Recorded Future Integration Module for Micro Focus ArcSight

Installation and Implementation Guide - v3.2.1

Contents

Requirements

- The Recorded Future integration package RF_ArcSight_3.2.1.zip
- A Recorded Future API token
- Admin credentials to ArcSight Manager (ESM)
- DNS resolution and HTTPS access to https://api.recordedfuture.com

Additional requirements if Asset and Zone Detection in RF OSINT:

- An ArcSight Asset Model with Zone ranges defined
- A base path zone URI of /All Zones/<Customer Name>

Contents of the package

File list from RF_ArcSight_3.2.1.zip:

- Installation_and_Implementation_Guide-v3.2.1.pdf:
  This file.
- Recorded_Future.arb:
  This file is imported into the ArcSight ESM. It contains lists, rules etc required to correlate with Recorded Future data.
- package.zip:
  This ZIP archive contains programs used to fetch the data from Recorded Future and add it to the ArcSight ESM server. See installation instructions below.

Setting up the integration module

Instructions for an ESM running on Linux

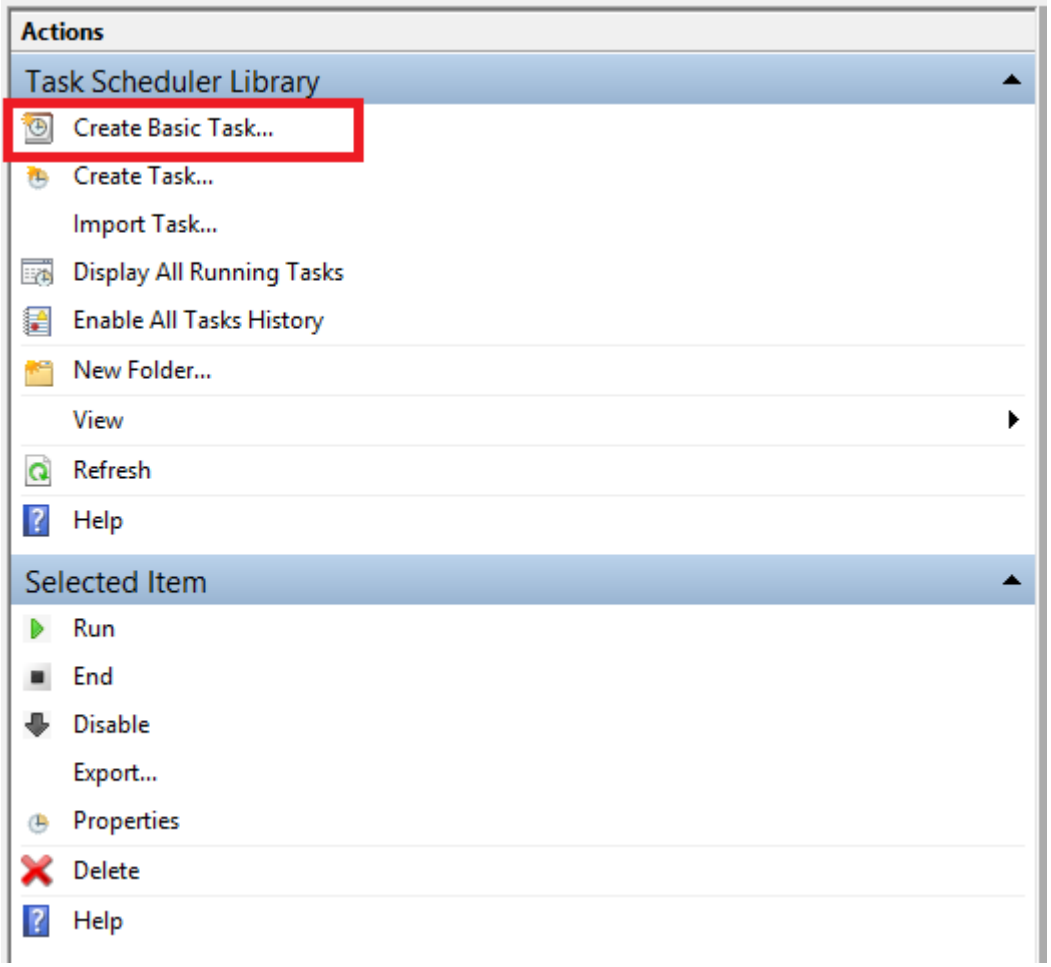
1. Unpack the `RF_ArcSight_3.2.1.zip`, ex in /tmp:
   Ex:
   ```
   cd /tmp/; unzip RF_ArcSight_3.2.1.zip
   ```
2. Unpack the package.zip file, ex into /opt/RF_ArcSight_3.2.1:
   ```
   cd /opt
   unzip /tmp/RF_ArcSight_3.2.1/package.zip
   ```
   The module is now installed in /opt/RF_ArcSight.
3. Using the ArcSight ESM console, import the arb file into ArcSight ESM. It is located in `/tmp/RF_ArcSight_3.2.1`.
4. Setup the module:
   a. Run the configuration script:
      Ex:
      ```
      cd /opt/RF_ArcSight_3.2.1
      python3 bin/arcsight_config.py
      ```

      See “Configuration” below.
   b. Verify that the script works, run:
      ```
      /opt/RF_ArcSight_3.2.1/bin/arcsight_uc1
      ```
      Check log in /opt/RF_ArcSight_3.2.1/log.
5. Setup cron to run the use case scripts. We suggest the following cron patterns:
   a. Automatic running for the use cases:
      ```
      */5 * * * * /opt/RF_ArcSight_3.2.1/bin/arcsight_uc1
      ```

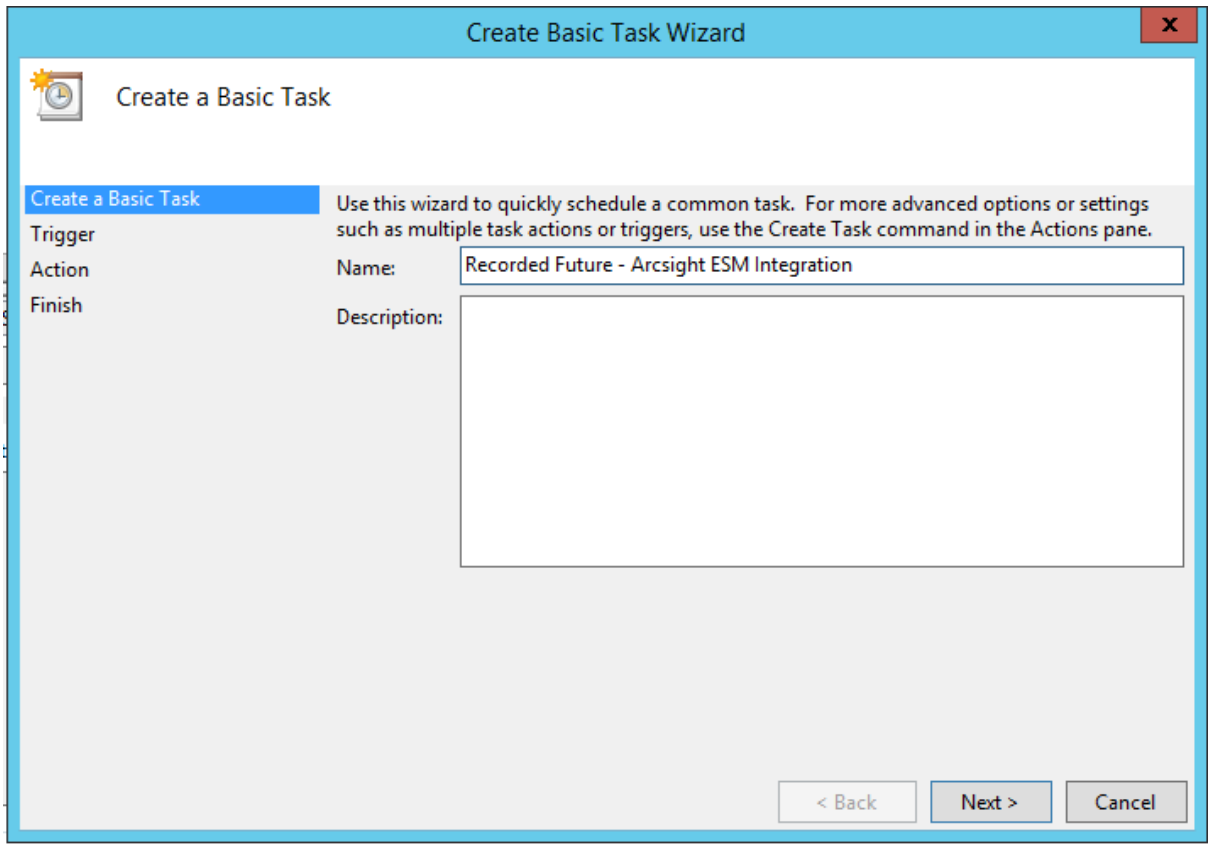
Instructions for running scripts on Microsoft Windows system

Test system - Windows Server Standard 2012 R2

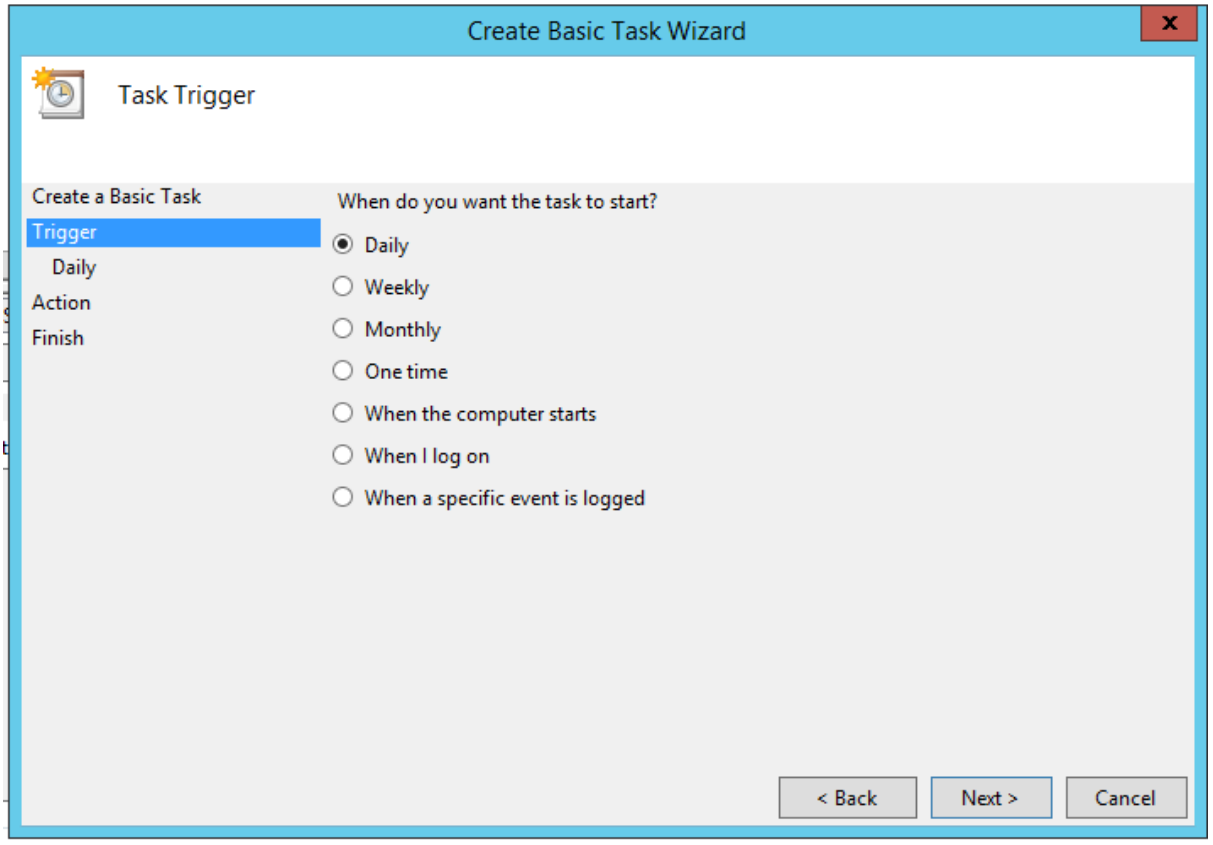
1. Install Python and add it to Windows Environment Variables (https://docs.python.org/2/using/windows.html)
2. Extract the content of the package.zip file to a specific location (Ex: C:\Users\Administrator\Desktop\RF_ArcSight_3.2.1)
3. All other configuration steps are the same as for linux (run arcsight_config.py)
4. Verify that the integration script is running properly (by running "python C:\Users\Administrator\Desktop\RF_ArcSight_3.2.1\bin\arcsight_uc1")
5. Add the "arcsight_uc1" script to scheduler
    a. Open Windows "Task Scheduler"
    b. From the "Actions" section select "Create Basic Task"



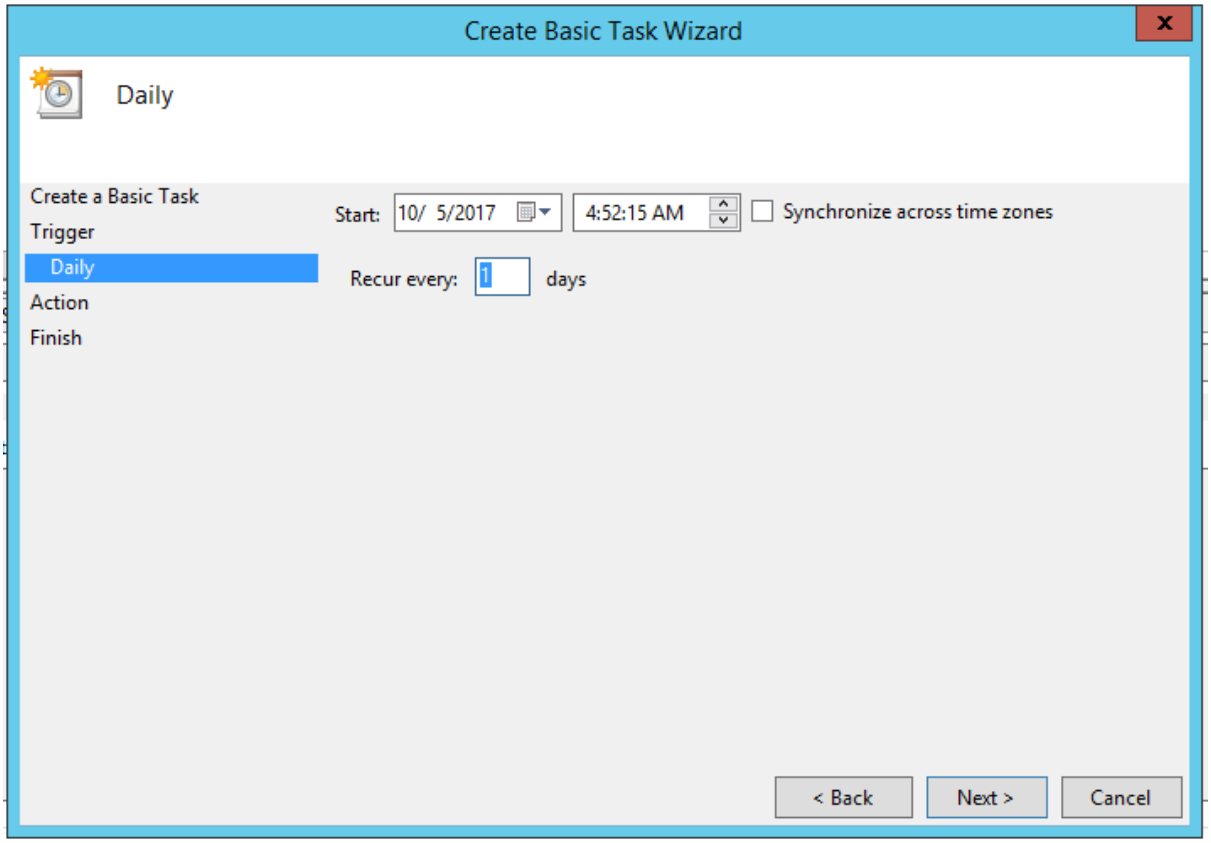
    c. Input a name for the new task and click "Next":



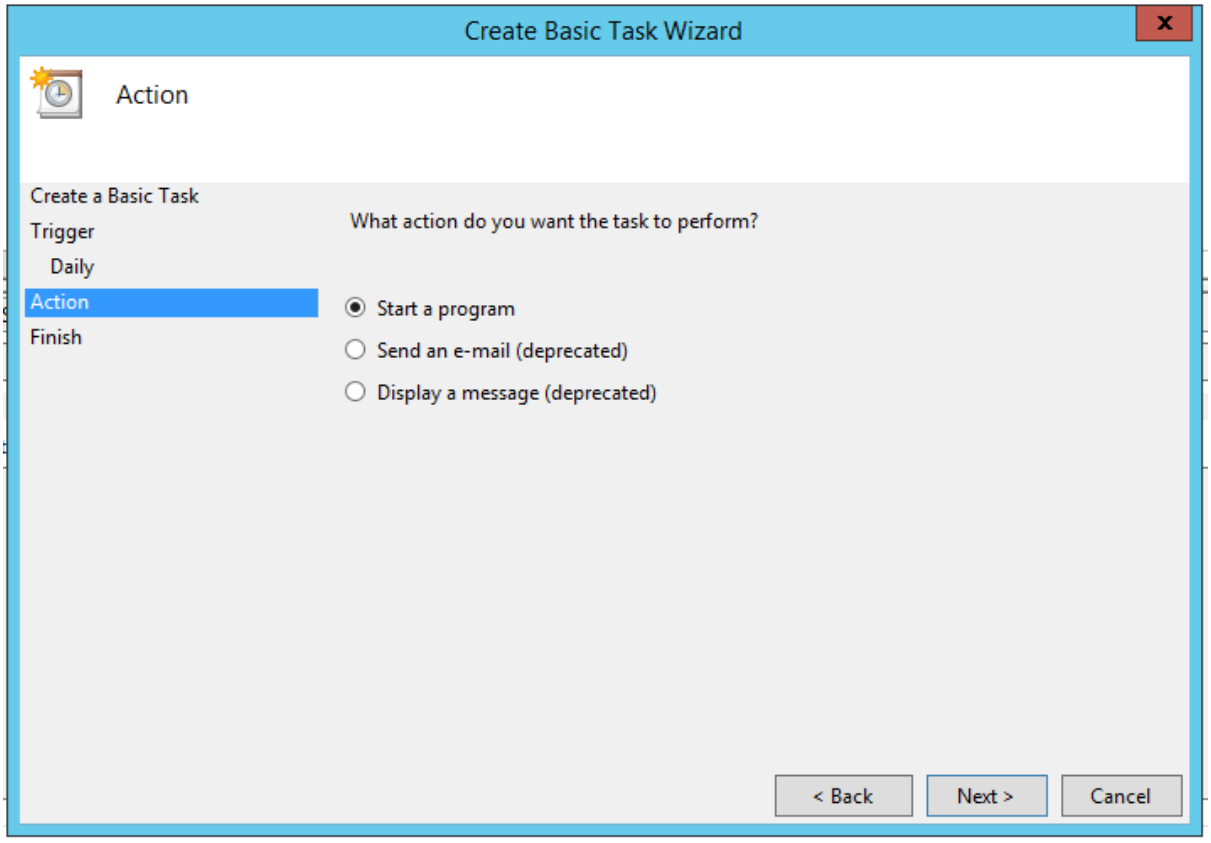
d. Select “Daily” in the Task Trigger step and click “Next”



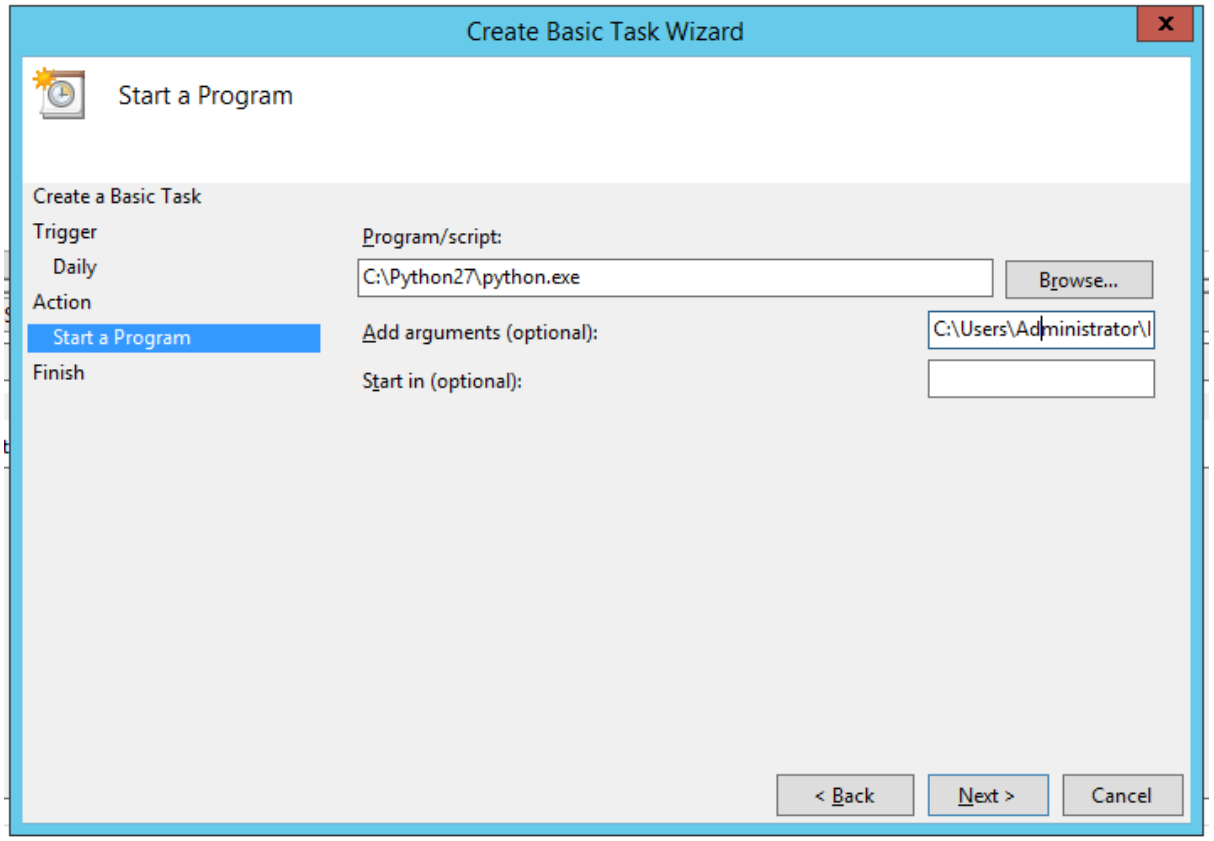
e. Select the time and date when you want the task to run for the first time and click “Next”



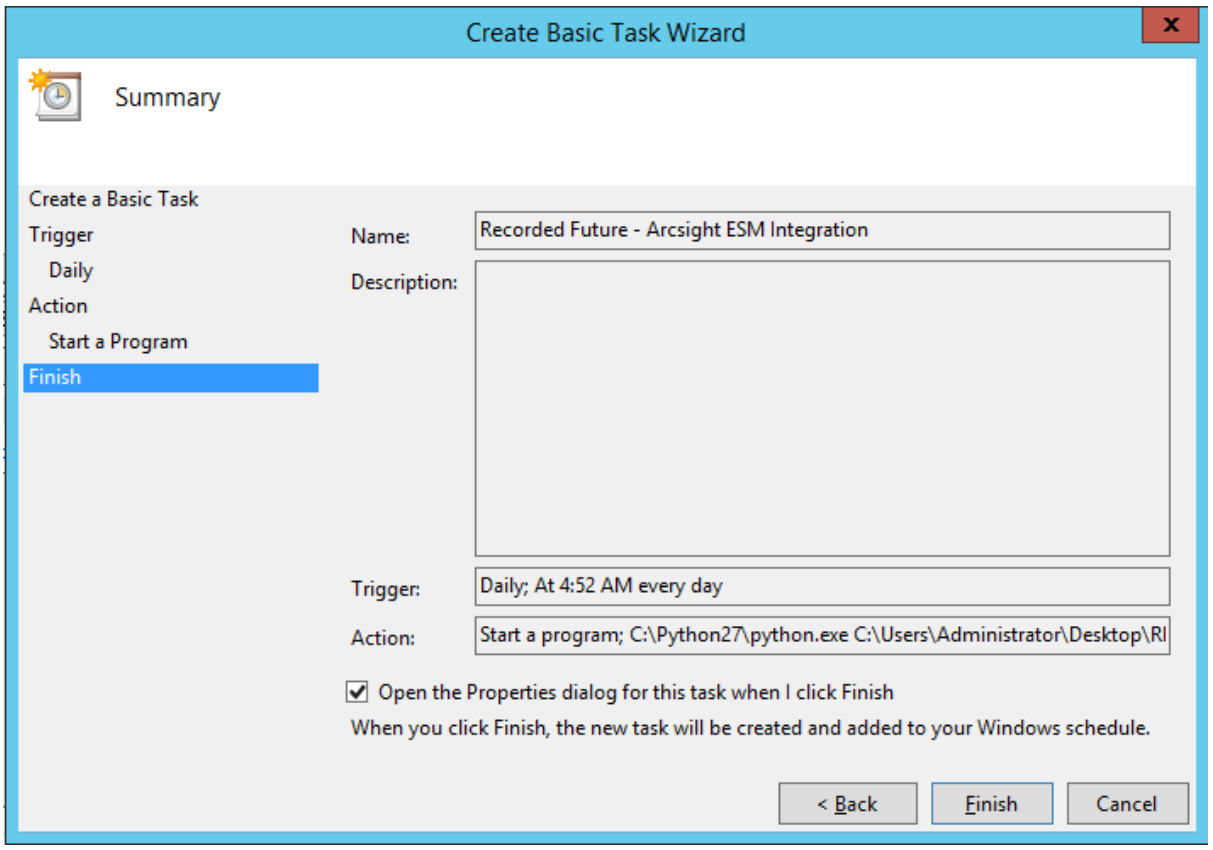
f. Select “Start a program” and click “Next”



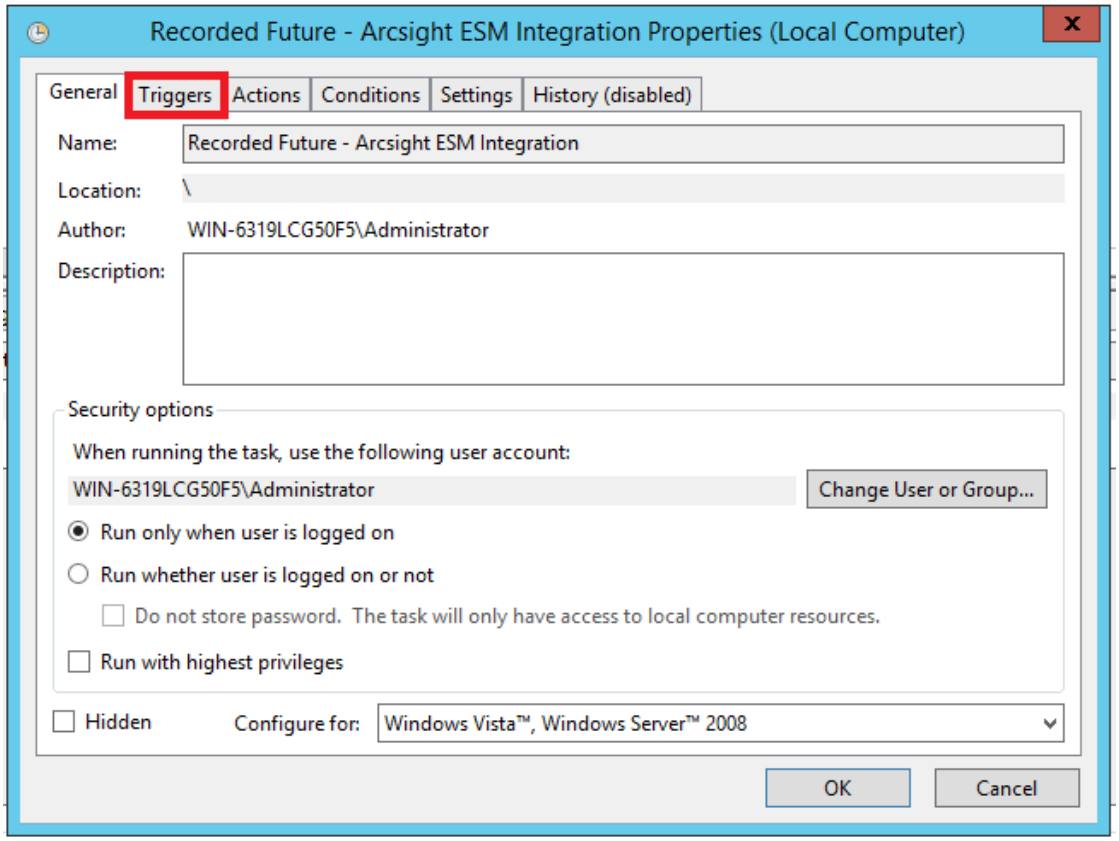
g. In the “Program/Script” section input the path to Python executable. In the “Add arguments” section input path to arcsight_uc1 file. Then click “Next”



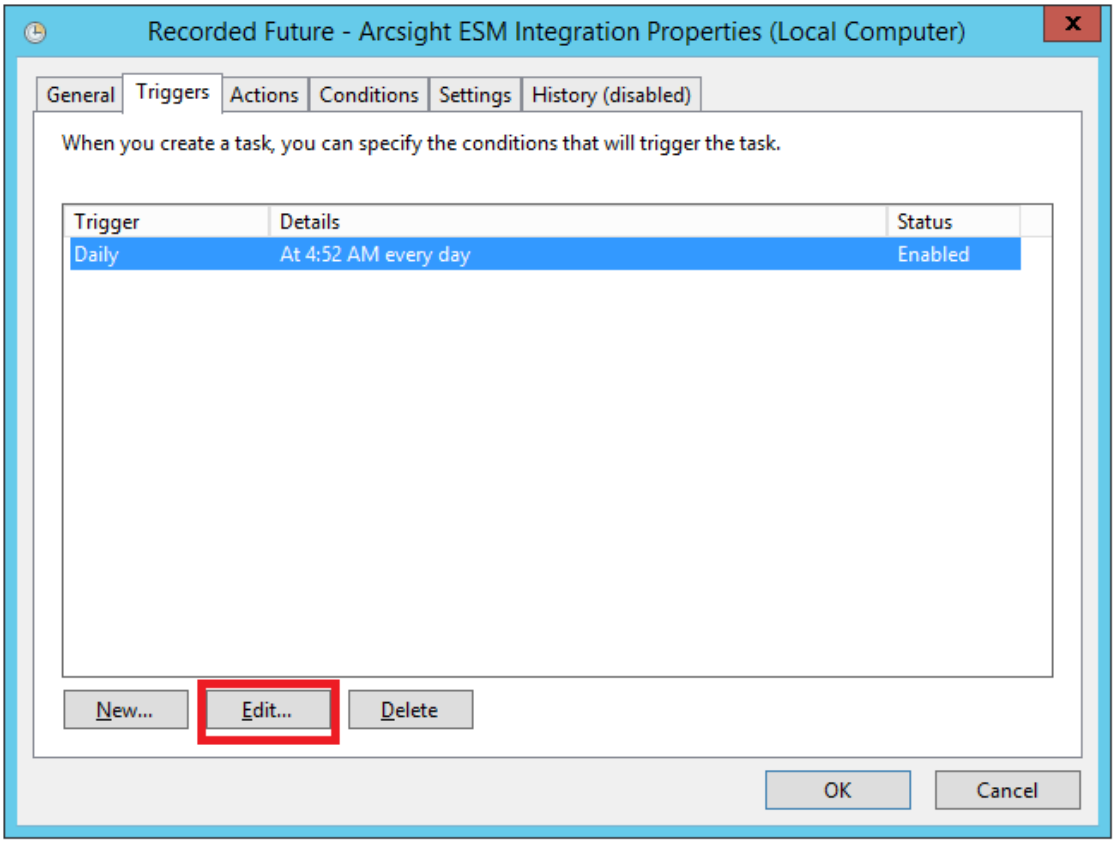
h. Check “Open the Properties dialog for this task when i click Finish” and click “Finish”



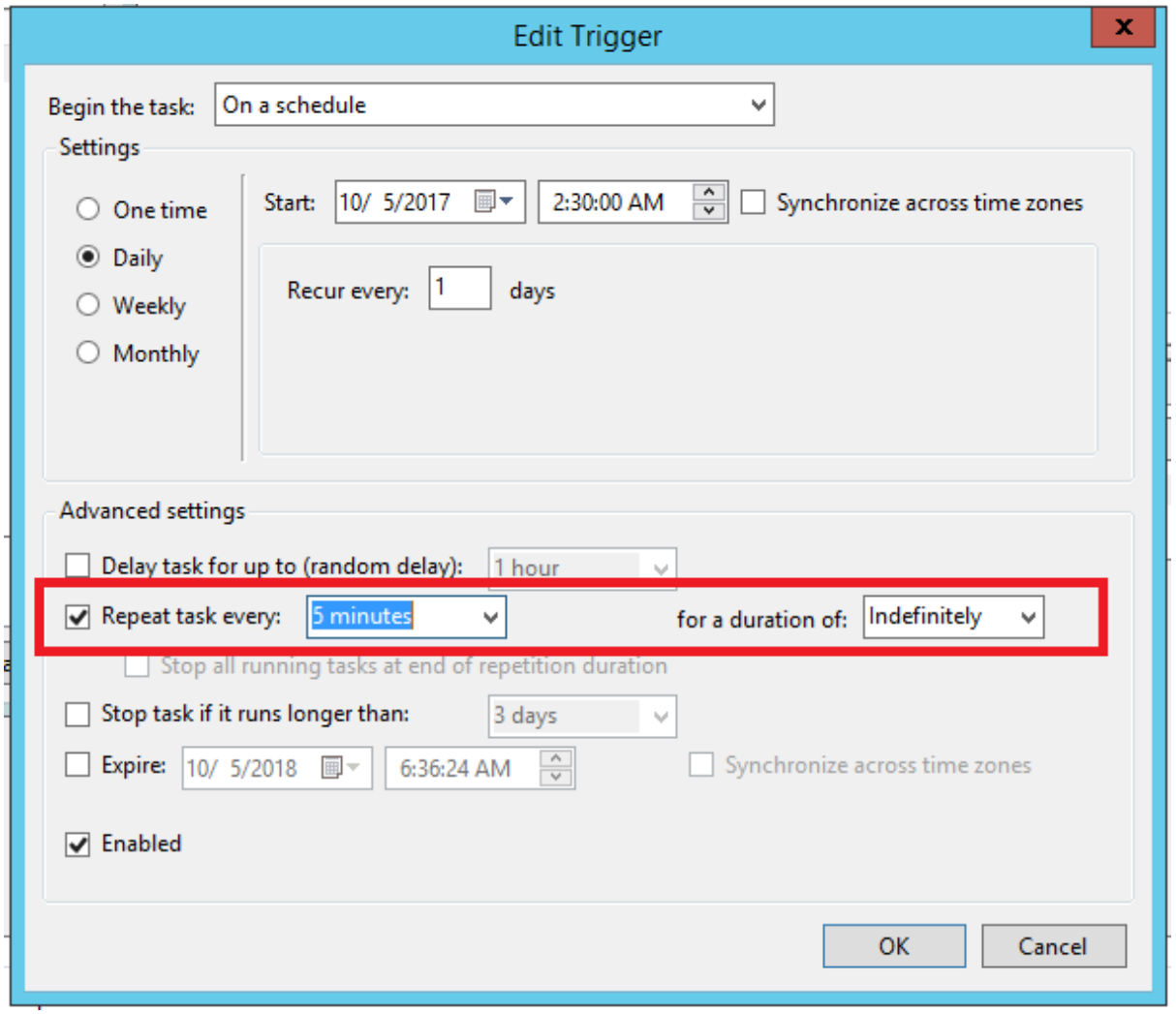
i. In the newly opened window access “Triggers” tab



j. Select the trigger and click ‘Edit“



k. Enable “Repeat task every 5 minutes for a duration of Indefinitely” and click “OK”



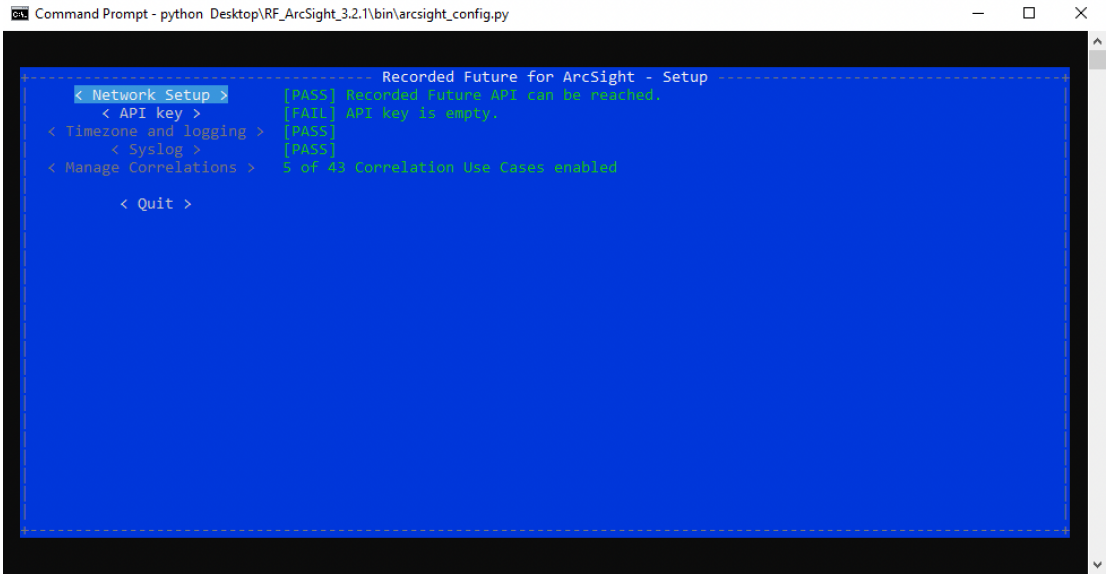
l. Click “OK” again to save the modification.

After performing these steps the task will run every hour and the database will be updated according to the timings in the configuration file.

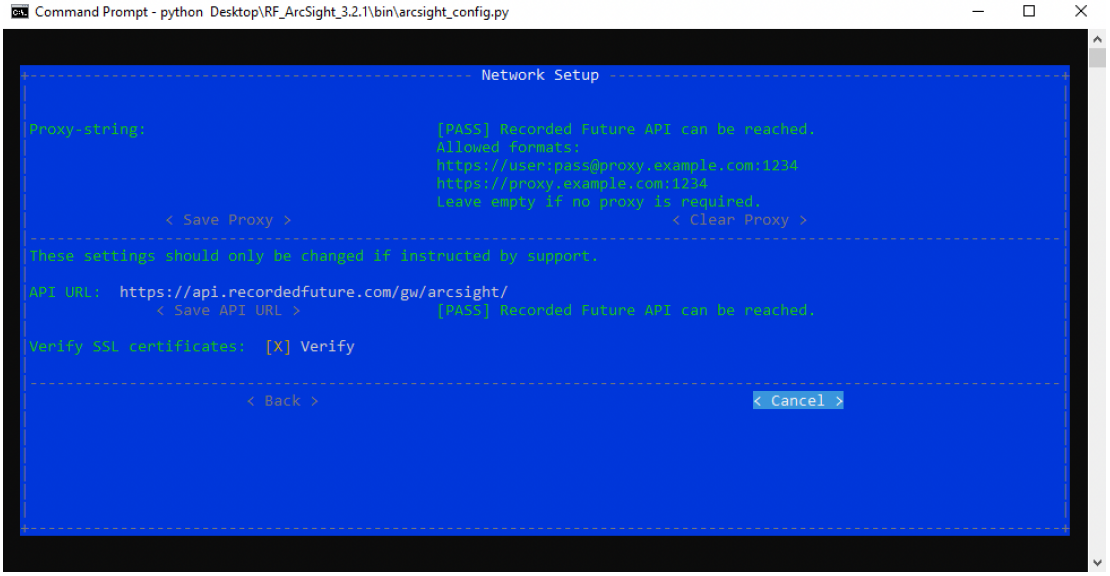
Configuration

The configuration script provides a Text User Interface to help with the setup and configuration of integration. Navigation is best done using the keyboard (arrow keys and tab).

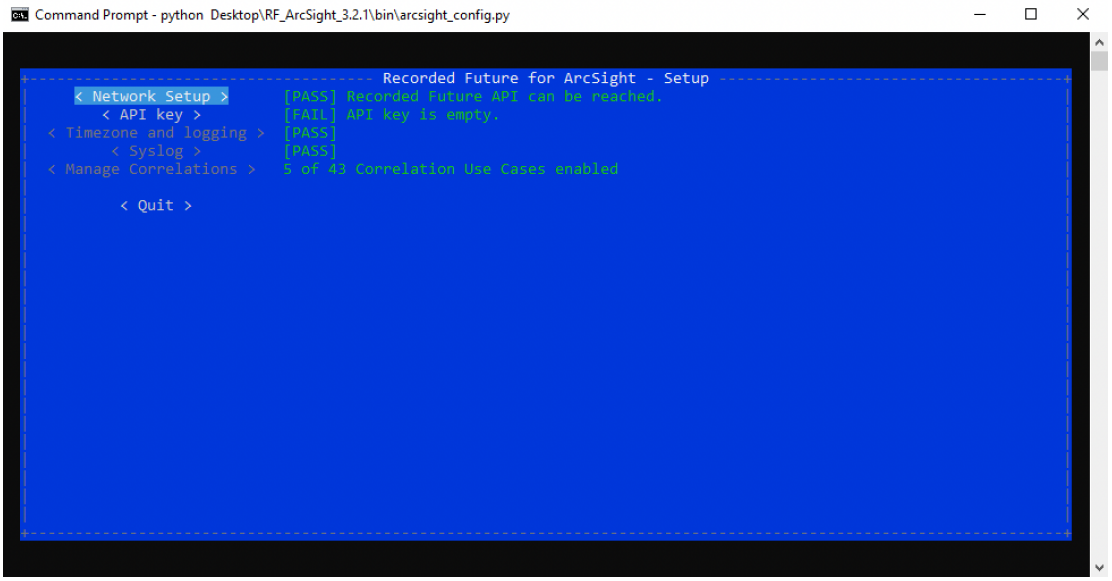
1. Start the configuration script as described in the setup instructions.



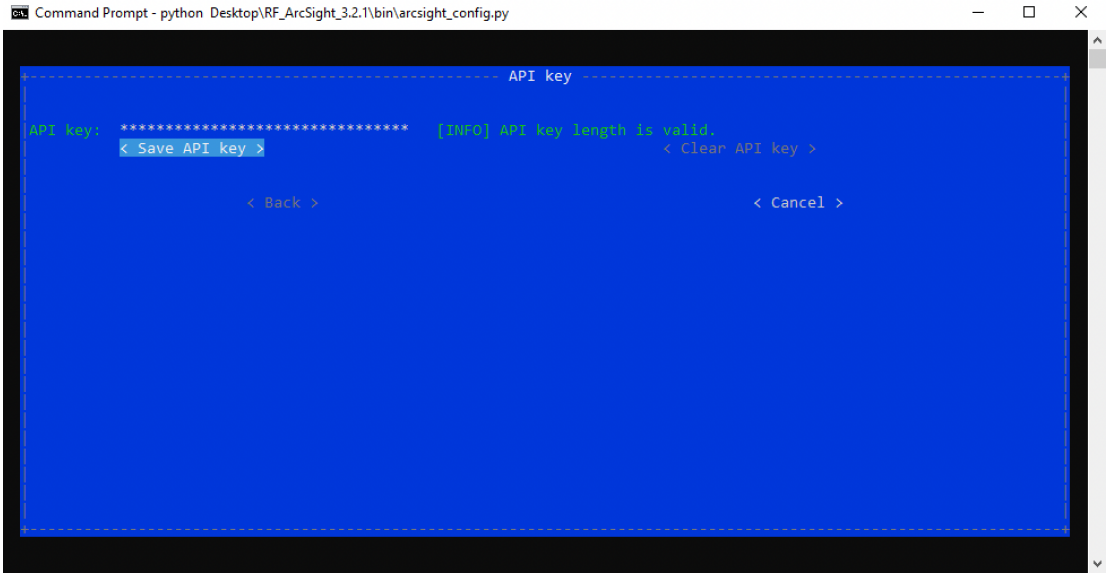
2. The script will verify whether the Recorded Future API is reachable or not. If not, select “Network Setup” and configure a proxy.



3. Once any setup for the network has been completed, the API key must be configured. Select “API key”.

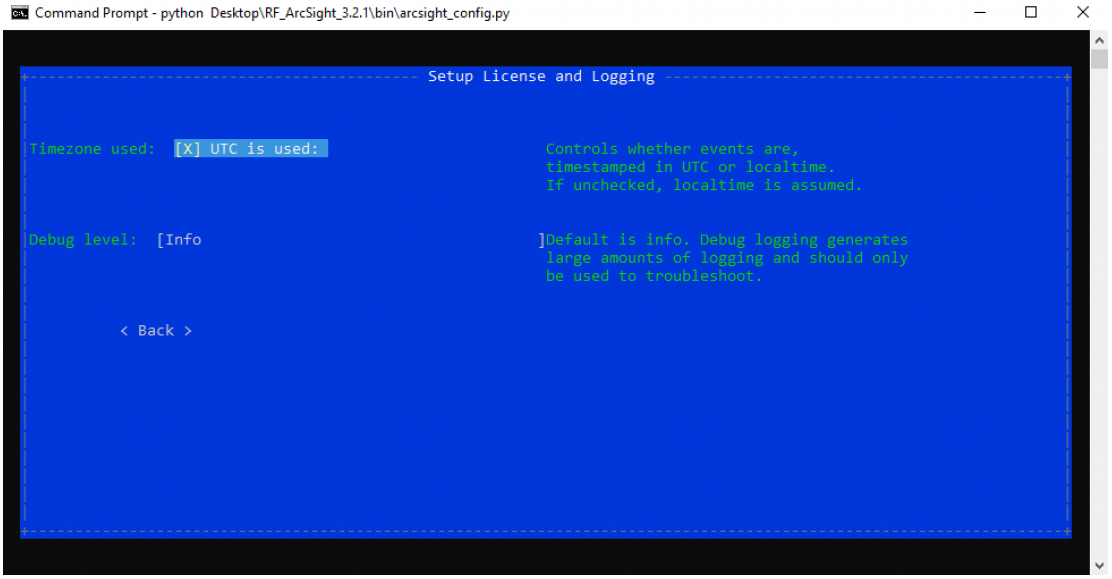


4. Enter your API key (aka token) and click “Save”.

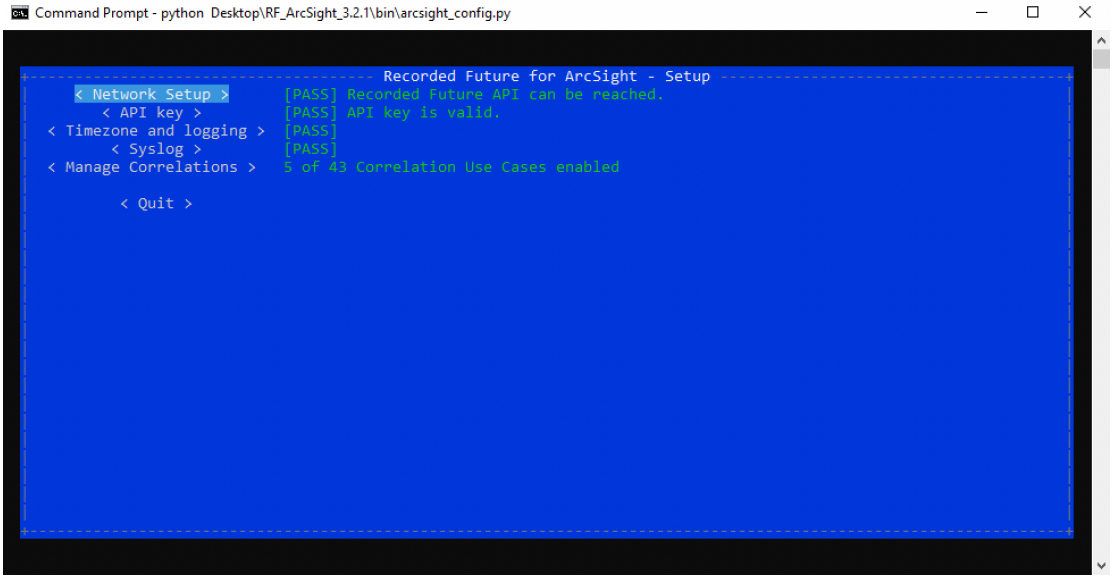


5. Once the API key has been validated, the “Back” button will available. Go back to the main view.
6. By default the integration will assume that the ArcSight integration is using UTC for events. If this is not the case, or if the log level of the ArcSight integration needs to be adjusted, select “Timezone and logging”.

7. If this is not the case, ie localtime is used, uncheck the UTC box. You may adjust logging if required.

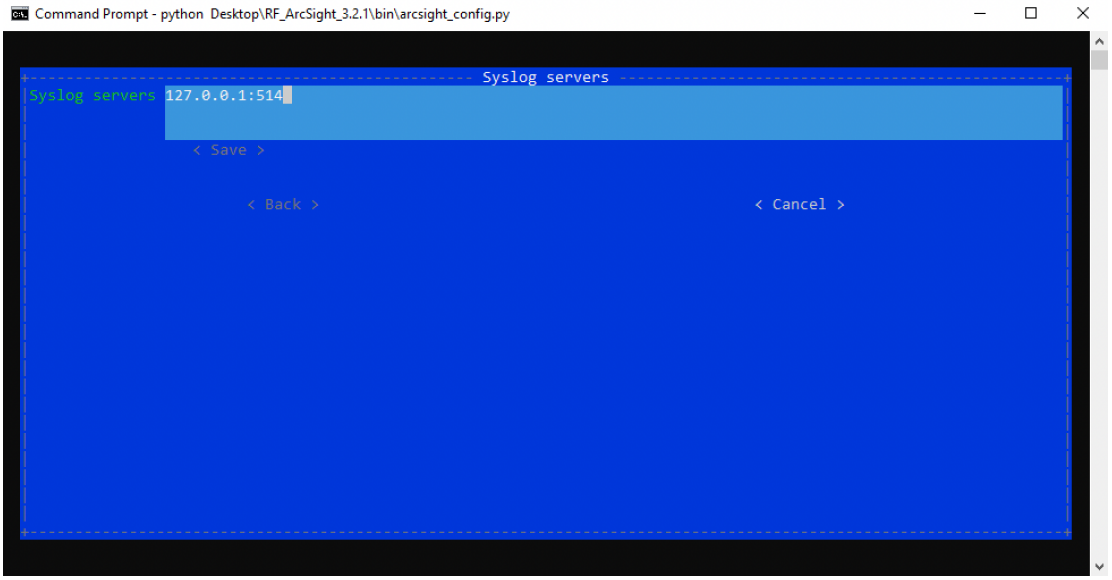


8. The initial setup is now done.



9. The integration transmits the contents of the Risk Lists as events to the ArcSight using the Syslog protocol. A syslog agent must have been configured for the ArcSight system.

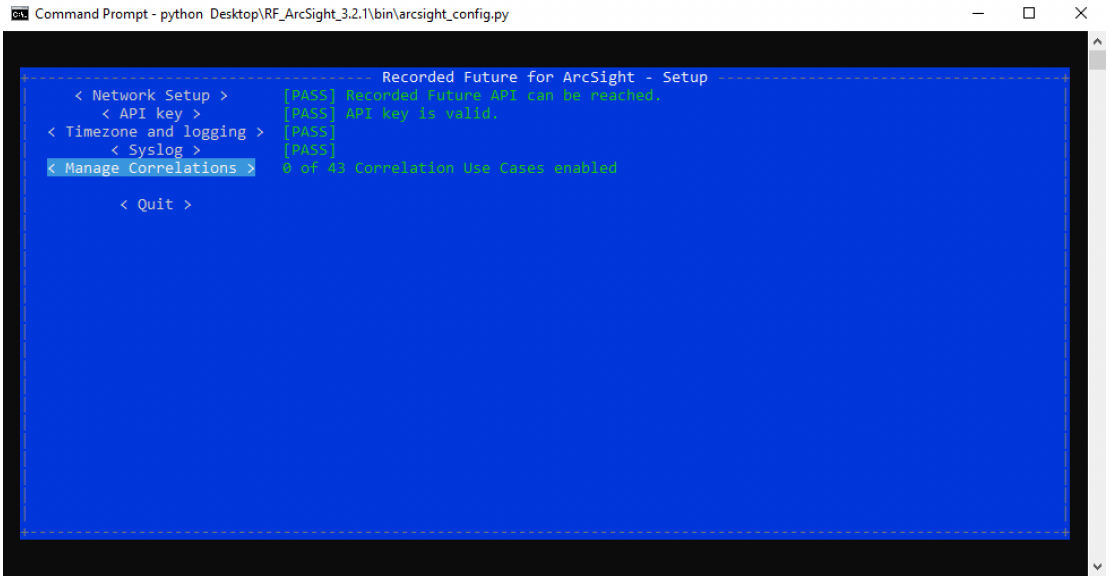
   If the integration is installed on the same host as the ArcSight system and this has been configured with an agent listening on the default port, no further action is required.



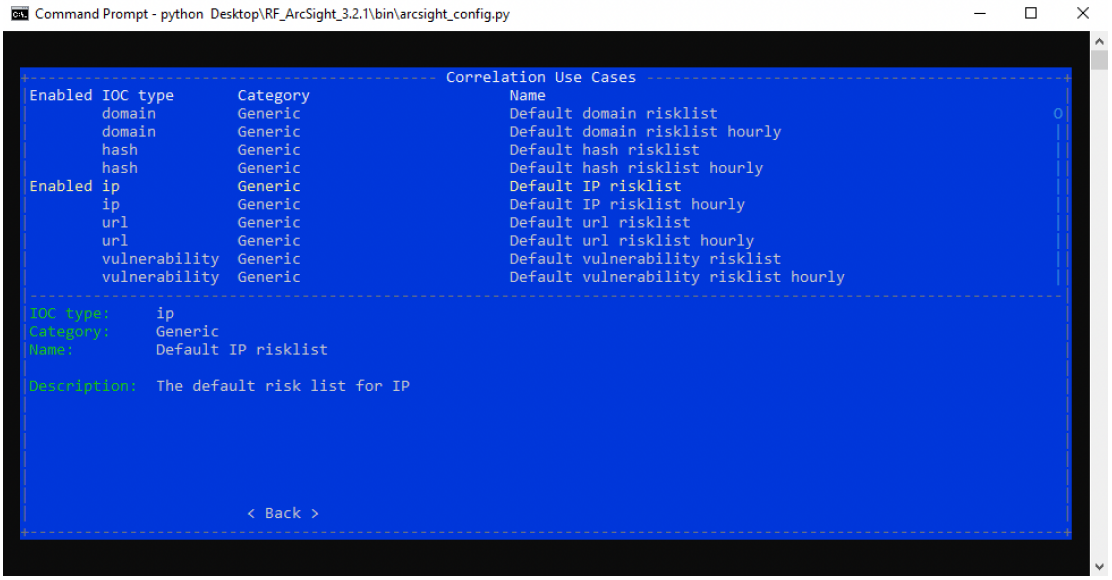
The default configuration will work.

If the integration is installed on a different host from the ArcSight system, the Syslog servers section must be updated. Multiple Syslog endpoints may be configurer. For each endpoint, add a line with IP name/number : Port number (ex localhost:514).

10. Add Correlation use cases is the next step. Select “Manage Correlations”:



11. Find the Correlation Use case that will be added. Details about the use case is shown below the list. Use the tab key to focus the Add button and use that to add the Correlation Use case. Repeat as needed.



Enable a use case using up and down arrows until it is highlighted, toggle between enabled or not by pressing the return key.

Configuration file

The configuration file is in standard config-file format. It is divided into a number of sections. See doc/arcsight.conf-example.

[default]	
rf_api_token	The Recorded Future API key
`utc_time`	If the timestamp should be in UTC or local time. Defaults to true.
`log_level`	Set the log level for the script that fetches the Correlation Use cases. Default is info.
[network]	
proxy	[Optional] Proxy information if traffic to https://api.recordedfuture.com/ must go through a proxy. Ex: http://proxy.example.com:8080
`verify_ssl`	[Optional] Toggles SSL verification (true/false). Defaults to true.
`api_url`	[Optional] Indicate a non-standard URL for the Recorded Future API. Only change if instructed to do so by Recorded Future support.
[syslog]	

host:port,host:port	Comma separated list of the IP or FQDN of one or more ArcSight Syslog Connectors. Typically localhost and port 514. If no port is specified, 514 will be used by default.
[(ip|domain|hash|vulnerability):usecase_id] (optional)	
enabled	Indicates whether the list is enabled or not (true/false).

* Attributes in bold are required.

Security considerations

The scripts in the bin directory can be run as any user. This user however needs write access to the lib- and log directories. No other write access is needed.

Update frequency

The cron pattern above makes the server run the script responsible for updating the risk lists every 5 minutes. The script only updates a list if there is an updated version on the Recorded Future API.

Usage

The integration module provides two functions to the ArcSight ESM:

1. A number of Active Lists intended to be used to correlate events:
    a. The IP risk list
    b. The Domain risk list
    c. The Hash risk list
    d. The Vulnerability risk list
    e. The URL risk list
2. Integration commands for the ESM console. When examining an event in an Active Channel, right clicking and selecting Integration Commands will provide access to Recorded Future's drill down commands for various columns (ex Source Address, Destination Dns Domain etc). Launching one of these commands will open a web page with the corresponding information card in Recorded Future's web service.

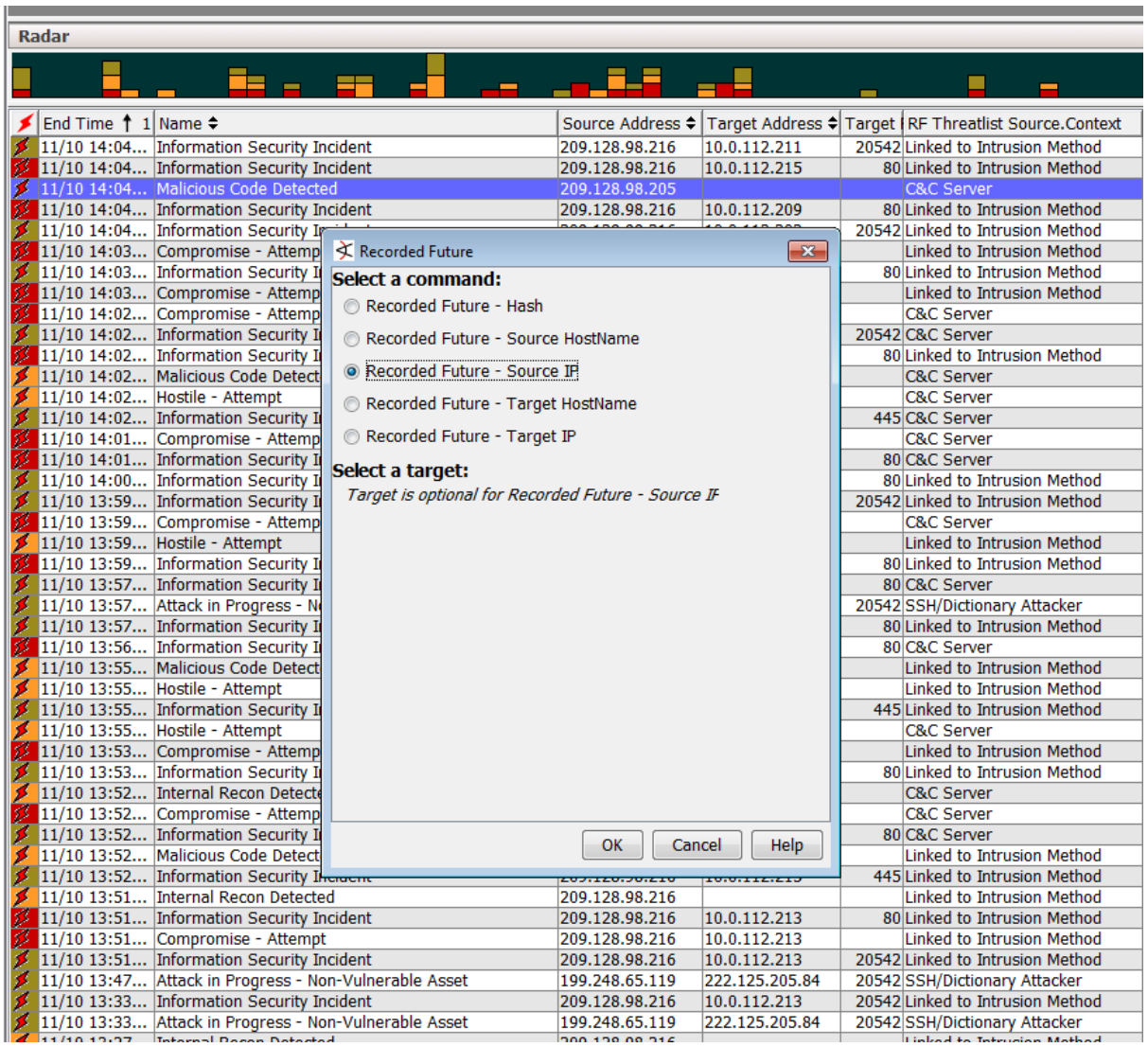


Figure 1: Integration Command Example

Appendix

Contents of package.zip

File List from “package.zip”:

Name	Description
rf/bin: executables	
`arcsight_uc1`	Script that will fetch the Risk Lists corresponding to the configured Correlation Use cases. The contents of the risk lists will be transmitted to the ArcSight system.
`arcsight_config.py`	Script that is used to manage setup and configuration of the integration.

rf/conf: configuration files (empty until integration is configured)	
arcsight.conf	Configuration file. This file will be created and managed by the arcsight_config.py script.
Doc: example files	
`arcsight.conf-example`	Example file for arcsight.conf.
lib: data and state files (empty until integration is running)	
etags.conf	This file contains a list of Correlation Use cases and etags. Each etag is used when requesting a Risk List from the API to determine if there is a more recent version of the risk list on the API. If the local system already is up to date, no update is done.
log: log files created by the scripts (empty until integration is running)	
*	Logs from the scripts. Automatic rotation will occur when a file exceeds 10MB. Five generations are kept.
site-python: various helper files	
*	Various python packages supporting the integration.

ArcSight ESM Content

Packaged content built on ESM 6.8c including 43 resources in v3.1.0:

Contents for Package: Recorded Future
Resource Count: 43

Type	Parent URI	Resource	De...
Group	/All Active Lists/	Recorded Future	
Group	/All Active Lists/Recorded Future/	Threat Feed	
Active List	/All Active Lists/Recorded Future/Threat Feed/	RF Domain ThreatList	
Active List	/All Active Lists/Recorded Future/Threat Feed/	RF Hash ThreatList	
Active List	/All Active Lists/Recorded Future/Threat Feed/	RF IP ThreatList	
Active List	/All Active Lists/Recorded Future/Threat Feed/	RF Vulnerability ThreatList	
Group	/All Field Sets/	Recorded Future	
Field Set	/All Field Sets/Recorded Future/	UC1 RF Enrichment View	
Group	/All Fields/	Recorded Future	
Group	/All Fields/Recorded Future/	UC1	
Field	/All Fields/Recorded Future/UC1/	RF Enrichment of Destination Dns D...	
Field	/All Fields/Recorded Future/UC1/	RF Enrichment of Destination Host	
Field	/All Fields/Recorded Future/UC1/	RF Enrichment of Destination IP	
Field	/All Fields/Recorded Future/UC1/	RF Enrichment of Hash	
Field	/All Fields/Recorded Future/UC1/	RF Enrichment of Source Dns Domain	
Field	/All Fields/Recorded Future/UC1/	RF Enrichment of Source Host	
Field	/All Fields/Recorded Future/UC1/	RF Enrichment of Source IP	
Group	/All Filters/	Recorded Future	
Filter	/All Filters/Recorded Future/	RF UC1 Base Domain Events	
Filter	/All Filters/Recorded Future/	RF UC1 Base Hash Events	
Filter	/All Filters/Recorded Future/	RF UC1 Base IP Events	
Filter	/All Filters/Recorded Future/	RF UC1 Base Vulnerability Events	
Group	/All Integration Commands/	Recorded Future	
Integration Command	/All Integration Commands/Recorded Future/	Recorded Future - Destination DNS...	
Integration Command	/All Integration Commands/Recorded Future/	Recorded Future - Destination Host...	
Integration Command	/All Integration Commands/Recorded Future/	Recorded Future - Destination IP	
Integration Command	/All Integration Commands/Recorded Future/	Recorded Future - Hash	
Integration Command	/All Integration Commands/Recorded Future/	Recorded Future - Source Dns Dom...	
Integration Command	/All Integration Commands/Recorded Future/	Recorded Future - Source Host Name	
Integration Command	/All Integration Commands/Recorded Future/	Recorded Future - Source IP	
Group	/All Integration Configurations/	Recorded Future	
Integration Configuration	/All Integration Configurations/Recorded Future/	Recorded Future	
Package	/All Packages/Recorded Future/	Recorded Future	
Group	/All Rules/Real-time Rules/	Recorded Future	
Group	/All Rules/Recorded Future/	UC1 (Context)	
Rule	/All Rules/Recorded Future/UC1 (Context)/	Add to RF Domain ThreatList	
Rule	/All Rules/Recorded Future/UC1 (Context)/	Add to RF Hash ThreatList	
Rule	/All Rules/Recorded Future/UC1 (Context)/	Add to RF IP ThreatList	
Rule	/All Rules/Recorded Future/UC1 (Context)/	Add to RF Vulnerability ThreatList	

Recorded Future CEF Events

Events are generated in ArcSight "Common Event Format" and sent via syslog to an already installed Syslog SmartConnector.

Example raw CEF events to update the IP risk list:

```
<29>Nov 11 17:26:14 127.0.0.1 CEF:0|Recorded Future|Threat Intel|3.2.1|Ip
IOC|Threat Intel Data|3|src=5.225.184.153 cs1Label=Rule cs1=Recent
Positive Malware Verdict cs2Label=Score cs2=65
```

Example of raw CEF event to update the Domain risk list:

```
<29>Nov 11 17:26:14 CEF:0|Recorded Future|Threat Intel|3.2.1|Domain
IOC|Threat Intel Data|3|destinationDnsDomain=cicero-dropbox.tk
cs1Label=Rule cs1=C&C DNS Name cs2Label=Score cs2=90 cs3Label=Domain
cs3=cicero-dropbox.tk
```

Example of raw CEF event to update the Hash risk list:

```
<29>Nov 11 17:26:14 CEF:0|Recorded Future|Threat Intel|3.2.1|Hash
IOC|Threat Intel
Data|3|fileHash=5b408cc95eace6dbe0dbe647252157930f459ec0243b3525bce37fe0bb
496ebb cs1Label=Rule cs1=Positive Malware Verdict cs2Label=Score cs2=70
cs3Label=Algorithm cs3=SHA-256
```

Example of raw CEF event to update the Vulnerability risk list:

```
<29>Nov 11 17:26:14 CEF:0|Recorded Future|Threat Intel|3.2.1|Vulnerability
IOC|Threat Intel Data|3|msg=CVE-2017-8671 cs1Label=Rule cs1=NIST Severity:
High cs2Label=Score cs2=65 cs3Label=Vulnerability cs3=CVE-2017-8671
```