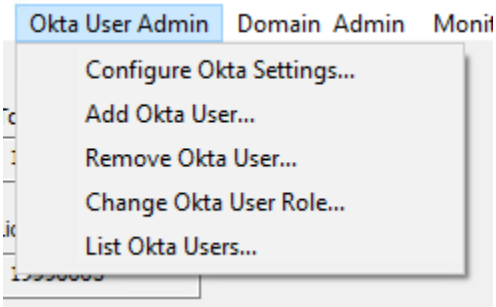


Here you will enter the information you gathered earlier, the **Client ID**, **Client Secret**, and **OAuth Token URL**. The **Okta Admin Login and Password** fields can be any account with access. This account will be added as the first F-Response Collect administrator account.

Click **OK**. Once the details have been successfully verified and added it's time to turn on OKTA Authentication. See Authentication Type for details on changing the authentication mode for your Collect Server.

OKTA Management

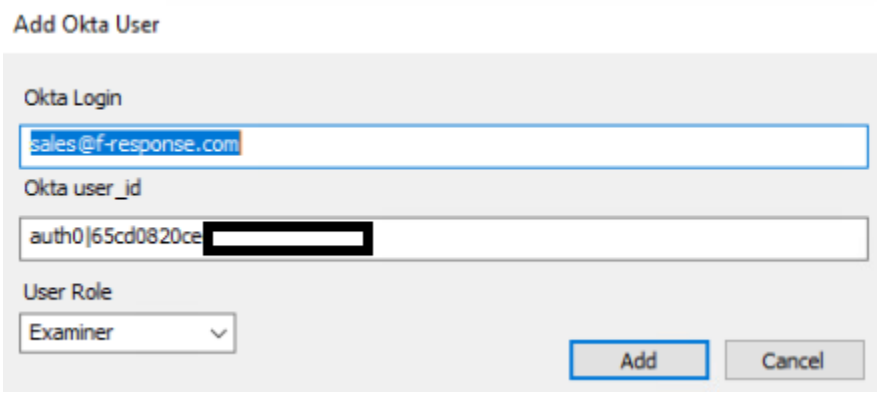
Okta users can be managed in the dashboard and you can see the list of options in the Okta User Admin drop down menu.



We'll cover each option below.

Adding Okta Users

You can add additional F-Response Collect Okta users and assign Examiner or Administrator roles to each account in the Dashboard as well. To do this, you will need the **Okta Login** and **User_id** for each user.



Enter the login and user_id and choose the appropriate role from the User Role drop down box. Click Add and you will be prompted to add the details for next user on your list, click Cancel when complete.

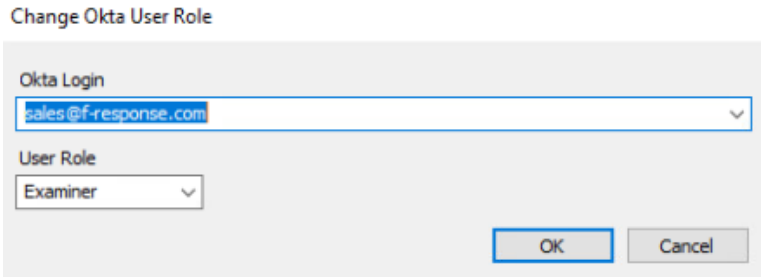
Remove Okta Users

The process to remote access for an Okta user from the F-Response Collect Server is very simple. From the Dashboard go to the Okta User Admin drop down menu and choose Remove Okta User.

Select the user you wish to remove from the dropdown menu and click OK.

Change the Okta User Role

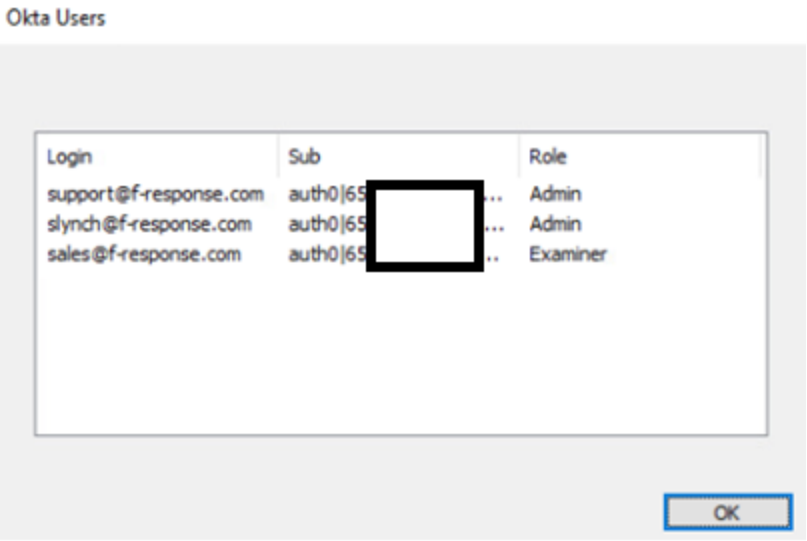
To change an existing Okta User's role, select Change Okta User Role from the Okta User Admin drop down menu.



Select the user and role you wish to assign to from the drop-down menus and click OK to make the change.

List Okta Users

You can obtain a list of all the current users and their roles on the F-Response Collect Server in the Dashboard under **Okta User Admin -> List Okta Users…**



Additional Options

IPv4 Restrictions

Customers looking to apply additional access controls to their Collect server can use the following addition to the frescollect.cfg file to restrict examiner access to select IP addresses. Examiners will still have to login.

IP addresses must be provided in the following format, individual addresses, or ranges. See examples below:

“iprestrictions”:[“IP1”,”IP/NET”,”IP3”]

Ex. “iprestrictions”:[“192.168.2.1”,”172.16.10.0/24”, “10.0.1.2”]

Changing Listening Port(s)

Customers looking to alter the listening ports from the default (443) can do so they adding the following values to the frescollect.cfg file and restarting the F-Response Collect service/server:

“port”:XXX

Ex ”port”:8080

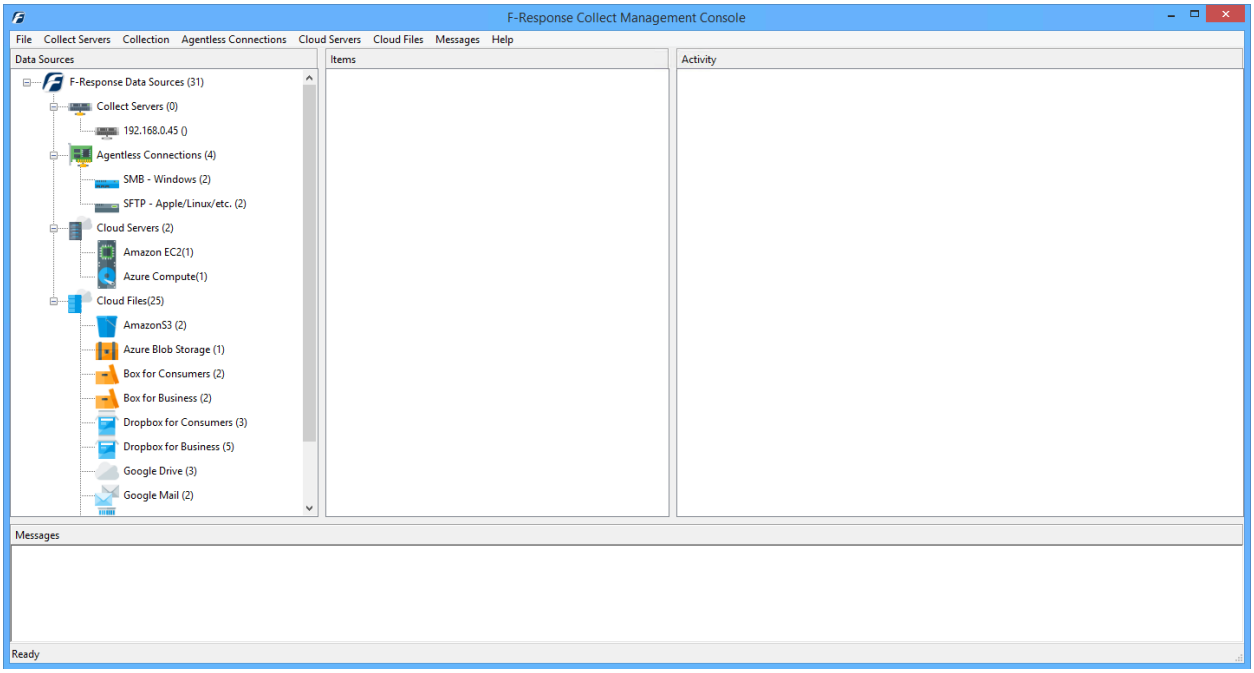
Getting started with the F-Response Collect Management Console

Installation

Download and run the **F-Response-Collect-Examiner-Installer-<versionnumber>.exe** on a Windows computer from the F-Response Website: https://f-response.com/support/downloads If you are upgrading a current installation do not uninstall--simply run the new executable over the existing version to upgrade and keep your settings.

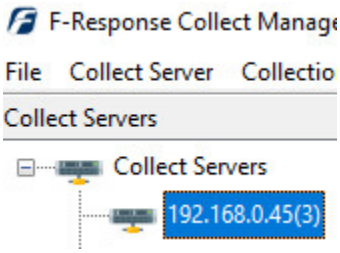
Note: You will need your license number to download the software. (Ex: 1999x)

Overview



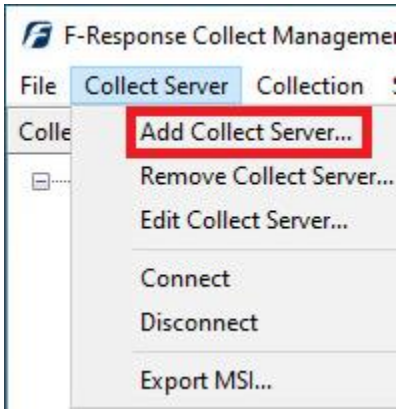
The F-Response Collect Management Console operates with a left to right workflow.

The number that appears in parentheses to the right of the Collect Server indicates the number of current active Collections.

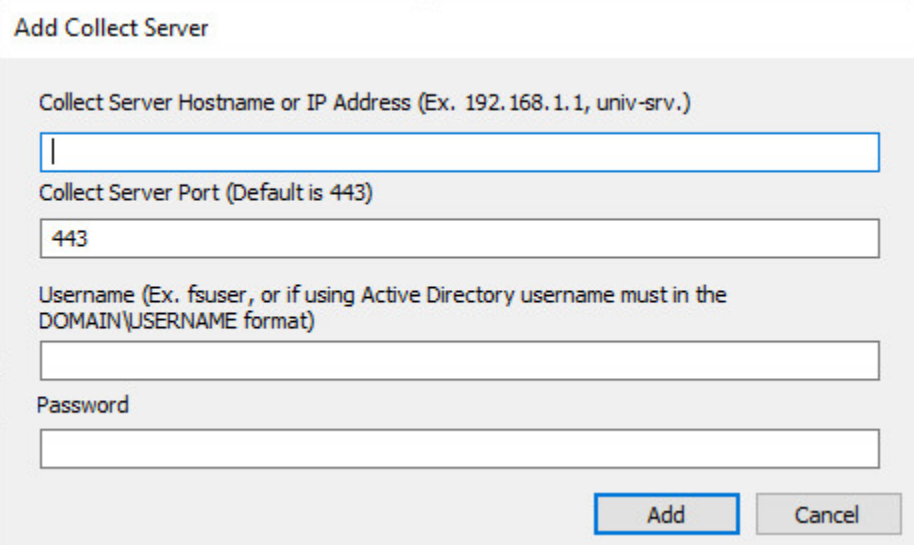


Adding a Collect Server

A Collect Server can be added to the F-Response Collect Management Console by choosing the **Collect** drop-down menu, and clicking on **Add Collect Server…**



This will open the Add Collect Server window.



These four fields are as follows:

Collect Server Hostname or IP address: Each Collect server must be entered individually, enter only one Collect server or IP address here.

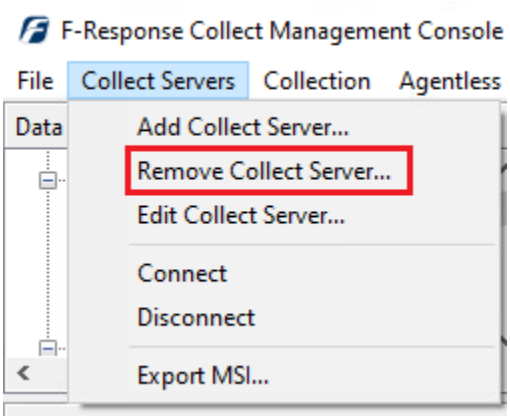
Collect Port: This field is populated with the default port 443 but can be reconfigured if necessary (change must be made on the server itself before adding here).

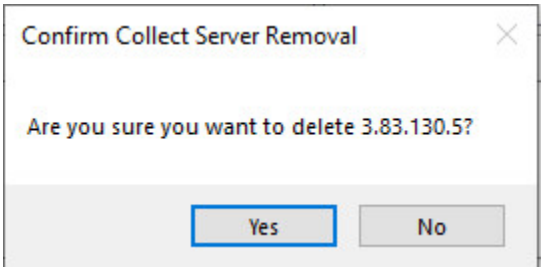
Username: The local or Active Directory user that has been assigned an Examiner role on the Collect server.

Password: The local or Active Directory account password.

Removing a Collect Server

A Collect Server can be removed from the F-Response Collect Management Console by first double-clicking on it to disconnect, then choosing the Collect Server drop-down menu, and clicking on **Remove Collect Server…**

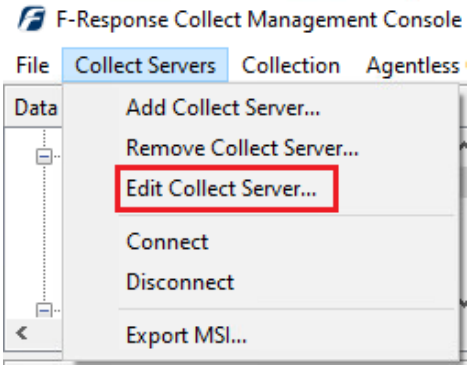




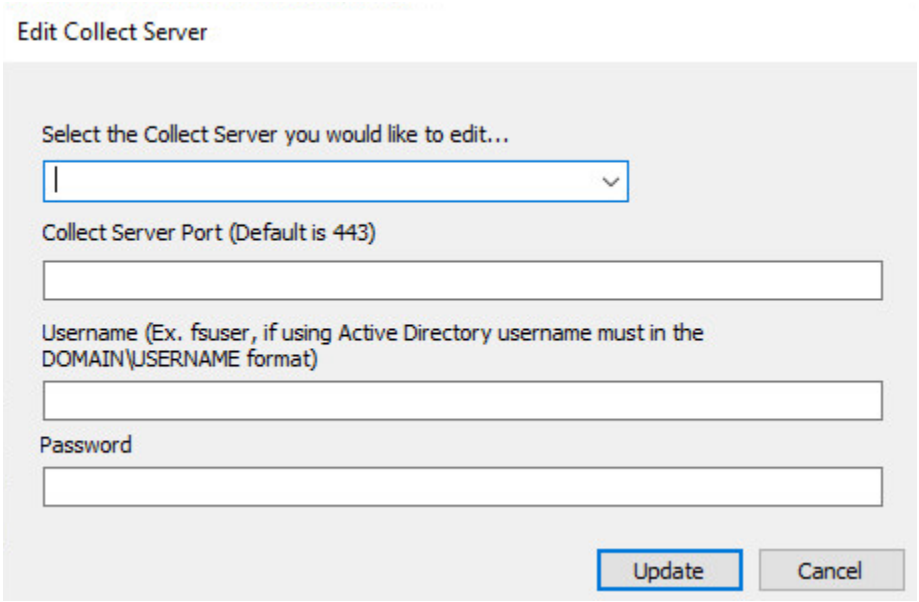
This will open the Confirm Collect Server window where you can click Yes to finalize the removal of the server.

Edit a Collect Server

You can edit any of the existing fields for a Collect server in the console by simply choosing **Edit Collect Server** from the **Collect Server** drop-down menu.



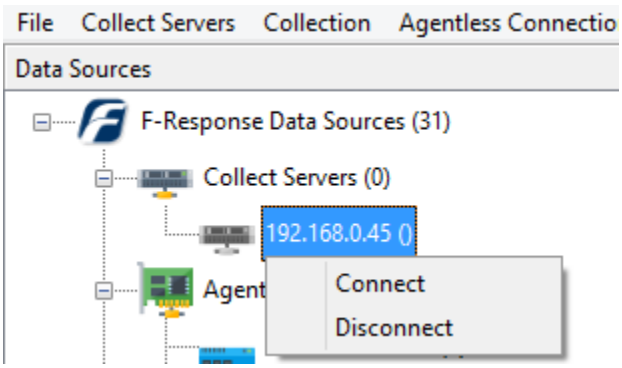
This will open the Edit Collect Window:



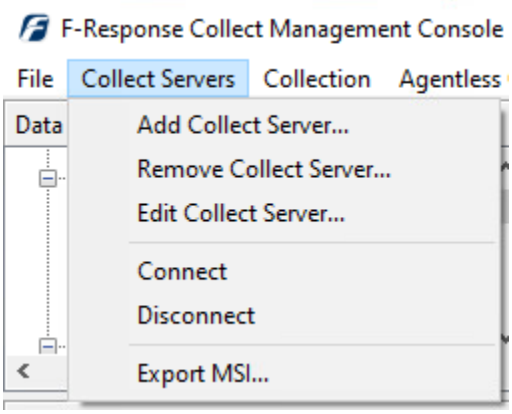
Choose the Collect server you would like to edit from the drop-down list then edit the appropriate fields. Click **Update** to confirm the changes.

Connecting or Disconnecting from a Collect Server

To connect or disconnect from a Collect server in the F-Response Collect Management Console simply highlight the Collect server in the left most column, then double-click on it to immediately connect/disconnect, or right click and choose to **Connect** or **Disconnect**:



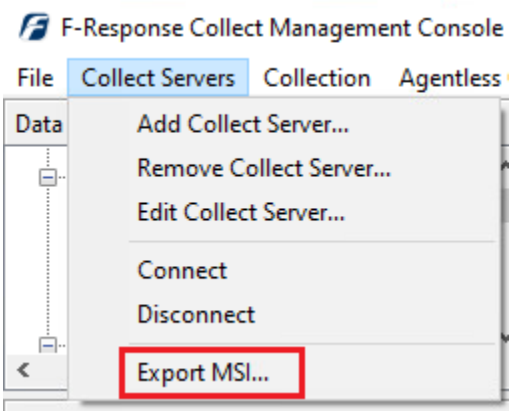
Alternatively, highlight the Collect server then choose **Connect** or **Disconnect** from the **Collect Server** drop-down menu:



Active collections will continue to run regardless if the Console is connected.

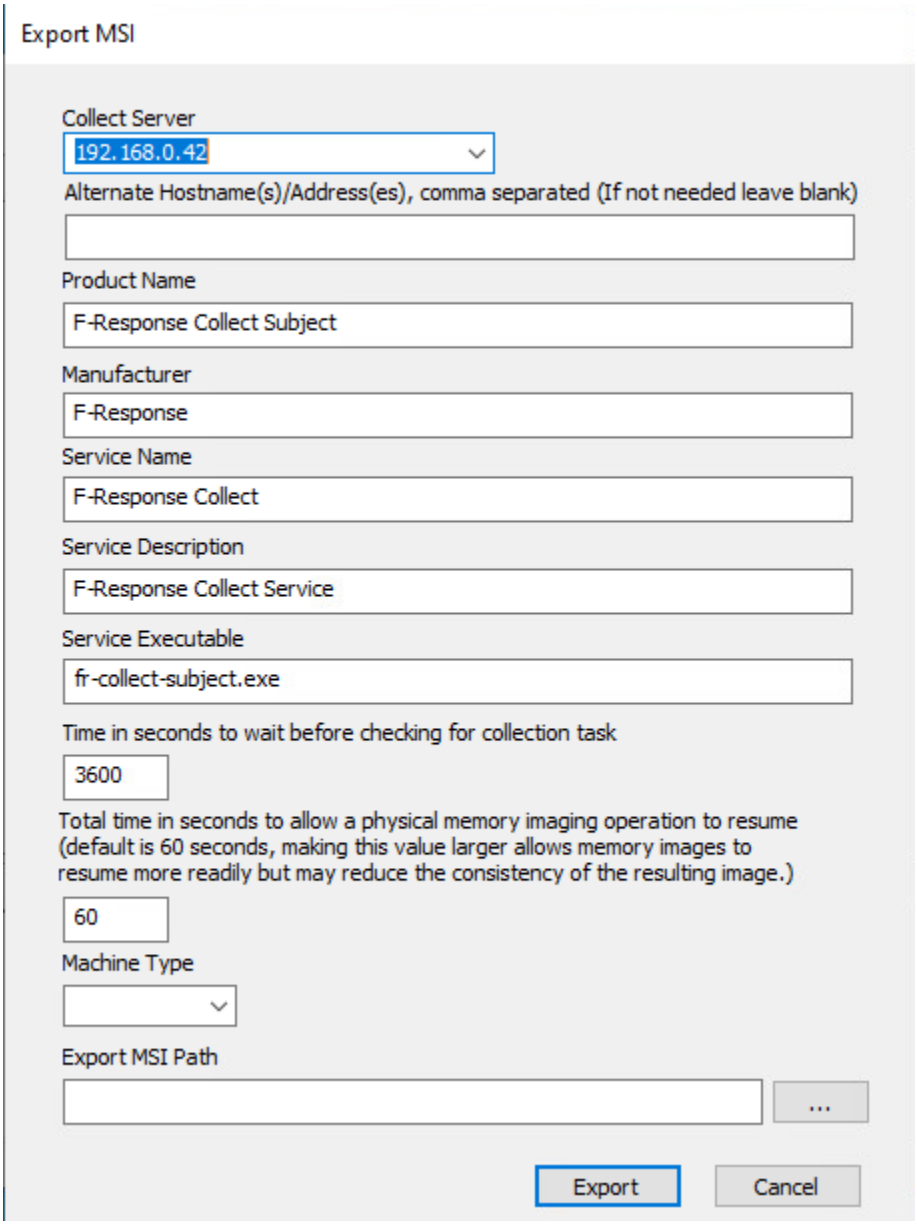
Subject MSI

F-Response Collect Windows subject software is available as an MSI (Microsoft Software Installer), suitable for deployment using 3rd party tools. To create a MSI for distribution to the subject computers, choose **Export MSI…** from the **Collect Server** drop down menu:



Export MSI Settings

The **Export MSI** window will open. There are 8 fields here to consider before exporting the MSI.



Collect: Choose the Collect server you would like the subject computer to use from the drop-down list.

Alternate Hostname or IP Address: (Optional) if a subject cannot reach the Collect server's IP, the external or NAT'd address(es) can be entered here, comma separated. Use this if your Collect server has multiple addresses assigned and you would like the subject to try them in sequence.

Product Name: Allows you to set the MSI's product name (will be visible in Add and Remove Programs).

Manufacturer: Allows you to set the MSI's manufacturer (will be visible in Add and Remove Programs).

Service Name: Collect runs as a service on the remote subject computer, create a service name that does not conflict with an existing service.

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

Service Executable: This is the executable name that will be assigned when the subject software is deployed.

Collection Check Time: The number of seconds the service will wait before checking into the Collect server to see if it is assigned to a collection. The default is 3 minutes (180 seconds).

Physical Memory Resumption Time: As described in the Export MSI window, the time in seconds a physical memory operation will continue to attempt to resume if connectivity is lost.

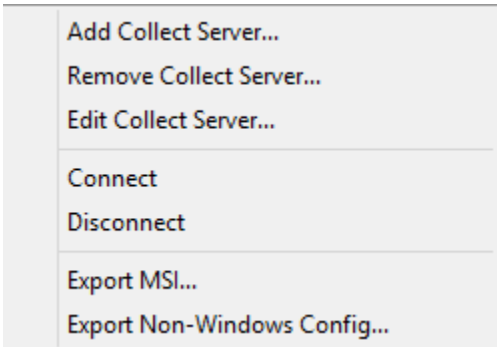
Machine Type: This is the machine type (64 or 32 bit). MSI packages must match the machine type they are being installed on.

Export MSI Path: The location where you would like to place the MSI.

Click the Export button to create the MSI in the specified folder path and you will receive a notification in the Messages Panel when the export is complete.

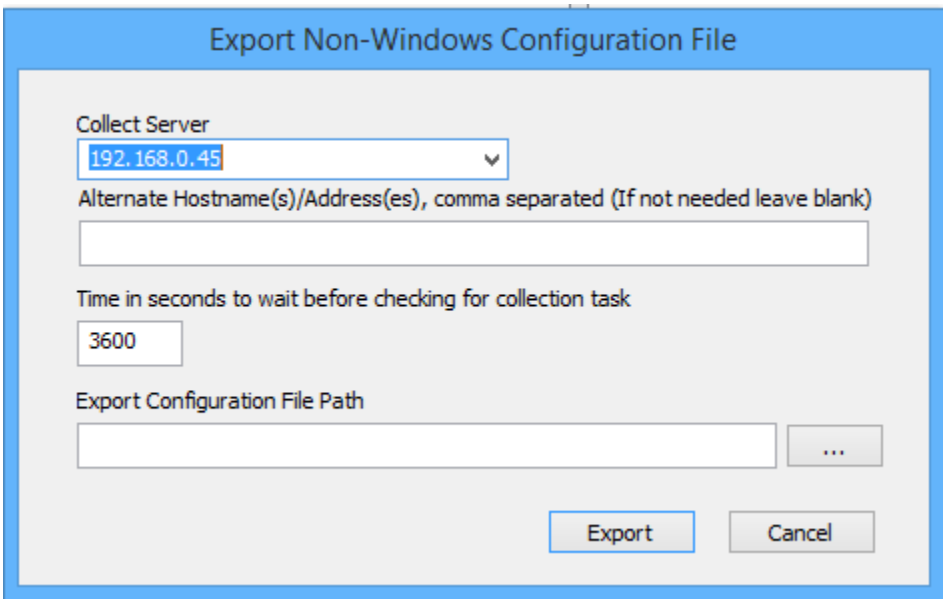
Subject (Non-Windows)

F-Response Collect Non-Windows software is available as an RPM (Redhat Package Manager) package, suitable for deployment using 3rd party tools to remote Linux machines. You will find the latest F-Response Collect subject RPM on our downloads page https://www.f-response.com/support/downloads, however you will need to export a system specific configuration file to replace the default configuration file provided in (/etc/fr-collect-sub/fr-collect-sub.cfg) using the drop down menu:



Export Non-Windows Configuration File Settings

The **Export Non-Windows Configuration File** window will open. There are 4 fields here to consider before exporting the configuration file.



Collect Server: Choose the Collect server you would like the subject computer to use from the drop-down list.

Alternate Hostname or IP Address: (Optional) if a subject cannot reach the Collect server's IP, the external or NAT'd address(es) can be entered here, comma separated. Use this if your Collect server has multiple addresses assigned and you would like the subject to try them in sequence.

Collection Check Time: The number of seconds the service will wait before checking into the Collect server to see if it is assigned to a collection. The default is 3 minutes (180 seconds).

Export Configuration File Path: The location where you would like to place the Configuration File.

Click the Export button to create the fr-collect-sub.cfg file in the specified folder path and you will receive a notification in the Messages Panel when the export is complete.

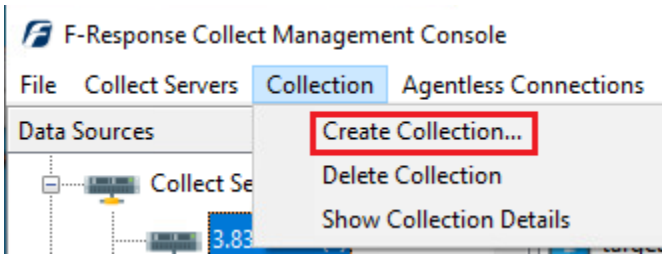
For more specific information on running F-Response Collect on remote non-Windows machines, please see the Mission Guides our website: https://www.f-response.com/support/missionguides

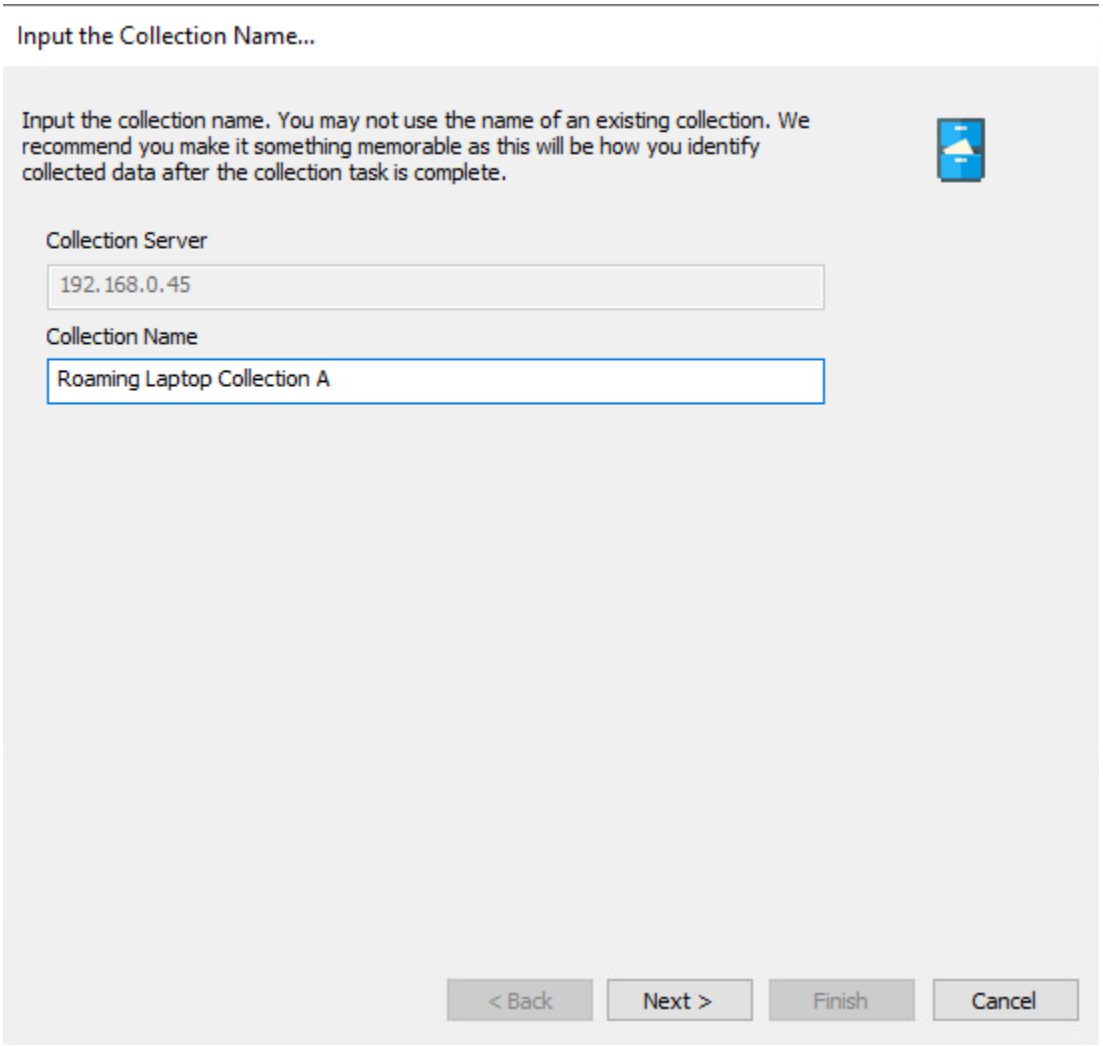
Collections

The heart of F-Response Collect is creating collections. A collection is group of instructions containing one or more subjects and devices that you would like to collect.

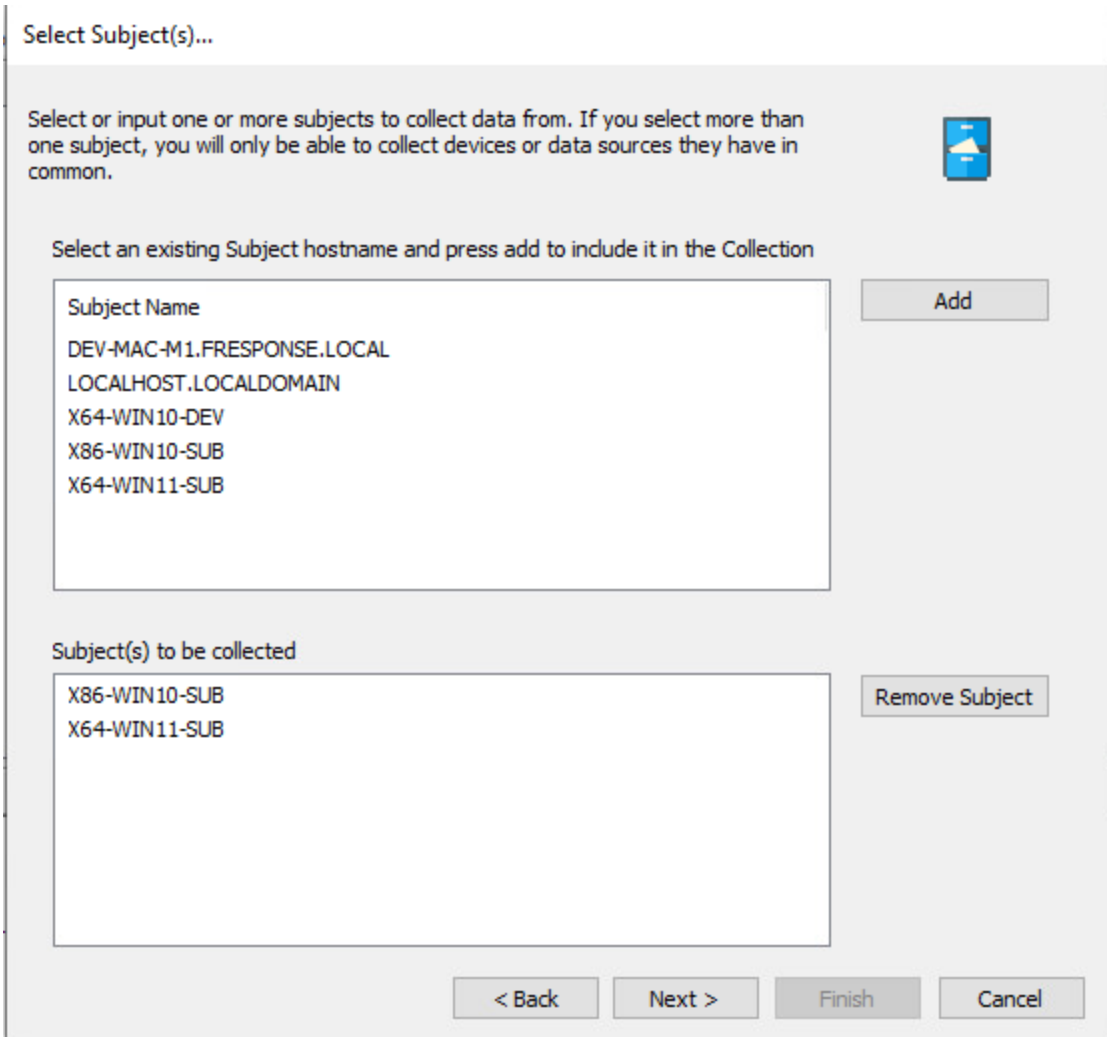
Creating Collections

To create a collection, highlight the Collect Server in the left column and choose **Create Collection…** from the **Collection** dropdown list. This will open the **Create Collection…** wizard.

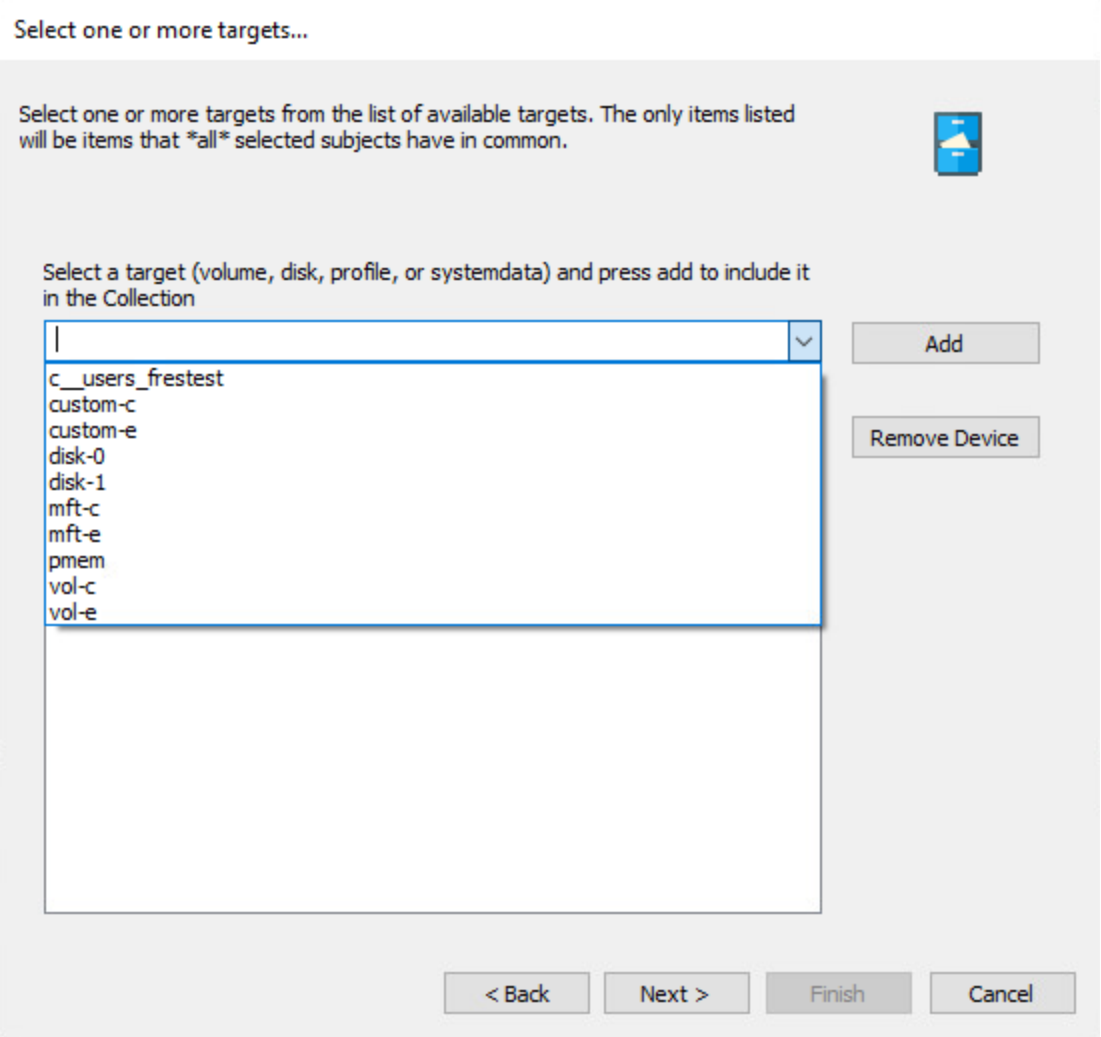




The first step in creating a collection is to give it a name. The name must be unique and cannot match an existing collection.



After setting the name you will need to select one or more subject hostnames from the available list. Subjects are added to this list by connecting to the Collect server and checking if they are needed in a collection. In order to make sure this list is populated with the subject you wish to collect data from, you need to make sure the F-Response Collect Subject MSI has been installed on the remote machine and that it has connected at least once to your F-Response Collect server.



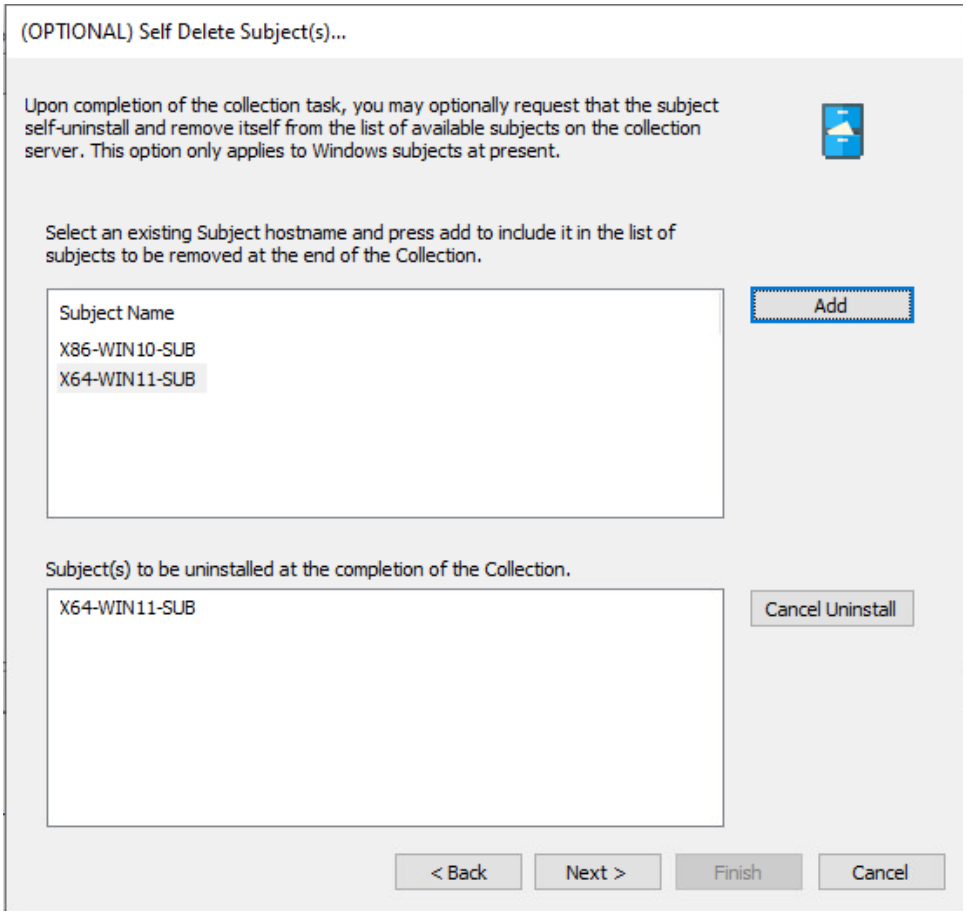
Once you have added one or more subjects to your collection, you will need to select one or more devices. If multiple subjects were selected in the prior dialog, then the subset of their mutual devices is all you will see. The following device types are currently available:

- "disk-x"
  - Physical disk image of the device number indicated, disk-0 translates to PhysicalDrive0. (A full device image, includes allocated and unallocated space).
- "vol-x"
  - Physical volume image of the device letter indicated, vol-c translates to c:\\. (A full device image, includes allocated and unallocated space).
- "X__Profilename"
  - File and folder collection of a specific profile as detected on the system. This is not a full device collection and does not include deleted items. This is a complete collection of the contents of a specific directory (and all directories beneath it). C__Users_frestest translates to C:\\Users\frestest. If there is a loss of connectivity, a profile collection will resume at zero.
- "custom-X"
  - Custom targeted file/folder collection based on string matching where 'X' is the volume to be processed. If there is a loss of connectivity, a custom collection will resume at zero.

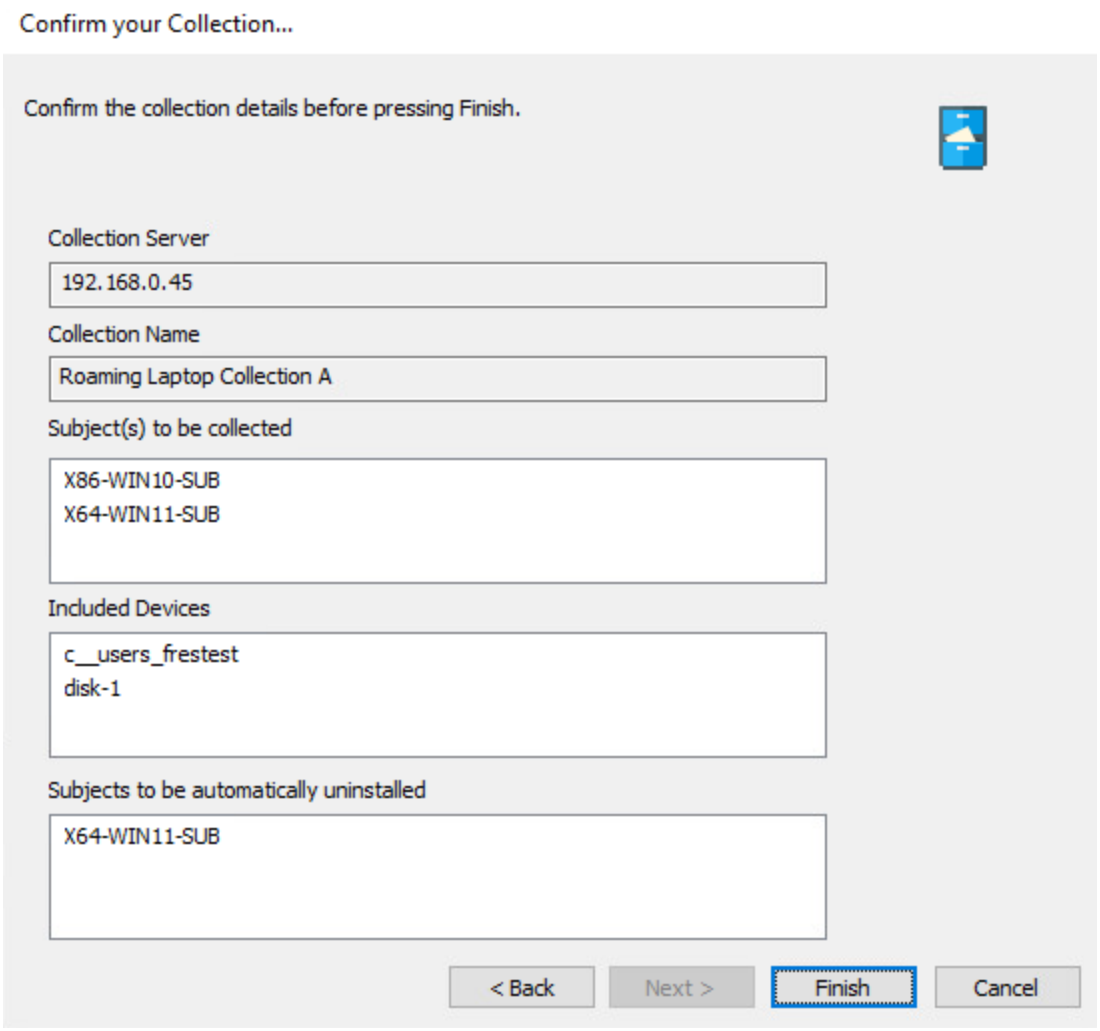
- “pmem”
    - Physical memory of the subject machine (Windows Only). Physical memory imaging does not follow the standard automatic resumption model. If there is a loss of connectivity, a physical memory image will only resume where it left off if the resumption happens within 60 seconds of the last read operation. If not, resumption will restart from the beginning of physical memory, i.e. page zero.
- “mft-X”
    - Master File Table (MFT) of the remote subject volume (provided it is NTFS). If there is a loss of connectivity, an MFT collection must resume at zero.

Self Delete

If you would like F-Response to uninstall itself from the remote computer(s) once the collection is complete you can specify in the **(OPTIONAL) Self Delete Subject(s**) window.



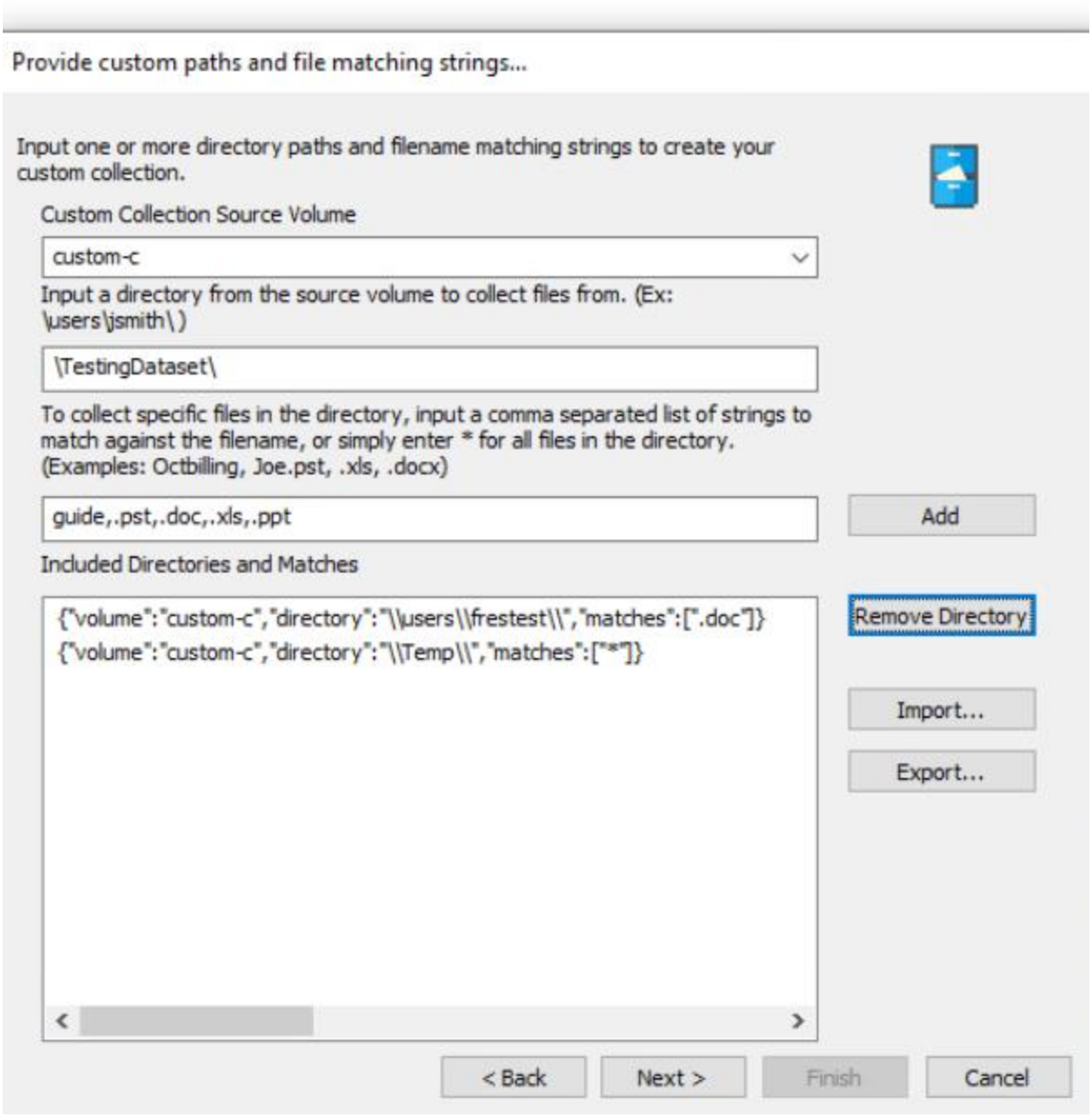
Highlight the subject(s) you wish to remove F-Response from and click the **Add** button. To remove a subject from the uninstall list simply highlight and click **Cancel Uninstall**. Once you are satisfied with the list (or there are no subjects you want to delete F-Response from) click **Next>**.



Once you are satisfied with the specific details of this collection, click the **Finish** button to begin the collection.

Custom file collection

When creating a collection and choosing a custom volume to collect data from, you will be prompted to provide specific details:



Choose the custom volume you wish to search from the **Custom Collection Source Volume** drop down menu. The options presented from the list are created by your previous choices leading up to this screen.

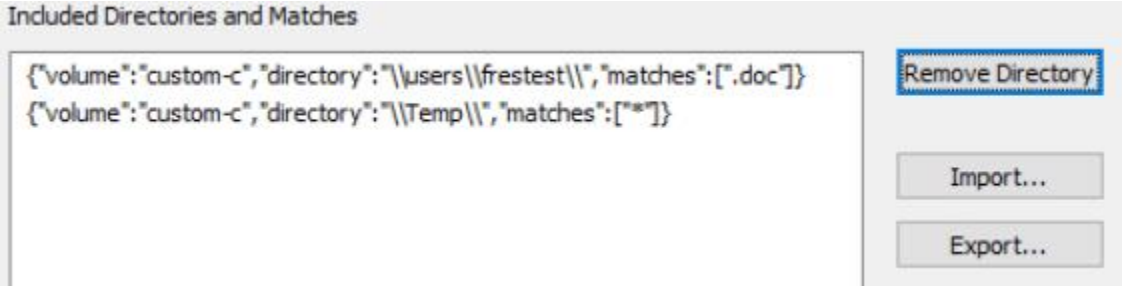
Next, specify the source directory on the volume to collect data from. For example, to collect from the entire Windows directory you would enter "**\Windows**". To search the entire volume simply enter a backslash "\" to specify the search to begin at the root.

The final step is to craft your filename matching string(s). Please note this feature uses simple string matching and **not** regular expressions. The wildcard character * is available but only to denote all files in the directory and cannot be combined with other characters. Each string is separated by a comma and is not case sensitive.

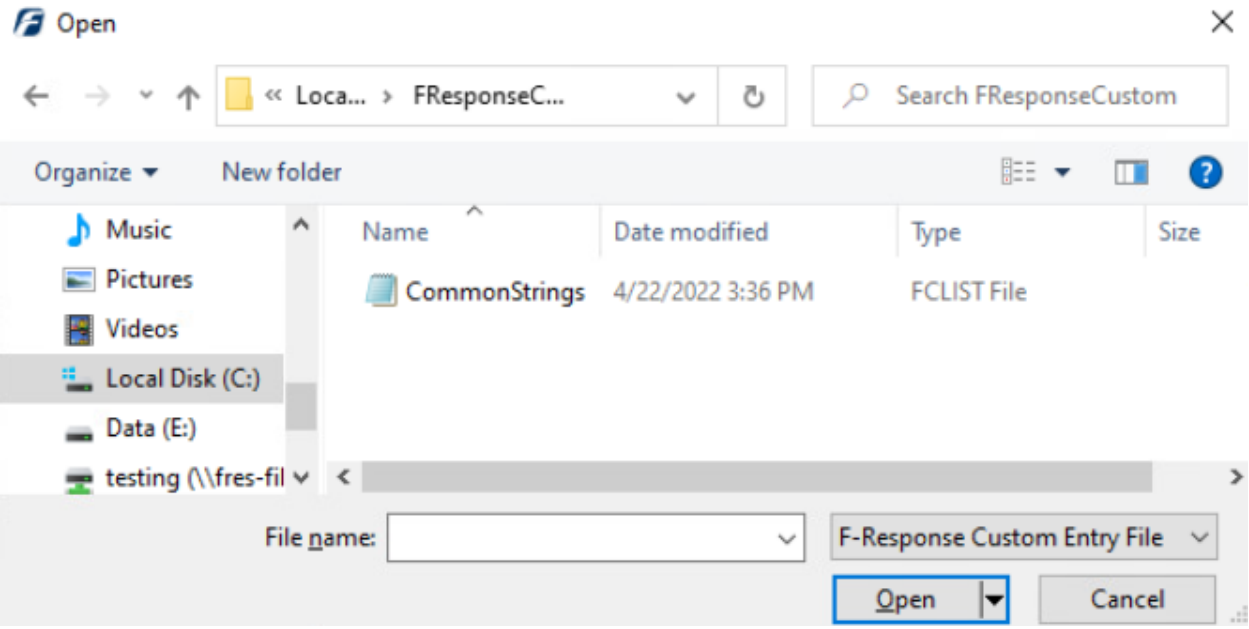
Once you are satisfied with the filename match you have crafted click Add to include it in the list below. The filename match is converted to JSON format as shown in the example above. Click Next once you are satisfied with your list.

Import/Export

You also have the option to save commonly used custom collections to reuse later. Once you have created your list of included directories and matches, click the **Export…** button to save your list as a F-Response Custom Entry file for future import.



Saved string lists can be imported when needed by clicking the **Import…** button and browsing to the location of F-Response Custom Entry file.

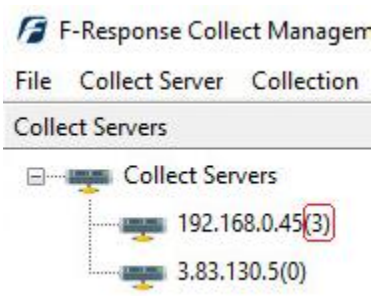


The file will be imported and populate the **Included Directories and Matches** list.

A string can be removed from the **Included Directories and Matches** list at any time by highlighting the entry and clicking **Remove Directory**.

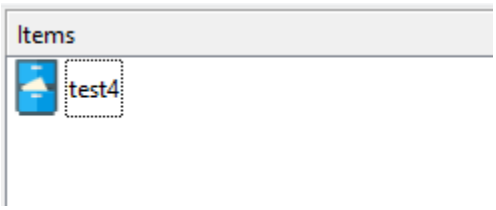
Viewing Collections

Examiners will only be able to view collection details and download images they have created while users assigned an Administrator role on the Collect Server can view and manage all images in the collection path.

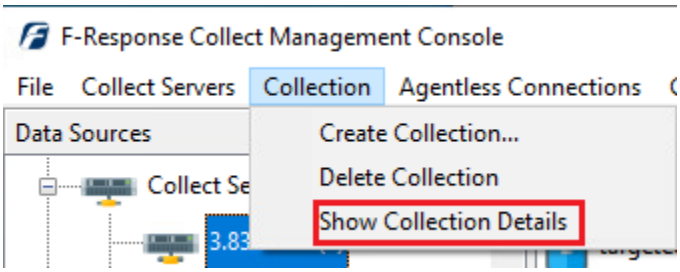


The number of collections on a collect server is visible to the right of the server in the **Collect Servers** column.

Again, the console is based on a left to right workflow. Select the collect server in the left column to view the list of **Collections** in the next column to the right.

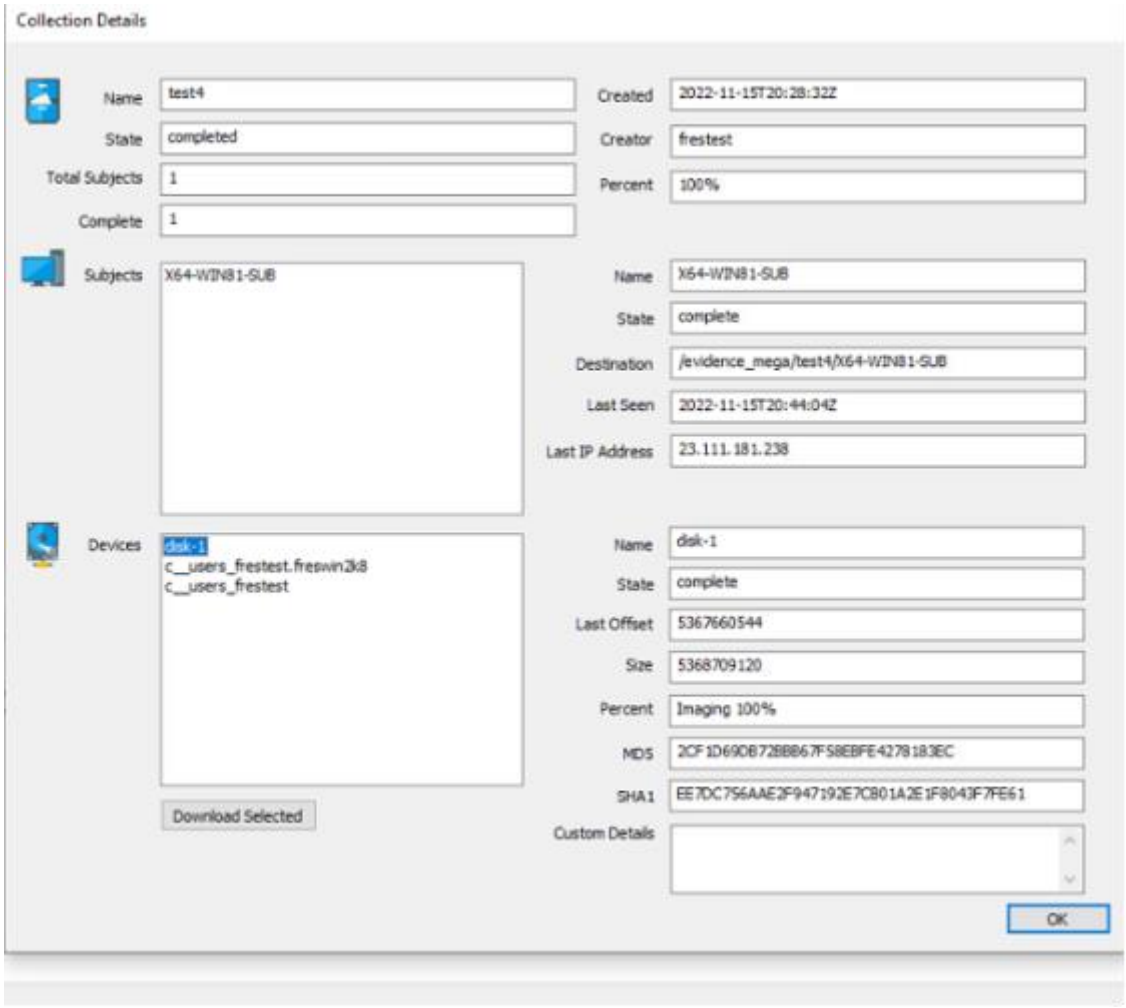


The **Items** column will list the names of each collection created.



For more details on a specific collection, right click and choose **Show Collection Details** or highlight it and choose **Show Collection Details** from the **Collection** dropdown menu.

Collection Details



Collection Details contains the following information:

Name: The name that was created for the collection

State: Will display the current state of pending, in process, or completed.

Total Subjects: The total number of subject computers in the collection

Complete: The number of subject computers successfully collected.

Created: The time the image was created and started. All timestamps throughout F-Response Collect use ISO8601 GMT time.

Creator: The examiner that created the collection.

Percent: The percentage completed for the overall collection.

Selecting a subject will populate the following subject information:

Name: The subject's hostname.

State: Will display the current state of pending, in process, or complete.

Destination: The directory on the collect server where data from this collection and subject will be stored.

Last Seen: The last time that subject send data to the server for that collection. All timestamps throughout F-Response Collect use ISO8601 GMT time.

IP Address: The last reported IP address of the subject.

Selecting a device will populate the following device information:

Name: The name of the device.

State: Will display the current state of pending, in process, or completed.

Last Offset: The last byte offset collected from.

Size: The size in bytes of the collected item.

Percent: The current percentage complete.

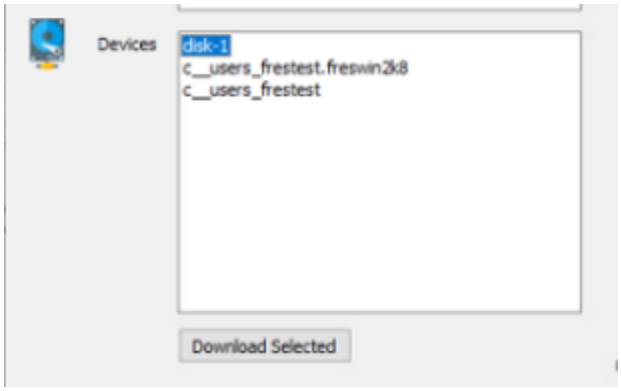
MD5: The MD5 hash of the item, if complete.

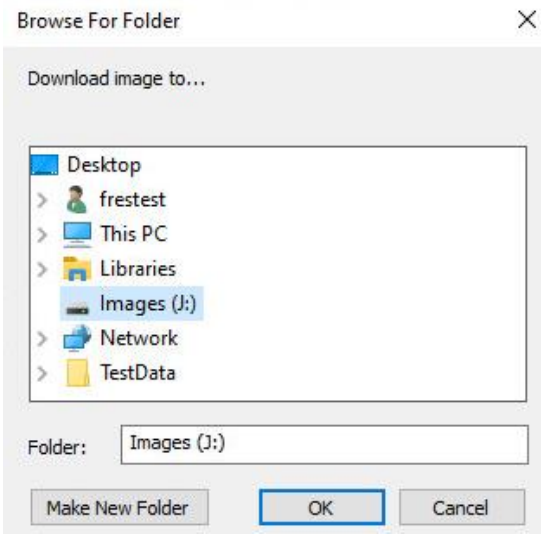
SHA1: The SHA1 hash of the item, if complete.

Custom Details: If the target was a custom collection, the specific details (JSON) is a provided here.

Downloading Completed Images

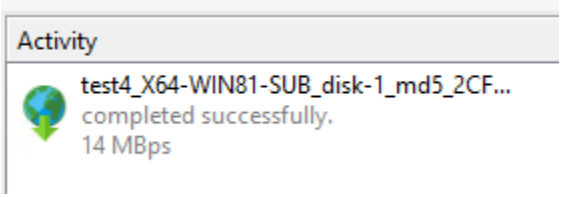
Once the status of a device in the Devices column changes to complete, the Download Selected button will become active. Select the device and press “Download Selected” to start the download process.



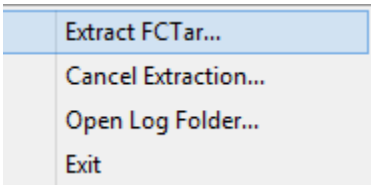


Choose a location to download a copy of the raw image file.

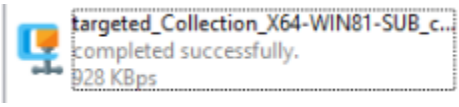
Once the image download is complete you will see a notification in the **Messages** pane:



Extracting FCTAR Images



If your collection included a profile, you will need to download the .FCTAR file(s) to your local machine and extract their contents. You will find the extract option in the file menu. You do **not** need to be logged into a Collect Server to extract a saved FCTAR file. Note: It is possible to exceed file name lengths with extracted profile content, we highly suggest you use a Virtual Hard Disk as your destination path. Creating and mounting a Virtual Hard Disk (VHD) is beyond the scope of this document.

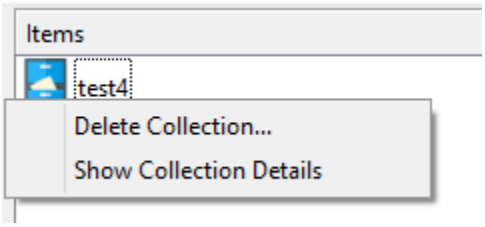


Deleting a Collection

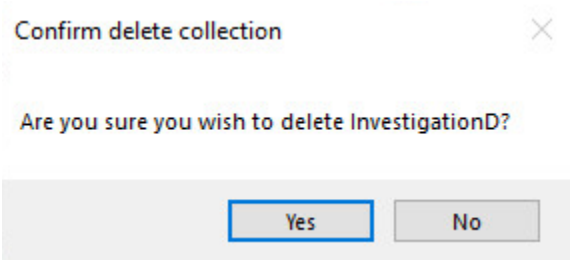
Examiners can view and delete only collections they have created. F-Response users assigned an Administrator role on the Collect Server can view and delete any collections in the repository.

***Note when a collection is deleted from the Console it is removed from the repository on the Collect Server and cannot be recovered.**

To delete a collection, highlight the collection and choose Delete Collection… from the Collection dropdown menu, or simply right click and choose the option:



A warning prompt will appear asking to confirm the deletion from both the console and server repository. **All images that are part of the collection will be deleted.**



Click yes to complete the deletion of the collection and its associated image files.

Agentless Connections

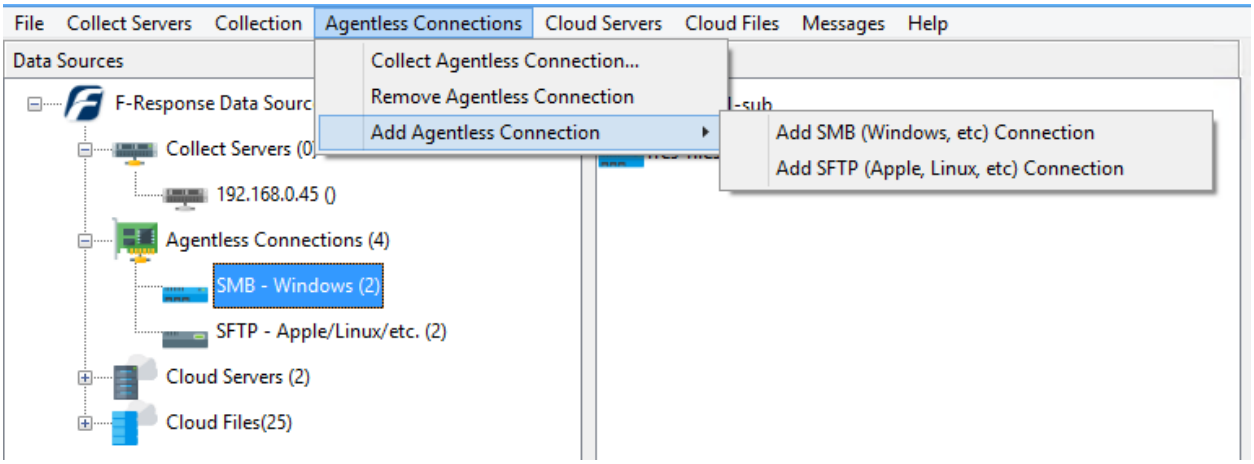
F-Response offers agentless collection from remote subject machines leveraging SMB and SFTP connections. In situations where otherwise you could not install a F-Response executable to fully access the remote machine's resources, Agentless Connection will allow you to collect logical files and folders and preserve the file dates/times.

This is an excellent option to consider when trying to collect data from newer security chip enhanced Apple hardware, Non-Windows Operating systems such as Linux, Solaris, and AIX, remote shares, or NAS devices.

SMB Connection (Windows Systems)

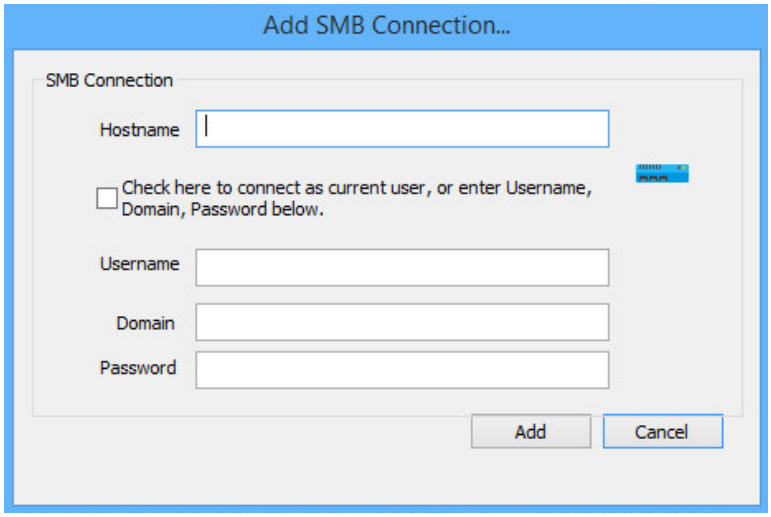
The SMB protocol (present on most Windows systems and NAS[1] devices) is a simple way to collect to a VHD or local directory while preserving files dates/times.

To configure an SMB connection, select **Agentless Connections** from the dropdown menu, then **Add Agentless connection →Add SMB (Windows, etc) Connection**, or simply double click **SMB -Windows** in the Data Sources column to bring up the **Add SMB Connection** window.



Add SMB Connection…

[1] Network Attached Storage.



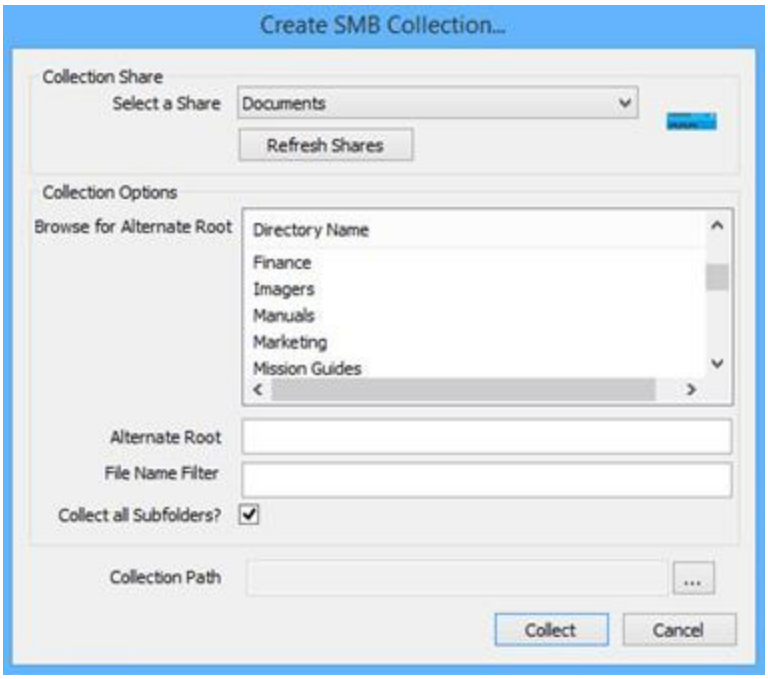
Add Agentless SMB Connection dialog…

Use the "Add SMB Connection…" dialog to input a new connection. You will need the hostname or IP of the remote computer and sufficient credentials for access[2]. Click the **Add** button when complete and the hostname will appear in the **Items** column.

You have two credential options. Either using the currently logged in user when attempting to perform the collection, or inputting a username, domain, and password value. If you use the currently logged in user, be sure to note that the software will not save your user information, and will instead execute any collection as the current management console user at the time.

Once the host has been added to the Items column a collection can be created. To open the **Create SMB Collection…** window, highlight the hostname in the **Items** column and choose **Collect Agentless Collection…** from the **Agentless Connections** drop-down menu, or simply double click the hostname in the **Items** column.

[2] Note: Regardless of credential levels used (Admin, Domain Admin), some system files may be locked by the OS and unavailable for collection using SMB.



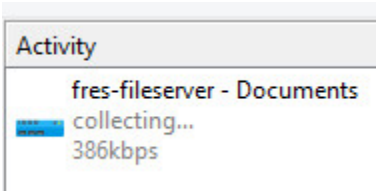
First, select the share from the **Select a Share** dropdown box.

Under the **Collection Options** portion of the window, there are a few options available to adjust the scope of a collection. Browse through the **Directory Name** to locate a specific directory if needed. The directory chosen will populate the **Alternate Root** field below. The collection scope can be narrowed further by adding a **File Name** filter[3], such as "**pdf**" to collect only files with pdf in the filename.

You may choose to tighten the scope further by selecting or deselecting the **Collect all Subfolders?** option. Turning this off will mean only the content of the selected folder is collected, any subfolders will be ignored.

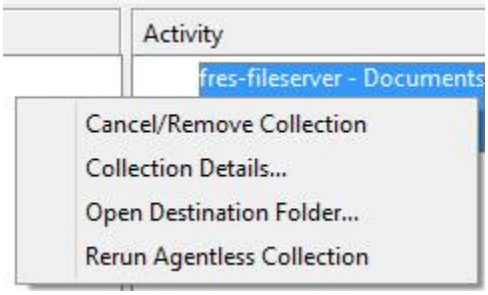
Lastly, choose a location to store the collected data under **Collection Path.**

When ready, click the Collect button to begin the collection. The collection will appear in the Activity column.



Active collection activity…

Completion will be noted in the activity window. You may right click on the collection for a list of options:



[3] The filename filter simply compares the inputted text against the name of the file. For example, by inputting "pdf" both "this_is_not_a_pdf.txt" and "this_is_a_pdf.pdf" would be collected. To limit on file extension, simply add a period to the front. I.e. ".pdf"

Cancel/Remove Collection will cancel a running collection or remove a completed collection from the activity column. This action will not delete the collected data from the storage location.

Collection Details… will provide a quick summary of the collection such as the number of files copied, current collection state, collection duration, etc.

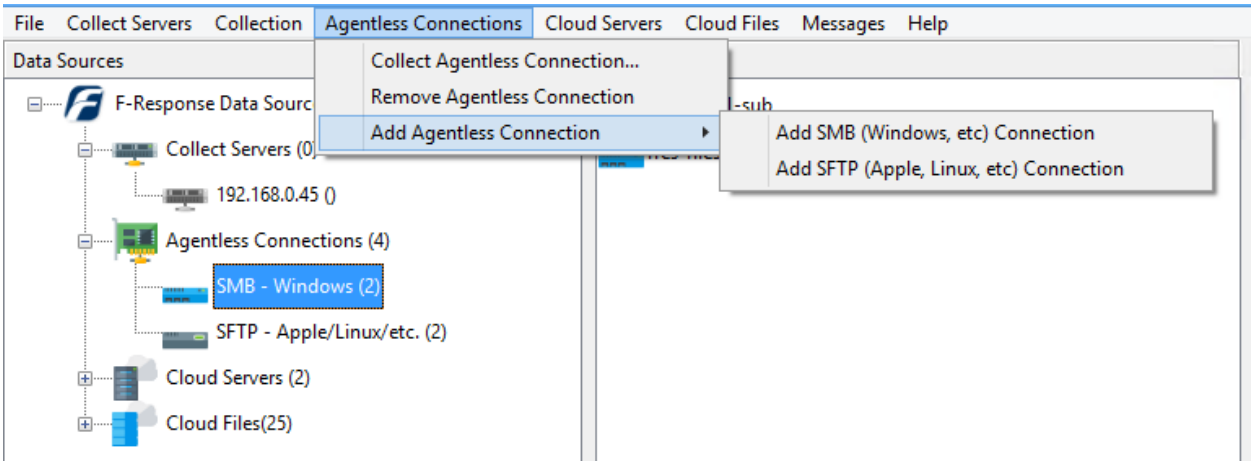
Open Destination Folder… will open the location chosen to store the collection to review the data.

Rerun Agentless Collection If errors occurred for specific files during collection, this option will execute the collection again, focused only on the uncollected files. **This option is only available when collecting to a Local Directory.**

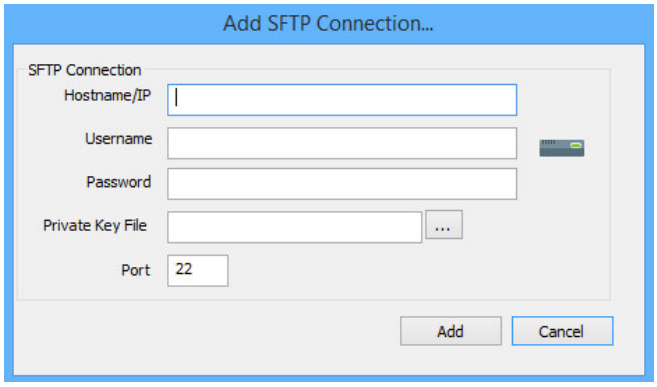
SFTP Connection (Non-Windows)

Secure FTP or SFTP is a common file sharing protocol on Non-Windows operating systems (Apple OSX, Linux, Solaris, AIX, etc.) SFTP can be used to collect to a VHD or local directory while preserving file dates/times.

To configure a SFTP connection, select **Agentless Connections** from the dropdown menu, then **Add Agentless connection →Add SFTP (Apple, Linux, etc) Connection**, or simply double click **SFTP - Apple/Linux/etc.** in the Data Sources column to bring up the **Add SFTP Connection** window.



Add SFTP Connection…



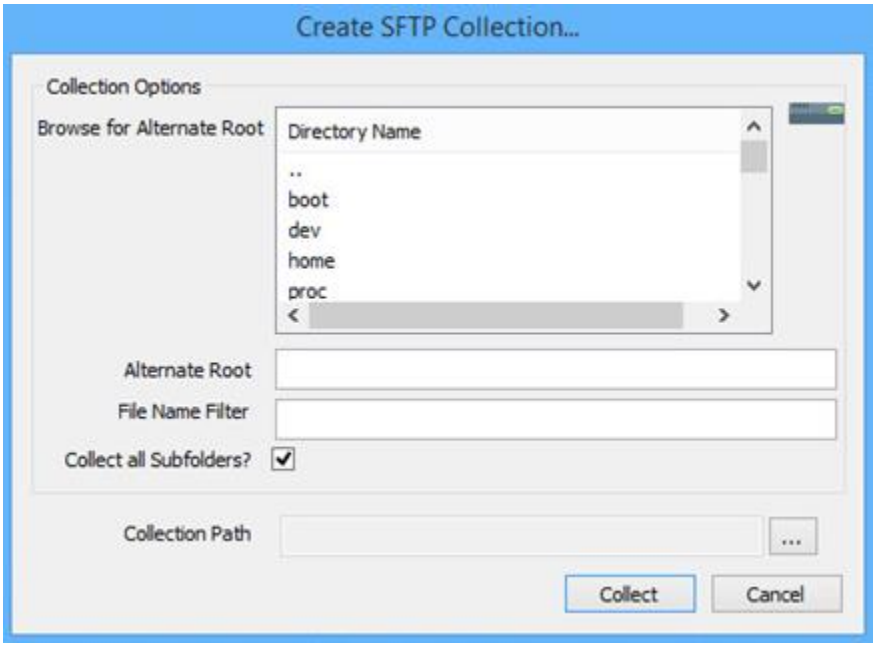
Add SFTP Connection Dialog

Use the "Add SFTP Connection…" dialog to input a new connection. You will need the hostname or IP of the remote computer and sufficient credentials for access[4]. Click the **Add** button when complete and the hostname will appear in the **Items** column.

[4] Note: Regardless of credential levels used (root), some system files may be locked by the OS and unavailable for collection using SFTP.

If a **Private Key File** is needed it can be added in this field, and the Port can be adjusted if the remote computer is not using the default port, TCP port 22. Click the **Add** button when complete and the hostname or IP will appear in the **Items** column.

Once the host has been added to the Items column a collection can be created. To open the **Create SFTP Collection…** window, highlight the hostname in the **Items** column and choose **Collect Agentless Collection…** from the **Agentless Connections** drop-down menu, or simply double click the hostname in the **Items** column.

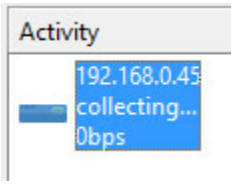


Under the **Collection Options** portion of the window, there are a few options available to adjust the scope of a collection. Browse through the **Directory Name** to locate a specific directory if needed. The directory chosen will populate the **Alternate Root** field below. The collection scope can be narrowed further by adding a **File Name** filter[5], such as "**pdf**" to collect only files with pdf in the filename.

You may choose to tighten the scope further by selecting or deselecting the **Collect all Subfolders?** option. Turning this off will mean only the content of the selected folder is collected, any subfolders will be ignored.

Lastly, choose a location to store the collected data under **Collection Path.**

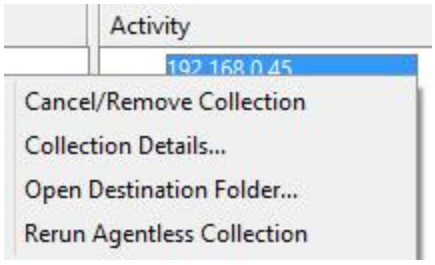
When ready, click the Collect button to begin the collection. The collection will appear in the Activity column.



Active Collection Activity…

[5] The filename filter simply compares the inputted text against the name of the file. For example, by inputting "pdf" both "this_is_not_a_pdf.txt" and "this_is_a_pdf.pdf" would be collected. To limit on file extension, simply add a period to the front. I.e. ".pdf"

Completion will be noted in the activity window. Right click on the collection for a list of options:



Cancel/Remove Collection will cancel a running collection or remove a complete collection from the activity column. This action will not delete the collected data from the storage location.

Collection Details… will provide a quick summary of the collection such as the number of files copied, current collection state, collection duration, etc.

Open Destination Folder… will open the location chosen to store the collection to review the data.

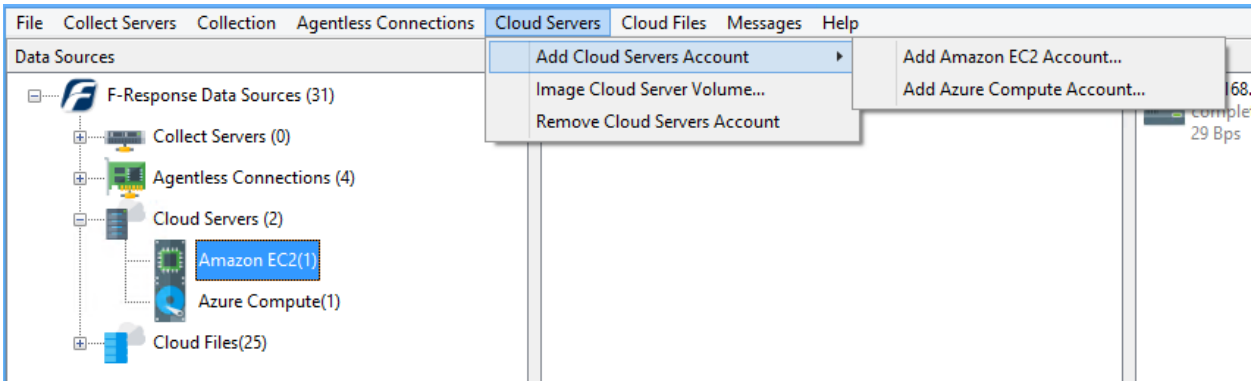
Rerun Agentless Collection If errors occurred for specific files during collection, this option will execute the collection again, focused only on the uncollected files. **This option is only available when collecting to a Local Directory.**

Collecting from Cloud Server Providers

Using the Management Console to collect Cloud Server Volume Snapshots

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

The F-Response Management Console offers the ability to collect cloud server volume snapshots from multiple cloud computing providers. For a complete list of options as well as details on how to leverage this capability, please refer to the provider specific Mission Guide[6] on our website.



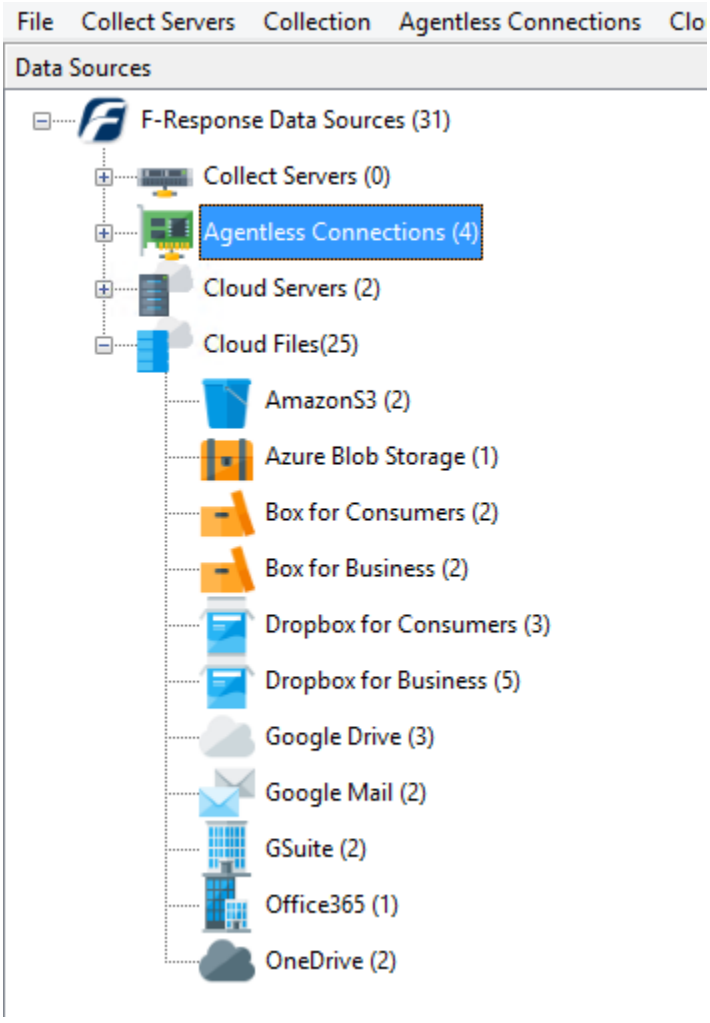
F-Response Cloud Servers Providers

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

Collecting from Cloud Files providers

Disclaimer: F-Response provides access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources are by their very nature volatile. F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection. *For the latest details on collecting from specific cloud providers, please refer to the Mission Guides on our website: https://f-response.com/support/missionguides*

The F-Response Management Console offers the ability to perform cloud provider data collections to Native Directory locations. All supported providers (which varies by F-Response License) are visible in the Data Sources pane. Configuring access to these providers varies greatly by provider, therefore for the most accurate information see the appropriate Mission Guide[7] on the F-Response Website.

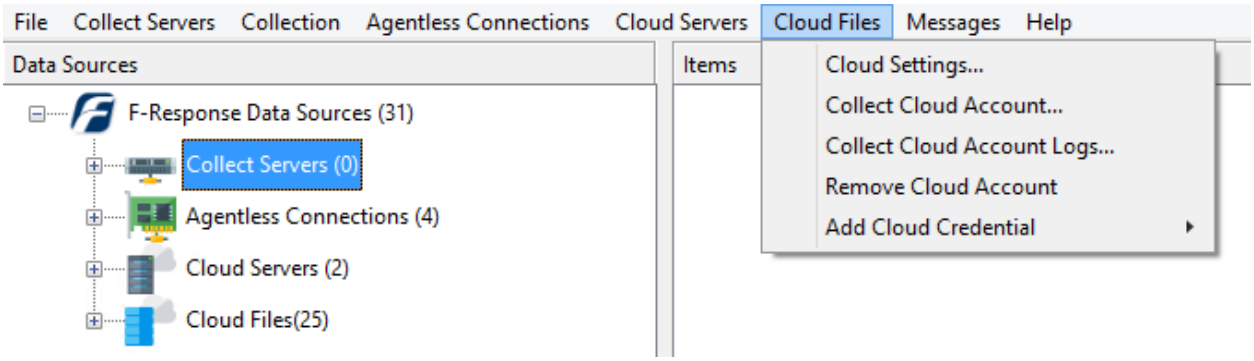


F-Response Cloud Providers

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

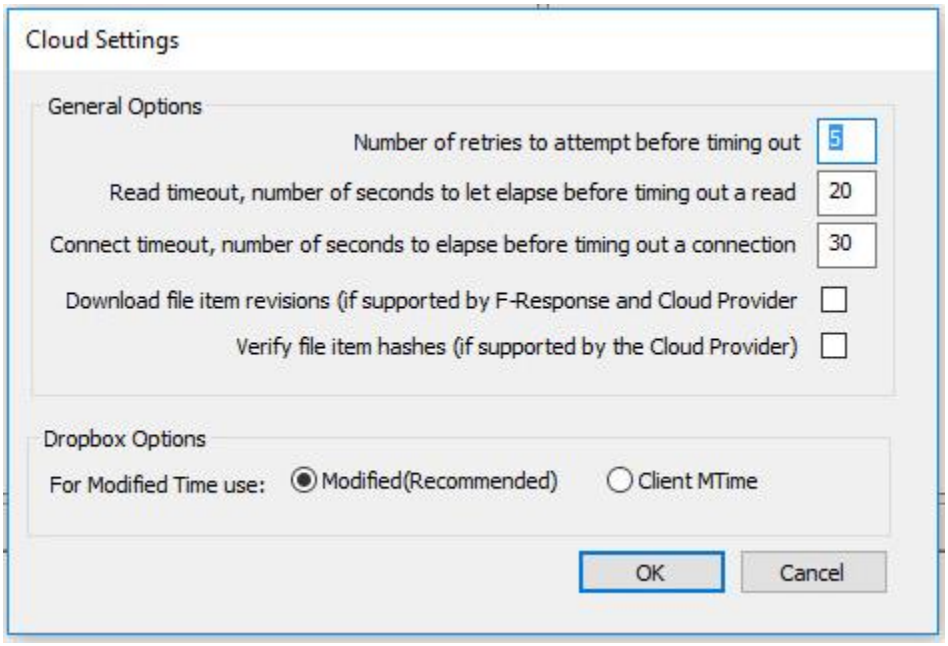
Configuring Cloud Settings

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



Cloud Menu

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



Cloud Provider Settings

NUMBER OF RETRIES TO ATTEMPT BEFORE TIMING OUT

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

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

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

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

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

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

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

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

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

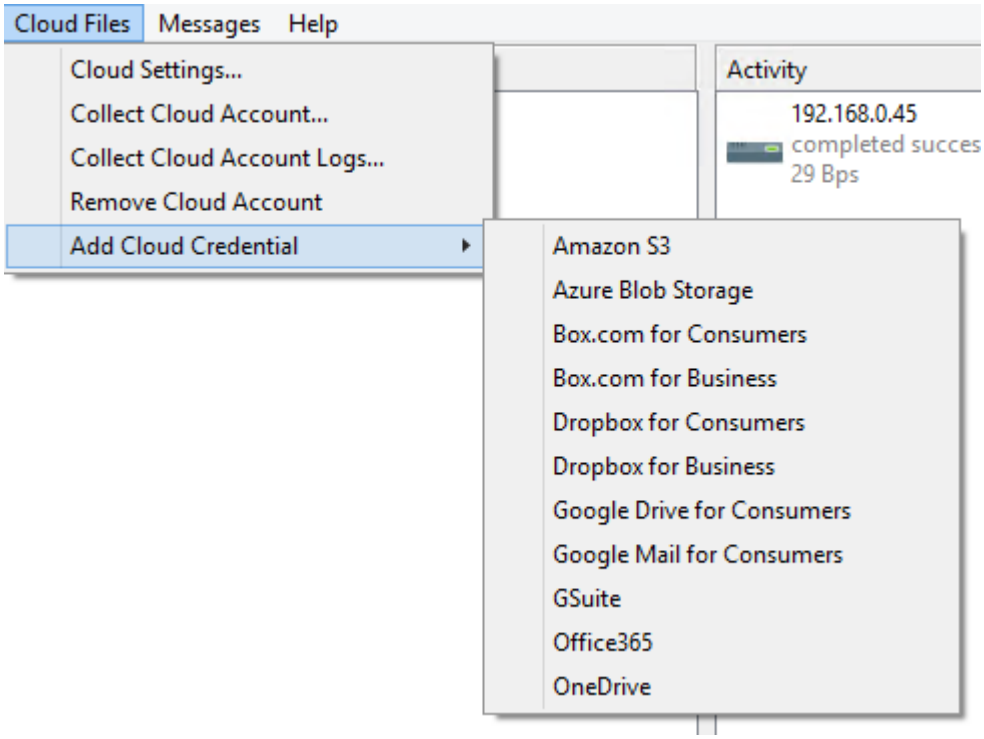
Dropbox Options

FOR MODIFIED TIME USE:

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

Configuring Cloud Credentials

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

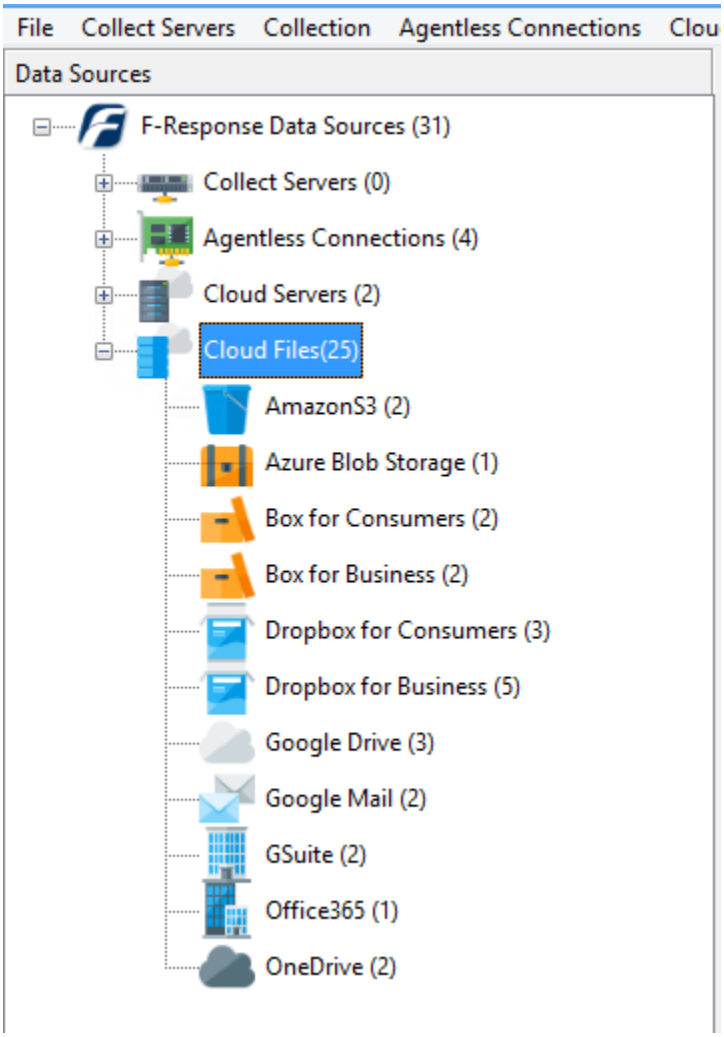


Provider Credentials

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

Collecting a Cloud Account

After successfully adding one or more cloud accounts you will find them visible in the Items column.



Individual and business accounts

Double clicking on an individual account will trigger a dialog for collection of that account, more details on specific dialogs by provider are available in the individual provider Mission Guides on our website: https://f-response.com/support/missionguides

Appendix A.

Legal Notices

Trademarks

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

Statement of Rights

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

Disclaimer

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

Patents

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

Appendix B.

Release History

8.7.1.33 -> Updated 3rd party libraries for cloud file access and enumeration. Modified Collect Server data locks to prevent inaccessible subjects when multiple examiners are tasking the same subject machine. Updated the console to enforce updated naming when a collection is created or deleted. Added start and end times to the collection log.

8.7.1.28 -> Improved logging for Okta authentication on the Collect server. Added start and end date time values to individual collection notes (newly created collections only) as well as examiner details.

8.7.1.27 -> Added Okta authentication as an option. Corrected issue with collecting team folder from Dropbox for Business.

8.7.1.19 -> Change Product Summary Information during MSI export to match product and manufacturer as provided. Added server authentication token to allow subjects to authenticate server collection requests. Added Strict-Transport-Security header to server responses.

8.7.1.17 -> Added new self-delete option when creating collections. Windows subjects may now be instructed to self-uninstall at the completion of the collection. This will be remove the software from the subject machine and remove it from the list of recently checked in subjects on the Collect Server. Corrected minor file time issue when collecting from Google Mail. All Gmail file times are zeroed out and match the documentation in the mission guide.

8.7.1.9/8.7.1.10/8.7.1.11 -> Added option to increase the window for resumption of physical memory collection beyond the default 60 seconds. Added support for Google Compute collection in Cloud Servers and changed GUI to reflect Google Workspace from GSuite. Corrected an issue that would have left image files behind under Windows Collect Servers after delete (Be sure to check manually and remove old image files after moving to this new release!). Completely overhauled the custom and profile collection process for all supported platforms. Added an option to export CSV of Subject and Examiner history to the F-Response Configuration Console. Corrected an issue with Collect subjects not starting on certain Windows configurations. Correct Unicode to UTF-8 conversion in file collection for profile and custom collections.

8.6.1.4 -> Added new F-Response Collect executable for Linux subjects (x86_64 only). Added new target option, Master File Table (MFT) for Windows subjects. Corrected issue with alternate hostname export. Corrected F-Response Box.com collection to use localhost instead of 127.0.0.1 as per recent change at Box. Modified EC2 server collection to prompt for one or more regions.

8.5.1.14 -> Corrected issue with running Agentless, Cloud Servers, and Cloud Files collection. Added capability to locate and properly handle Dropbox for Business Teams Folders. Corrected the F-Response Collect Management Console application link. Updated the error display to provide more detailed error messaging. Added restrictions to collection name to prohibit non-filesystem safe characters. Corrected alternate hostname export. Disabled web configuration pages by default. To re-enable web pages for configuration until they are removed at a later date, add “webremove”:false, to your frescollect.cfg and restart.

8.5.1.10/8.5.1.11/8.5.1.12 -> Added a new Collect Management console, including access to Cloud Files, Cloud Servers, and Agentless Collections. F-Response Collect Subjects now detect metered connections and will not execute if the subject’s network access is considered restricted or metered. This will only happen on more recent versions of Windows 10 and better. Corrected an issue with fragmented uploads to the Collect Server.

4.1.1.1 -> Added Physical Memory collection for F-Response Collect. Added the option to install and run the F-Response Collect server on the Windows platform.

4.0.1.10 -> Added Redhat Enterprise 8 RPM for F-Response Collect server. Altered Alternate Hostnames/Ips to allow for multiple addresses, subject will try each in sequence. Only useful when your server has both internal and external ranges and you would like the subject to try both. Altered IP restrictions to allow ranges as well as individual addresses. Corrected memory leak in subject and addressed issue with profile file collection completion. Altered MSI to wrap server variable in quotes to allow for comma separated values. Improved restart detection.

4.0.1.7 -> Added Custom Collection options and improved restart process for both Custom and Profile target collections.

3.0.1.12 -> Corrected profile restart issues and added new F-Response Collect Server configuration tool as well as the option to remove the web administration interface. The web interface will be deprecated and removed in a future release.

3.0.1.9 -> Corrected issues with restarting failed profile collections when Volume Shadow Copy already exists, added error handling code for when files cannot be read from the VSS during a profile collection.

3.0.1.7 -> Added the ability to collect and extract profile content (requires latest subject executables).

2.0.1.4 -> Removed select TLS crypto suites that caused issues with certain interactions.

2.0.1.3 -> Moved the hashing process into the subject to deliver a more robust experience and provide instant hashing at the end of a collection. 2.0.1.3 require both the server and the subjects be replaced to achieve this new functionality. Added auto-resumption to examiner image download (storage panel) in the event the download fails for whatever reason. Added new “iprestrictions” option to the collect server configuration file to further restrict examiner access by IP address.

1.0.1.28 -> Updated hashing process to provide additional feedback. Addressed message delivery for UI to provide consistent view.

Initial Release -> 1.0.0.24

Appendix C.

Master Software License Agreement

AGILE RISK MANAGEMENT LLC MASTER SOFTWARE LICENSE AGREEMENT

TERMS AND CONDITIONS

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

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

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

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

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

2. Grant of Software License.

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

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

3. Software License Restrictions.

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

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

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

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

6. Confidentiality.

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

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

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

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

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

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

8. Limitations and Exclusions.

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

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

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

9. Verification.

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

10. Support Services

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

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

11. Miscellaneous.

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

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

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

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

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

11.6. Redistribution Compliance.

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

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

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

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

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

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

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

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

==========

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

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

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

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

==========

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

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

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

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

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

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

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

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 Hoguin <essen@ninenines.eu>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix D

Log Formats

The following log formats are available:

- Standard (CSV)
  - function, username, datetime, type, message
- QRadar
  - datetime, Hostname LEEF:1.0|F-Response|F-Response Collect|8.0|INFO|function=,username=,type=,message=
- Splunk
  - datetime, hostname=,function=,username=,type=,message=

Function	**removedomain**
Content	Removed Active Directory Domain <DOMAIN>.
Reason	Indicates when an Active Directory login Domain has been removed.

Function	**adddomain**
Content	Added Active Directory Domain <DOMAIN>.
Reason	Indicates when an Active Directory login Domain has been added.

Function	**testdomain**
Content	Testing <DOMAIN\USERNAME>'s AD Domain.
Reason	Indicates when the Collect is testing whether the user resides in that domain and the configured groups.

Function	**validateaduser**
Content	Validated Active Directory user <USERNAME>. Unable to validate <USERNAME>, error <ERROR>.
Reason	Indicates success or failure in validating a user against the configured Active Directory.

Function	**getusertoken**
Content	Login user <USERNAME> successful.
Reason	Indicates successful login.

Function	**verifytoken**
Content	Unable to verify token, error <ERROR>. Verified token from local system for user <USERNAME>.
Reason	Indicates successful verification of a token.

Function	**setauthtype**
Content	Successfully set auth type to <AUTHTYPE>. Failed to set authtype <AUTHTYPE>, error <ERROR>. Failed to set authtype <AUTHTYPE>, not a valid authtype.
Reason	Indicates success or failure in setting authorization type.

Function	**adduser**
Content	Added user <USERNAME>, role <ROLE>.
Reason	Indicates success in adding a user.

Function	**removeuser**
Content	Removed user <USERNAME>.
Reason	Indicates success in removing a user.

Function	**listusers**
Content	Listed users.
Reason	Lists users (only valid with local users).

Function	**changeuserrole**
Content	Changed user <USERNAME> role to <ROLE>.
Reason	Indicates changed user role (only valid with local users).

Function	**changeuserpassword**
Content	Changed user <USERNAME> password.
Reason	Indicates changed user password (only valid with local users).

Function	**changeownpassword**
Content	Changed user <USERNAME> password.
Reason	Indicates changed own password (only valid with local users).

Function	**load_der**
Content	Unable to load <DERFILE>, error <ERROR>. Unable to read registry value <REGISTRY> der, error <ERROR>. Unable to open registry <REGISTRY>, error <ERROR>. Unable to open DER file <DERFILE>, error <ERROR>.
Reason	These messages indicate errors with loading the cryptography parameters.

Function	**validate_license**
Content	License validation error <ERROR> with reason <REASON>.
Reason	Indicates an error during license validation with license.f-response.com.

Function	**configureproxy**
Content	Set proxy host to <PROXYHOST> and port to <PROXYPORT>.
Reason	Indicates setting the proxy host and port.

Function	**setlogtype**
Content	Changed logtype to <LOGTYPE> and loglocation to <LOGLOCATION>.
Reason	Indicates setting the log type.

Function	**listsubjects**
Content	Listed subjects.
Reason	Indicates listing of subjects that have connected at one time.

Function	**listexaminers**
Content	Listed examiners.
Reason	Indicates listing of examiners that have connected at one time.

Function	**purgesubjects**
Content	Remove subject history.
Reason	Indicates removing the subject history.

Function	**purgeexaminers**
Content	Remove examiner history.
Reason	Indicates removing the examiner history.

Function	**SubjectError**
Content	Various errors as reported on the subject computer.
Reason	Indicates a subject has reported an error to the Collect server.

Function	**saveimagedata**
Content	Cannot locate memcache for file <FILE>.
Reason	Indicates an internal error writing to the memory cache. Is the server running out of available memory?

Function	**generatehashes**
Content	Starting hashing process for file <FILE>.
Reason	Server is creating file hashes for the collected image.

Function	**saveimagedataprocess**
Content	Error writing to <FILE>, Reason <REASON>.
Reason	Indicates the Collect server was unable to save data to the image file. Are you running out of storage space?

Function	**updatesubjectcollection**
Content	Cannot remove collection from subjectcollection. Subject <SUBJECT> is missing.
Reason	Indicates an inconsistent data state for the subject and its collection details. Please contact support.

Function	**setcollectionpath**
Content	Admin set the collection path to <PATH>.
Reason	An admin user has set the collection path to a new location.

Function	**uninstallsubjects**
Content	Admin has marked <SUBJECTS> for uninstallation.
Reason	An admin user has directed the Collect server to tell listed subjects to uninstall their software on next check-in.

Function	**getsubjectkey**
Content	Examiner <EXAMINER> has retrieved the subject key.
Reason	An examiner has retrieved the alphanumeric subject key necessary for connecting a subject to the Collect server.

Function	**createcollection**
Content	Examiner <EXAMINER> created collection <COLLECTION>.
Reason	An examiner user has created a new collection.

Function	**deletecollection**
Content	Examiner <EXAMINER> deleted collection <COLLECTION>.
Reason	An examiner user has deleted a collection.

Function	**getadmincollections**
Content	Admin <ADMIN> retrieved complete list of all collections.
Reason	An admin user has retrieved a list of all collections.

Function	**getcollections**
Content	Examiner <EXAMINER> has retrieved a list of collections.
Reason	An examiner user has retrieved a list of collections they created.

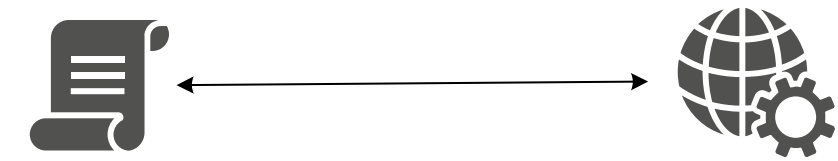
Appendix E

Automating F-Response Collect

Scripting F-Response Collect requires a programming language and environment that can handle the following:

- HTTP POST
- JSON (Read and Write)

F-Response Collect Scripting Model



Custom Scripts

F-Response Collect Server
Https://<SERVERIP/HOSTNAME>/rpc

F-Response Collect uses JSON POST style communication between the script and the remote F-Response Collect Server directly to execute commands and receive responses.

JSON Request Format

F-Response Collect JSON POST requests must be in the following format to be understood by the F-Response Collect RPC Web Service.

```
{
        "function": "list_api",
        "values": {
                "value1": "one",
                "value2": 2
        }
}
```

- Function (“function”)
  - This string value represents the function your script wishes to call. You will find a complete list of the available functions in this document.
- Values (“values”)
  - This object contains zero or more values depending on the chosen function.

Example Request

```
POST /rpc HTTP/1.1
Authorization: <AUTHORIZATION TOKEN>
```

```
Content-Type: application/json
…

{
      "function": "list_api",
      "values": {}
}
```

JSON Response Format

F-Response Collect JSON POST responses are in JSON format and conform to one of the two following formats:

200 – OK Responses

A successful response includes contents specific to the request.

400 – ERROR Responses

```
{
      "error": "error text"
}
```

A failure response includes error text that contains additional details on the unsuccessful request.

Obtaining an Authorization Token

In order to make requests to F-Response Collect you must have an authorization token. Tokens are valid for 24 hours, and should not be shared.

The following is the JSON POST format for requesting an authorization token:

```
POST /rpc
…
{
 "function":"GetUserToken",
 "values":{
  "username":"myuser",
  "password":"mypassword"
}
}

200 OK

{

  "username": "myuser",
  "role": 1,
  "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODkwNDUyNTcsInVzZXJuYW1lIjoiRlJFU1BPTlNFXFxtc2hhbm5vbiIsInJvbGUiOjJ9.nlYz1aNYphpIYjkU5PCldHWv8h0dv3-4JDpgTgLhc-0",
  "subjectkey":
"925cfe10d9078e92ad1695a47c207e2780c8402d3a2d4644cc48c08449ac7e1e"
}}
```

Function Reference

NewCollection

Values: name,subjects,devices.

Help: Creates a new collection on the Collect Server.

Example:

```
POST /rpc
…
{
 “function”:”NewCollection”,
 “values”:{
    “name”:”mytestcollection”,
    “subjects”:[“pc1”,”joeuserpc2”,”homelaptop”],
    “devices”:[“vol-c”]
}
}

200 OK

{
  “collectionid”:UUIDValue
}
```

GetCollections

Values: none.

Help: Returns a JSON of all active collections for you user account.

Example:

```
POST /rpc
…
{
 “function”:”GetCollections”,
 “values”:{
           }
}

200 OK

{
  …
}
```

DeleteCollection

Values: collectionid.

Help: Deletes a collection on the Collect Server.

Example:

```
POST /rpc
…
{
 "function":"DeleCollection",
 "values":{
    "collectionid":UUIDValue
}
}

200 OK

{
  …
}
```

DropUserToken

Values: token.

Help: Deletes the user token to effectively log off the user.

Example:

```
POST /rpc
…
{
 "function":"DropUserToken",
 "values":{
    "token":"…"
  }
}

200 OK

{
  "response":true
}
```

Appendix F

Alternate SSL Certification Configuration

F-Response Collect provides a generic SSL certificate and private key for securing web access to the server, however, you may replace these values with your own certificate and key. Generating a certificate and private key is outside the scope of this document. For the purposes of this appendix we will assume you have a certificate file and corresponding private key.

You will need to place both files in an accessible directory. We recommend placing them outside the installation folder as the contents of this directory may change with new installations of F-Response Collect. Once you have selected or created the directory you will need to place the certificate and private key file in the directory, and then locate the frescollect.cfg file. This file should be located in the original F-Response Collect installation directory or /etc/frescollect.

This file is in JSON format.

You will need to add the following entries to the file and restart the F-Response Collect Service to change the SSL certificate used.

“sslcert”:”C:\\path\\to\\cert.crt”,”sslkey”:”C:\\path\\to\\private.key”