

Industrial IoT with HALO Smart Sensors using TCP

Integration guide

Unification Group
May 2023

Genetec™

Contents

HALO SMART SENSOR – Event identifiers and sensor identifiers ...	2
Instructions.....	3
1. HALO SMART SENSOR – Configuration of Device Name.....	3
1.1 Set up Device Name.....	4
2. HALO SMART SENSOR – Configuration for External Messaging and Heartbeat	5
2.1 Set up Primary Integration.....	6
2.2 Set up Heartbeat.....	7
3. HALO SMART SENSOR – Configuring actions	8
4. GENETEC CONFIG TOOL – Industrial IoT plugin configuration	9
4.1 Create an Industrial IoT plugin instance	9
4.2 Create and configure a TCP server.....	10
5. GENETEC CONFIG TOOL – Configuration devices from device type	11
5.1 To import the preconfigured device type for HALO sensors:	12
5.2 Adjust imported rules:	13
5.3 Create a device using the Device types	14
6. GENETEC CONFIG TOOL – Optional configuration	15
6.1 Adding a camera to the HALO device	15
6.2 Adding HALO Dashboard as a camera (Optional)	16
6.3 Customizing configuration (if required).....	17
Operations	19
Monitoring Maps	19
Monitoring Events	19
Monitoring Dashboard	20
Reporting	20
Appendix	21

Integration guide for HALO SMART SENSOR devices with Industrial IoT plug-in

Introduction

The HALO Smart Sensors can be integrated into Genetec Security Center Video Management Software. This integration requires the Genetec Industrial IoT plugin to be installed and licensed. See [Genetec Industrial IoT Plugin Guide 5.0.2](#) for installation and setup instructions.

The Industrial IoT plugin allows data transmission to Security Center through different transmission protocols. In this guide, data is sent from the HALO device to Security Center through Transmission Control Protocol (TCP).

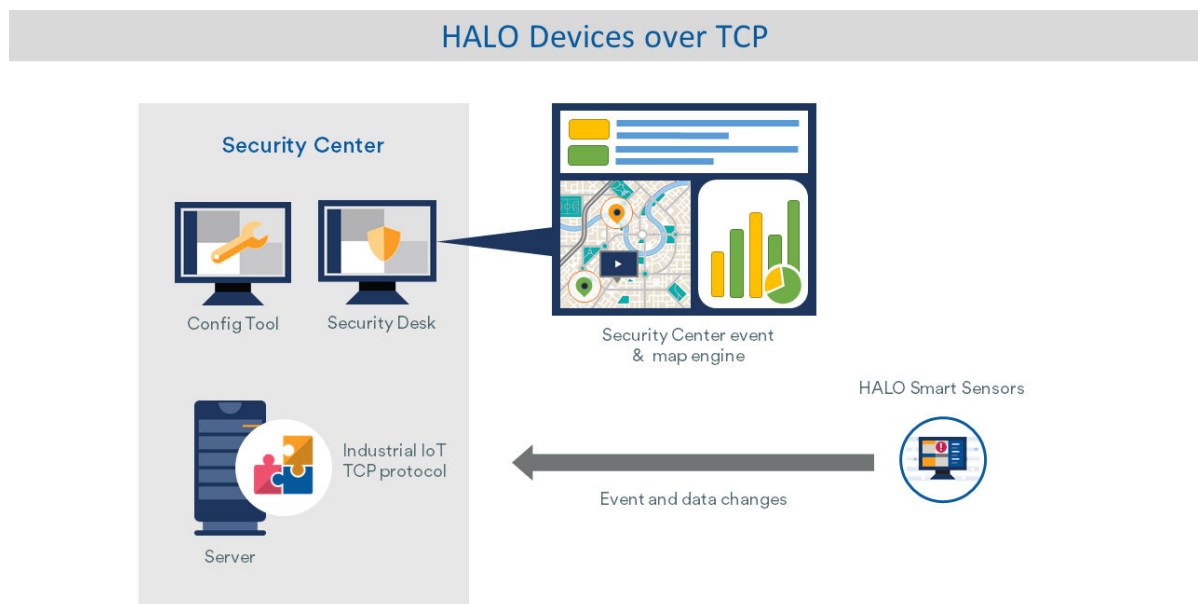


Figure 1

HALO sensors can send information to the Genetec Industrial IoT plugin in two ways:

Events – specific trigger conditions can be set on the HALO device web page for one or multiple types of measurements collected by the sensor. When these conditions are met, the device raises an event in Security Center and sends the value that was measured at the time of the event. This allows the user to verify if the triggered event was intentional. Raised events can be set to trigger alarms by configuring rules.

Note: Using events does not allow for Security Center to display a history of the measurements recorded by the HALO device. However, the use of events minimizes the amount of data that must be transmitted to Security Center.

Data points – HALO devices can send measurements at pre-determined intervals to Security Center through data points. Data points make it possible to display a graphical representation of the HALO device’s measurements. Measurement thresholds can be set to trigger alarms by configuring rules inside Security Center.

Starting with the Industrial IoT plugin version 5, data points are no more limited by licence.

Note: This integration was tested using version **5.11.1** of Genetec Security Center and **IIoT 5.0.2** with HALO Smart Sensor models 2C and 3C running **2.8.1** firmware.

HALO SMART SENSOR – Event identifiers and sensor identifiers

Event identifiers are used to identify events collected by the HALO sensor through Security Center events. They can be set or changed in the **Events** tab of the HALO configuration web page (see Figure 2).

Sensor identifiers are used to identify specific measurements collected by the HALO sensor through Security Center data points. Their names cannot be reconfigured. Refer to [Table 1](#) for a complete list of sensor identifiers.

Note: If an event identifier matches a sensor identifier, setting up a data point and an event with these identifiers will create an issue: The event’s data will be overwritten every time the data point receives data. To fix this issue, change the event identifier on the HALO device webpage so it does not match any sensor identifier, then change the regular expression of the Security Center event accordingly.

Events ×

Event Identifier	Data Source	Threshold	Pause	UID	
Aggression	Aggression	20	0		Advanced Test
Gunshot	Gunshot	50	0		Advanced Test
Help	Keyword 1 Keyword: Help Emergency	50	0		Advanced Test
Masking	PM10 (10 µm particulates) µg/m³	35	0		Advanced Test
Tamper	Move (mm/100)	1400	0		Advanced Test
THC	PM10 (10 µm particulates) µg/m³	35	0		Advanced Test
Vape	PM10 (10 µm particulates) µg/m³	35	0		Advanced Test

Save Changes Close

Figure 2

Instructions

1. HALO SMART SENSOR – Configuration of Device Name

The **Device Name** will be used as the unique identifier for this integration. This is the value that will be used automatically by the HALO device to replace %NAME% in the integration configuration.

- a) Log into the HALO Smart Sensor configuration web page and click on the **Device** tab.

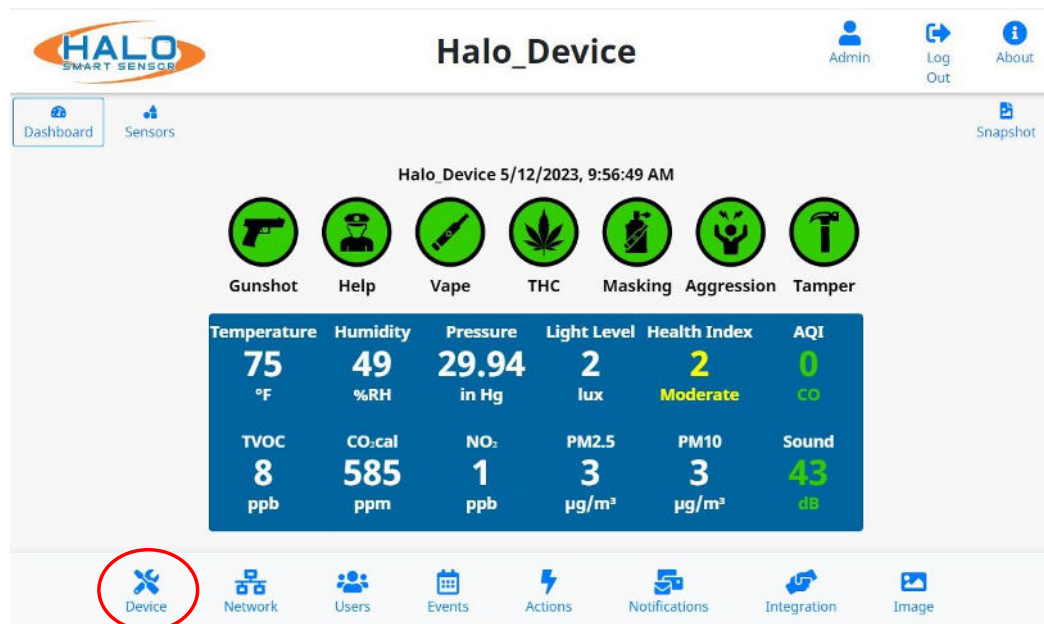
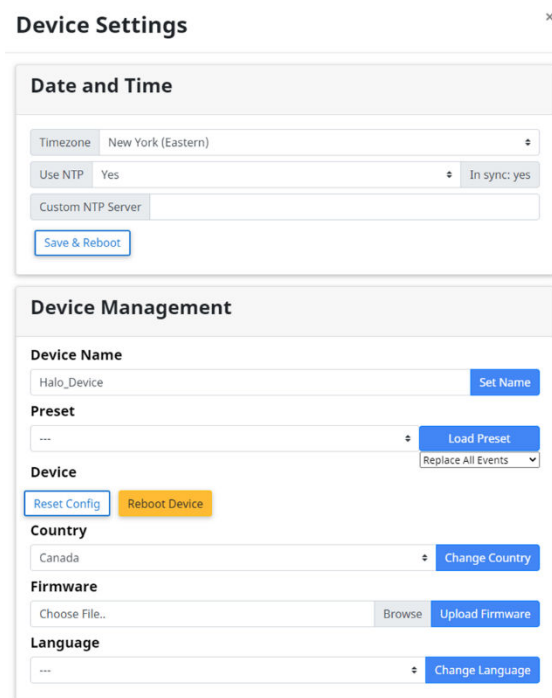


Figure 3

1.1 Set up Device Name

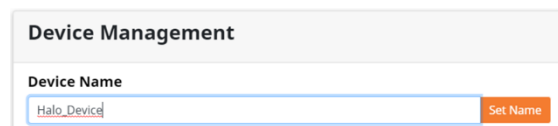
In the **Device Settings** page:



The screenshot shows the 'Device Settings' window with two main sections: 'Date and Time' and 'Device Management'. The 'Date and Time' section includes a 'Timezone' dropdown set to 'New York (Eastern)', a 'Use NTP' toggle set to 'Yes', and an 'In sync: yes' status. The 'Device Management' section contains several fields and buttons: 'Device Name' with the text 'Halo_Device' and a 'Set Name' button; 'Preset' with a dropdown menu and a 'Load Preset' button; 'Device' with 'Reset Config' and 'Reboot Device' buttons; 'Country' with a dropdown set to 'Canada' and a 'Change Country' button; 'Firmware' with a 'Choose File...' button and an 'Upload Firmware' button; and 'Language' with a dropdown menu and a 'Change Language' button.

Figure 4

- Access the **Device Management** section.
- Type in the desired name ("Halo_Device" in this example) in the **Device Name** text field.
 - It must be unique (within your installation).
 - Made of one or more characters without any spaces.
 - Will be used as **Device ID** in the IIoT plugin later.




This close-up shows the 'Device Management' section with the 'Device Name' field containing the text 'Halo_Device' and an orange 'Set Name' button to its right.

Figure 5

- Click the **Set Name** button.
- At a minimum, load the **Security** pre-set by selecting **Security** in the Preset combo box and pressing **Load Preset** button.

Preset



The screenshot shows the 'Preset' dropdown menu with 'Security' selected and a 'Load Preset' button to its right.
- Close the **Device** tab (either click to **X** in the top right or use the **Close** button at the bottom)

2. HALO SMART SENSOR – Configuration for External Messaging and Heartbeat

The following configuration allows for both types of data collection to be used (events and data points). The External Messaging dialog box is used to send data to trigger events, whereas the Heartbeat dialog box is used to send data to create a data point.

- a) Log into the HALO Smart Sensor configuration web page and click on the **Integration** tab.

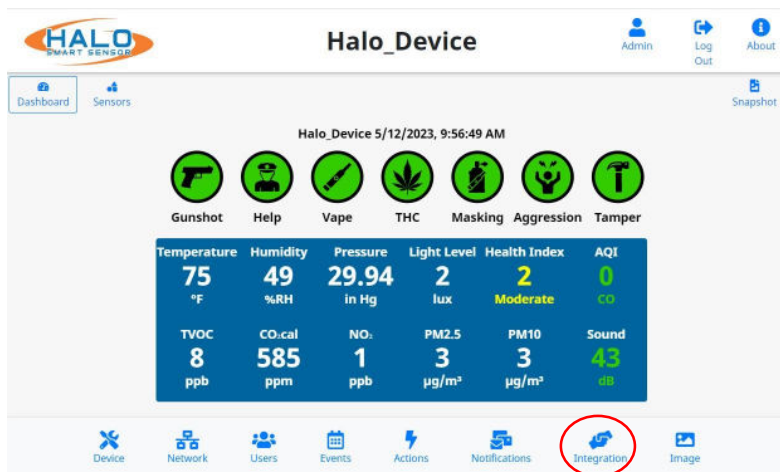


Figure 6

2.1 Set up Primary Integration

In the Integration tab:

- In the **Primary Integration** section, Select **Genetec** in the **Integration Partner** drop down list.
- In the **Address** box, set the text field to the IPv4 (Internet Protocol Version 4) address of the machine where the IIoT plugin is installed.
- In the **Port** box, set to an unused port of the machine where IIoT plugin is installed. It will need to match the port of the TCP server defined later.

Note: TCP connections are identified by a source port and a destination port. If several HALO devices need to be connected to Security Center, they can all use the same port, which means a single TCP server is enough for multiple HALO devices.

- Click the **Save** button.

Primary Integration

Integration Partner: --- Apply Settings ---

Protocol: ☒ TCP ☐ HTTP Repeat Holdoff: 5 sec

Set String: DeviceId=%NAME% %EID%=true; ☒ On ☐ Off

Reset String: DeviceId=%NAME% %EID%=false; ☒ On ☐ Off

Above you can use:

%NAME% - device name	%THR% - event threshold	%FWVER% - firmware version
%IP% - ip address	%VAL% - sensor value	\\ - 1 back slash
%MAC% - mac address	%DATE% - local date of event	\n - new line
%EID% - event id	%TIME% - local time of event	\r - carriage return
%SOURCE% - data source	%PSWD% - password	\u#### - hex char code
	%USER% - user	More

Address: 172.16.10.191 Port: 5000

[Save](#) Status: OK

Figure 7

2.2 Set up Heartbeat

- Scroll down to the Heartbeat window.
- In the **Heartbeat** section, Select **Genetec** in the **Integration Partner** drop down list.
- In the **Address** box, set the text field to the IPv4 (Internet Protocol Version 4) address of the machine where the IIoT plugin is installed.
- In the **Port** box, set to the same port as previously entered in **Primary Integration** section.
- Click the **Save** button.

Note: The **Interval** field sets the interval at which the HALO sensor will send data to Security Center. It can be lowered to collect more measurements within a certain period or increased to lighten the load of data Security Center must process.

Heartbeat

Integration Partner: Genetec

Protocol: ☒ TCP ☐ HTTP

Message: DeviceId=%NAME% %ALLSENSORS@% On ☒ Off ☐

Above you can use:		
%NAME%	- device name	%EVENTS%
%IP%	- ip address	%EVENTVALS%
%MAC%	- mac address	%ACTIVE%
%FWVER%	- firmware version	%SENSOR:id%
		%DATE%
		%TIME%
		\\
		\n
		\r
		\u####

Interval: 60 sec Address: 1.2.3.4 Port: 5000

[Save](#) Status: OK

☐ Heartbeat Email

Figure 8

3. HALO SMART SENSOR – Configuring actions

- a) From the HALO device configuration main web page, click on the **Actions** tab.

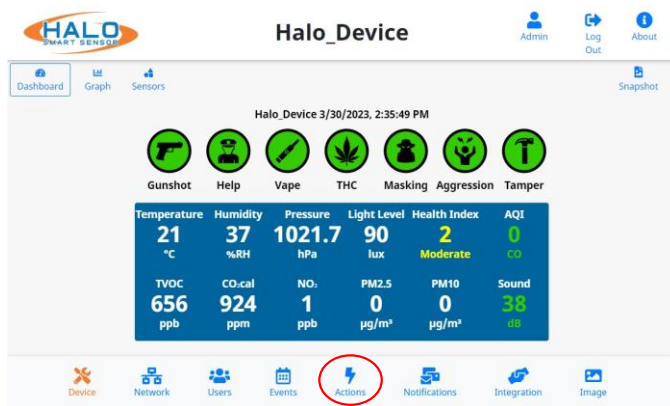


Figure 9

- b) Check the **Primary Integration Set** and **Reset** checkboxes for each of the event identifiers.
- c) Click the **Save** button at the bottom right of the screen to save settings.

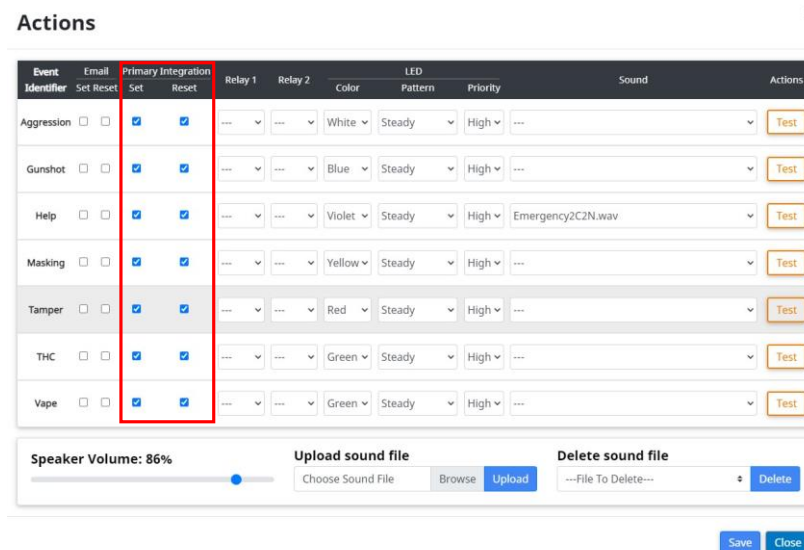


Figure 10

4. GENETEC CONFIG TOOL – Industrial IoT plugin configuration

4.1 Create an Industrial IoT plugin instance

- Log on Config Tool using your administrator credentials.
- In the **Tasks** tab, in the **Administration** section, click on the **Plugins** icon.

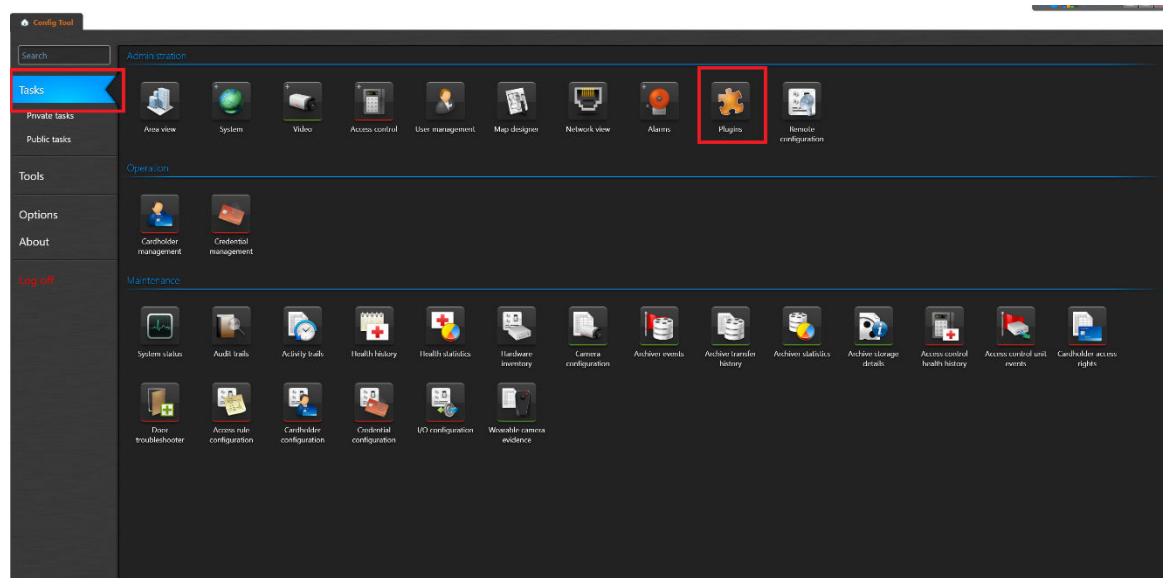


Figure 11

- In the plugins tab, click on the **green plus button** at the bottom left of the screen and select the **Plugin** option.
- In the pop-up window, select the **Industrial IoT** plugin type. The Database server field and database field should be filled in by default. You can rename the plugin in the **Basic Information** tab if needed. Otherwise just click **Next** and finish creating the role.

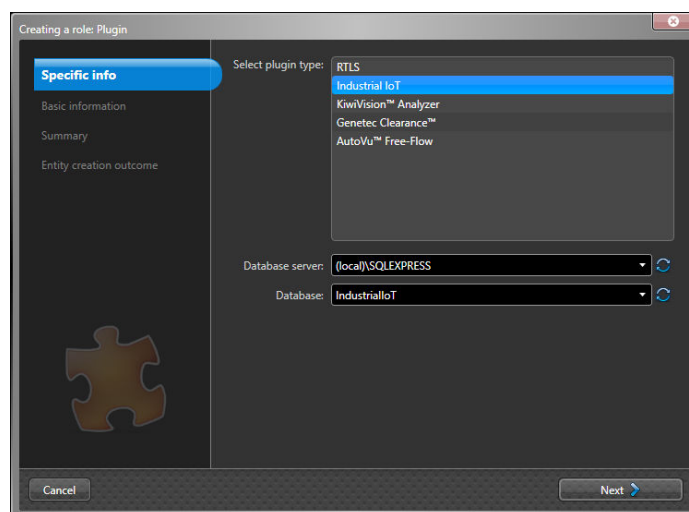


Figure 12

4.2 Create and configure a TCP server

- Select your plugin instance in the tab on the left-hand side of the screen.
- Select the **Protocols** tab.
- Select **TCP Server**
- Click on the **green plus button** at the bottom of the **TCP Servers box** to add a TCP server.
- In the **Name** text field, enter a name for the server (In this example, it is HALO).
- In the **Port** text field, enter the port number established earlier on the HALO device configuration web page.
- Select **String** in the **Message delimitation method** combo box.
- In the **End of message delimiter** text field, enter “;” (without quotes).

Note: The **Type** field should be set to “plain text” and the **Encoding** field should be set to “UTF-8”. There is no need to change the value of these fields.

- Uncheck the Create a device automatically box. The field Device ID regular expression should appear.
- Enter the following String in the **Device ID regular expression** field:

DeviceId=(\S+)

Note: It must be entered “as is”. Capitalization and extra space could render the integration to fail.

- Click on the **Apply** button at the bottom right of the screen.

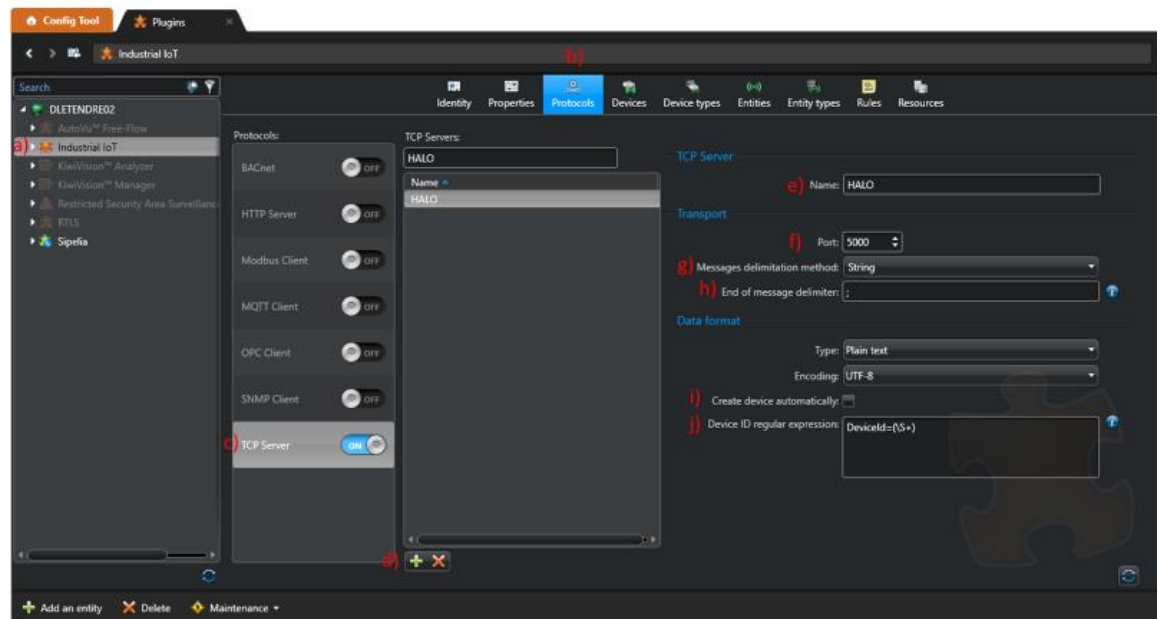


Figure 13

5. GENETEC CONFIG TOOL – Configuration devices from device type

Industrial IoT plugin comes with predefined type that can be easily imported. It is still possible to import and export configuration pre-sets for a device type through JSON files. Make sure you use the appropriate JSON file for your version of IIoT. These settings can include data point, event, custom state configurations and rules configured with that device type.

Note: When a device type is imported, its rules will create a warning on the Industrial IoT plugin. The reason why this happens is because the **alarm** and **event** fields of each rule will be empty. The rules therefore need to be linked to the alarms and events of your choice for the warning to disappear.

Note: The HALO device configuration pre-set provided by Genetec contains regular expressions (regex) which refer to event identifiers from a HALO device (ex. "Vape", "Noise", "Aggression"). These event identifiers might not match the ones on your own HALO devices. You can edit regular expressions in each event and data point of the device type (Config Tool) or edit the event identifiers of each HALO device (HALO config web page) to make the regular expressions and event identifiers match. The provided template includes 36 data points and 7 events.

5.1 To import the preconfigured device type for HALO sensors:

- a) Open the Config Tool app and login with administrator credentials.
- b) Click on the **Plugins** task.
- c) Select the **Industrial IoT** plugin instance on the left-hand side of the screen.
- d) Click on the **Device Types** tab.
- e) Click on **import**, select **TCP_HALO_FW_2_8_1_DeviceType_v5_0_2.json** file, and click **Open**.

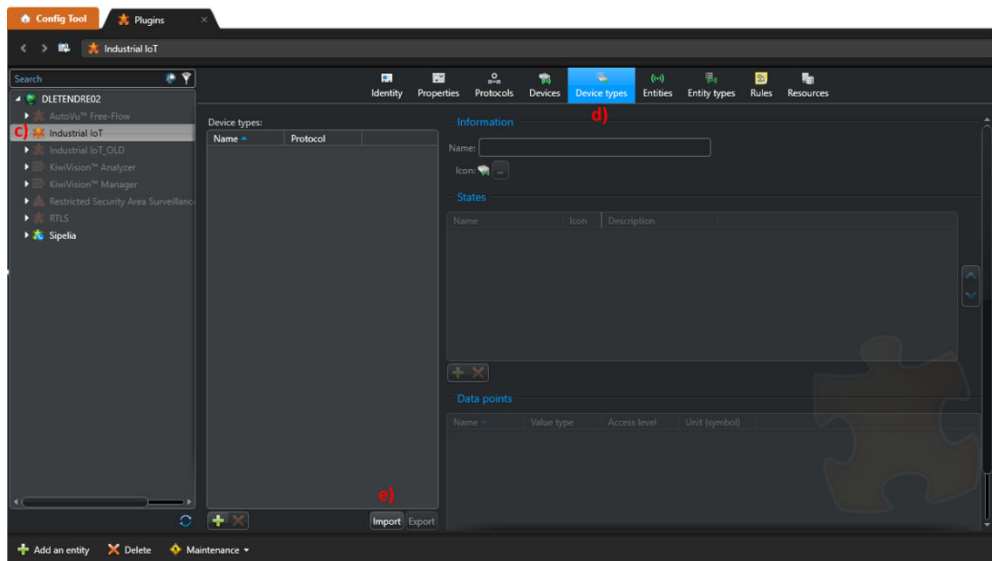


Figure 14

- g) Click **OK**.

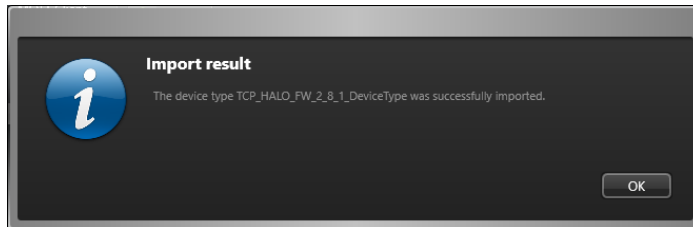


Figure 15

5.2 Adjust imported rules:

As mentioned previously, the Industrial IoT will generate “Warnings” as imported rules will need to be re-attached to events and alarms present in your system. First you need to define the required custom event and alarms. In this example, 1 event is used for monitoring and 9 different alarms are used.

- a) Access the **Rules** tab. Rules with a “Warning” condition will appear in yellow color.

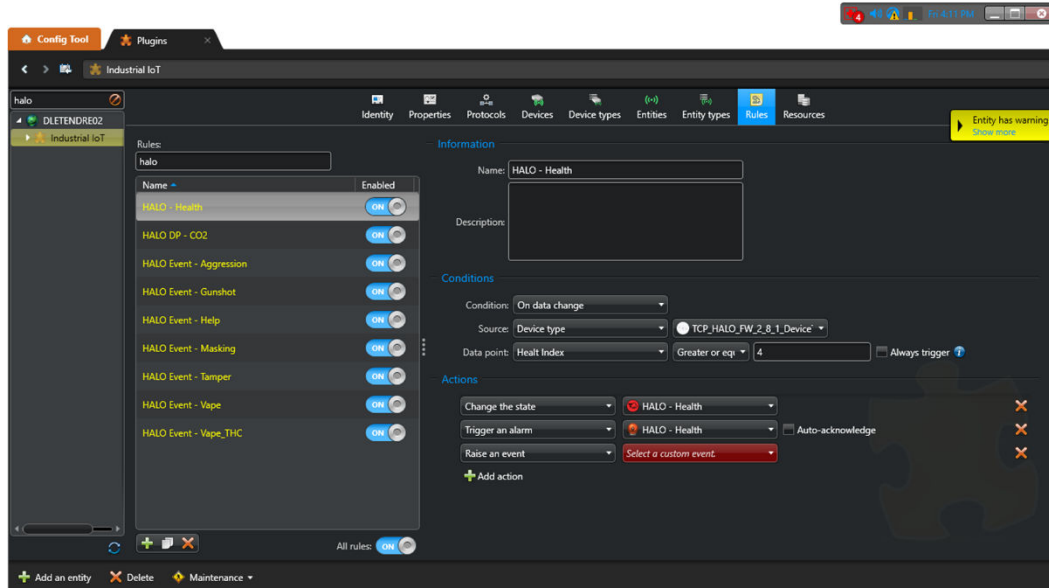


Figure 16

- b) Select each rule and assign the appropriate event and alarm.
 c) Once completed, the adjusted rule will turn white. When all rules have been adjusted, the “Warning” will disappear.

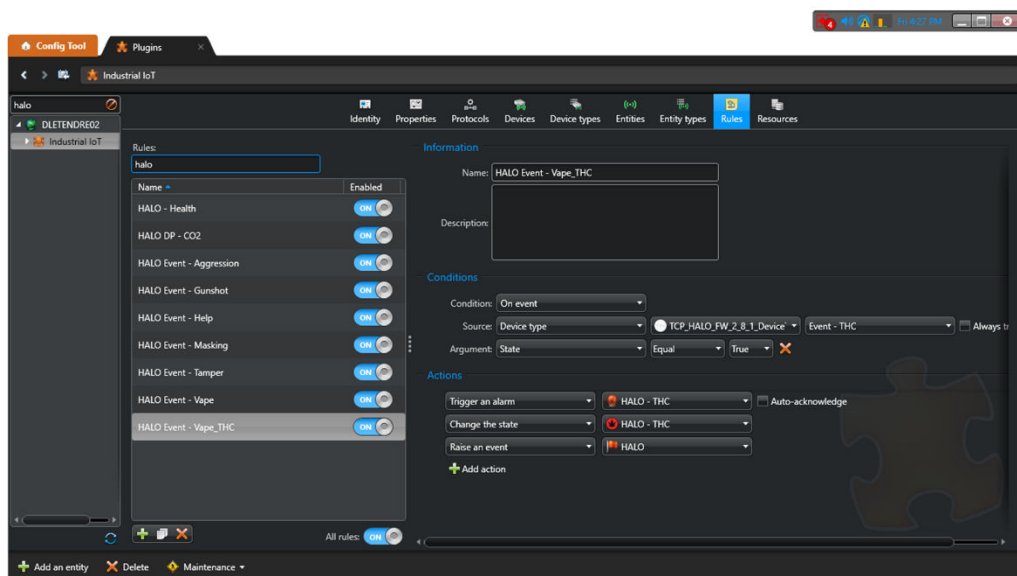


Figure 17

5.3 Create a device using the Device types

- a) Select the **Devices** tab.
- b) Click on the **green plus button** at the bottom of the screen to add a device.
- c) In the **Name** text field, enter a name for the device (In this example, it is "Halo_Device").
- d) The **Type** field select **TCP_HALO_FW_2_8_1_DeviceType**.
- e) In the **Protocol** field, select **TCP Server**.
- f) The **TCP Server** field should appear. Select the server that was previously created (in this example, it is "HALO").
- g) The **Device ID** field should appear. Enter the Halo device ID number that was previously chosen on the HALO configuration web page (in this example, it is Halo_Device).
- h) Click on the **Add** button.
- i) Click on the **Apply** button at the bottom right of the screen.

The device is now created and can be selected under the instance of Industrial IoT on the left-hand side of the screen.

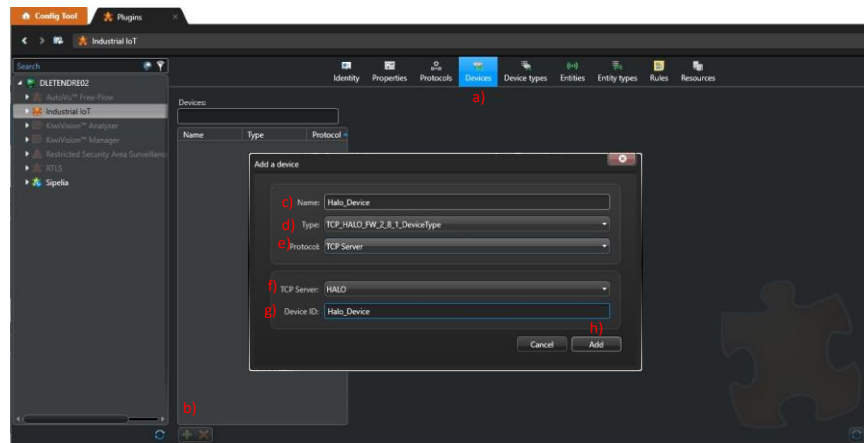


Figure 18

Note: Depending on the HALO model you have some data points (INP, Motion and PEOPLE) might not receive value, it is normal

6. GENETEC CONFIG TOOL – Optional configuration

6.1 Adding a camera to the HALO device

- a) Select the appropriate device in the tree view in the left section.

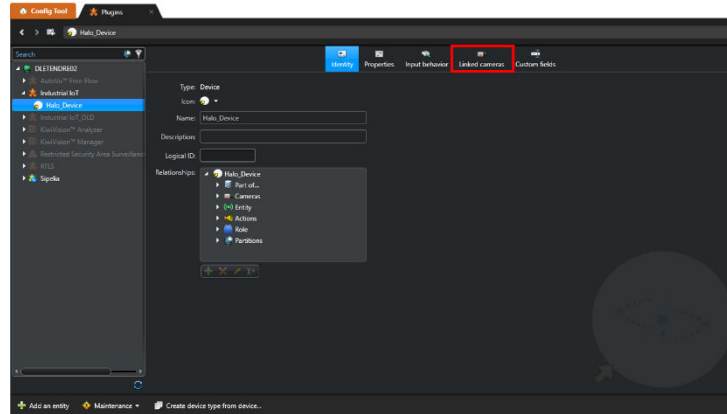


Figure 19

- b) Click the **Linked cameras** icon.
- c) Click on the **green plus button** at the bottom of the screen to add a camera.
- d) Select the appropriate camera and click **OK**.

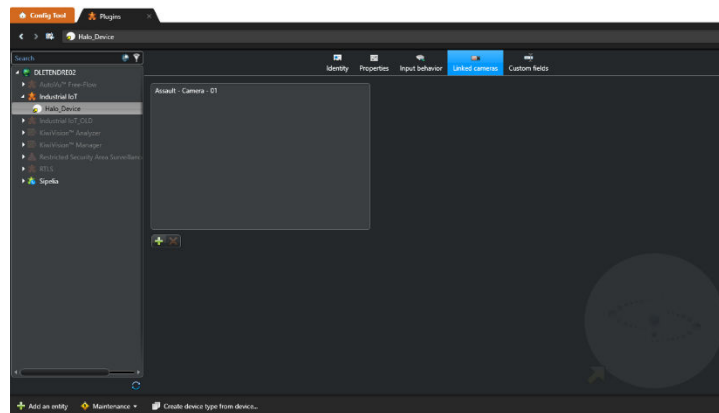


Figure 20

6.2 Adding HALO Dashboard as a camera (Optional)

- a) Click the **Add an entity** button at the bottom left of the screen.
- b) Select **Video unit**.
- c) Select **IPVideo Corporation** in the Manufacturer field.
- d) Select **Halo Smart Sensor** in the Product type field.
- e) Enter the **IP Address** of the unit in the IP Address field.
- f) Enter **80** in the HTTP port field.
- g) Select **Specific** for the Authentication.
- h) Enter appropriate Username and Password to access your HALO device.
- i) Click **Add and close**.

Figure 21

- j) Follow the steps in [6.1](#) to attach the newly created camera to the unit.

6.3 Customizing configuration (if required)

There are two ways to collect data from the HALO sensor:

1. Set trigger conditions in the HALO configuration web page and create events in the Config Tool app that will get raised when these conditions are met.
2. Collect data from the device through a data point and create rules directly in the Config Tool app. This allows for greater customization and to record (and display) HALO sensor measurements.

The following sections will describe the necessary steps to create actions based on data point value.

Creating Rules for Data point

For this example, we will set a rule to trigger a NOISE alarm when the Noise data point picks up a value greater than 60.

Under the **Rules** tab:

- a) Click on the **green plus button** under the rules box.
- b) Choose a name and a description for the rule (in this example, it is "HALO Noise above 60").
- c) For **Conditions**, select **On data change**.
- d) For **Source**, select **Device type** and select **TCP_HALO_FW_2_8_1_DeviceType**.

Note: Instead of setting the rule for all HALO attached to the type like in this example, it is possible to select a single Device so it will apply only to that specific device.

- e) For **Data point**, select the data point for which you would like to create a condition (here, it is Noise)
- f) In the new box on the right of the previous box, select an operator and a value to compare the measurement to (here, it is "greater than 60")
- g) Under **Actions**, select **Trigger alarm** in the combo box. Select the alarm that corresponds to the trigger (here, it is "NOISE alarm")
- h) For reference, you can also add Raise an event.
- i) If you previously configured state, you could add an action to change it so it will display a specific icon (state) on the device when the rule is triggered.
- j) Click on **Apply** at the bottom right of the screen.

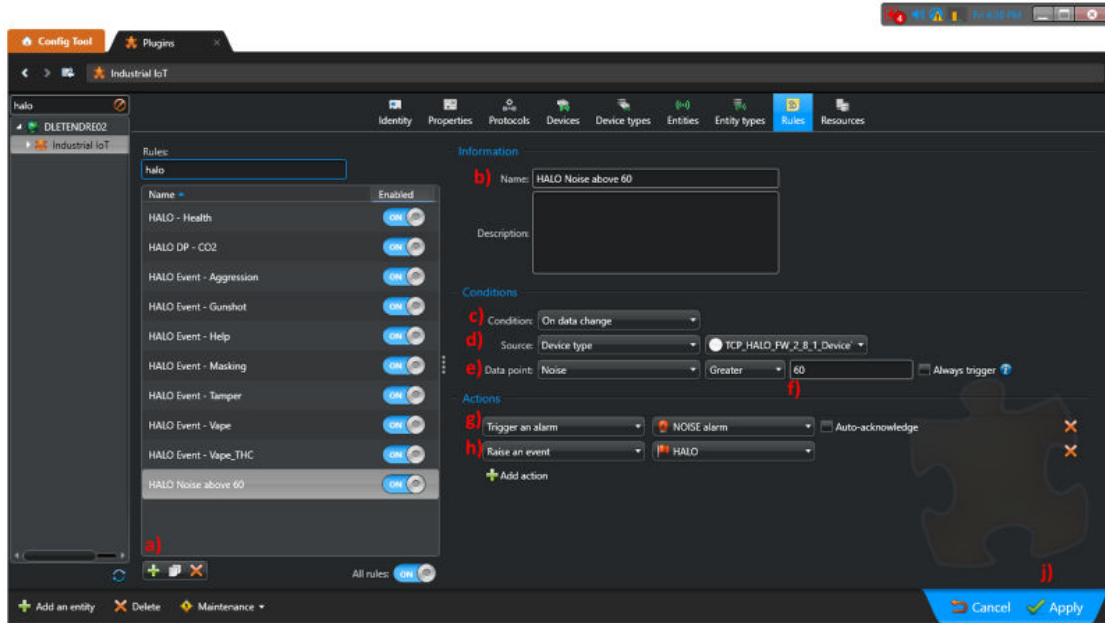


Figure 22

Operations

Monitoring Maps



Figure 23

Monitoring Events

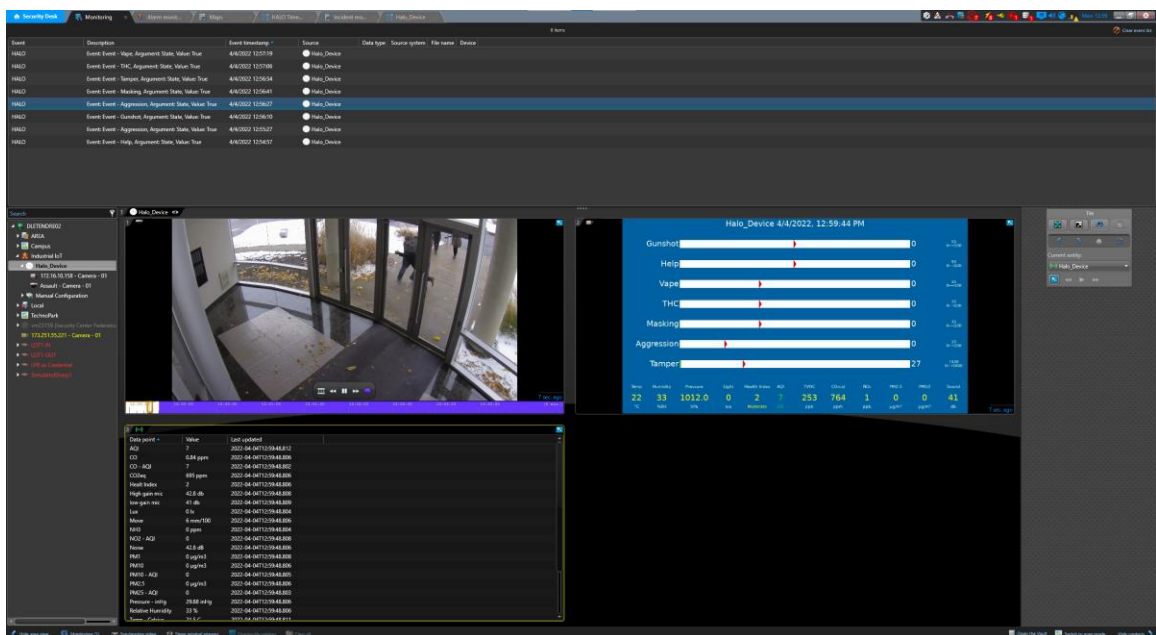


Figure 24

Monitoring Dashboard

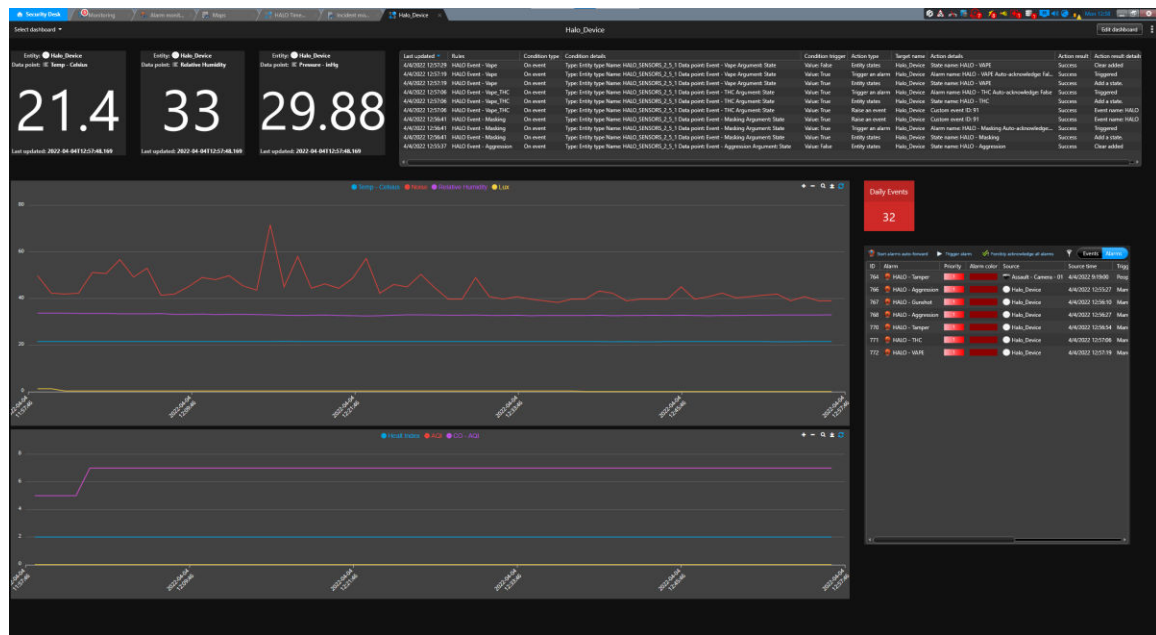


Figure 25

Reporting

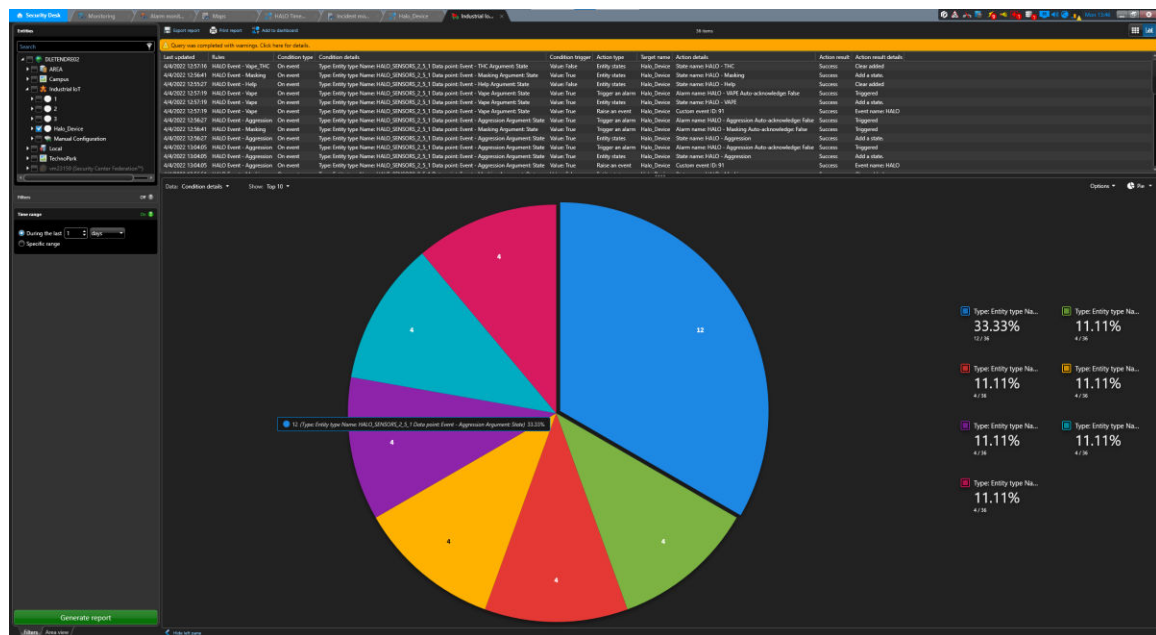


Figure 26

Appendix

IIoT Datapoint
AccX=@([^@]+)@
AccY=@([^@]+)@
AccZ=@([^@]+)@
AQI=@([^@]+)@
Aud1=@([^@]+)@
C=@([^@]+)@
CO=@([^@]+)@
CO2cal=@([^@]+)@
CO2eq=@([^@]+)@
COAQI=@([^@]+)@
F=@([^@]+)@
Gun=@([^@]+)@
HGMic=@([^@]+)@
HI=@([^@]+)@
HIco2=@([^@]+)@
HIhum=@([^@]+)@
HIIno2=@([^@]+)@
HIpm1=@([^@]+)@
HIpm10=@([^@]+)@
HIpm2.5=@([^@]+)@
HItvoc=@([^@]+)@
INP=@([^@]+)@

Table 1

IIoT Datapoint
KW1=@([^@]+)@
KW2=@([^@]+)@
KW3=@([^@]+)@
LGMic=@([^@]+)@
Lux=@([^@]+)@
Motion=@([^@]+)@
Move=@([^@]+)@
NH3=@([^@]+)@
NO2=@([^@]+)@
NO2AQI=@([^@]+)@
Noise=@([^@]+)@
panic=@([^@]+)@
PEOPLE=@([^@]+)@
P-Hg=@([^@]+)@
P-hPa=@([^@]+)@
PM1=@([^@]+)@
PM10=@([^@]+)@
PM10AQI=@([^@]+)@
PM2.5=@([^@]+)@
PM25AQI=@([^@]+)@
RH=@([^@]+)@
TVOC=@([^@]+)@