MS Doc : [Microsoft Sentinel Incident Bi-directional sync with ServiceNow | Microsoft Community Hub](https://techcommunity.microsoft.com/blog/microsoftsentinelblog/microsoft-sentinel-incident-bi-directional-sync-with-servicenow/1667771)

============================================================================

Snow Integration:

IPAAS: using IPAAS integration: using keys and API url’s.

Snow Inc create: Using Data connector: Using snow Instance in customer environment.

Before onboarding any client snow over IPASS,

Inform IPAAS team or snow team of client to configure bidirectional sync.

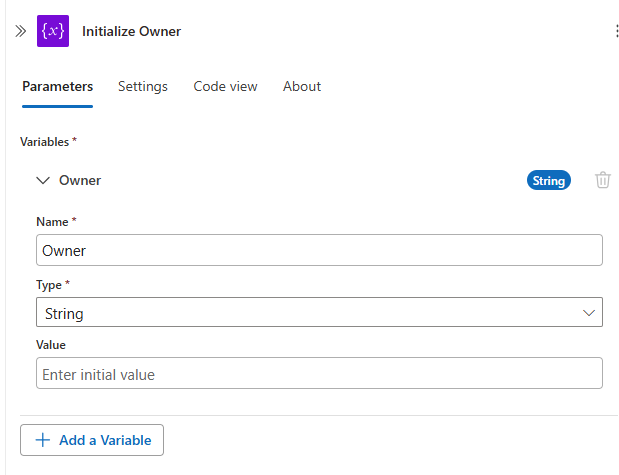
Now they will be asking us endpoint URLs where they will be sending response from Snow, always ask them to implement response fro below scenarios:

* **Business rules:**
* When snow ticket is created
* When snow ticket is updated (Work notes)
* When snow ticket is resolved (resolution notes)
* **To Get Endpoint URL**.,

First create logic app following below steps and after that under “Manual” we can see http URL, copy that and share it as endpoint URL.

**Using IPAAS: (Ex: CreateipassSNOWTicket-ENECO)**

Microsoft sentinel trigger >> initialize required variables >> make a API (HTTP)calls to get API token from client secret.

 A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

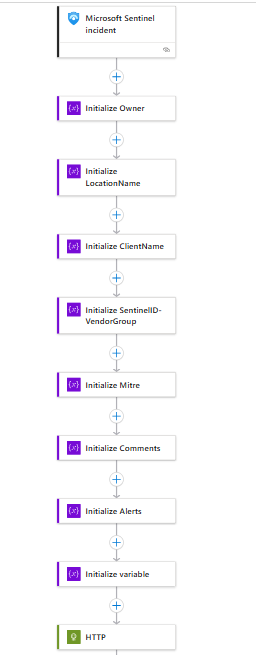
AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.  
To make API call need below details,

**URL for generating token:** get it from any of logic app integrated or from IPAAS team. Under Body copy paste client Id and secret value. (Note: This will just differ from region to region, we can copy if region is same.)

Method: POST.

Now it will generate the API token.

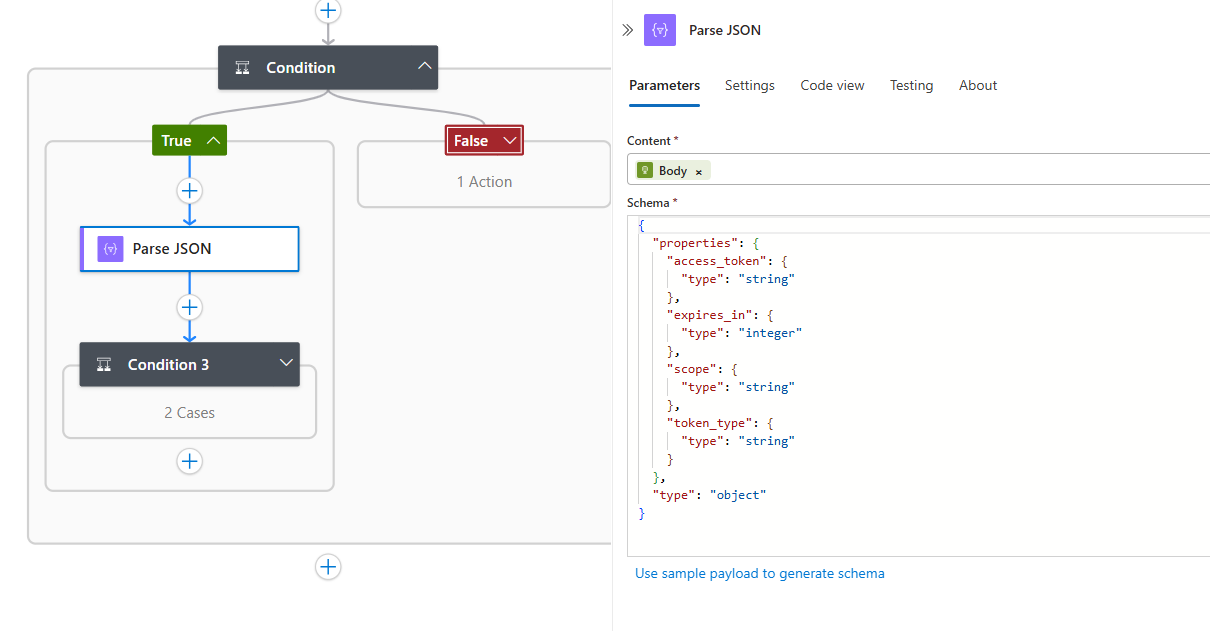
A screenshot of a computer

AI-generated content may be incorrect.

Apply a condition, if API token generated successfully i.e. http=200, then

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Parse the token value.

Now apply condition as Toke Type == bearer, if yes,

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

Now parse all required fields, take those from any existing PB,

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

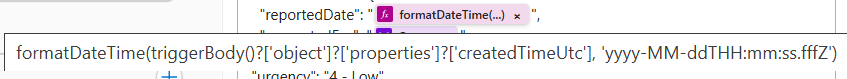
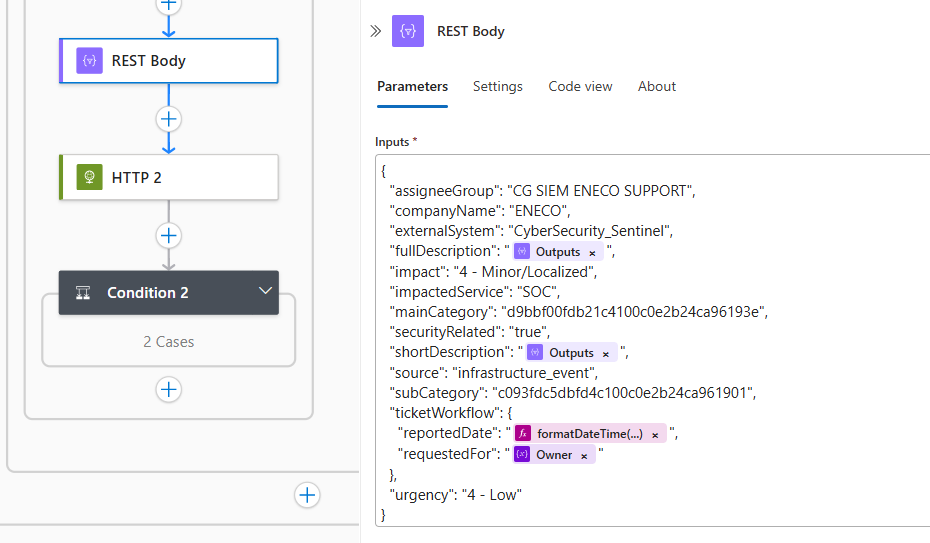
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.



Now make another API call which will be creating the ticket.

Under HTTP,

URL: copy it from any existing PB

Company name: Respective name

UUID: Copy it from existing PB which is in same region

Now the INC is created, parse it and update in sentinel Incident.x

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

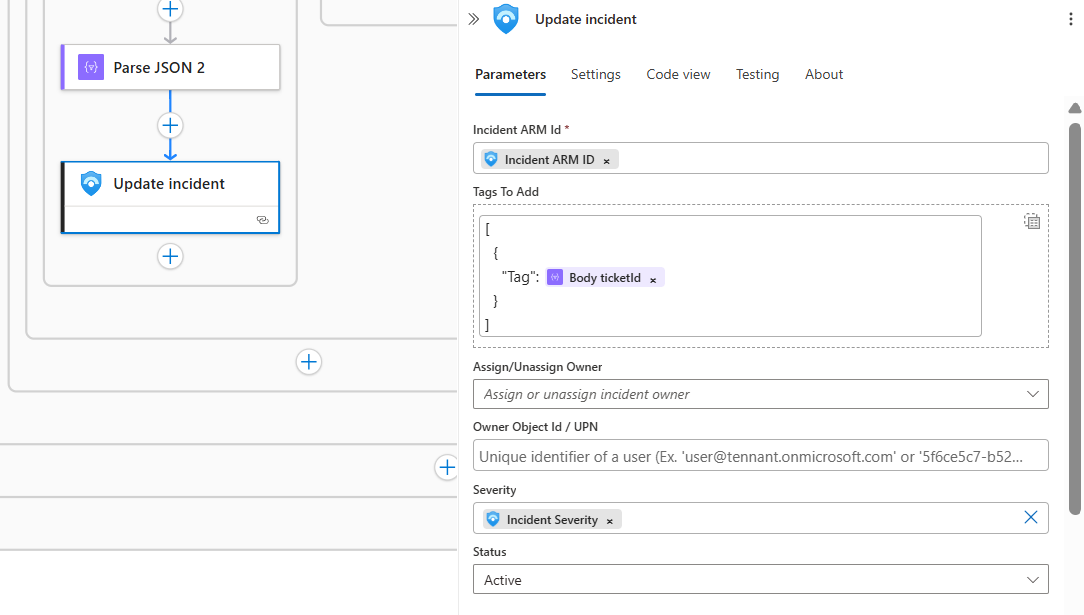
A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

Use the schema below above:





============================================================================**Closing the Incident via Playbooks (Bidirectional Sync):**

**Ex: Close-SentinelIncident-from-SNOW -- refer this.**

To Establish this first get the App registered in Entra ID of Client Environment with relevant permissions (Check Akshay doc for permissions).