

IBM Resilient



Security Orchestration, Automation and Response Platform

Carbon Black Protection Integration V1.0.2

Release Date: September 2019

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 Carbon Black Protection Integration.

Overview

This integration consists of 12 functions which call various APIs to perform different actions, such as retrieving approval request details, updating approval requests and deleting files. It also contains a polling component to create incidents in the Resilient platform that correspond to approval requests in Carbon Black Protection.

Installation

You download the function package to a Resilient integration server, and from there you deploy the functions and components to a Resilient platform. These procedures are provided in the [Resilient Integration Server Guide \(PDF\)](#).

The functions included this package have the following requirements, which are above and beyond those listed in the *Resilient Integration Server Guide*.

- Resilient platform is version 30 or later.
- Carbon Black Protection v8.1 or later.

After installing the package, Resilient Circuits creates a new section, [fn_cb_protection], in the app.config file. You need to edit the following settings in that section.

```
[fn_cb_protection]
# Name or IP address of your CbProtect server
server=10.200.1.1

# Access token issued by the CbProtect administrator
token= XXXX-XXXX-XXXX-XXXX

# If your CbProtect server has a self-signed TLS certificate, you cannot verify
it:
# verify_cert=false

# Interval (seconds) for automatic escalation of approval requests, set 0 to
disable
# Suggest 300 as a starting point, which will check CbProtect every 5 minutes
escalation_interval=0

# Optional: query for which requests to escalate; default is to escalate all
open approval requests
# escalation_query=resolution:0

# Optional: path to a custom template file for the escalated incident
# template_tile=/usr/integration/bit9_escalation.jinja

# Optional: set this to only escalate a single request ID, e.g. when testing a
custom template
# test_single_request=999
```

Create a Custom Layout

In order to view the status of the Carbon Black Protection integration, go to the Layout tab in Resilient and create an Incident Tab named Cb Protection. Drag the Cb Protect incident fields from the Fields column on the right to the Incident: CbProtection tab column in the middle of the page and then hit the Save button.

The screenshot shows the Resilient platform's customization settings for creating a new incident layout. The left sidebar lists various tabs like New Incident Wizard, Incident Tabs, and Artifacts. Under Incident Tabs, 'Cb Protection' is selected. The main area shows the 'Incident: Cb Protection' tab configuration. On the right, there are three columns: 'Fields' (containing incident fields like Cb Protect Computer, Cb Protect Computer ID, etc.), 'Data Tables' (empty), and 'Views' (containing Address, Analytics Widget, Artifacts Widget). A 'Save' button is visible at the top right of the tab configuration area.

Now you can go to the Cb Protection tab and view that status of the Approval and Ban requests.

The screenshot shows a web-based application interface for managing security incidents. At the top, there's a navigation bar with links for Dashboards, Simulations, Incidents, Create, and Actions. The main title of the page is "Cb Protection Approval Request for firefox.exe - Cb Protect ...".

Summary

ID	2186	Description	test approval 09/04/2019 11:10 a.m.
Phase	Initial		
Severity	-		
Date Created	09/04/2019		
Date Occurred	09/04/2019		
Date Discovered	09/04/2019		
Was personal information or personal data involved?	No		
Incident Type	-		

People

Created By	Resilient Sysadmin
Owner	Resilient Sysadmin
Members	There are no members.

Related Incidents

#2185 Cb Protection Approval Request f...
#2184 Cb Protection Approval Request f...
#2183 Cb Protection Approval Request f...

Description

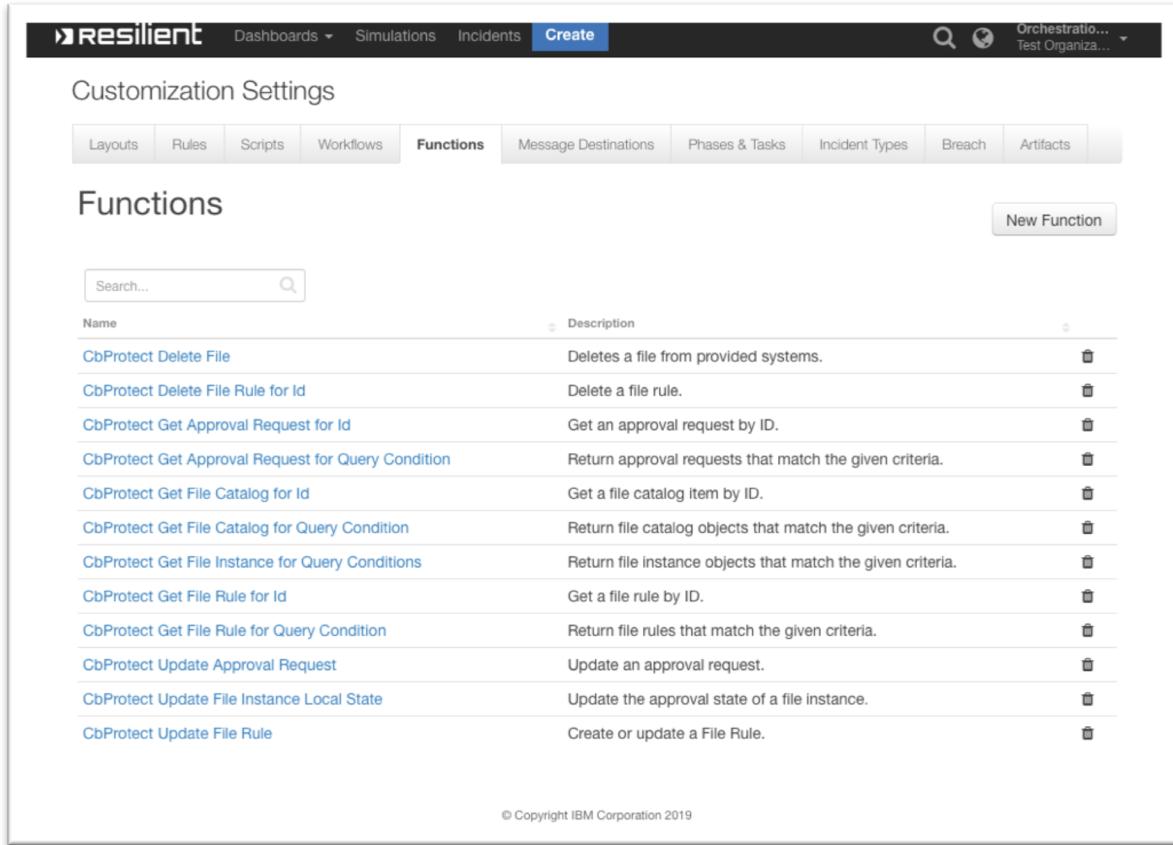
test approval 09/04/2019 11:10 a.m.

Cb Protection

Tasks	Details	Breach	Notes	Members	News Feed	Attachments	Stats	Timeline	Artifacts
Cb Protection									
Cb Protection									
Edit									
Cb Protect Computer	WORKGROUP\RSWINDOWS10-3								
Cb Protect Computer ID	1								
Cb Protect Details	Approval Request Details								
Cb Protect Enforcement Level	Low (Monitor Unapproved)								
Cb Protect File Catalog Id	32013								
Cb Protect File Path	c:\users\rswindows10-3\appdata\local\mozilla firefox								
Cb Protect Filename	firefox.exe								
Cb Protect Request Id	46								
Cb Protect Request Priority	Medium								
Cb Protect Request Status	Submitted								
Cb Protect Triggered On	09/04/2019 11:11:19								
Cb Protect User	annmarie.meier.norcross@ibm.com								

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 and rules that show how the functions can be used. You can copy these workflows and rules for your own needs.

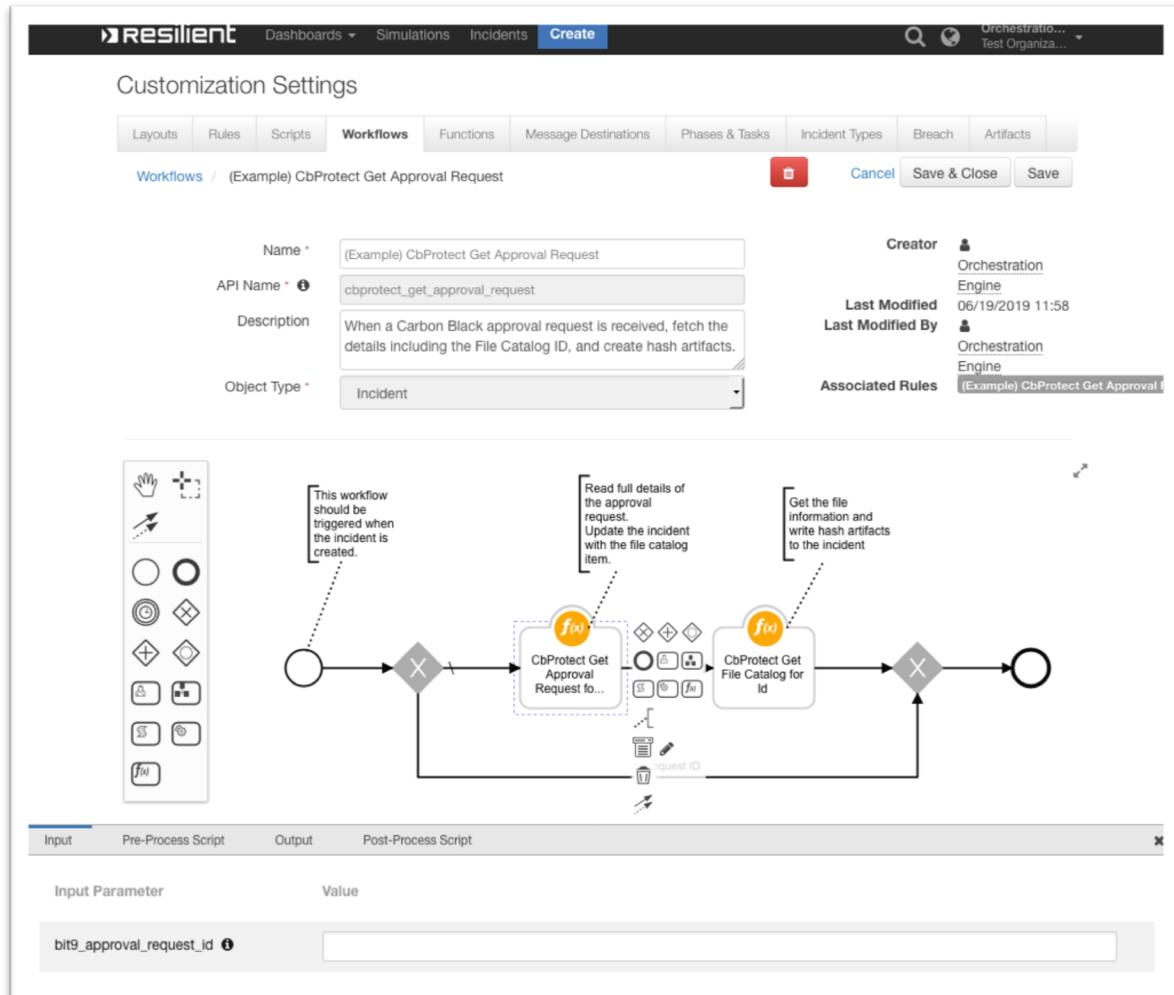


The screenshot shows the Resilient platform interface with the 'Functions' tab selected in the top navigation bar. The main content area displays a list of functions, each with a name and a brief description. A search bar is at the top left, and a 'New Function' button is at the top right. The table has two columns: 'Name' and 'Description'. Each row contains a delete icon. At the bottom of the page, there is a copyright notice: '© Copyright IBM Corporation 2019'.

Name	Description
CbProtect Delete File	Deletes a file from provided systems.
CbProtect Delete File Rule for Id	Delete a file rule.
CbProtect Get Approval Request for Id	Get an approval request by ID.
CbProtect Get Approval Request for Query Condition	Return approval requests that match the given criteria.
CbProtect Get File Catalog for Id	Get a file catalog item by ID.
CbProtect Get File Catalog for Query Condition	Return file catalog objects that match the given criteria.
CbProtect Get File Instance for Query Conditions	Return file instance objects that match the given criteria.
CbProtect Get File Rule for Id	Get a file rule by ID.
CbProtect Get File Rule for Query Condition	Return file rules that match the given criteria.
CbProtect Update Approval Request	Update an approval request.
CbProtect Update File Instance Local State	Update the approval state of a file instance.
CbProtect Update File Rule	Create or update a File Rule.

bit9_approval_request_get: CbProtect Get Approval Request for Id

Given an approval request's ID, the function returns the details of the approval request. The function takes one input, bit9_approval-request_id, which is a number. The following is an example of this function in the (Example) CbProtect Get Approval request workflow.



bit9_approval_request_query: CbProtect Get Approval Request for Query Condition

This function takes one input, bit9_query which is a query string, and returns the approval requests that match the given query condition. The following is an example of this function in the (Example) CbProtect Get Appr Req for Q 'fileName:notepad.exe' workflow. You can set a different query condition following the guidelines

<https://developer.carbonblack.com/reference/enterprise-protection/8.0/rest-api/#query-condition> and review the all approval request properties to query here

<https://developer.carbonblack.com/reference/enterprise-protection/8.0/rest-api/#approvalrequest>.
fileName:notepad.exe represents name of the file on the agent.

Customization Settings

Workflows / (Example) CbProtect Get Appr Req for Q 'fileName:notepad.exe'

Name: (Example) CbProtect Get Appr Req for Q 'fileName:notepad.exe'

API Name: example_cbprotection_query_approval_request

Description: Queries for approval requests based on the provided query.

Object Type: Incident

Creator: Orchestration Engine 06/19/2019 11:57 Last Modified By: Orchestration Engine

Associated Rules: (Example) CbProtect Get Appro

Start your workflow here

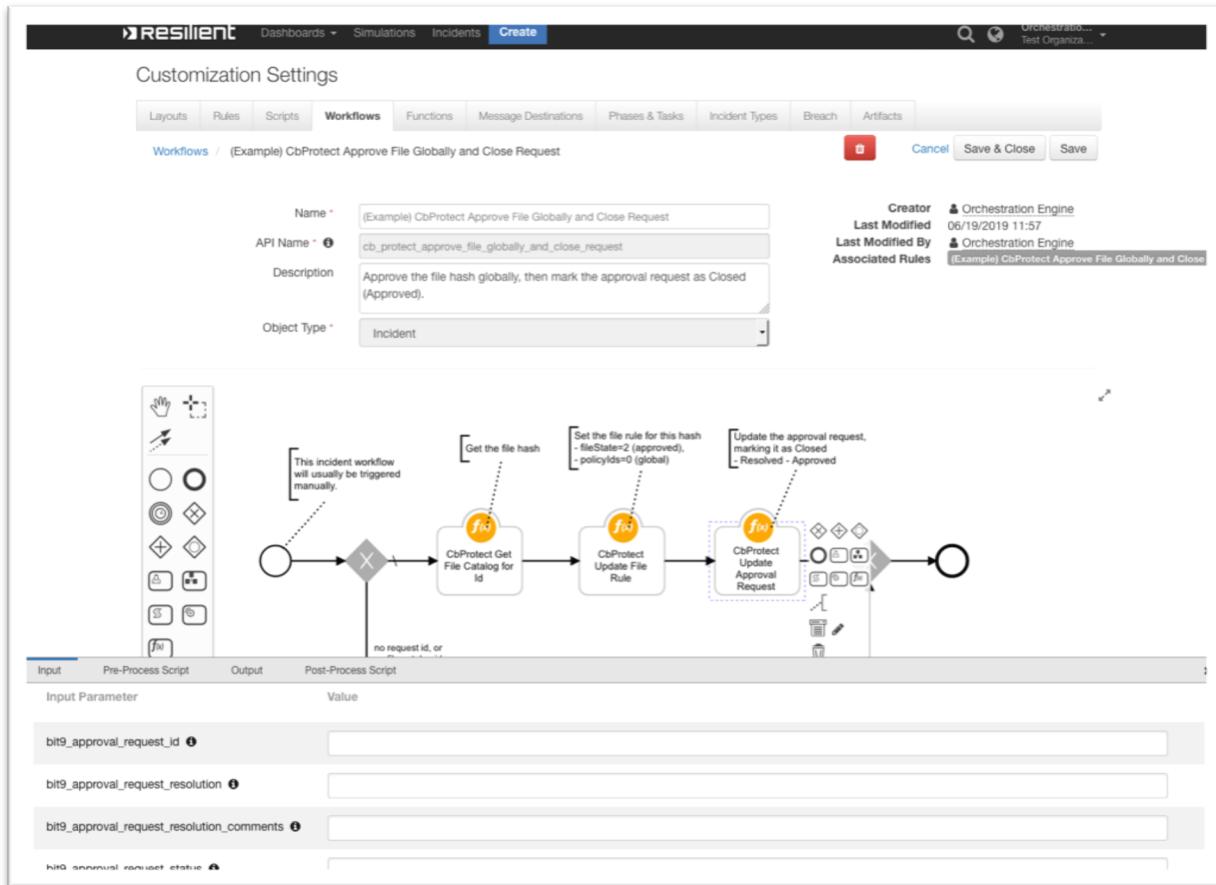
Queries for approval requests with the file name notepad.exe

A note is created with the results

Input Parameter: bit9_query Value: fileName:notepad.exe

bit9_approval_request_update: CbProtect Update Approval Request

This function accepts as input a request ID, approval request resolution, comments, and status. With these, it updates an approval request. The following is an example of this function in a workflow:



bit9_file_delete: CbProtect Delete File

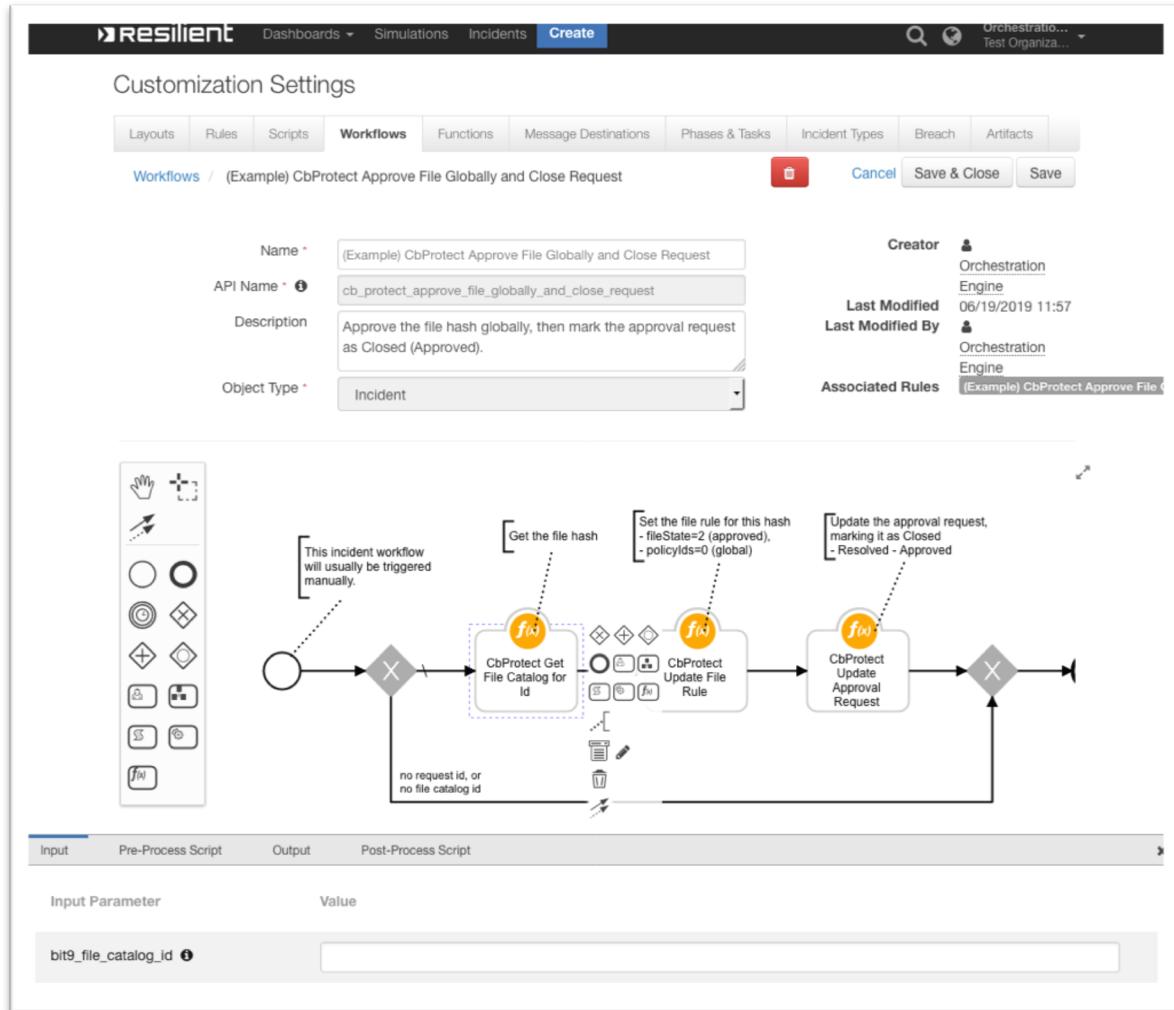
This function deletes a file from one or all computers using Carbon Black Protection. Set the bit9_file_action input to delete by file hash or file name (choose file hash to set catalog ID). Set the bit9_computer_id input for a specific computer, or use "0" to select all computers. Then, depending on the chosen file action, set the catalog ID, file hash, or file name. The following is an example of this function in the (Example) CbProtect Delete File By Hash workflow:

The screenshot shows the Resilient platform's 'Customization Settings' interface for a workflow. The workflow is titled '(Example) CbProtect Delete File By Hash'. The input parameters include:

- bit9_file_action: DeleteFileByHash
- bit9_computer_id: (empty)
- bit9_file_catalog_id: (empty)
- bit9_file_hash: (empty)

bit9_file_catalog_get: CbProtect Get File Catalog for Id

Returns the file catalog details based on the catalog ID provided. The following is an example of this function in the (Example) CbProtect Approve File Globally and Close Request workflow:



bit9_file_catalog_query: Cbprotect Get File Catalog for Query Condition

Returns file catalogs and their details from a provided query string. The following is an example of this function in (Example) CbProtect Get File Catalog for Query Condition workflow. You can set a different query condition following the guidelines

<https://developer.carbonblack.com/reference/enterprise-protection/8.0/rest-api/#query-condition>

and review the all file catalog properties to query here

<https://developer.carbonblack.com/reference/enterprise-protection/8.0/rest-api/#filecatalog>.

The screenshot shows the Resilient platform's 'Workflows' section. A new workflow is being created with the following details:

- Name:** (Example) CbProtect Get File Catalog for Query Condition
- API Name:** example_cbprotection_query_file_catalog
- Description:** Get the details of the file catalog matching the single Cb Protect query condition. Results of the query are written to an incident note. An example of a single query condition: 'trust:1'
- Object Type:** Incident

Associated Rules: (Example) CbProtect Get File Catalog for

Workflow Diagram:

```
graph LR; Start((Start your workflow here)) --> Script[CbProtect Get File Catalog for Qu...]; Script --> End(( ));
```

Annotations:

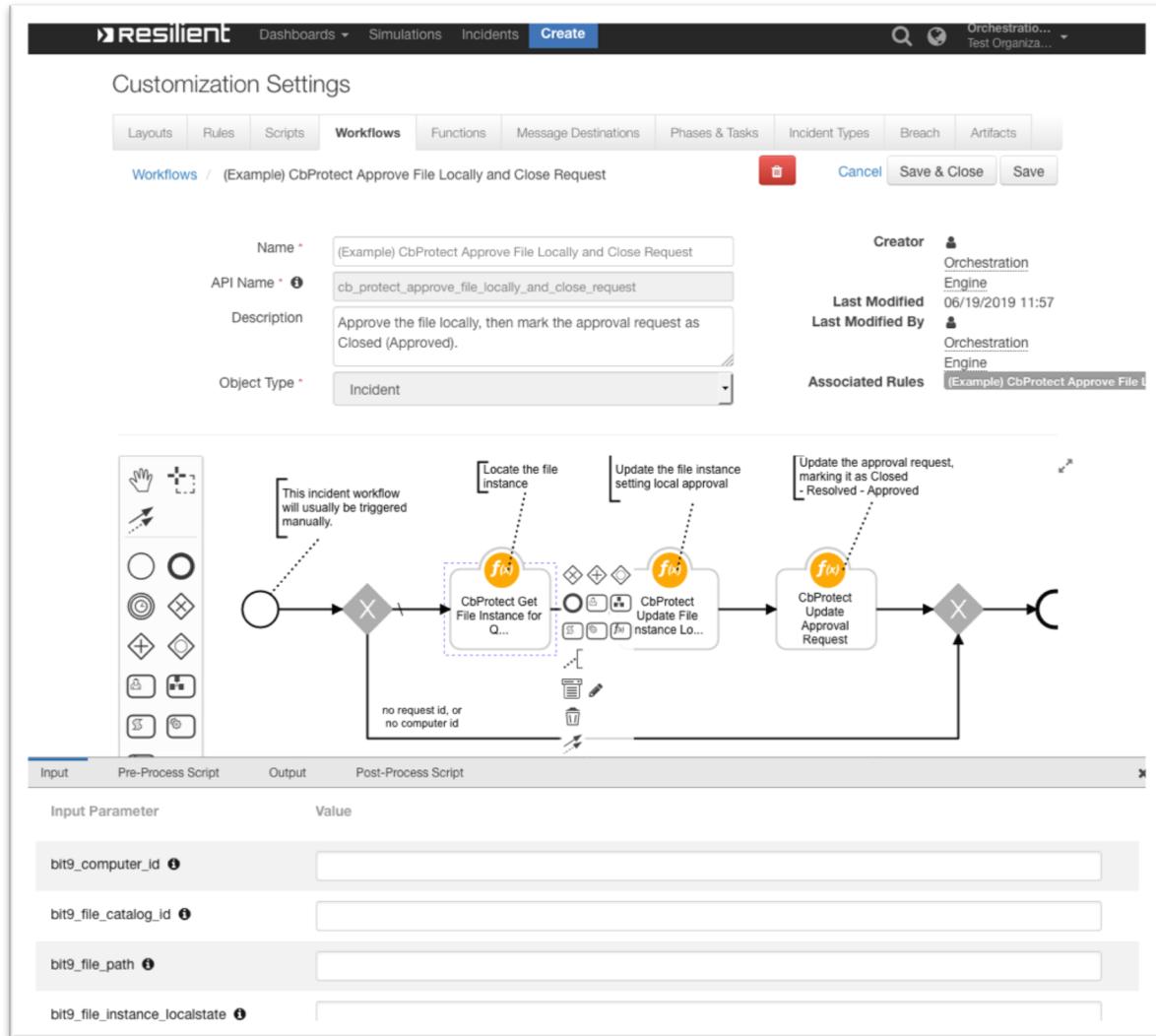
- Get the file catalog for files matching the result of the single Cb Protect query condition.
- An incident note is created containing the results.
- Start your workflow here.

Post-Process Script:

```
1 content=u'Results from CbProtect Get File Catalog by Query Condition: {} items found\n{}'.format(results.count, results.pretty_results)
2
3 incident.addNote(helper.createPlainText(content))
4 # {'count': 656, 'items': [{"u'trust': 1, 'u'pathName': 'u'c:\\windows\\syswow64', 'u'fileName': 'u'ktmw32.dll', 'u'sha256': u'3c9fc4fb08d51c5024b3f5a2794b724ed17c3b45e434ebe845478c3301
```

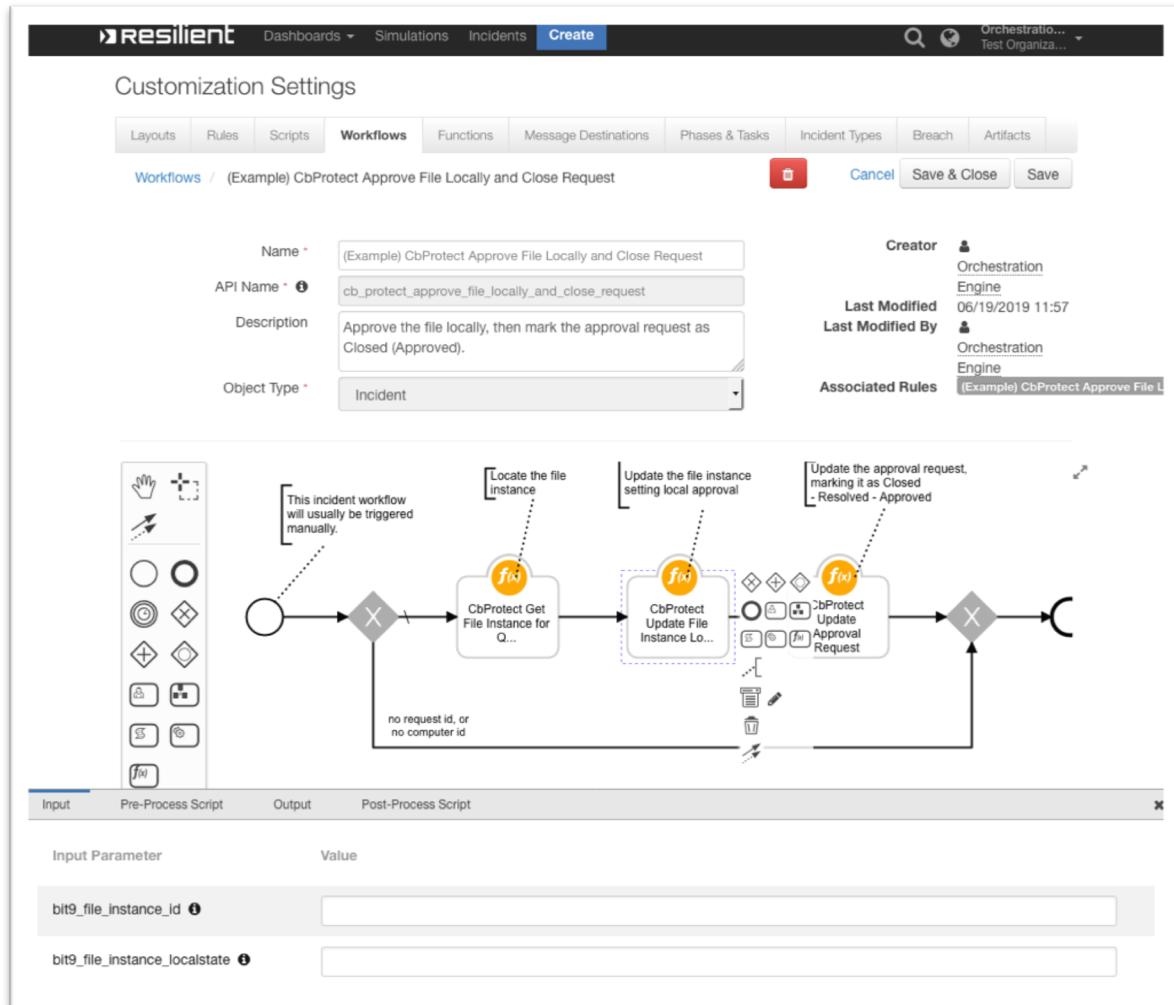
bit9_file_instance_query: CbProtect Get File Instance for Query Conditions

Returns file instance objects that match the given criteria from the inputs. The following is an example of this function in the (Example) CbProtect Approve File Locally and Close Request workflow:



bit9_file_instance_update: CbProtect Update File Instance Local State

Updates a file instance's local approval/banned setting. This function has inputs for the file instance ID and the local state (for example, approved = 2). The following includes an example of this function in the (Example) CbProtect Approve File Locally and Close Request workflow:



bit9_file_rule_update: CbProtect Update File Rule

This function updates a file rule in Carbon Black based on the data passed as inputs. The following is an example of this function in the (Example) CbProtect Approve File Globally and Close Request workflow:

Customization Settings

Workflows / (Example) CbProtect Approve File Globally and Close Request

Name: (Example) CbProtect Approve File Globally and Close Request
API Name: cb_protect_approve_file_globally_and_close_request
Description: Approve the file hash globally, then mark the approval request as Closed (Approved).
Object Type: Incident

Creator: Orchestration Engine
Last Modified: 06/19/2019 11:57
Last Modified By: Orchestration Engine
Associated Rules: (Example) CbProtect Approve File

```
graph LR; Start(( )) --> TriggerX(( )); TriggerX -- "This incident workflow will usually be triggered manually." --> GetCatalog{CbProtect Get File Catalog for Id}; GetCatalog -- "no request id, or no file catalog id" --> EndX(( )); GetCatalog -- "Get the file hash" --> UpdateRule{CbProtect Update File Rule}; UpdateRule -- "Set the file rule for this hash - fileState=2 (approved), - policyIds=0 (global)" --> ApprovalRequest{CbProtect Update Approval Request}; ApprovalRequest -- "Update the approval request, marking it as Closed - Resolved - Approved" --> EndC(( ));
```

Input Parameter Value

bit9_file_rule_id	1
bit9_file_catalog_id	
bit9_file_rule_name	
bit9_file_rule_description	
bit9_file_rule_filestate	
bit9_file_rule_sourcetype	5
bit9_file_rule_policyids	
bit9_file_rule_hash	

Carbon Black Protection Resilient Polling Component

This integration contains a polling component that automatically escalates approval requests into the Resilient platform. To enable this feature, the `escalation_interval` variable in the `app.config` file must be set to an integer greater than 0. This integer represents the interval in number of seconds for the automatic escalation of approval requests. It is recommended to start at 300, which checks every 5 mins.

You can also set optional values, such as `escalation_query`, which escalates approval requests that match the query; if not set, it defaults to all open approval requests. In addition, you can set `template_file` to the location of a custom jinja template file; if not set, the default template file is used. To create your own custom jinja file, you should use the default jinja file as a reference. This file can be found when expanding the package in the following directory:

```
fn_cb_protection-<version#>/fn_cb_protection/data/
```