

# Genian NAC Integrations

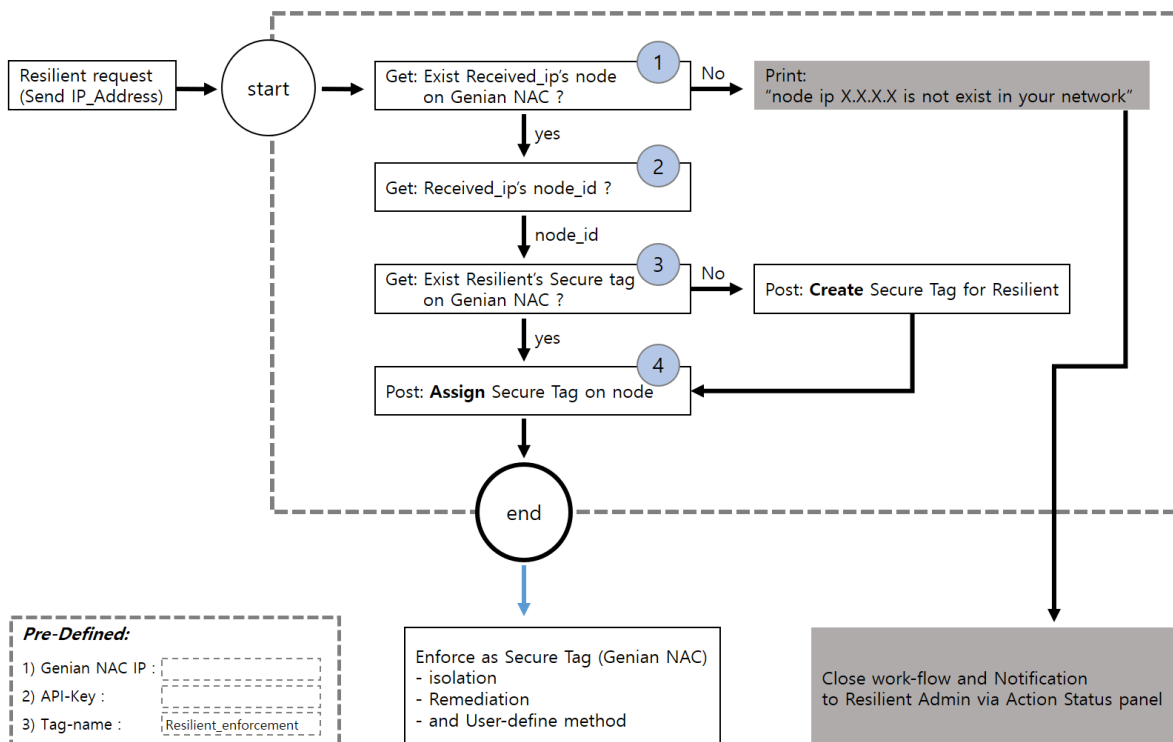
Resilient Functions simplify development of integrations by wrapping each activity into an individual workflow component.

These components can be easily installed, then used and combined in Resilient workflows.

## Overview

The Genian NAC function contains the ability to apply a tag to a system managed in NAC from the Resilient Platform.

This document describes the Genian NAC function, its customization options, and how to configure it in custom workflows.



## Requirement Product version

Product name	Version	Note
IBM Resilient	3.5	
Genian NAC	NAC-CT64-R-85669-5.0.31.0402 later	Release date 2020.5 after

## Installation

Before installing, the following information regarding Genian NAC should be prepared.:

- The API-Key of Genian NAC's connector
- The IP or URLs info of Genian NAC Policy Center
- The tag Name of Resilient\_enforcement in Genian NAC

### Create API-Key of Genian NAC's connector

Move to 'Management > User', select 'Task > Add User' then create Genian NAC's connector

- Administrator Role: superAdmin
- Click the 'Generate API Key' in General menu

### Validating Genian NAC Policy Center ip information

- Determine the ip address or URL of Genian NAC Policy Center

### Specifying the tag name to be assigned to the node under control.

- Make sure there is no "black". ("\_" is allowed)
- Ex)Resilient\_isolation

### Step 1: installation Genian NAC Resilient-Circuits

**unzip the package and install the resulting .tar.gz via pip**

```
Resilient> pip install pk_genian_nac-1.0.0.tar.gz
```

Modifying config.py

Move to [ ~ pk\_genian\_nac-1.0.0/pk\_genian\_nac/util ]

#### **Edit config.py**

```
nac_server=aaa.bbb.ccc.ddd  
  
api_key=12345678-1234-1234-1234-1234567890ab  
  
tag_name=XXXXXXXXXXXX
```

#### **Applying config.py**

```
Resilient> resilient-circuits config -u
```

note : In the operating same app, just modify setting values, in  
"/home/resadmin/.resilient/app.config".

### Step 2: import the workflows and function

```
Resilient> resilient-circuits customize
```

### Step 3: Run Resilient Circuits

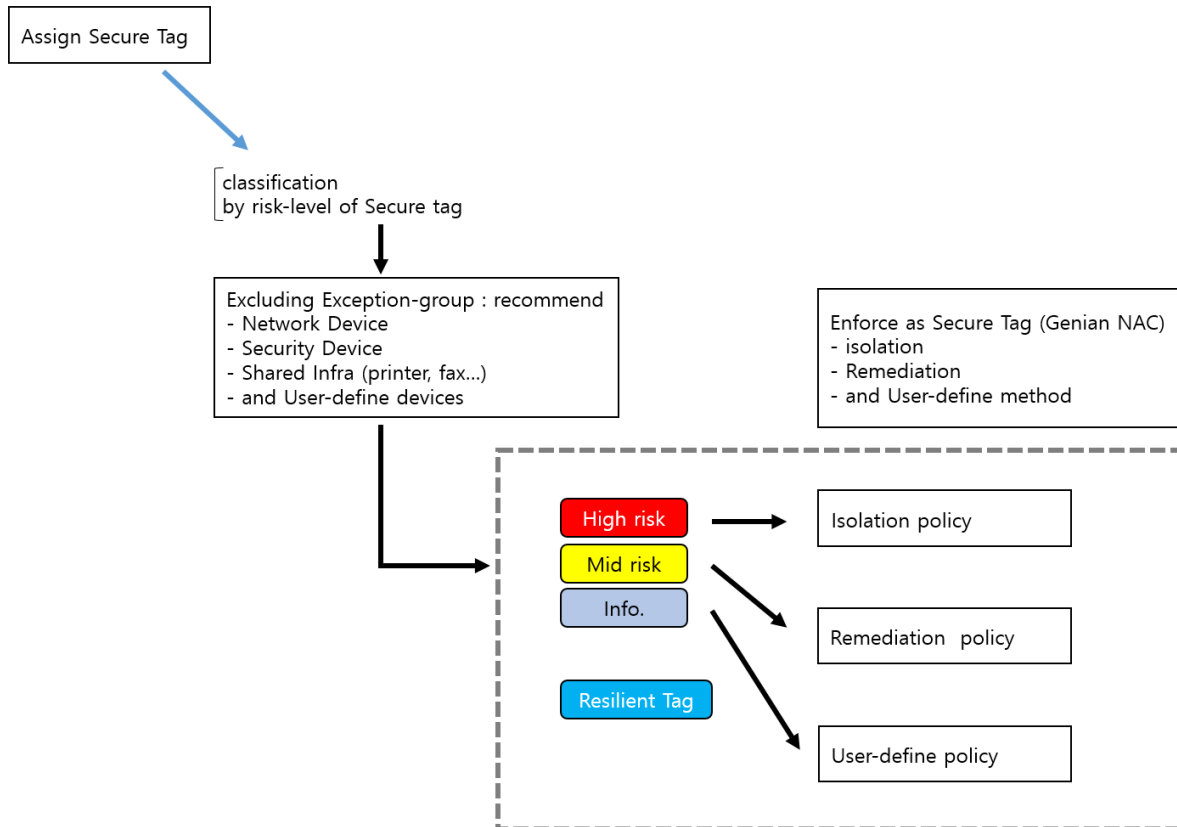
```
Resilient> resilient-circuits run
```

**Installation process completed**

## Test & Using: node isolation

The security manager can control the node in various ways by using the secure tag of the Genian NAC.

Below is a flowchart on which Secure Tag operates on the node.



## Creating Policy using Secure tag

# This chapter is Guide to the establishment of policies for controlling nodes to which Secure tag is applied.

### Step 1: Creating Secure Tag

- Move to 'Preferences > Properties > Tag'
- Click 'Tasks > Create'
- Enter as follows

Cat.	Value	Ref.
Name	<b>Resilient_enforcement</b>	
Description		
Color	<b>Tag's color</b>	
Schedule	<b>Lifetime, 3days</b>	<b>Tag's release time</b>

- Click 'save'

### Step 2: Creating Node group based on Secure tag

- Move to 'Policy > Group > Node'
- Click 'Tasks > Create'
- Enter the General setting values ('ID' is essential)
- Set the condition to the following:

Cat.	Value	Ref.
Criteria	<b>Tag</b>	
Operator	<b>Is equal to</b>	
Value	<b>Resilient_enforcement</b>	

- Click 'save'

### Step 3: Creating policy to isolate nodes

- Move to 'Policy > Enforcement Policy'
- Click 'Tasks > Create'
- Under General enter an ID and Description and set the Status to Enabled.
- Follow the wizard to create a new Enforcement Policy. Select the previously created "Resilient\_enforcement" Node Group, do not select any permissions (all access will be blocked by default)
- enable Captive Portal and enter a message to be displayed to the end user
- With all configurations now in place, the Genians Network Sensor must be switched from Passive to Active mode to facilitate the Layer 2 quarantine of non-compliant nodes on the network. Navigate to System > Sensor > Edit Sensor Settings and set the Sensor Operating Mode to Active then click Update at the bottom of the page



### Step 4: Testing

If you apply Artifacts in Resilient,

1. The Resilient generates a log that Secure Tag is applied.
2. In Genian NAC, the node is classified into the Resilient\_encouragement group.
3. The node is isolated from the network and The CWP(Blocking Information page) appears.

### <Result>

- Genian NAC's log : Tagging and Changed enforcement Policy

Logs						
Logs		Status Logs		 1 Week		 Add filters
						System/License
2020-05-08 12:06:29	Policy	172.29.52.220	172.29.52.180	00:0C:29:2D:E5:84	Enforcement Policy changed. OLD='Default Policy', NEW='Resilient_enforced', BY='Node Information Change'	
2020-05-08 12:06:29	Settings Edited	172.29.52.220	172.29.52.180	00:0C:29:2D:E5:84	Node Tag added. PROPERTY='Resilient_enforcement', RETENTION=2 day(s) 23 hour(s) 59 minute(s) 59 second(s), ADMIN=resilient ADMIN_IP=127.0.0.1	

- Resilient\_enforcement tag applied to 172.29.52.180(Resilient Sent IP)

<input type="checkbox"/>	NT AG SS	Anomaly	Status	Connectivity	IP	MAC	Status	Enforcement Policy	Hostname (Name)
<input type="checkbox"/>					172.29.52.3	AC:1F:6B:66:66:3B		Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.4	44:8A:5B:6A:A2:95	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.30	D0:50:99:3C:38:CC	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.31	00:0C:29:7D:69:8F		Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.32	00:0C:29:8D:F4:A2		Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.35	50:E5:49:A5:87:3B	V6	Default Policy ⓘ	CLIENT-WIN10
<input type="checkbox"/>					172.29.52.50	44:8A:5B:F4:49:6A		Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.100	D0:50:99:5B:CA:32	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.150	08:35:71:12:5B:AF	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.151	08:35:71:12:5C:3B	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.180	00:0C:29:2D:E5:84		Resilient_enforced ⓘ	
<input type="checkbox"/>					172.29.52.200	00:0C:29:D4:5A:14		Default Policy ⓘ	DESKTOP-N8NT90G
<input type="checkbox"/>					172.29.52.201	00:0C:29:B5:6E:DC	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.210	00:0C:29:06:DB:6E	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.220	00:0C:29:D1:38:BD			eth0
<input type="checkbox"/>					172.29.52.220	00:0C:29:D1:38:BD			eth0
<input type="checkbox"/>					172.29.52.252	94:DE:80:CE:40:26	V6	Default Policy ⓘ	
<input type="checkbox"/>					172.29.52.254	1C:AA:07:33:91:52		Default Policy ⓘ	

- Isolated & The CWP(Blocking Information page) appears.

CWP (Captive Web Portal)
172.29.52.220/cwp2/faces/common/design/standard/main.xhtml
English

Node Information IP=172.29.52.180, MAC=00:0C:29:2D:E5:84

Your devices is isolated by Resilient

An Agent is required. Click on "Install Agent" button to install an Agent.

Login required. Please click on "Login" button to login.

Login OK Install Agent Update Status

Notice

No. Title Posted By Posted

No records found.