



Gisual: Commercial Inbound Webhook Receiver Config Build Document (CBD)

Prepared By:
Dan Tembe
dan.tembe@sciencelogic.com

Date: 01/26/2026

Contents

Glossary of Terms.....	3
Introduction.....	3
Prerequisites & Assumptions:.....	3
Limitations	4
Version Requirements.....	4
Default Template	6
Installation.....	6
Webhook Message Collector Setup	6
Skylar One Setup.....	6
Install & Configure Skylar One PowerPack components	6
Event Policies (2).....	13
Bulk Adding Latitude / Longitude via GQL	14
# To add latitude and longitude to Devices, using DID and GQL	14
# To verify latitude and longitude exists on devices, using DID and GQL.....	15
PowerPack Contents	16
Event Policies.....	16
Run Book Actions.....	16
Run Book Actions Variables:	16
Run Book Automation	17
Execution Environments	17
Sciencellogic Libraries.....	17
Revision History and Approvals	17

Glossary of Terms

Abbreviation	Full Name
AP	Access Point
CDB	Central Database
CLI	Command Line Interface
CU	Collector
CUG	Collector Group
DA	Dynamic Application
DB	Database
DCM	Dynamic Component Mapping
EE	Execution Environment
FQDN	Fully Qualified Domain Name
GA	General Availability
MCU	Message Collector
OOB	Out of Box
PPK	PowerPack
RBA	Run Book Automation
SL	ScienceLogic
UI	User Interface

Introduction

This document is an overview of how to integrate setup Gisual Commercial Power status Powerpack.

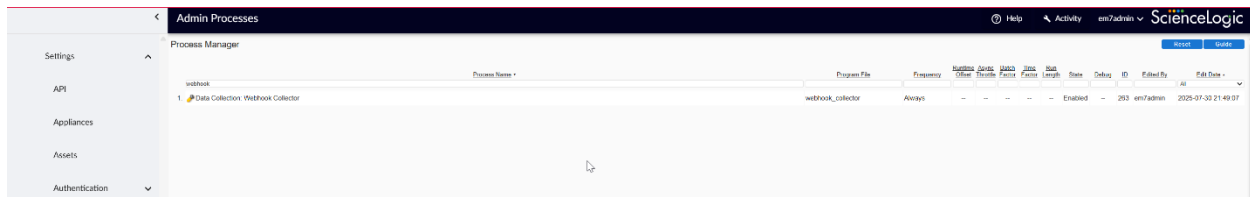
- A webhook handler for receiving alerts from Gisual Commercial Power Status

The objective of this document is to provide the Customer with a list of customer-specific requirements/design configuration settings, custom development specifications and overall architectural depiction. The details in this document cover the work ScienceLogic did during its engagement with the Customer.

Prerequisites & Assumptions:

1. The webhook message collector has a valid TLS (SSL) Certificate, can receive webhooks from external webhook sender (Gisual). The Gisual Webhooks are sent to HTTPS Port (TCP443).
 - Typically, the Network firewall team will help with the collector placement and port access.
 - Similarly, a TLS (SSL) certificate can be obtained and set up under the main domain of the company. For Example: for Sciencelogic (sciencelogic.com) – a subdomain (webhook.demo.sciencelogic.com) was used for TLS (SSL) certificate.
2. The Skylar One Administrator has already set up the message collector and aligned it to appropriate collector groups.

3. The user has already enabled the webhook process, in Skylar One.



4. The user must enable the Webhook configuration on the Message Collector

```
[em7admin@message_collector ~]$ sudo /opt/em7/share/scripts/configure_webhook.py activate
```

Limitations

- The webhook handler will only work for the specified JSON formats supported by Gisual.
- The webhook handler will only work with an active Bearer Token provided by Gisual.

Version Requirements

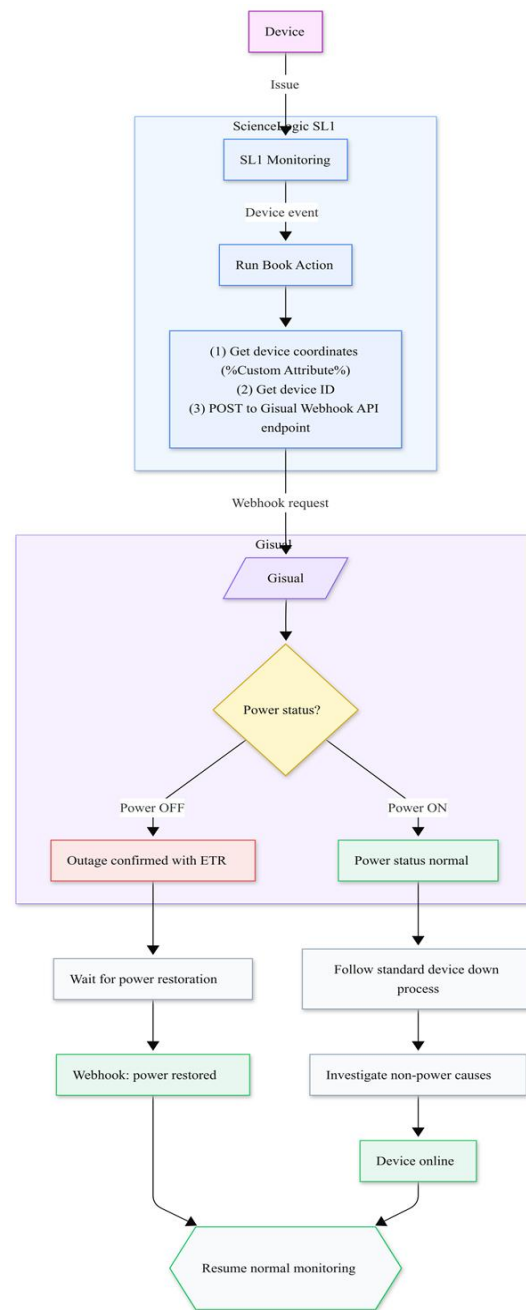
The minimum version for Skylar One is 12.3.2.

Workflow of Gisual Inbound

Webhook Monitored device in SL1 reports a down event (e.g.)

** The automation can be aligned to any active event policy in the runbook automation policy editor.*

- SL1 triggers a Run Book Action aligned to event policy (**or policies*) in Automation Policy Editor.
- Run Book Action queries the device DID and the Custom Attributes (LATITUDE/LONGITUDE)
- SL1 sends an API POST to the Gisual API with the coordinates and DID.
- Gisual evaluates local power conditions and returns one of two results.
 - If power OFF
 - Gisual sends a Webhook to SL1 with this detail (and an ETR)
 - SL1 generates an event – power outage on the device.
 - Gisual sends a updated webhook to SL1 – we then correlate this healthy event to the Critical Power Off even.
 - If power ON
 - SL1 gets a webhook with Power Status On
 - Customer to follow standard device down event resolution path.



Sample Webhook Payloads

Default Template

Gisual Webhook Online KB.

[How to Integrate with the Gisual Power Outage Intelligence Webhook API – Gisual Inc](#)

Installation

Webhook Message Collector Setup

https://docs.sciencelogic.com/latest/Content/Web_Events_and_Automation/Events/event_webhooks.htm

Please follow the directions in the webhook collector documentation to enable a message collector to ingest webhooks from external sources.

Once the message collector is set up, a valid TLS certificate is aligned, and the collector is accessible from the web (this can be limited to specific IP/URL that Gisual is going to be sending the Webhooks from).

Skylar One Setup

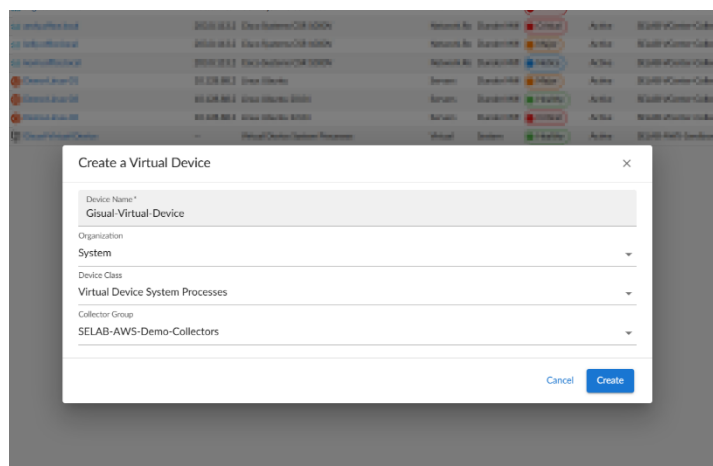
Install & Configure Skylar One PowerPack components

Follow the steps from SL's public documentation [here](#) to import the PPK.

The following Powerpack needs to be Imported and Installed:

1. Import and Install Gisual Commercial Power (webhooks)
2. Create a Virtual Device to align the Webhook Monitor.

Create Virtual Device



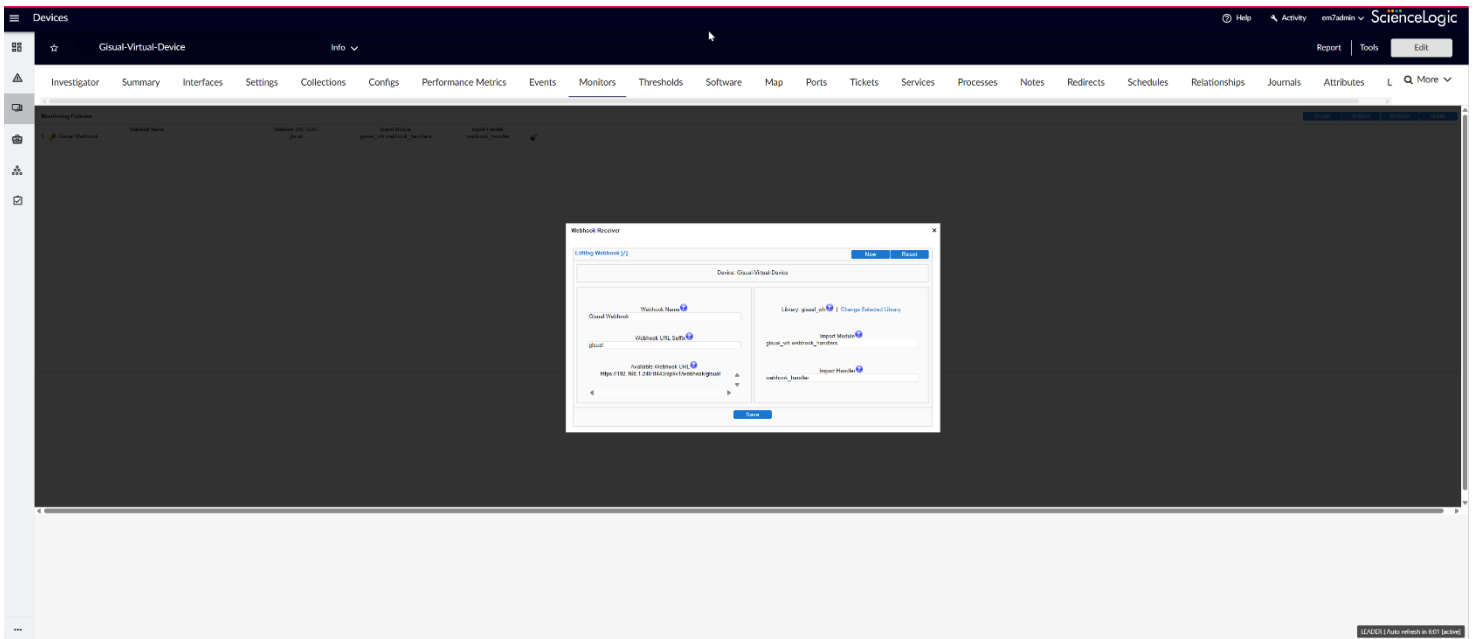
Webhook Monitor requires a device to be aligned to. The steps to align the webhook Monitor are below.

- Navigate to Registry > Devices > Device Manager
- Click Action > Create Virtual Device
- Populate these fields:

- Device Name: Arbitrary text field (make is unique so it is easy to search for later)
- Organization: Choose appropriate organization.
- Device Class: Choose
- Collector: Choose whichever collector group.
- Click “Create”

Create Webhook Policy

The webhook policy requires the user to select the device and the ScienceLogic Library prior to inputting anything into the form.



1. Navigate to Registry > Monitors > Webhooks
2. Click Create
3. Select device (device created in previous section)
4. Select ScienceLogic Library (gisual_wh)
5. Populate fields:
 - a. Webhook Name: Arbitrary text field (*Gisual Webhook*)
 - b. Webhook URL Suffix: Arbitrary text field (*gisual*)
 - c. Import Module: *gisual_wh.webhook_handlers*
 - d. Import Handler: *webhook_handler*
6. Click Save

Testing Webhook Ingestion before configuring Gisual Credential

Look at the port at which you are ingesting webhooks on the collector. This is set up in the Monitoring Policy on Virtual Device that was configured in the previous step.

For example: `https://local_ip_address:8443/api/v1/webhook/gisual`

To test if the webhook ingestion is working locally, the first step is to validate this by using the collector CLI and using curl command. You are looking for a 200 OK.

Command: `curl -k -w "%{http_code}" -X POST https://local_ip:8443/api/v1/webhook/gisual`

```
[em7admin@labsilo240 ~]$ curl -k -w "%{http_code}" -X POST https://192.168.1.240:8443/api/v1/webhook/gisual
200[em7admin@labsilo240 ~]$
```

Next test is to verify the same response (200 OK) is validated from the internet facing / public URL mapped to the webhook collector. And you also want to verify the TLS Certificate is valid.

```
Dashboard Getting Started labsilo220 SL1 12.5.1 - (Juneau - CA) SELAB-Gisual-Message-CU
[em7admin@webhook ~]$ curl -k -w "%{http_code}" -X POST https://webhook.demo.sciencelogic.com/api/v1/webhook/gisual
200[em7admin@webhook ~]$
```

Next Test the SSL Certificate is valid and is on correctly responding. Use the following commands

Command: `curl -k -s -o /dev/null -w "http_code=%{http_code}\ncert_expire=%{ssl_verify_result}\n" --cert-status --verbose https://public_url_webhook_collector/api/v1/webhook/gisual`

```
Capath: none
[5 bytes data]
TLSv1.3 (OUT), TLS handshake, Client hello (1):
[512 bytes data]
TLSv1.3 (IN), TLS handshake, Server hello (2):
[122 bytes data]
TLSv1.3 (IN), TLS handshake, [no content] (0):
[1 bytes data]
TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
[19 bytes data]
TLSv1.3 (IN), TLS handshake, [no content] (0):
[1 bytes data]
TLSv1.3 (IN), TLS handshake, Certificate (11):
[2877 bytes data]
TLSv1.3 (IN), TLS handshake, [no content] (0):
[1 bytes data]
TLSv1.3 (IN), TLS handshake, CERT verify (15):
[520 bytes data]
TLSv1.3 (IN), TLS handshake, [no content] (0):
[1 bytes data]
TLSv1.3 (IN), TLS handshake, Finished (20):
[52 bytes data]
TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
[1 bytes data]
TLSv1.3 (OUT), TLS handshake, [no content] (0):
[1 bytes data]
TLSv1.3 (OUT), TLS handshake, Finished (20):
[52 bytes data]
SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
ALPN, server accepted to use h2
Server certificate:
  subject: CN=webhook.demo.sciencelogic.com
  start date: Dec  2 21:11:32 2025 GMT
  expire date: Mar  2 21:11:31 2026 GMT
  issuer: C=US; O=Let's Encrypt; CN=R12
  SSL certificate verify ok.
No OCSP response received
Closing connection 0
[5 bytes data]
TLSv1.3 (OUT), TLS alert, [no content] (0):
[1 bytes data]
TLSv1.3 (OUT), TLS alert, close notify (256):
[2 bytes data]
http_codes=200
cert_expire=0
[em7admin@webhook ~]$
```

em7admin@webhook ~\$

webhook.demo.sciencel 23:49 12-Dec-25

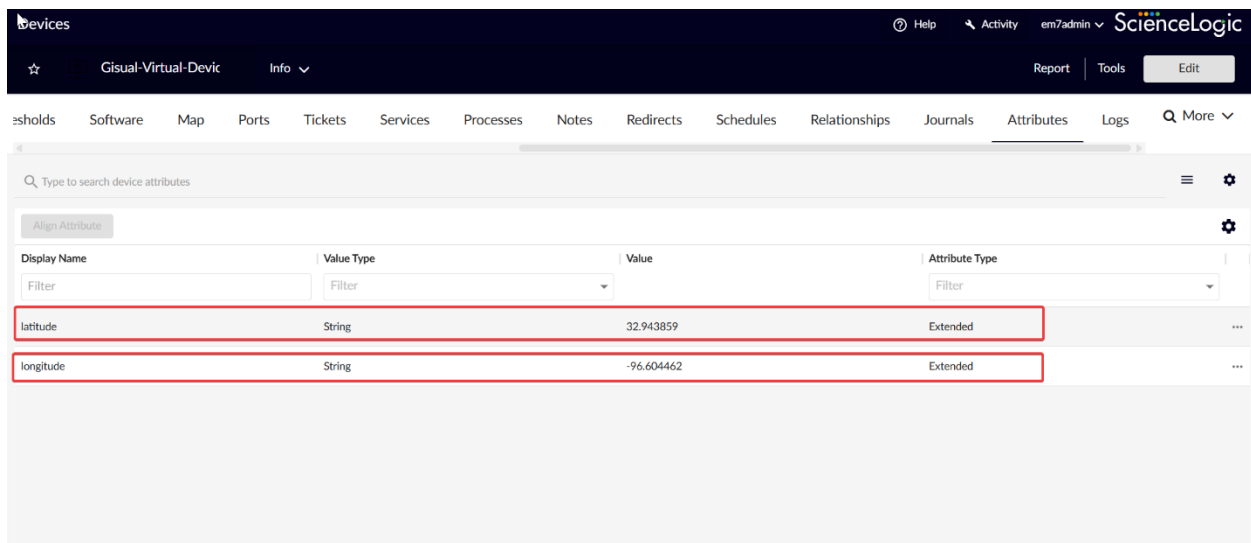
Enabling Devices to send API calls to Gisual.

With all the configuration complete for the Message Collector, you can now proceed to add custom attributes (2) to each device that will trigger an API call to check for power status to Gisual.

These devices require 2 Extended Custom Attribute

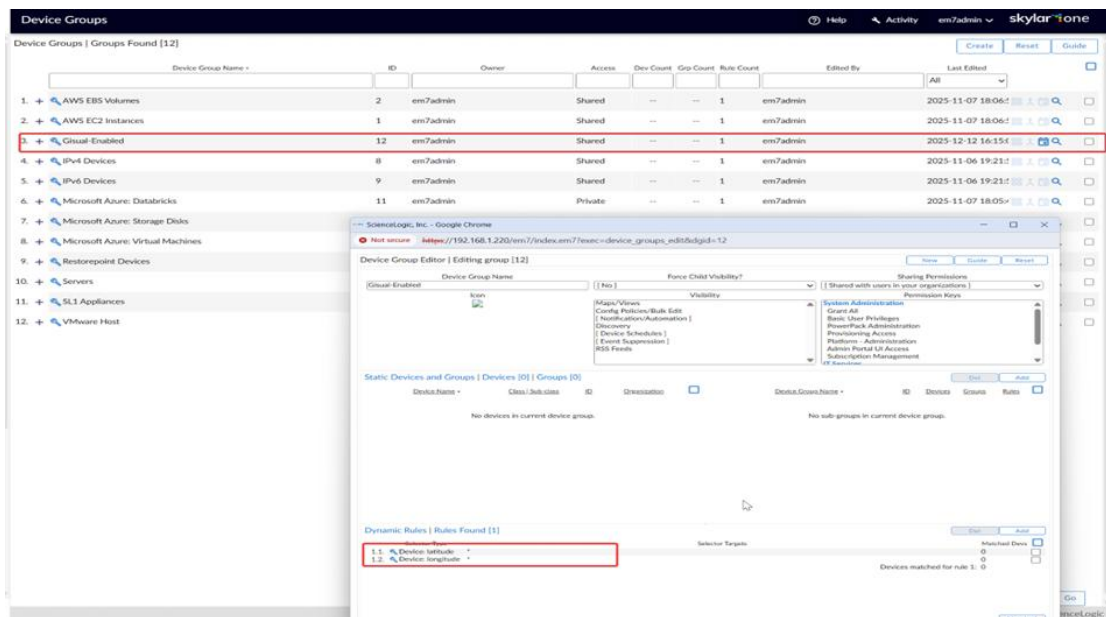
- latitude
- longitude

review below how the values are entered in for each extended custom attribute. It is key that



Display Name	Value Type	Value	Attribute Type
latitude	String	32.943859	Extended
longitude	String	-96.604462	Extended

Devices that will be aligned to “Gisual-Enabled” device group automatically once the “latitude” and “longitude” are aligned to the devices.



Create and align a credential to the Run Book Action

Navigate to Manage > Credentials

Create a new Universal Credential using the reference sample provided with the powerpack. “Gisual-sample” has reference values.

Below values should be added in. Gisual Bearer Token will be provided from Gisual. The Skylar One Callback URL is the public URL for your Webhook Message Collector you setup at the beginning of this setup process.

- Skylar One Callback URL *
- Gisual Webhook URL *
- Gisual Bearer Token *
- Enable Alert Generation
- Timeout (ms)

Edit Credential
×

Name*
Gisual-sample

All Organizations

Select the organizations the credential belongs to*

Skylar One Callback URL*
https://webhook.yourcompany.com/

Gisual Webhook URL*
https://api.gisualdemo.com/v10/inte

Gisual Bearer Token*

Enable Alert Generation
true

Timeout (ms)
1500

Credential Tester

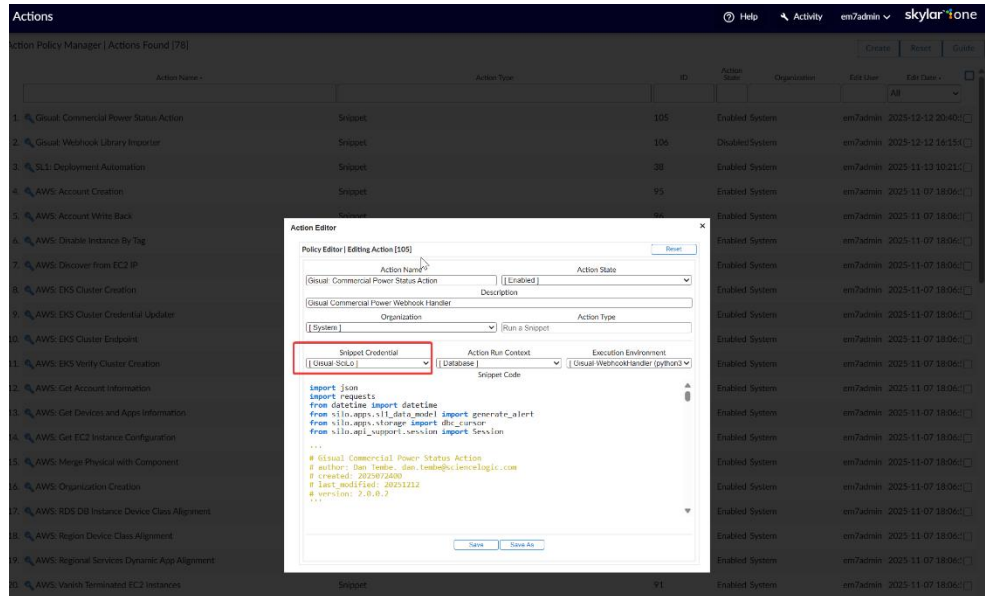
Select Credential Test
CUG | labsilo220.tembe.local: 192.168.1.220

Select Collector
CUG | labsilo220.tembe.local: 192.168.1.220

IP or Hostname to test*

Test Credential

Next step is to align this credential to the Runbook Action provided with the powerpack.



Edit the Automation Policy with correct events.

Edit the Automation Policy provided with the Powerpack and add in all the events you want to trigger an API call to Gisual for Power Status Validation.

Automation

HelpActivityem7admin▼skylarstone

Automation Policy Manager | Automation Policies Found [56]

CreateResetGuide

Automation Policy Name	ID	Policy State	Policy Priority	Organization	Devices	Events	Actions	Edited By	Last Edited	
1. Gisual: Commercial Power Automation	76	Enabled	High	System	1 group	All	1	em7admin	2025-12-12 20:44:...	
2. SL1: Deployment Automation	93	Enabled	Default System					admin	2025-11-13 10:23:...	
3. AWS: Account Creation								admin	2025-11-07 18:06:...	
4. AWS: Disable EBS In								admin	2025-11-07 18:06:...	
5. AWS: Disable EC2 a								admin	2025-11-07 18:06:...	
6. AWS: Disable or Dis								admin	2025-11-07 18:06:...	
7. AWS: Discover EC2								admin	2025-11-07 18:06:...	
8. AWS: EKS Cluster C								admin	2025-11-07 18:06:...	
9. AWS: EKS Cluster C								admin	2025-11-07 18:06:...	
10. AWS: Merge with EC								admin	2025-11-07 18:06:...	
11. AWS: Organization C								admin	2025-11-07 18:06:...	
12. AWS: RDS DB Instan								admin	2025-11-07 18:06:...	
13. AWS: Region Device								admin	2025-11-07 18:06:...	
14. AWS: Regional Servi								admin	2025-11-07 18:06:...	
15. AWS: Vanish Termin								admin	2025-11-07 18:06:...	
16. Microsoft Azure: Dis								admin	2025-11-07 18:05x	
17. Microsoft Azure: Dis								admin	2025-11-07 18:05x	
18. Microsoft Azure: Dis								admin	2025-11-07 18:05x	
19. Microsoft Azure: Dis								admin	2025-11-07 18:05x	
20. Microsoft Azure: Me								admin	2025-11-07 18:05x	
21. Microsoft Azure: Var								admin	2025-11-07 18:05x	
22. Microsoft Azure Data Lake Devices Classification Required	60	Enabled	Default System		All	1	1	em7admin	2025-11-07 18:05x	

Automation Policy Editor | Editing Automation Policy [76]

Policy Name: Gisual: Commercial Power Automation

Policy Type: [Active Events]

Policy State: [Enabled]

Policy Priority: [High]

Organization: [System]

Criteria Logic: [Severity >=] [Critical]

Match Logic: [Text search]

Match Syntax: []

[and no time has elapsed]

[since the first occurrence.]

[and event is NOT cleared]

[and all times are valid]

Repeat Time: [Only once]

Align With: [Device Groups]

☐ Include events for entities other than devices (organizations, assets, etc.)

☐ Trigger on Child Rollup

Available Device Groups: AWS EBS Volumes, AWS EC2 Instances, IPv4 Devices, IPv6 Devices, Microsoft Azure: Databricks, Microsoft Azure: Storage Disks

Aligned Device Groups: Gisual-Enabled

Available Events: [939] Critical: AKCP: AC Voltage sensor detects no current, [948] Critical: AKCP: DC Voltage sensor High Critical, [949] Critical: AKCP: DC Voltage sensor Low Critical, [938] Critical: AKCP: Dry Contact Sensor Low Critical, [944] Critical: AKCP: Smoke Detector Alert!, [942] Critical: AKCP: Water Sensor has detected water

Aligned Events: (All events)

Available Actions: SNMP Trap [1]: SL1 Event Trap, Snippet [5]: Automation Utilities: Calculate Memory Size for Each Action, Snippet [5]: AWS: Account Creation, Snippet [5]: AWS: Account Write Back, Snippet [5]: AWS: Disable Instance By Tag, Snippet [5]: AWS: Discover from EC2 IP

Aligned Actions: 1. Snippet [5]: Gisual: Commercial Power Status Action

SaveSave As

Page | 12

Visual Power Outage Alert: Power Status: power off

Visual Power Outage Alert: Power Status: power on

Event Policy Name
Gisual Power Outage Alert: Power Status: power on
☒ Enable Event Policy

Can be up to 128 characters in length.

CONFIGURING EVENT SOURCE

Choose the source of the events that will determine what SL1 will monitor in order to evaluate whether an event should be created. The string or regular expression entered below will be the content that SL1 looks for in an alert message to evaluate whether an event should be created.

Event Source
API

Type of Match
Regular Expression

Match String (Optional)
^(Gisual Power Outage Alert);(Power Status: power on)

This field is recommended for Syslog, API, and Email and can be up to 512 characters in length. Expression matching in SL1 is case sensitive.

Second Match String (Optional)

If this field is filled out, SL1 will look for alerts that match both strings.

MESSAGE AND SEVERITY

Determine the message and severity of an event created from this policy. The event message can accept variables and regular expressions to denote a part or the entirety of the original source message. The variables (eg: %M) used in the event message field cannot be used to populate other fields.

Event Message
%M

%M will display the original source message within the event message.

Event Severity
Healthy

☐ Use Interface Severity Modifier

TRIGGER FREQUENCY AND EXPIRY

Set the duration after which an event will clear if it does not reoccur. Also, configure the number of matches that SL1 needs to find within a defined time frame in order to generate an event. The fields associated with the checkboxes will be disabled until the checkboxes are selected.

☐ Event Auto Expiration

Expiration Time Frame
0

Unit of Time
minutes

☐ Multiple Matches Required to Trigger Event

Number of Alerts
0

Time Frame
0

Unit of Time
minutes

EVENT POLICY EVALUATION CONFIGURATION

Determine the order in which SL1 will evaluate log messages or alerts against similarly configured Event Policies.

Detection Weight
0

Enter a number between 0-20. SL1 evaluates policies with the lowest detection weight first.

☐ Multimatch: Create events for other Event Policies that match the same alert message

☐ Message Match: Generate separate events if SL1 finds the same alert message on the same device

SUPPRESSIONS

Suppressions prevent events created by this policy from being generated on selected devices or devices belonging to specific device groups.

Configure Suppressions

CONFIGURATIONS FOR EXTERNAL SYSTEM

This section is optional unless you would like to correlate events in SL1 with a third party system. Provide an ID for events generated by this policy so that when they appear in your external system, they can be traced back to SL1. Additionally, if events are being sent to an external system, providing a category will form a grouping of the events generated by this policy.

☐ Correlate events with an external system

External ID

☐ Categorize events with an external system

External Category

TOPOLOGY MASKING

This setting allows the nesting of events under parent devices events if there are parent-child relationships between devices. In order for this setting to work, two configurations need to be made - masking must be enabled on both parent and child devices. Lastly, if event categories are chosen, SL1 will look for maskable events on child and parent devices per category.

Masking
Disabled

Choose Categories

SETTINGS FOR DEVICE SUB-ENTITIES

This section is optional. SL1 can be configured to create events for specific entities like networkOs or interfaces instead of a device by inputting a regular expression that extracts the name of a sub-entity from a log message. The type of sub-entity should also be specified in the y-type field. If there are multiple entities as part of a log message, the order in which events should be created can also be defined. The resulting order can also be used in the event message field.

☐ Extract sub-entity using a Regular Expression

Identifier Pattern

Result order for multiple entities (Optional)

Sub-entity type (y-type)
None

Interface %2 Peer %1

AUTO-CLEAR

Determine if an event created from this policy should automatically clear events created by other chosen event policies

☒ Auto-Clear

Choose Event Policies

☐ Policy Name

☐ Gisual Power Outage Alert: Power Status: power off

Bulk Adding Latitude / Longitude via GQL

Here is a simplified method of adding Latitude and Longitude to a custom attribute via GQL.

To add latitude and longitude to Devices, using DID and GQL

```
mutation alignLatLon_did {
  deviceIDNum: alignCustomAttributes(
    type: device
    entity: 3043 # device ID change
    attributes: [
      { id: "latitude", value: "42.43741" } #Extended Cust Attrib Lat
```

```

        { id: "longitude", value: "-94.33544" } #Extended Cust Attrib Lon
    ]
  ) { __typename }
}

```

To verify latitude and longitude exists on devices, using DID and GQL

```

query checkLatLon {
  device(id: 339 ) {
    id
    name

    latitude: alignedAttribute(id: "latitude") {
      __typename
      ... on CustomStringAttribute {
        id
        label
        alignmentType
        index
        value
      }
    }

    longitude: alignedAttribute(id: "longitude") {
      __typename
      ... on CustomStringAttribute {
        id
        label
        alignmentType
        index
        value
      }
    }
  }
}

```

PowerPack Contents

Name	Version	Revision
Gisual Commercial Power (webhooks)	1.5	26

Event Policies

Name	Severity	Notes
Gisual Power Outage Alert: Power Status: power off	Critical	This is the initial event from Webhook we receive if Commercial Power is offline at a specific location.
Gisual Power Outage Alert: Power Status: power on	Healthy	This is the update event from Webhook we receive when Commercial Power restored. This policy auto-clears the above power off event.

Run Book Actions

Name	Notes
Gisual: Webhook Library Importer	Dummy RBA to import webhook library
Gisual: Commercial Power Status Action	This Runbook Action is aligned in the Automation Policy which "POST" to a Gisual Webhook API Endpoints and starts the Gisual workflow for power status check.

Run Book Actions Variables:

The Gisual Runbook Action has 4 variables that are configured either using the universal credential or changing the values in the Action Snippet.

Gisual API Configuration Variables.

Prod

```
SL1_CALLBACK_URL = 'https://webhook.company.com/api/v1/webhook/gisual'
GISUAL_TOKEN = 'Bearer 'Token-From-Gisual'
GISUAL_WEBHOOK_URL = 'https://api.gisual.com/v10/intel/wh' # Different for Prod/Demo
DEFAULT_TIMEOUT = 30 #seconds
ENABLE_ALERTS = 'true' # Convert string to boolean - true/false
```

Demo

```
SL1_CALLBACK_URL = 'https://webhook.company.com/api/v1/webhook/gisual' # Different for Prod/Demo
GISUAL_TOKEN = 'Bearer 'Token-From-Gisual'
GISUAL_WEBHOOK_URL = 'https://api.gisualdemo.com/v10/intel/wh' # Different for Prod/Demo
DEFAULT_TIMEOUT = 30 #seconds
ENABLE_ALERTS = 'true' # Convert string to boolean - true/false
```

SL1 Callback URL for webhook notifications

```

SL1_CALLBACK_URL = EM7_ACTION_CRED['callback_url']
GISUAL_TOKEN = 'Bearer ' + EM7_ACTION_CRED['api_token']
GISUAL_WEBHOOK_URL = EM7_ACTION_CRED['webhook_url']
DEFAULT_TIMEOUT = int(EM7_ACTION_CRED.get('cred_timeout', 30000)) / 1000.0
ENABLE_ALERTS = EM7_ACTION_CRED['enable_alerts'].lower() == 'true' # Convert
string to boolean

```

Run Book Automation

Name	Notes
Gisual-Dummy-Env-Importer	OPTIONAL - Dummy Automation Policy, enable and run one time to import the Gisual Webhook Library to the specific message collector.
Gisual: Commercial Power Automation	REQUIRED – Aligned to Device Group: Gisual-Enabled Dynamic Alignment: Extended Attributes - latitude - longitude

Execution Environments

Name	GUID	Env Type	Lib Count
Gisual-WebhookHandler	C5FFB90E7A443E3AE6AC3B872CF0E1C4	py3	3

Sciencelogic Libraries

Name	Version	Python Version	Notes
gisual_wh	1.1.5	3.6	Gisual Webhooks Inbound Handler
silos_api_support	0.1.4	3.6	Library to access SL1 APIs
silos_apps	3.6.9	3.6	Library of tools for building Snippet Dynamic Apps

Revision History and Approvals

This section lists the revisions made to this document, revision number and revised date, that will track changing information during the project's life cycle. The approval section will list the key stakeholders who have approved the document at a certain point. If several rounds of approval are required due to changing information, it will list several rows of approvals with different dates.

Revision Number	Revision Date	Revision Description
DRAFT Rev 1.0	09/09/2025	ScienceLogic drafted initial document version for Sciencelogic Sales Engineering Team review and update.
Revision 1.1	12/12/2025	Updated with new PPK version, troubleshooting and configuration details.

Revision 1.2	01/07/2026	Fixed incorrect library name in configure webhook policy topic. Added in GQL helper snippets for adding latitudes and longitudes. Added RBA variables.
Revision 1.3	01/26/2026	Corrected the Powerpack Version.