IBM Resilient

resilient

Incident Response Platform Integrations

McAfee ESM Functions and Case Polling Integration V1.0.0

Release Date: October 2018

Resilient Functions simplify development of integrations by wrapping each activity into an individual workflow component. These components can be easily installed, then used and combined in Resilient workflows. The Resilient platform sends data to the function component that performs an activity then returns the results to the workflow. The results can be acted upon by scripts, rules, and workflow decision points to dynamically orchestrate the security incident response activities.

This guide describes the McAfee ESM Functions and the ESM Case Polling Integration.

Overview

The McAfee ESM functions contain the ability to call multiple API endpoints within ESM, while the Case Polling Integration allows for creation of new incidents in the Resilient platform.

This document describes the McAfee ESM functions, its customization options, and how to configure them in custom workflows. Please note the functions and integrations will only work with an ESM version of 10 or higher.

Installation

Before installing, verify that your environment meets the following prerequisites:

- Resilient platform is version 30 or later.
- McAfee ESM version 10 or later.
- You have a Resilient account to use for the integrations. This can be any account that has the permission to view and modify administrator and customization settings, and read and update incidents. You need to know the account username and password.
- You have access to the command line of the Resilient appliance, which hosts the Resilient platform; or to a separate integration server where you will deploy and run the functions code. If using a separate integration server, you must install Python version 2.7.10 or later, or version 3.6 or later, and “pip”. (The Resilient appliance is preconfigured with a suitable version of Python).

Install the Python components

The functions package contains Python components that will be called by the Resilient platform to execute the functions during your workflows. These components run in the ‘resilient-circuits’ integration framework.

The package also includes Resilient customizations that will be imported into the platform later.

Ensure that the environment is up to date:

```
sudo pip install --upgrade pip
sudo pip install --upgrade setuptools
sudo pip install --upgrade resilient-circuits
```

To install the package:

```
sudo pip install --upgrade fn_mcafee_esm-<1.0.0>.tar.gz
```

Configure the Python components

The ‘resilient-circuits’ components run as an unprivileged user, typically named `integration`. If you do not already have an `integration` user configured on your appliance, create it now.

Perform the following to configure and run the integration:

1. Using ‘sudo’, become the integration user.

   ```
   sudo su - integration
   ```

2. Create or update the resilient-circuits configuration file.

   ```
   resilient-circuits config -c
   ```

   or

   ```
   resilient-circuits config -u
   ```

3. Edit the resilient-circuits configuration file.

   a. In the [resilient] section, ensure that you provide all the information needed to connect to the Resilient platform.

   b. In the [fn_mcafee_esm] section, edit the settings as follows:

   ```
   esm_url=<your_esm_server>
   esm_username=<your_esm_username>
   esm_password=<your_esm_password>
   verify_cert=[True|False]
   esm_polling_interval=0
   incident_template=<location_of_template_file>
   ```

   Use false for self-signed SSL certificates.

Deploy customizations to the Resilient platform

The package contains the function definition that you can use in workflows, and an example workflow and rule that show how to use the function.

Install these customizations to the Resilient platform with the following command:

```
resilient-circuits customize
```

Answer the prompts to deploy the function, message destination, workflow and rule. The following data will be imported.

```
Function inputs: mcafee_esm_alarm_triggered_end_time,
mcafee_esm_alarm_triggered_start_time,
mcafee_esm_alarm_triggered_time_range, mcafee_esm_case_id,
mcafee_esm_edit_case_json, mcafee_esm_qry_config,
mcafee_esm_qry_event_type, mcafee_event_id_list
Message Destination: McAfee ESM Message Destination
Functions: mcafee_esm_edit_case, mcafee_esm_get_case_detail,
mcafee_esm_get_case_events_detail, mcafee_esm_get_list_of_cases,
mcafee_esm_get_triggered_alarms, mcafee_esm_query
Workflows: McAfee ESM Close Case, Mcafee ESM Get Case Details, McAfee ESM
Get Case Events Detail, McAfee ESM Get Case List, McAfee ESM Get Triggered
Alarms, McAfee ESM Query
Rules: Close McAfee ESM Case, McAfee ESM Get Case Details, McAfee ESM Get
Case Events Detail, McAfee ESM Get Case List, McAfee ESM Get Triggered
Alarms, Run McAfee ESM Query
```

Run the integration framework

Run the integration manually with the following command:

```
resilient-circuits run
```

The resilient-circuits command starts, loads its components, and continues to run until interrupted. If it stops immediately with an error message, check your configuration values and retry. The following shows a successful connection to the Resilient platform and loading of components.

```
2018-04-10 12:05:09,686 INFO [app] Resilient server: 9.108.163.130
2018-04-10 12:05:09,687 INFO [app] Resilient org: TestOrg
2018-04-10 12:05:09,687 INFO [app] Logging Level: INFO
2018-04-10 12:05:09,688 WARNING [co3] Unverified HTTPS requests
(cafile=false).
2018-04-10 12:05:10,142 INFO [app] Components auto-load directory: (none)
2018-04-10 12:05:10,306 INFO [component_loader] Loading 7 components
2018-04-10 12:05:10,307 INFO [component_loader]
'fn_mcafee_esm.components.mcafee_esm_get_case_detail.FunctionComponent'
loading
```

```
2018-04-10 12:05:10,307 INFO [component_loader]
'fn_mcafee_esm.components.mcafee_esm_get_list_of_cases.FunctionComponent'
loading

2018-04-10 12:05:10,307 INFO [component_loader]
'fn_mcafee_esm.components.mcafee_esm_get_case_events_detail.FunctionCompon
ent' loading

2018-04-10 12:05:10,307 INFO [component_loader]
'fn_mcafee_esm.components.mcafee_esm_edit_case.FunctionComponent' loading

2018-04-10 12:05:10,307 INFO [component_loader]
'fn_mcafee_esm.components.mcafee_esm_get_get_triggered_alarms.FunctionComp
onent' loading

2018-04-10 12:05:10,307 INFO [component_loader]
'fn_mcafee_esm.components.mcafee_esm_query.FunctionComponent' loading

2018-04-10 12:05:10,307 INFO [component_loader]
'fn_mcafee_esm.components.mcafee_esm_case_polling.ESM_CasePolling loading

2018-04-10 12:05:10,308 WARNING [actions_component] Unverified STOMP TLS
certificate (cafile=false)
2018-04-10 12:05:10,309 INFO [stomp_component] Connect to
9.108.163.130:65001
2018-04-10 12:05:10,310 INFO [actions_component]
'fn_mcafee_esm.components.mcafee_esm_get_case_detail.FunctionComponent'
function 'mcafee_esm_get_case_detail' registered to
'mcafee_esm_message_destination'
2018-04-10 12:05:10,310 INFO [actions_component]
'fn_mcafee_esm.components.mcafee_esm_get_list_of_cases.FunctionComponent'
function 'mcafee__esm_get_list_of_cases' registered to
'mcafee_esm_message_destination'
2018-04-10 12:05:10,310 INFO [actions_component]
'fn_mcafee_esm.components.mcafee_esm_get_case_events_detail.FunctionCompon
ent' function 'mcafee_esm_get_case_evenets_detail' registered to
'mcafee_esm_message_destination'
2018-04-10 12:05:10,310 INFO [actions_component]
'fn_mcafee_esm.components.mcafee_esm_edit_case.FunctionComponent' function
'mcafee_esm_edit_case' registered to 'mcafee_esm_message_destination'
2018-04-10 12:05:10,310 INFO [actions_component]
'fn_mcafee_esm.components.mcafee_esm_get_triggered_alarms.FunctionComponen
t' function 'mcafee_esm_get_triggered_alarms' registered to
'mcafee_esm_message_destination'
2018-04-10 12:05:10,310 INFO [actions_component]
'fn_mcafee_esm.components.mcafee_esm_query.FunctionComponent' function
'mcafee_esm_query' registered to 'mcafee_esm_message_destination'
2018-04-10 12:05:10,310 INFO [app] Components loaded
2018-04-10 12:05:10,312 INFO [app] App Started
2018-04-10 12:05:10,414 INFO [actions_component] STOMP attempting to
connect
2018-04-10 12:05:10,414 INFO [stomp_component] Connect to Stomp...
2018-04-10 12:05:10,437 INFO [client] Connection established
2018-04-10 12:05:10,537 INFO [client] Connected to stomp broker
[session=ID:resilient.localdomain-40775-1523276401752-5:3, version=1.2]
2018-04-10 12:05:10,538 INFO [stomp_component] Connected to
failover:(ssl://9.108.163.130:65001)?maxReconnectAttempts=1,startupMaxReco
nnectAttempts=1
2018-04-10 12:05:10,538 INFO [stomp_component] Client HB: 0  Server HB:
15000
2018-04-10 12:05:10,538 INFO [stomp_component] No Client heartbeats will
be sent
```

```
2018-04-10 12:05:10,538 INFO [stomp_component] Requested heartbeats from
server.
2018-04-10 12:05:10,539 INFO [actions_component] STOMP connected.
[mcafee_esm_case_polling] Polling for cases in ESM is occurring
2018-04-10 12:05:10,641 INFO [actions_component] Subscribe to message
destination 'mcafee_esm_message_destination'
2018-04-10 12:05:10,642 INFO [stomp_component] Subscribe to message
destination actions.<orgID>.mcafee_esm_message_destination
```

Configure Resilient Circuits for restart

For normal operation, resilient-circuits must run continuously. The recommend way to do this is to configure it to automatically run at startup. On a Red Hat appliance, this is done using a systemd unit file such as the one below. You may need to change the paths to your working directory and app.config.

The unit file should be named ‘resilient_circuits.service’:

```
sudo vi /etc/systemd/system/resilient_circuits.service
```

The contents:

```
[Unit]
Description=Resilient-Circuits Service
After=resilient.service
Requires=resilient.service
[Service]
Type=simple
User=integration
WorkingDirectory=/home/integration
ExecStart=/usr/local/bin/resilient-circuits run
Restart=always
TimeoutSec=10
Environment=APP_CONFIG_FILE=/home/integration/.resilient/app.config
Environment=APP_LOCK_FILE=/home/integration/.resilient/resilient_circuits.
lock
[Install]
WantedBy=multi-user.target
```

Ensure that the service unit file is correctly permissioned:

```
sudo chmod 664 /etc/systemd/system/resilient_circuits.service
```

Use the systemctl command to manually start, stop, restart and return status on the service:

```
sudo systemctl resilient_circuits [start|stop|restart|status]
```

Log files for systemd and the resilient-circuits service can be viewed through the journalctl command:

```
sudo journalctl -u resilient_circuits --since "2 hours ago"
```

Case Polling Description

When loaded and set to poll, the case polling integration spawns a new thread to handle all the polling and creation of incidents. For this to happen, set `esm_polling_interval` to a positive integer within the app.config file. This will enable ESM polling and set the polling interval in seconds, to disable polling set this to an integer less than 1. Setting `incident_template` can be set to the location of a jinja template used to create incident data, if this is not set, the integration will default to using the default packaged template

When the component is loaded and `esm_polling_interval` is a positive integer, a new thread is created. This thread reaches out to the ESM server and, using the `caseGetCaseList` endpoint, returns a list of cases that are open and assigned to the logged-in ESM user. From here, this list is cross-referenced with active incidents within the Resilient platform. If the case already exists as an active incident in the Resilient platform, it moves on to the next case; otherwise, a new incident is created in the Resilient platform based on the case data from the `caseGetCaseDetail` endpoint.

When the incident is created, the McAfee ESM Case ID custom field is set to the ID of the case in ESM to ensure the connection between cases and incidents.

The incident template file can be edited to meet custom needs. The suggested way of accomplishing this is copying the default template that comes with the integration to a new directory and editing it from there. This template can be found at:

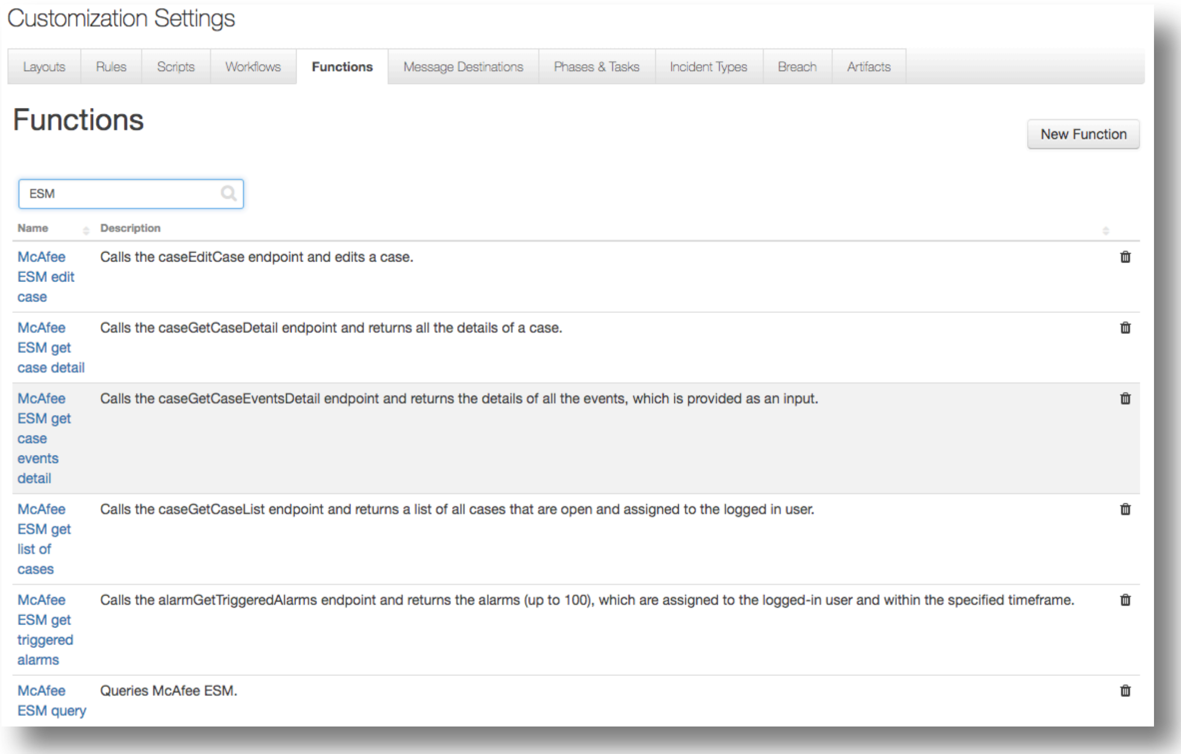
```
<python_env>/lib/<python_version>/site-packages/fn_mcafee_esm/data/templates/
```

The template utilizes jinja. The documentation can be found at http://jinja.pocoo.org/docs/2.10/. Once the custom template is finished, set its location in the config file at:

```
incident_template=<location_of_template>
```

Function Descriptions

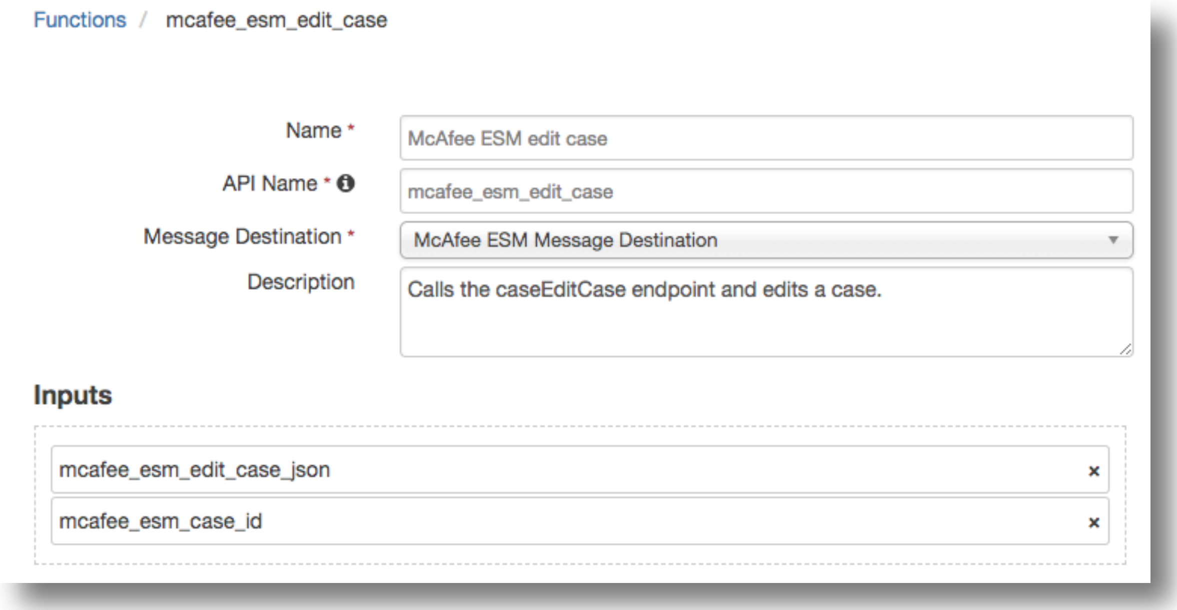
Once the function package deploys the functions, you can view them in the Resilient platform Functions tab, as shown below. The package also includes example workflows that show how the function can be used. You can copy and modify these workflows and rules for your own needs.



Name	Description
McAfee ESM edit case	Calls the caseEditCase endpoint and edits a case.
McAfee ESM get case detail	Calls the caseGetCaseDetail endpoint and returns all the details of a case.
McAfee ESM get case events detail	Calls the caseGetCaseEventsDetail endpoint and returns the details of all the events, which is provided as an input.
McAfee ESM get list of cases	Calls the caseGetCaseList endpoint and returns a list of all cases that are open and assigned to the logged in user.
McAfee ESM get triggered alarms	Calls the alarmGetTriggeredAlarms endpoint and returns the alarms (up to 100), which are assigned to the logged-in user and within the specified timeframe.
McAfee ESM query	Queries McAfee ESM.

McAfee ESM Edit Case

The McAfee ESM Edit Case Function calls the `caseEditCase` ESM endpoint. This enables the function to edit any incident. The function accepts two inputs, `mcafee_esm_case_id`, which is the numeric ID of the case in ESM, and `mcafee_esm_edit_case_json` which is a JSON string that is used to edit the case. The `mcafee_esm_edit_case_json` is a text with value input type and comes with a few example input JSON strings.



Functions / mcafee_esm_edit_case

Name * McAfee ESM edit case

API Name * mcafee_esm_edit_case

Message Destination * McAfee ESM Message Destination

Description Calls the caseEditCase endpoint and edits a case.

Inputs

mcafee_esm_edit_case_json ×

mcafee_esm_case_id ×

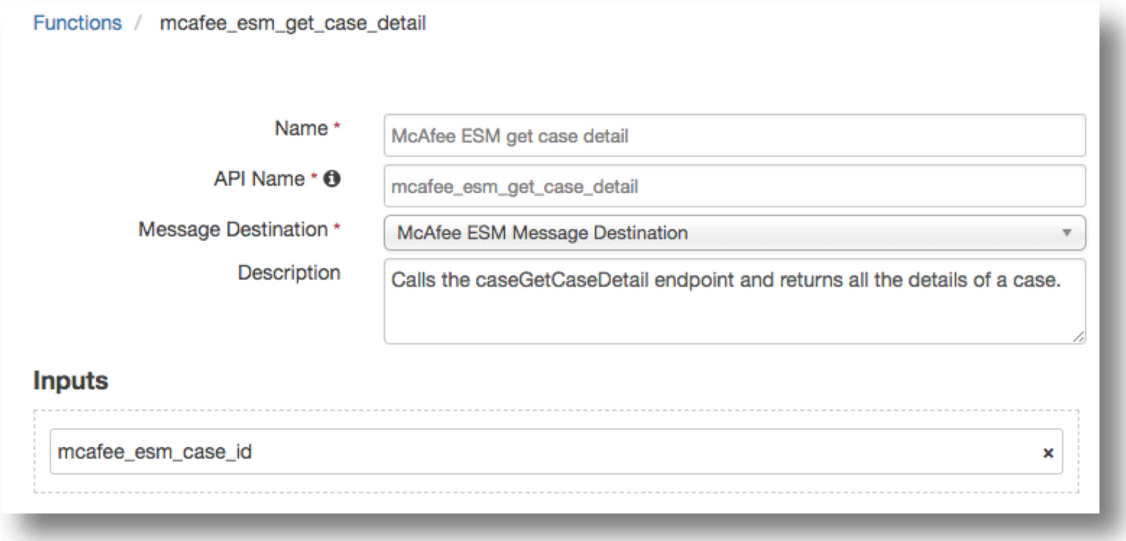
The function calls the `caseGetCaseDetail` endpoint in ESM and then combines the results from that call with the string in the `mcafee_esm_edit_case_json` input. The resulting combination is used as the JSON post data for editing the case..

The default workflow for this function closes the case in ESM when the case is closed in the Resilient platform.

McAfee ESM Get Case Detail

The McAfee ESM Get Case Detail Function calls the `caseGetCaseDetail` endpoint in ESM and returns all the information on that specific case. The function takes one input, mcafee_esm_case_id, which is the numeric ID of the case represented in ESM.

The default workflow adds a note to the incident that provides additional details about the case in ESM.



Name * McAfee ESM get case detail

API Name * mcafee_esm_get_case_detail

Message Destination * McAfee ESM Message Destination

Description Calls the caseGetCaseDetail endpoint and returns all the details of a case.

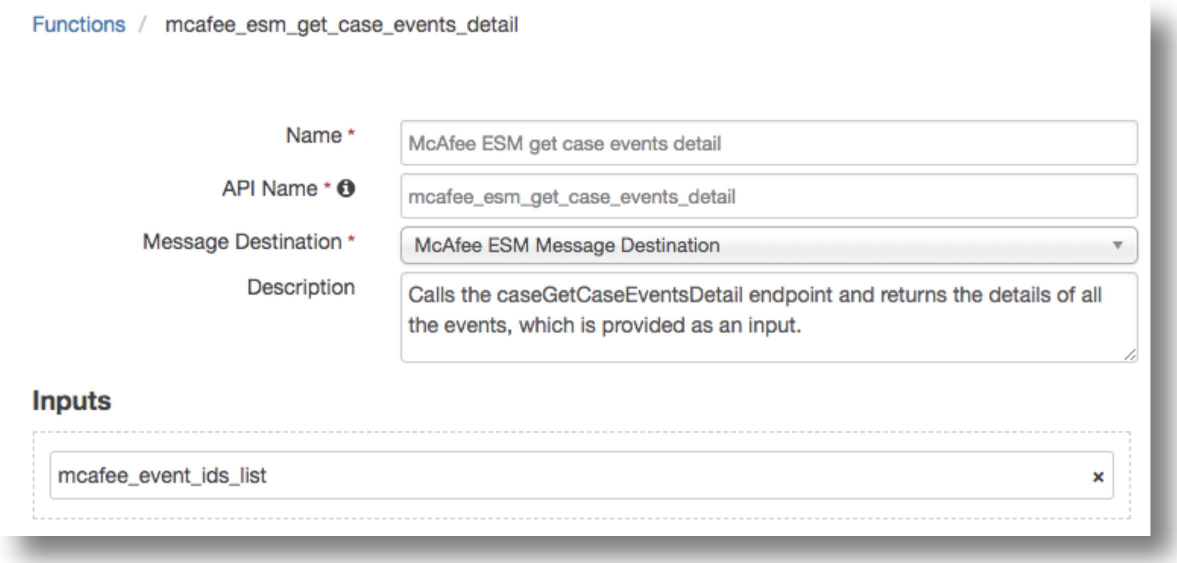
Inputs

mcafee_esm_case_id ×

McAfee ESM Get Case Events Detail

The McAfee ESM Get Case Events Detail Function calls the `caseGetCaseEventsDetail` ESM endpoint and returns all information about each of the events. This function takes one input, `mcafee_event_eds_list`, which is a string that represents the comma-separated list of event IDs to be passed to the API.

The default workflow for this function has an object type Data Table. When triggered on a row with an event ID in the McAfee ESM Event List Data Table, adds additional details about the event to the data table row.



Name *: McAfee ESM get case events detail

API Name *: mcafee_esm_get_case_events_detail

Message Destination *: McAfee ESM Message Destination

Description: Calls the caseGetCaseEventsDetail endpoint and returns the details of all the events, which is provided as an input.

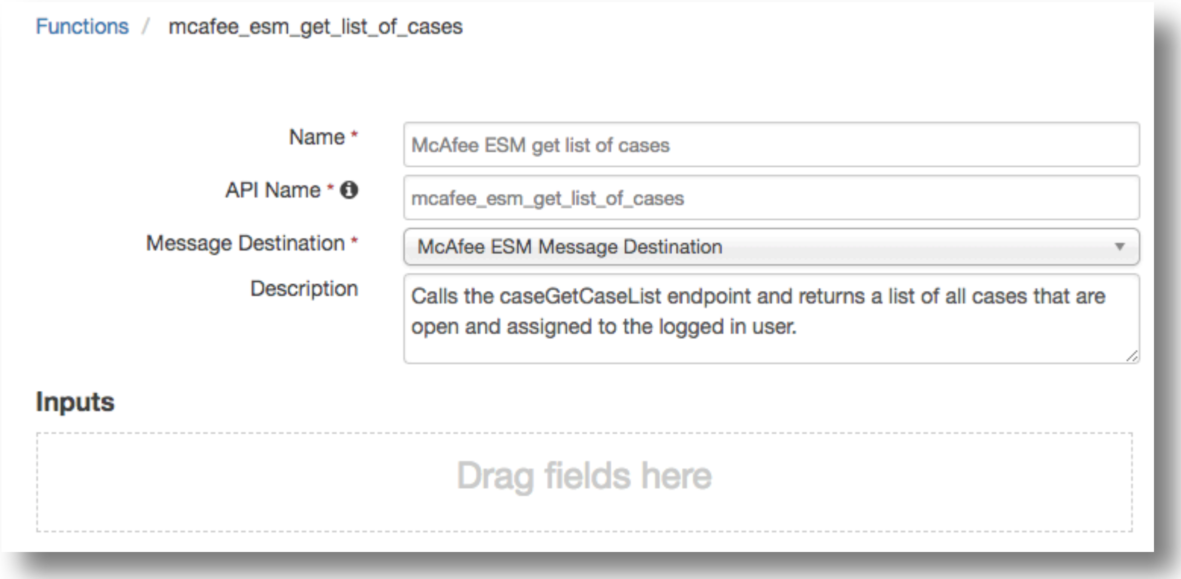
Inputs

mcafee_event_ids_list

McAfee ESM Get List of Cases

The McAfee ESM Get List of Cases Function calls the `caseGetCaseList` endpoint and returns the list of all open cases in ESM that are also assigned to the logged-in ESM user. This function does not take any inputs.

The default workflow for this function adds a note to an incident stating the number of open cases assigned to the logged-in user in ESM, in addition to populating McAfee ESM Event List data table with event IDs.



Functions / mcafee_esm_get_list_of_cases

Name * McAfee ESM get list of cases

API Name * mcafee_esm_get_list_of_cases

Message Destination * McAfee ESM Message Destination

Description Calls the caseGetCaseList endpoint and returns a list of all cases that are open and assigned to the logged in user.

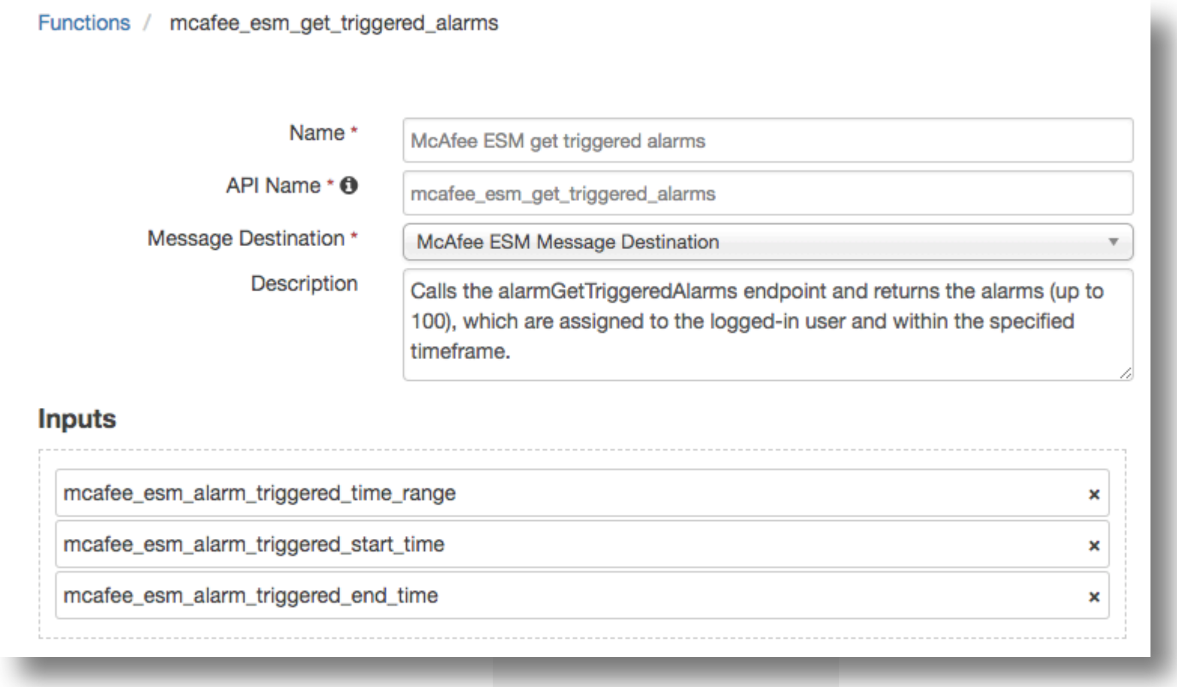
Inputs

McAfee ESM Get Triggered Alarms

The McAfee ESM Get Triggered Alarms Function uses the `alarmGetTriggeredAlarms` ESM endpoint to return up to the last 100 alarms assigned to the logged-in ESM user within the designated time frame. This function accepts three inputs:

- `mcafee_esm_alarm_triggered_time_range` allows for quick and easy decision making when setting the specified time range of when to return the alarms.
- `mcafee_esm_alarm_triggered_start_time` and `mcafee_esm_alarm_triggered_end_time` allows the user to set the designated start and end date/times. These settings override the `mcafee_esm_alarm_triggered_time_range` input. Note the accepted date-time format for ESM API calls is in the following format: `2018-07-18T16:32:42.238Z`.

The default workflow for this function, when triggered, returns alarms assigned to the logged-in ESM user within the last 30 days and populates the McAfee ESM Triggered Alarms data table.



Functions / mcafee_esm_get_triggered_alarms

Name * McAfee ESM get triggered alarms

API Name * mcafee_esm_get_triggered_alarms

Message Destination * McAfee ESM Message Destination

Description Calls the alarmGetTriggeredAlarms endpoint and returns the alarms (up to 100), which are assigned to the logged-in user and within the specified timeframe.

Inputs

mcafee_esm_alarm_triggered_time_range ×

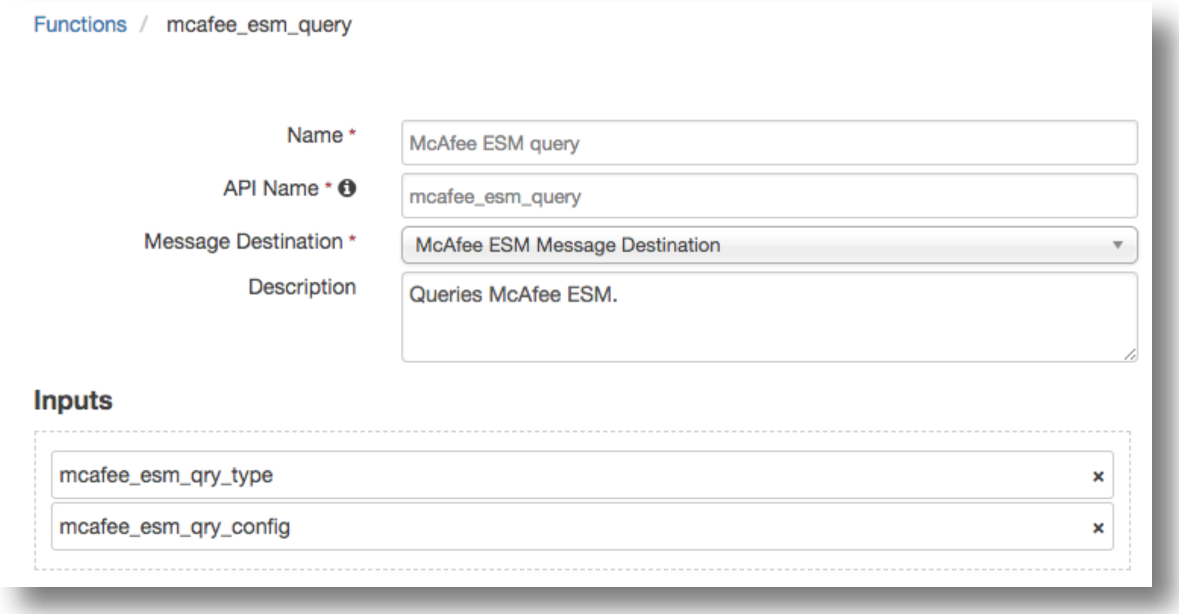
mcafee_esm_alarm_triggered_start_time ×

mcafee_esm_alarm_triggered_end_time ×

McAfee ESM Query

The McAfee ESM Query Function queries ESM based on the inputs and returns the results. This function takes two inputs, `mcafee_esm_qry_type` is a select input used to specify the type of query. The `mcafee_esm_qry_config` is a string input which represents the JSON of the query config.

The default workflow for this function queries ESM for a specific event ID within the last 30 days and returns the number of occurrences as a note to the incident.



Name * McAfee ESM query

API Name * mcafee_esm_query

Message Destination * McAfee ESM Message Destination

Description Queries McAfee ESM.

Inputs

mcafee_esm_qry_type

mcafee_esm_qry_config

Troubleshooting

There are several ways to verify the successful operation of a function.

- Resilient Action Status

  When viewing an incident, use the Actions menu to view Action Status. By default, pending and errors are displayed. Modify the filter for actions to also show Completed actions. Clicking on an action displays additional information on the progress made or what error occurred.

- Resilient Scripting Log

  A separate log file is available to review scripting errors. This is useful when issues occur in the pre-processing or post-processing scripts. The default location for this log file is: `/var/log/resilient-scripting/resilient-scripting.log`.

- Resilient Logs

  By default, Resilient logs are retained at `/usr/share/co3/logs`. The `client.log` may contain additional information regarding the execution of functions.

- Resilient-Circuits

  The log is controlled in the `.resilient/app.config` file under the section `[resilient]` and the property `logdir`. The default file name is `app.log`. Each function will create progress information. Failures will show up as errors and may contain python trace statements.

Support

For additional support, contact support@resilientsystems.com.

Including relevant information from the log files will help us resolve your issue.