



Resilient SOAR Platform Outbound Email Functions Guide V1.0.7

Date: April 2020

Licensed Materials – Property of IBM © Copyright IBM Corp. 2010, 2020. All Rights Reserved. US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Resilient SOAR Platform Outbound Email Functions Guide

Version	Publication	Notes
1.0.7	April 2020	Initial Release after internal development by Professional, no prior release notes
1.0		Initial publication.

Table of Contents

Overview	1
Installation	2
Workflow Description	4
Example: Send Incident Email HTML	4
Example: Send Incident Email Text	5
Function Descriptions	6
Send Email	6
Rules	7
Example: Send Incident Email HTML	7
Example: Send Incident Email Text	8
Troubleshooting	9
Support	10

Overview

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.

The Outbound Email workflow function provides a way of sending email from the Resilient platform.

The Outbound Email integration package provides the following functionality:

- Send a plain text or HTML-formatted email by triggering a Resilient action
- Add incident data to the email body as well as incident attachments to the outgoing email

This document describes the function, workflow, and rule included in the package.

Installation

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

- Your Resilient platform version is 30 or later. If supporting the Resilient for MSSPs multi-organization feature, Resilient platform V33 or later is required.
- A Resilient integration server running Resilient Circuits V30 or later. To setup an integration server, see https://ibm.biz/res-int-server-guide.
- A dedicated Resilient account to use as the API user. This can be any account that has the permission to create incidents, and view and modify administrator and customization settings. You need to know the account username and password.

NOTE: Should you later change the dedicated Resilient account to another user, the new user must also have the permission to edit incidents, in addition to the permission to create incidents and view and modify administrator and customization settings. The edit permission is necessary so that the integration can continue to modify or synchronize the incidents escalated by the original user account.

If supporting the Resilient for MSSP feature, the Resilient account must have permission to access the configuration, global dashboard and all child organizations.

Perform the following procedure to install the Outbound Email package.

- 1. Download the IBM Resilient Outbound Email .zip file from the <u>IBM Security App</u> <u>Exchange</u>.
- 2. Copy the zip file to your Integration Server and SSH into it.
- 3. Unzip the package:

```
unzip fn outbound email-x.x.x.zip
```

4. Change directory into the unzipped directory:

```
cd fn_outbound_email-x.x.x
```

5. Install the package:

```
pip install fn outbound email-x.x.x.tar.gz
```

6. Import the configurations into your file:

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

7. Import the fn_outbound_email customizations into your Resilient platform:

```
resilient-circuits customize -y -l fn-outbound-email
```

8. Open the config file, scroll to the bottom and edit your [fn_outbound_email] configurations:

```
[fn outbound email]
# SMTP SERVER (IP ADDRESS OR FQDN)
smtp server=xxx.xxx.xxx.xxx
smtp user=xxx
smtp password=xxx
# SMTP PORT NUMBER: 25 or 587/2525
smtp_port=25
# SMTP CONNECTION TIMEOUT IN SECONDS
smtp conn timeout=20
# SMTP SSL MODE = (starttls, ssl, None)
smtp ssl mode=None
# SSL Cert
# If your email server uses a self-signed SSL/TLS certificate, or some
# other certificate that is not automatically trusted by your machine,
# specify the file below, e.g. 'path/to/certificate.pem' OR
# set to true if using system cert store OR
# set to false if disabling SSL verification
#smtp ssl cafile=~/path/to/email cert.cer
```

- 9. Save and close the app.config file.
- 10. Optionally, run selftest to test the integration you configured:

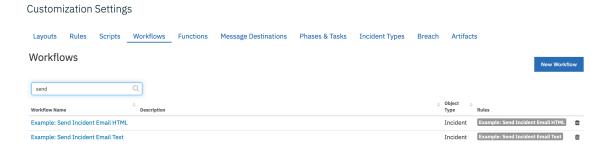
```
resilient-circuits selftest -l fn-outbound-email
```

11. Run Resilient Circuits or restart the service on Linux or Windows.

resilient-circuits run

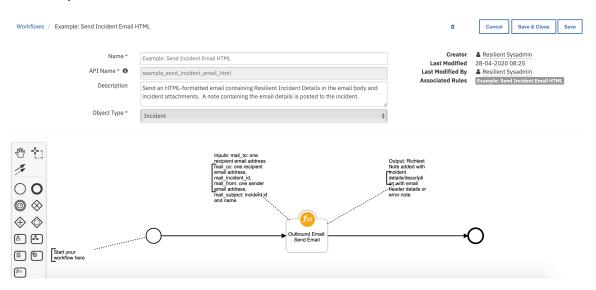
Workflow Description

Once the function package deploys the workflows, you can view them in the Resilient platform Workflow tab, as shown below. The rules are also deployed and may be viewed in the Rules tab.

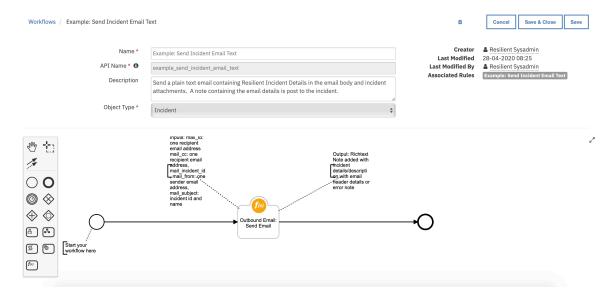


The workflows themselves will be as shown below.

Example: Send Incident Email HTML

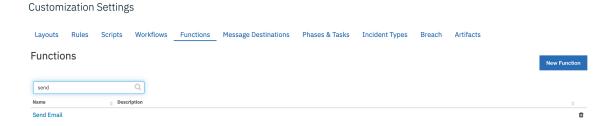


Example: Send Incident Email Text



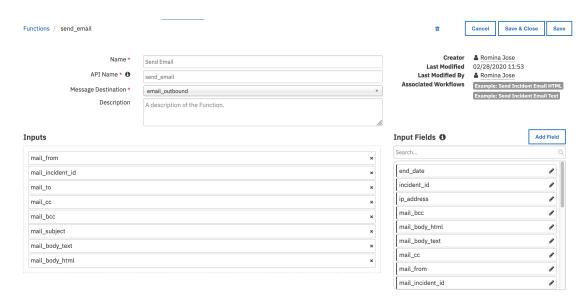
Function Descriptions

Once the function package deploys the function, you can view it in the Resilient platform Functions tab, as shown below.



The function itself will be as shown below.

Send Email



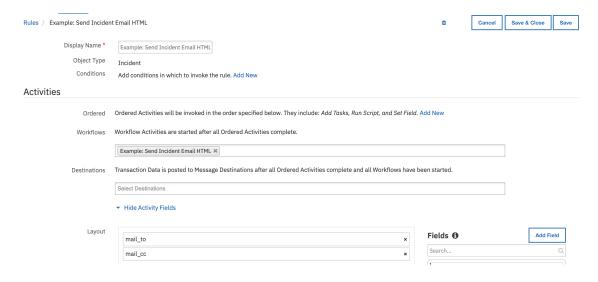
Rules

Once the function package deploys the rules, you can view them in the Resilient platform Rules tab, as shown below.

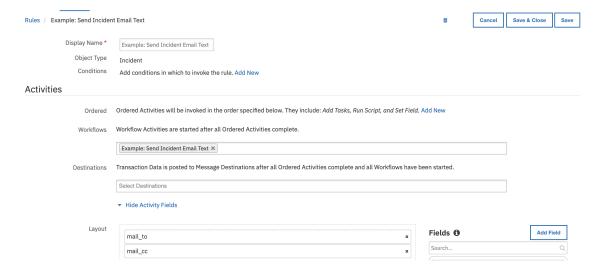


The rules themselves will be as shown below.

Example: Send Incident Email HTML



Example: Send Incident Email Text



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 support, visit https://ibm.com/mysupport.

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