Secureworks CTP Functions for IBM Resilient

Release Notes

v1.0.0

- Initial Release

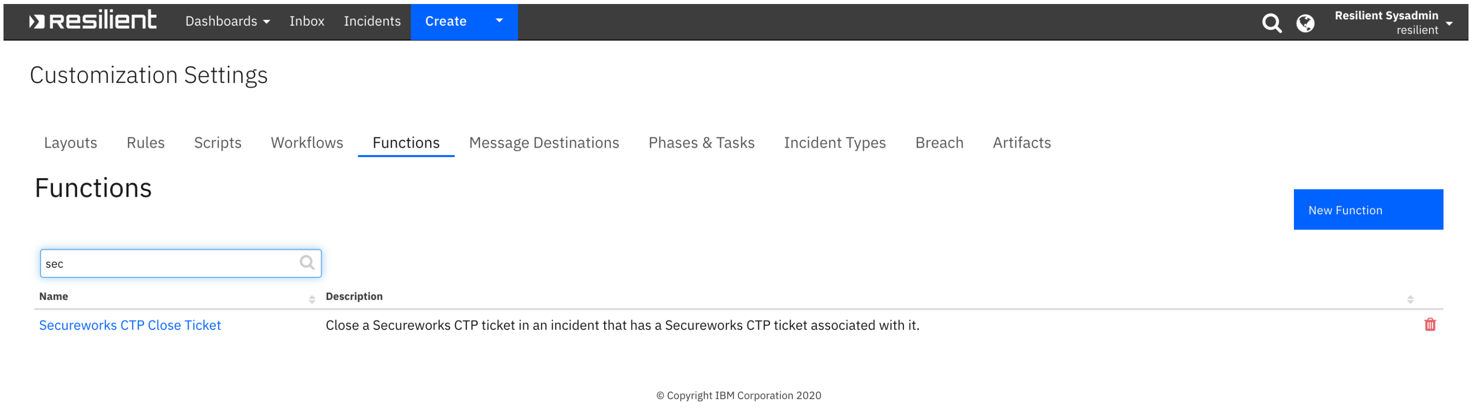
Overview

The Secureworks Counter Threat Platform (CTP) uses the global visibility gained from gathering and analyzing data from clients all over the world to more accurately identify, contain and eradicate cybersecurity threats. By combining up-to-the-minute threat intelligence with the CTP's machine learning and analytics capabilities, organizations can make faster, more informed decisions about how to predict, prevent, detect, and respond to threat activity.

CTP is used with the Secureworks SOC team when they find a security issue that needs to be communicated to the customer. The issues can be informational, research-based or require proscriptive actions by the customer. Secureworks CTP provides a “ticket-like” interface that allows you acknowledge, add files and notes, and provide ability to close tickets.

The Secureworks CTP integration implements the following functionality in Resilient:

- Poll Secureworks CTP for tickets and create a corresponding incident in the Resilient platform for each ticket.
- Get Secureworks CTP ticket workLogs and attachments and add them as notes and attachments in the corresponding Resilient incident.
- Close a Secureworks CTP ticket when the corresponding Resilient incident is closed.



Name	Description
Secureworks CTP Close Ticket	Close a Secureworks CTP ticket in an incident that has a Secureworks CTP ticket associated with it.

Requirements

- Resilient platform >= `v35.2.32`
- An Integration Server running `resilient_circuits>=30.0.0`
  - To set up an Integration Server see: ibm.biz/res-int-server-guide

    - If using API Keys, minimum required permissions are:
        - Org Data: Read, Edit

Installation

- Download the `fn_secureworks_ctp.zip` .
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip fn_secureworks_ctp-x.x.x.zip
```

- **Change Directory** into the unzipped directory:

```
$ cd fn_secureworks_ctp-x.x.x
```

- **Install** the package:

```
$ pip install fn_secureworks_ctp-x.x.x.tar.gz
```

- Import the **configurations** into your app.config file:

```
$ resilient-circuits config -u -l fn-secureworks-ctp
```

- Import the fn_secureworks_ctp **customizations** into the Resilient platform:

```
$ resilient-circuits customize -y -l fn-secureworks-ctp
```

- Open the config file, scroll to the bottom and edit your fn_secureworks_ctp configurations:

```
$ vi ~/.resilient/app.config
```

Config	Required	Example
base_url	Yes	`https://api.secureworks.com/api/ticket/v3`
username	Yes	`user@example.com`
password	Yes	``
query_ticket_grouping_types	Yes	`INCIDENT:SECURITY`
query_limit	Yes	`10`

Config	Required	Example
assigned_to_customer	Yes	`true`
polling_interval	Yes	`600`
close_codes	No	`Authorized Activity,Confirmed Security Incident,Duplicate,Incident Misidentified,Inconc`
cafile	No	``

- **Save** and **Close** the app.config file.
- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-secureworks-ctp
```

- **Run** resilient-circuits or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

Uninstall

- SSH into your Integration Server.
- **Uninstall** the package:

```
$ pip uninstall fn-secureworks-ctp
```

- Open the config file, scroll to the [fn_secureworks_ctp] section and remove the section or prefix `#` to comment out the section.
- **Save** and **Close** the app.config file.

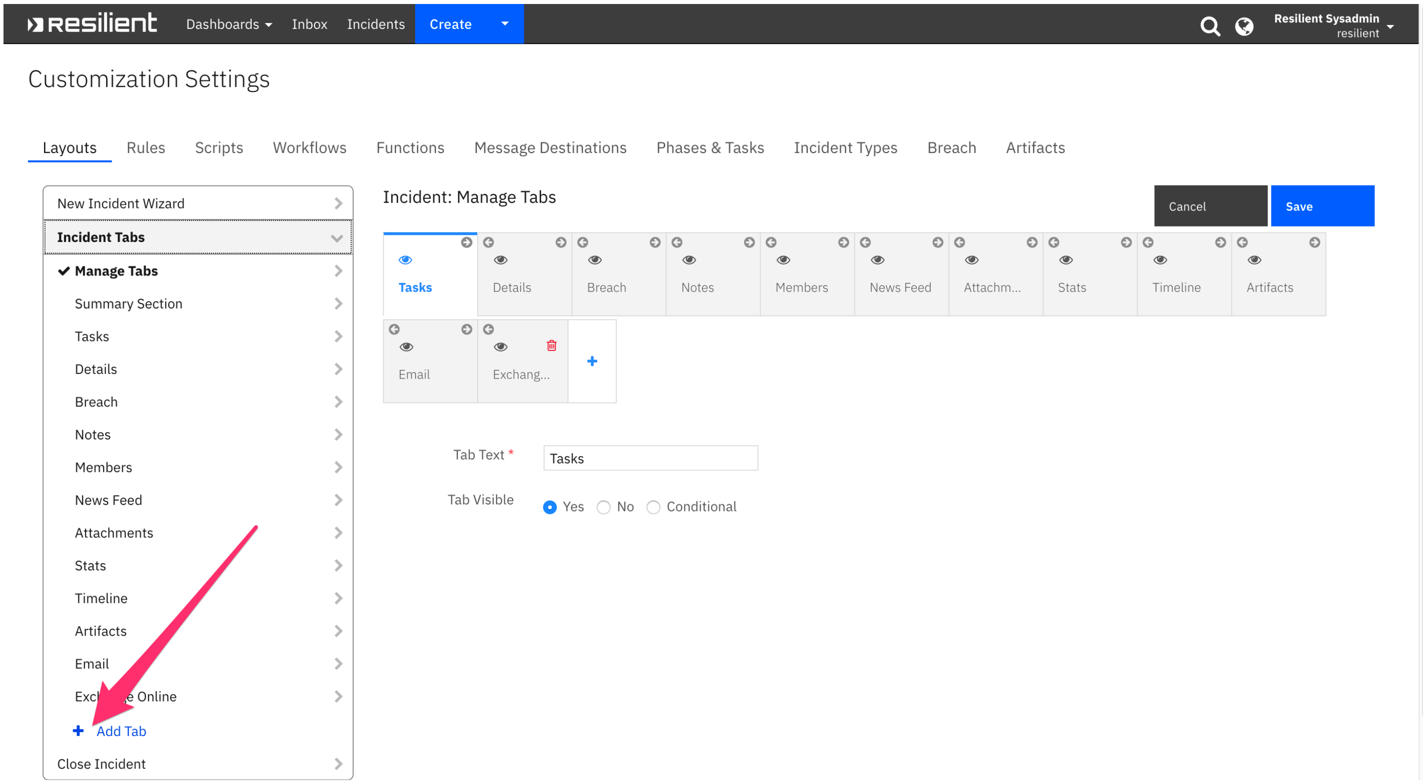
Custom Layouts

Customize Secureworks CTP and Close Incident Layouts to provide Secureworks specific information in the Resilient UI.

Secureworks CTP Layout Tab

Create a Secureworks CTP custom incident tab so that you can view Secureworks CTP ticket information in one place.

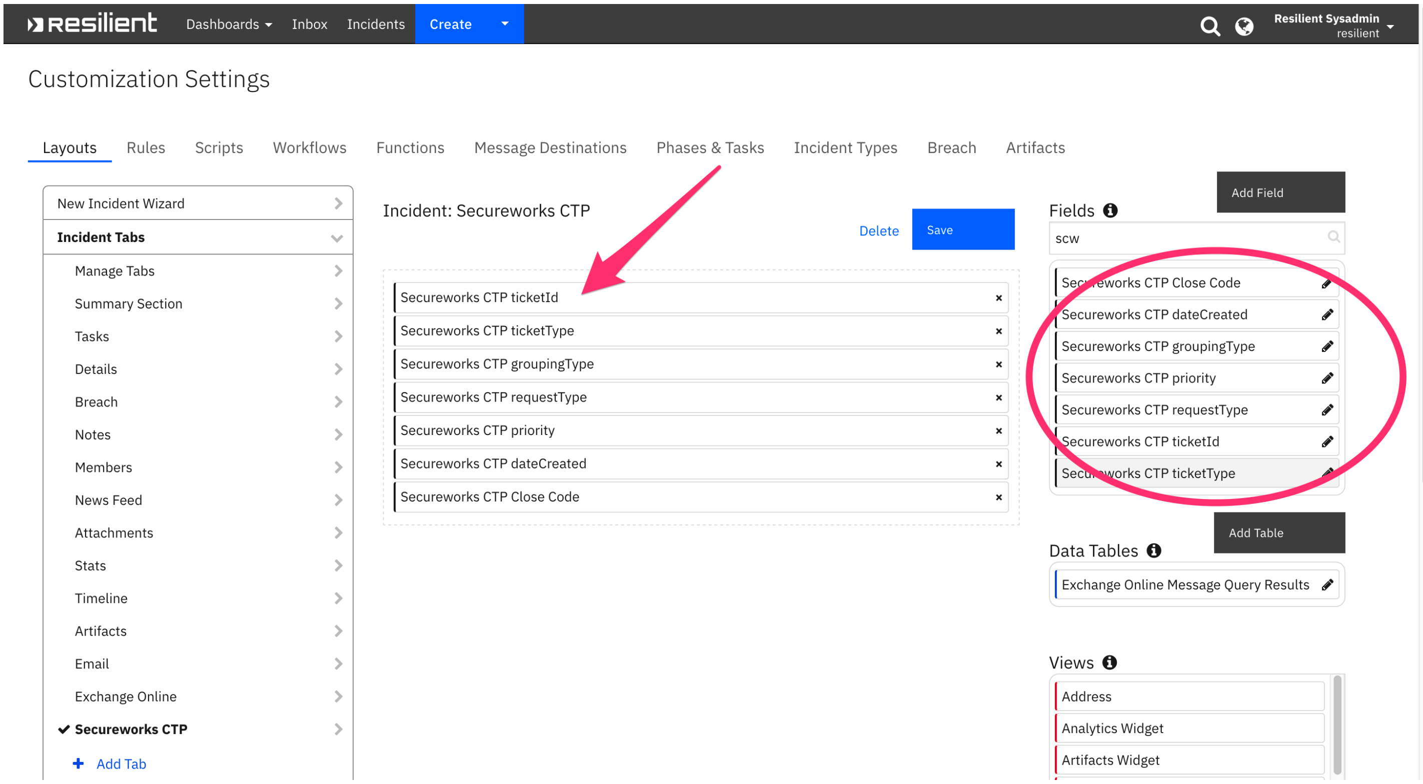
- Go to the Customizations Settings -> Layouts tab.
- Click the Incident Tabs menu item on the left.
- Click the Add Tab button.
- Enter Secureworks CTP in Add a Tab popup and click Add.



Tab Text * Tasks

Tab Visible ● Yes ○ No ○ Conditional

- Next, search for the Secureworks CTP (scwx) custom incident fields in the Fields search bar.
- Drag Secureworks custom incidents fields on to the layout in the center of the screeen.
- Click Save.



Secureworks CTP ticketId
Secureworks CTP ticketType
Secureworks CTP groupingType
Secureworks CTP requestType
Secureworks CTP priority
Secureworks CTP dateCreated
Secureworks CTP Close Code

Fields search: scw

Secureworks CTP Close Code
Secureworks CTP dateCreated
Secureworks CTP groupingType
Secureworks CTP priority
Secureworks CTP requestType
Secureworks CTP ticketId
Secureworks CTP ticketType

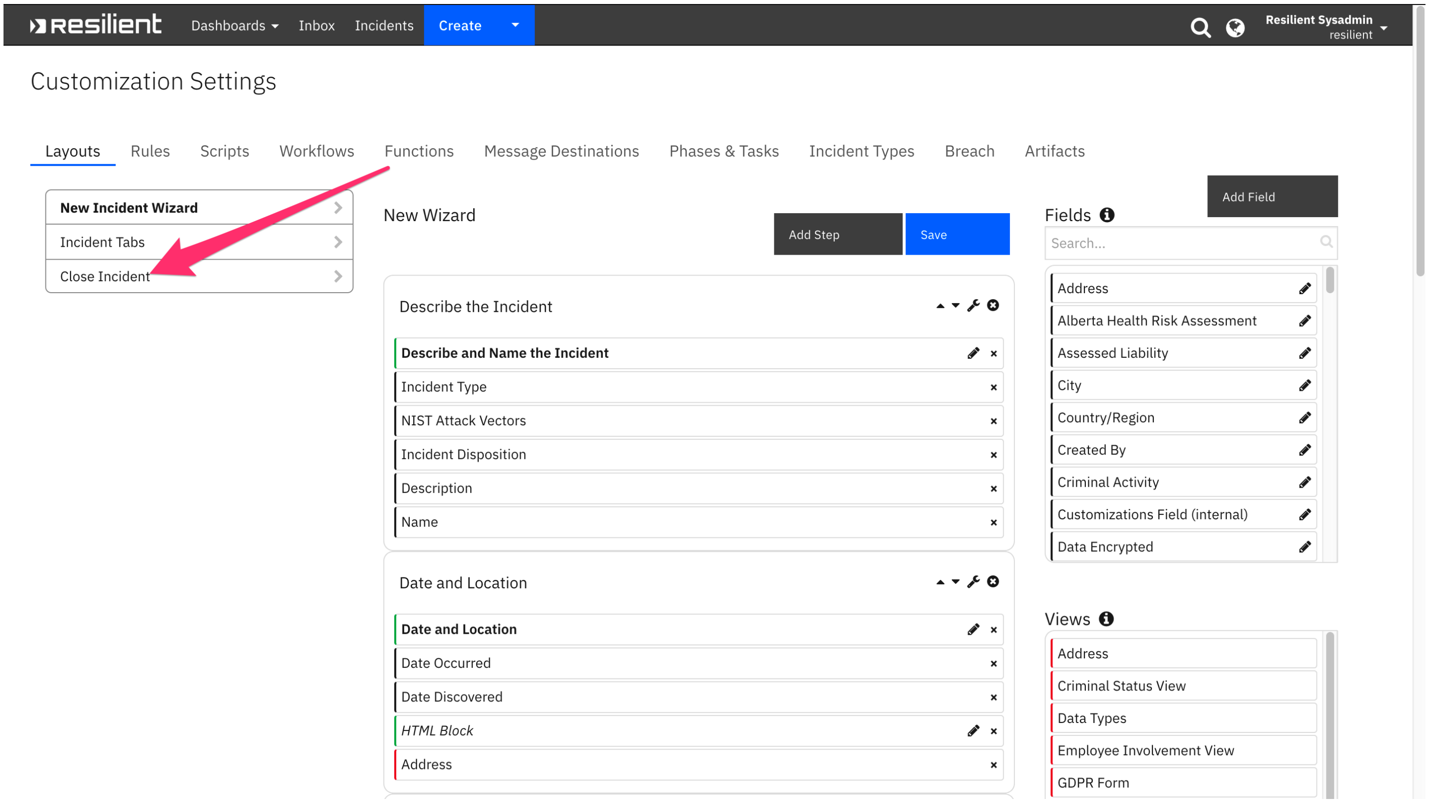
Data Tables: Exchange Online Message Query Results

Views: Address, Analytics Widget, Artifacts Widget

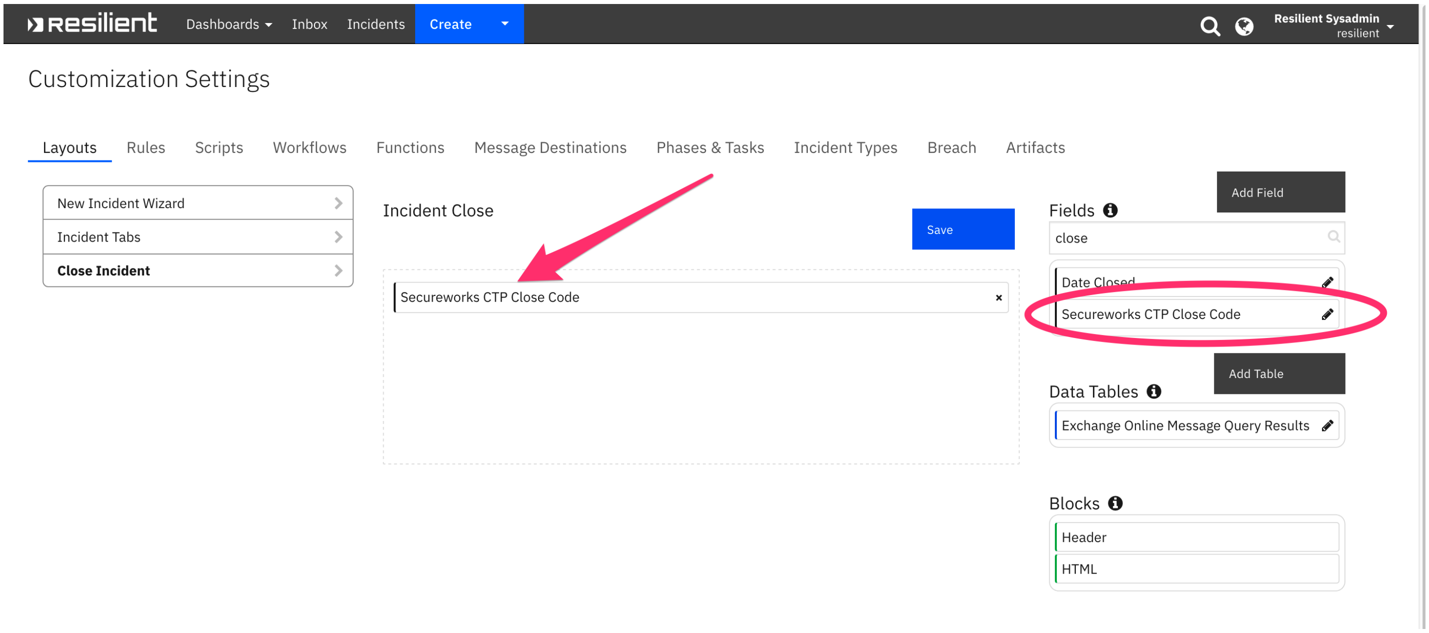
Close Incident Layout Tab

Modify the Close Incident tab so the the Secureworks close code can be selected from the Close Incident popup from Resilient.

- Go to the Customizations Settings -> Layouts tab.
- Click the Close Incident menu item on the left as shown in the screenshot below.



- Next, search for the Secureworks CTP Close Code custom incident fields in the Fields search bar.
- Drag the Secureworks CTP Close Code onto the Close Incident layout tab.



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

Name	Version	Author	Support URL
fn_secureworks_ctp	1.0.0		https://ibm.com/mysupport