None

Table of Contents

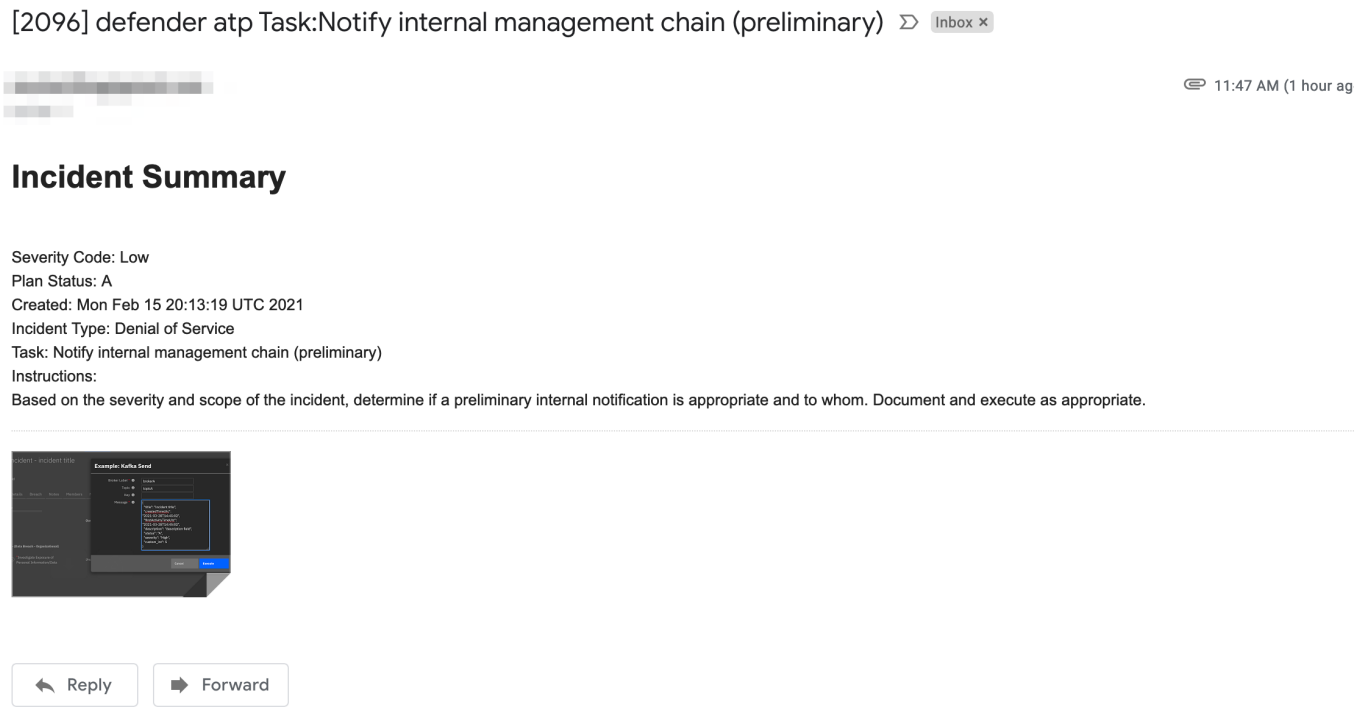
Release Notes

Version	Date	Notes
v1.3.0	7/2021	Username in app.config does not need to be an email
v1.2.1	5/2021	Bug fix for python 2
v1.2.0	4/2021	Added capability for task attachments
v1.1.1	2/2021	Bug fixes associated with sending attachments
v1.1.0	10/2020	Bug fixes and send all or specific attachments
v1.0.9	5/2020	App Host compatibility
v1.0.8	4/2020	Initial Release after internal development by Professional Services, no prior release notes

- For customers upgrading from v1.2.1, the app.config file must be manually edited.

Overview

Resilient Circuits Components for 'fn_outbound_email'



Resilient Circuits Components for 'fn_outbound_email'

Key Features

- Send email to lists of recipients (to, cc, bcc)
- Format email using a predefined html template or specify your own template
- Send attachments with the email at the incident level or task level.
- Example rules included at the incident and task levels

Requirements

This app supports the IBM Resilient SOAR Platform and the IBM Cloud Pak for Security.

Resilient platform

The Resilient platform supports two app deployment mechanisms, App Host and integration server.

If deploying to a Resilient platform with an App Host, the requirements are:

- Resilient platform >= `37.0.5832`.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

If deploying to a Resilient platform with an integration server, the requirements are:

- Resilient platform >= `37.0.5832`.
- The app is in the older integration format (available from the AppExchange as a `zip` file which contains a `tar.gz` file).
- Integration server is running `resilient_circuits`.
- If using an API key account, make sure the account provides the following minimum permissions:
    - Org Data: Read and Edit
    - Incident: Read

    - Functions: Read

The following Resilient platform guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *Integration Server Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *System Administrator Guide*: provides the procedure to install, configure and deploy apps.

The above guides are available on the IBM Knowledge Center at ibm.biz/resilient-docs. On this web page, select your Resilient platform version. On the follow-on page, you can find the *App Host Deployment Guide* or *Integration Server Guide* by expanding **Resilient Apps** in the Table of Contents pane. The System Administrator Guide is available by expanding **System Administrator**.

Cloud Pak for Security

If you are deploying to IBM Cloud Pak for Security, the requirements are:

- IBM Cloud Pak for Security >= 1.4.
- Cloud Pak is configured with an App Host.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

The following Cloud Pak guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings. From the Table of Contents, select Case Management and Orchestration & Automation > **Orchestration and Automation Apps**.
- *System Administrator Guide*: provides information to install, configure, and deploy apps. From the IBM Cloud Pak for Security Knowledge Center table of contents, select Case Management and Orchestration & Automation > **System administrator**.

These guides are available on the IBM Knowledge Center at ibm.biz/cp4s-docs. From this web page, select your IBM Cloud Pak for Security version. From the version-specific Knowledge Center page, select Case Management and Orchestration & Automation.

Proxy Server

The app **does not** support a proxy server.

Installation

Install

- To install or uninstall an App or Integration on the *Resilient platform*, see the documentation at ibm.biz/resilient-docs.
- To install or uninstall an App on *IBM Cloud Pak for Security*, see the documentation at ibm.biz/cp4s-docs and follow the instructions above to navigate to Orchestration and Automation.

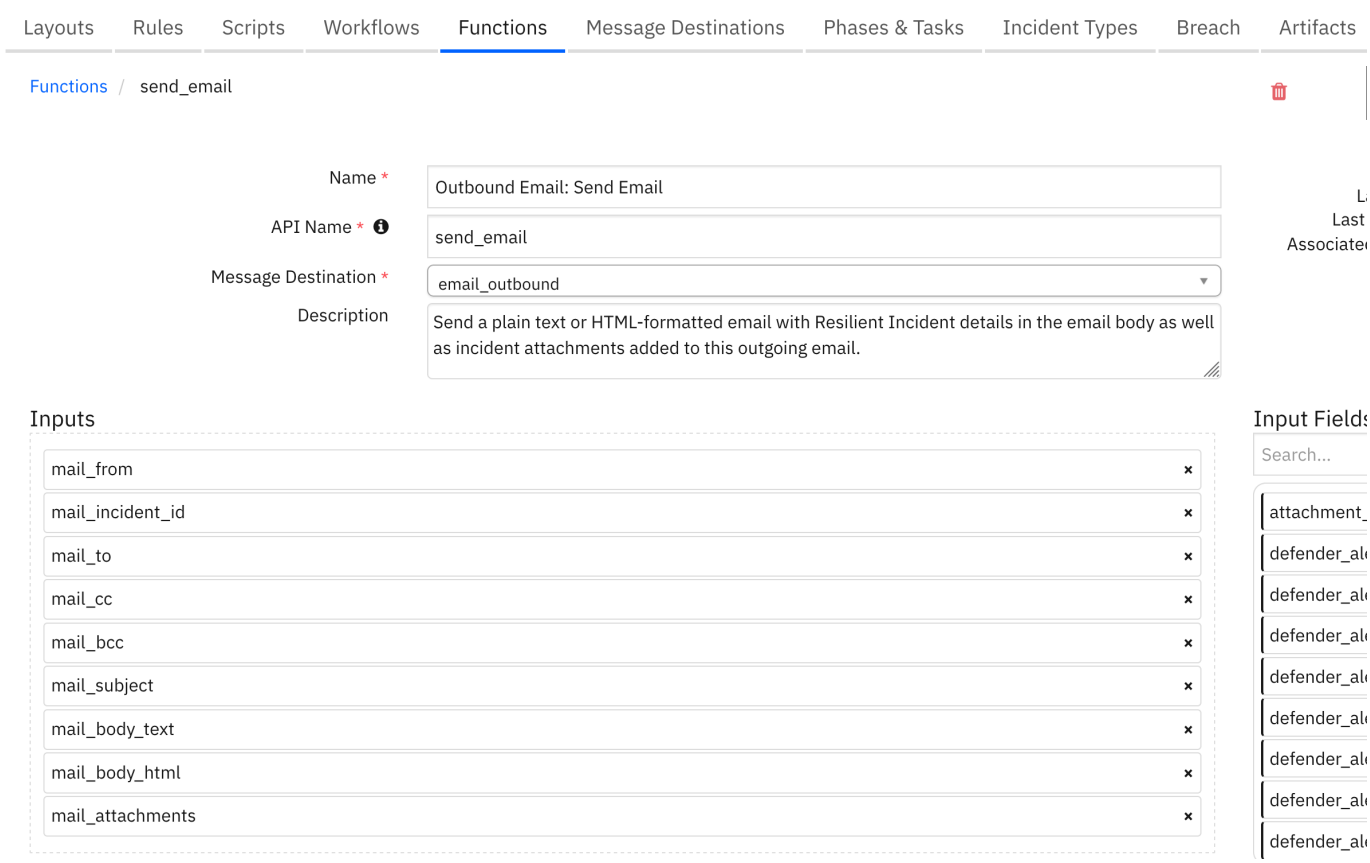
App Configuration

The following table provides the settings you need to configure the app. These settings are made in the app.config file. See the documentation discussed in the Requirements section for the procedure.

Config	Required	Example	Description
smtp_server	Yes	`xxx.xxx.xxx.xxx`	*IP Address or fully qualified domain name for smpt server*
smtp_user	Yes	``	*smtp authication user*
smtp_password	Yes	``	*smtp authication user password*
from_email_address	No	`a@example.com`	*Email address to send emails from*
smtp_port	Yes	`25`	*Defaults to unauthenticated, 587/2525 for TLS*
smtp_conn_timeout	Yes	`20`	*Timeout value in seconds to wait for a connection*
smtp_ssl_mode	Yes	`None`	*set to 'starttls' when using smtp_user and smtp_password*
smtp_ssl_cafile	Yes	``	*false or /path/to/smtp_certifcate.pem or crt file*
template_file	Yes	`data/example_send_email.jinja`	*/path/to/template.jinja for rendering the email body*

Function - Outbound Email: Send Email

Send a plain text or HTML-formatted email with Resilient Incident details in the email body as well as incident attachments added to this outgoing email.



▶ Inputs:

Name	Type	Required	Example	Tooltip
`mail_attachments`	`text`	No	–	comma separated list of attachments or '*' for all
`mail_bcc`	`text`	No	–	comma separated list of bcc recipients
`mail_body_html`	`text`	No	–	jinja template file to use to produce html email content from incident data. This content overrides the use of the `template_file` setting in our app.config file
`mail_body_text`	`text`	No	–	Already rendered email body content
`mail_cc`	`text`	No	–	comma separated list of cc recipients
`mail_from`	`text`	No	–	email sender
`mail_incident_id`	`number`	No	–	incident_id
`mail_subject`	`text`	No	–	email subject
`mail_to`	`text`	No	–	comma separated list of email recipients

▶ Outputs:

```
results = {
    # TODO: Copy and paste an example of the Function Output within this
```

```
code block.
    # To view the output of a Function, run resilient-circuits in DEBUG mode
and invoke the Function.
    # The Function results will be printed in the logs: "resilient-circuits
run --loglevel=DEBUG"
}
```

▶ Example Pre-Process Script:

```
inputs.mail_to = rule.properties.mail_to
inputs.mail_cc = rule.properties.mail_cc
inputs.mail_attachments = rule.properties.mail_attachments
inputs.mail_incident_id = incident.id
inputs.mail_from = "changeme@resilientsystems.com"
inputs.mail_subject = u"[{0}] {1}".format(incident.id, incident.name)

inputs.mail_body_html = """{% set NOT_FOUND = ["Not Found!","-","None",None]
%}
{% macro get_row(label,field_name) -%}
    {% set value = template_helper.get_incident_value(incident,field_name)
%}
    {% set style = "font-family: Calibri; color: rgb(31,73,125)" %}
    {% if value and value not in NOT_FOUND and not value.startswith('-') %}
    <tr>
        <td width="100" style="{{style}}; font-weight:bold">{{ label }}</td>
        <td style="{{style}}">{{ value | striptags }}</td>
    </tr>
    {% endif %}
{%- endmacro %}
<table width="100%" >
<tr>
    <td colspan="2">
        <h3 style="color: rgb(68,114,196)">INCIDENT DETAILS</h3>
        <hr size="1" width="100%" noshade style="color:#FFDF57"
align="center"/>
    </td>
</tr>
    {{ get_row('Severity:','severity_code') }}
    {{ get_row('Status:','plan_status') }}<br>
    {{ get_row('Created:','create_date') }}<br>
    {{ get_row('Category:','incident_type_ids') }}
<tr>
    <td colspan="2">
        <br><h3 style="color: rgb(68,114,196)">INCIDENT DESCRIPTION</h3>
        <hr size="1" width="100%" noshade style="color:#FFDF57"
align="center"/>
    </td>
    {{ get_row('Description:','description') }}
</tr>
</table>
<br>
"""
```

▶ Example Post-Process Script:

```
if results.success:
  noteText = u"""Email Sent if mail server is valid/authenticated\n
  <br>From: {0}<br> To: {1}<br> CC: {2}<br> BCC: {3}<br> Subject: {4} <br>
  Body: {5} <br>""".format(results.content.inputs[0].strip("u\"[]"),
results.content.inputs[1].strip("u\"[]"),
results.content.inputs[2].strip("u\"[]"),
results.content.inputs[3].strip("u\"[]"),
results.content.inputs[4].strip("u\""), results.content.text)
else:
  noteText = u"Email NOT Sent\n From: {0}\n To:
{1}".format(results.content.inputs[0].strip("u\"[]"),
results.content.inputs[1].strip("u\"[]"))
incident.addNote(helper.createRichText(noteText))
```

Rules

Rule Name	Object	Workflow Triggered
Example: Send Incident Email HTML	incident	`example_send_incident_email_html`
Example: Send Incident Email Text	incident	`example_send_incident_email_text`
Example: Send Task Email HTML	task	`example_send_task_email_html`

Troubleshooting & Support

Common connection issues with TLS and TroubleShooting

Use `resilient-circuits selftest -l fn-outbound-email` to confirm if your connection is successful.

```
fn-outbound-email:
    SMTP AUTH extension not supported by server.
    selftest: failure, Elapsed time: 0.416000 seconds
```

- Email servers are often restrictive on which applications/users that are authorized to send emails, for instance if you have 2FA authentication enabled on a gmail account, you must add a specific application password or allow less secure apps (Not recommended)

  https://hotter.io/docs/email-accounts/app-password-gmail/

  https://hotter.io/docs/email-accounts/secure-app-gmail/

- Occasionally, mailservers may indicate that emails have been sent successfully (including a successful note on the the associated incident) and yet they be blocked by the receiving mailserver due to

insecure spam filters. This is a limitation of SMTP authentication mechanism.

- The port of TLS handshakes may also differ between mailservers (587/2525), a short history of port allocation can be found at: https://pepipost.com/blog/25-465-587-2525-choose-the-right-smtp-port/
- More info on smtp protocol:

  https://pepipost.com/blog/what-is-smtp
- Some mailservers will not work with this level of authentication/protocal.

For Support

This is a IBM Community provided App. Please search the Community https://ibm.biz/resilientcommunity for assistance and use the My Support link to open a support case.