The upcoming weeks i will be releasing a lot of new things to help people use and understand the API's available for ArcSight ESM and ArcSight Logger, after that i would like to create some new custom functionality and scripts that the community can enjoy, the only issue is that it would not really be efficient to create something that no one would want to use.

Please let me know if there is any custom work that you would love to see when it comes to interaction with these two products. All will be released on github in case people would like to make their own changes and tweaks, together with proper documentation and commented code for learning purposes.

Any type of request is appreciated, and the only requirement is that it is not related to a product that is behind a license wall as i would not be able to test it or access API documentation to the product.

A few examples of requests that i can think off:

1. Slack or messaging notifications. Being able to create a rule action that notifies your slack channel when an alert happens.

2. Open Source threat intelligence framework, scripts that retrieve threat intelligence sources from a large amount of open source feeds, being able to choose which ones you want to use, and feeding it to ESM through a syslog connector.

3. Logger interaction script. Something that you can manually run to for example return the results of a query in CLI. Could also be scheduled to create scheduled exports of certain queries.

**UPDATE:**

First version of Request Tracker integration with ESM has been released:

<https://community.softwaregrp.com/t5/ArcSight-User-Discussions/Unofficial-ESM-Request-Tracker-RT-Ticketing-Integration-released/td-p/1672538>

First version of the ArcSight Logger API documentation examples:

<https://community.softwaregrp.com/t5/ArcSight-User-Discussions/Unofficial-API-documentation-and-examples-Part-1-3-ArcSight/td-p/1674083>

Unofficial RT Ticketing Integration for ArcSight ESM released

*[Marius2](https://community.microfocus.com/members/marius2)*

[**Marius2**](https://community.microfocus.com/members/marius2)[*over 4 years ago*](https://community.microfocus.com/cyberres/arcsight/f/arcsight-discussions/171120/unofficial-rt-ticketing-integration-for-arcsight-esm-released)

Even though freetime wasn't exactly on my side the last few weeks, i managed to compile the initial version of the ESM integration with Request Tracker.

As a part of the ongoing community integrations, where the community can request certain integrations to be added to the ESM by other community members, the first version of the RT Ticketing System integration has been released, as requested by

More information about RT can be found [Here](https://bestpractical.com/request-tracker/).

The initial release comes with functionality to automatic create tickets in RT based on rule actions or manual integration commands in the ESM Console, and documentation on how to install and configure it.

It also supports mapping any information from the correlated event to the ticket created through the basic but easy to use template system.

It has now undergone testing, and following the documentation will now get you from start to finish without issues.

As an initial release, it also means that while all functionality might be in place, there is always room for improvements, some of them would be:

* Adding new events to existing tickets (Almost done)
* Proper logging and configurable logging directory.
* Better templating, or support for multiple template files.
* Better error checking on API requests.
* Debug mode.
* Better README format, better explanations and proof reading.

If you want to try it out, but do not have a RT test environment, a complete finished RT image exists for docker here (which is what i used while developing the integration, so it works just fine!):

<https://hub.docker.com/r/netsandbox/request-tracker/>

If there is any questions, issues, feedback or anything else, do not hesitate to post it either here, or in a github issue for the project. Contributions through PR's are always welcome as well!

The files and documentation can be found at the current location:

<https://github.com/arcsight-unofficial/arcsight-esm-requesttracker>

PS: All new and cool integrations will also be released on the arcsight-unofficial github, so follow it to keep yourself up 2 date! Anything i upload there will also be posted here in this community.

# Unofficial API documentation and examples Part 1/3 - ArcSight Logger API

*[Marius2](https://community.microfocus.com/members/marius2)*

[**Marius2**](https://community.microfocus.com/members/marius2)[*over 4 years ago*](https://community.microfocus.com/cyberres/arcsight/f/arcsight-discussions/171260/unofficial-api-documentation-and-examples-part-1-3---arcsight-logger-api)

It tok some time, but the initial first part is now finalized. I spent some extra time changing up the stylings and making sure that all examples are working correctly, so that i can reuse them in the ESM version.

This is released in 2 projects, and all installation and usage documentation is located on each link:

**Local API documentation:**

This is a local webservice or just static html files that can be used to navigate all different API endpoints available on the ArcSight Logger, including examples in certain programming languages.

URL: <https://github.com/arcsight-unofficial/arcsight-logger-api-documentation>

**Postman API examples collection:**

A collection of API examples using Postman <https://www.getpostman.com/>

This collection enables you to easily interact with the Logger API to test against your own environments without having to do any programming or scripting beforehand.

URL <https://github.com/arcsight-unofficial/arcsight-logger-api-examples>

Hoping to get some nice feedback on this, and feel free to also send in any PR requests or fill out a github issue if you notice something wrong.