



Calipsa® and Manitou® Integration User Guide

October 2026

Contents

Introduction 2

Prerequisites 2

Configuring Media Gateway 2

 Connector 2

 Data Mapping.....3

 Line Driver.....4

Calipsa Setup 4

 Getting Started 4

 Configuring Webhooks 5

 Mapping Keywords 6

Where to find the AccountID in the Manitou Web Client 8

Testing the HTTP Connection.....8

Using Webhooks 9

Transmitter Setup in Manitou 10

Introduction

This guide covers the steps required to integrate your cameras that are connected to the Calipsa platform into Manitou via the Media Gateway.

Prerequisites

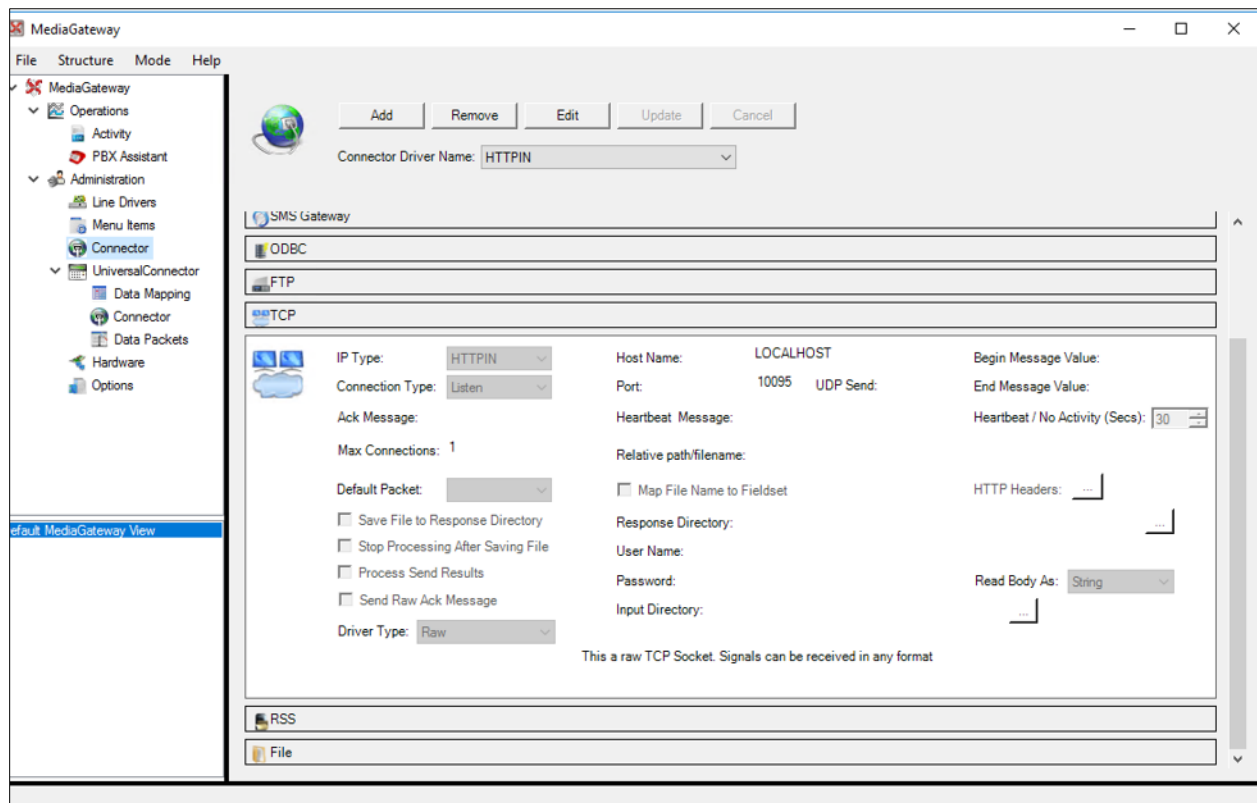
For Manitou integrations, the central station needs these technologies properly installed:

- TCP Connector
- Media Gateway
- Calipsa VCC Driver

Configuring Media Gateway

Connector

To run Calipsa integration, enable a TCP > HTTPIN driver in Media Gateway.

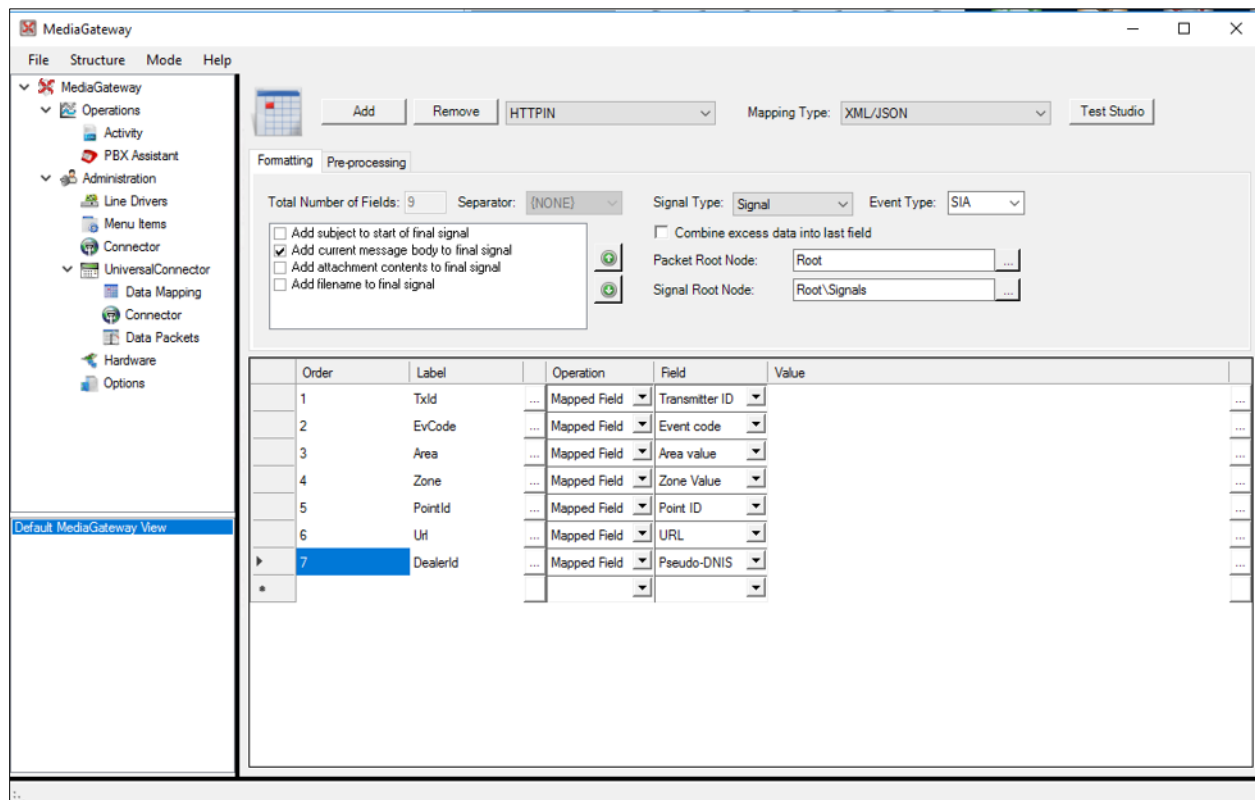


Set the **Host Name** and **Port** number. This host and port need to be covered by a valid SSL certificate. This SSL certificate must be configured in your Media Gateway settings under Options > TCP/IP > HTTPIN Connector Certificate.

Provide the URL and port to Manitou Support to enable the Integration Service. Once Support has enabled the service, they will provide you with a CSID, username, and password for the Calipsa integration. Use the CSID, username, and password to configure sites in Calipsa webhooks detailed later in this document.

Data Mapping

Add a fieldset for Data Mapping for the Media Gateway.



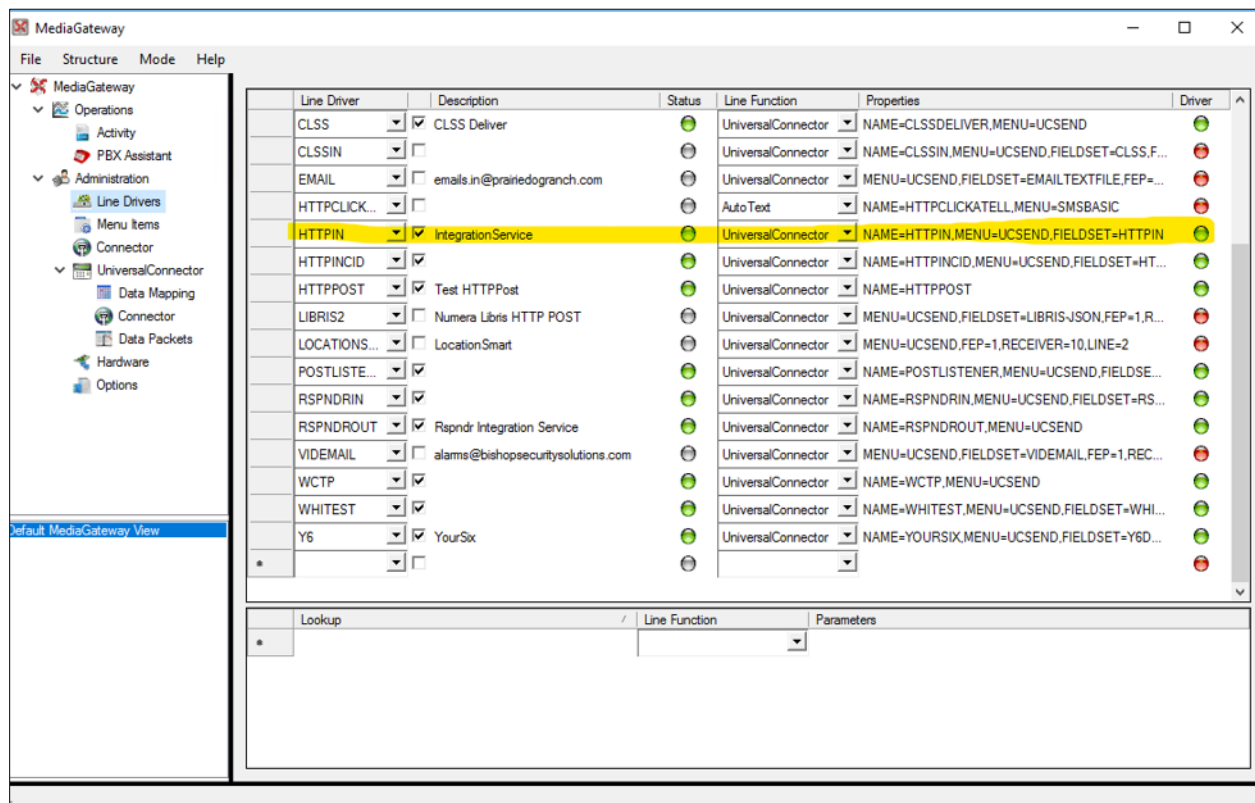
1. TxId > Mapped Field > Transmitter ID
2. EvCode > Mapped Field > Event code
3. Area > Mapped Field > Area value
4. Zone > Mapped Field > Zone value
5. PointId > Mapped Field > Point ID
6. Url > Mapped Field > URL

7. DealerId > Mapped Field > Pseudo-DNIS

DealerId data mapping is only needed if you need dealer separation for alarms coming in or if you otherwise use DNIS for Transmitter identification. Configure your Pseudo-DNIS and add the line for DealerId that maps to the Receiver Line Prefix that you will use for Calipsa transmitters.

Line Driver

A line driver for the connector and fieldset should be configured using the UCSEND menu item. This should have the fieldset set to the one just configured for the HTTPIN connector.



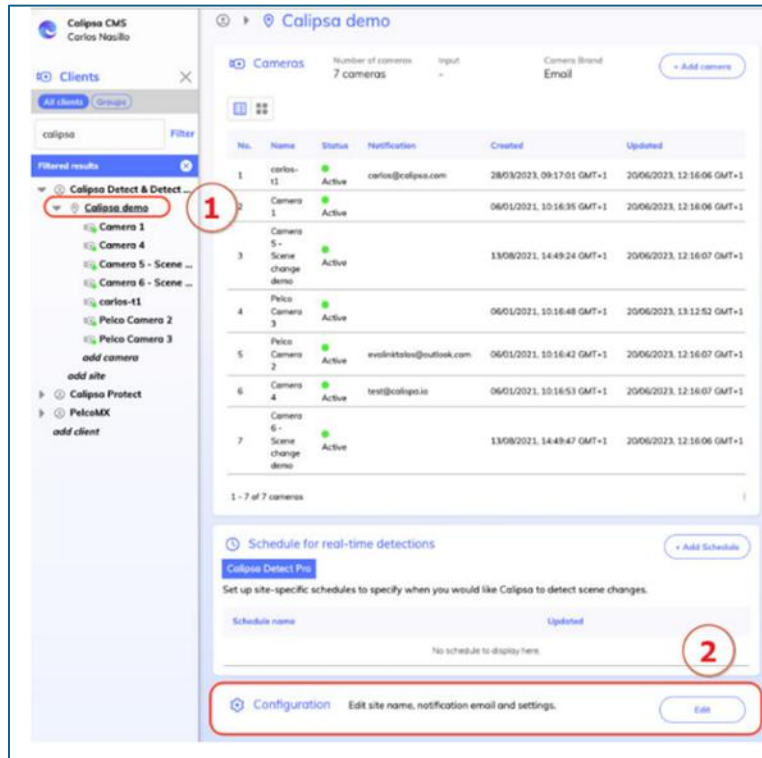
Calipsa Setup

Getting Started

To get started, log into Calipsa, and navigate to the Site Configuration page.

1. Select the Calipsa site from list shown in the left menu.

- Next to Configuration, click **Edit**.

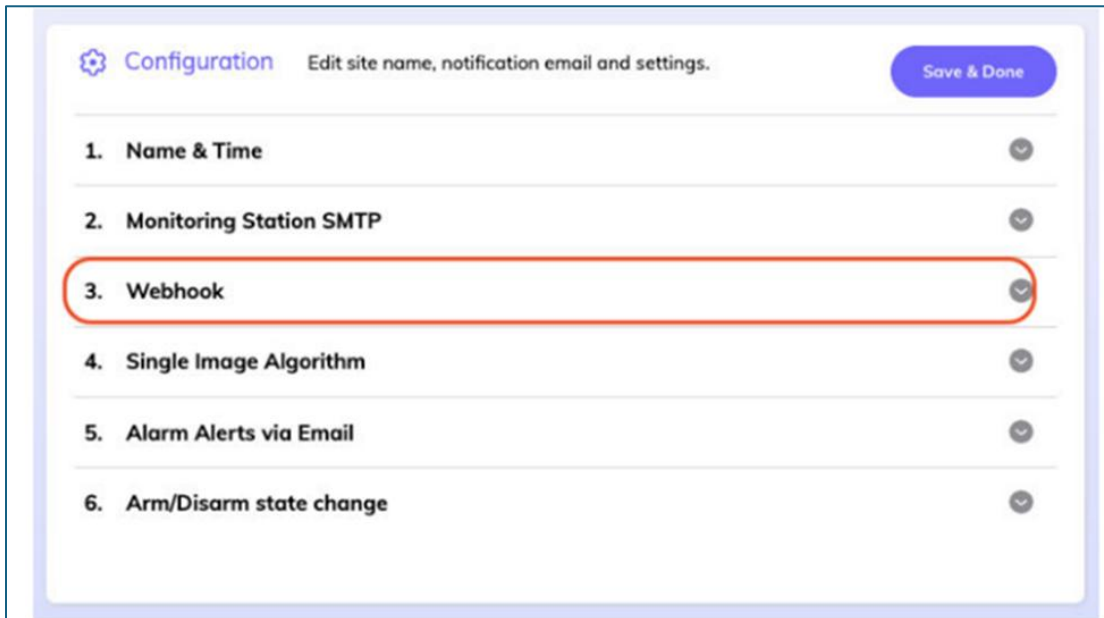


Configuring Webhooks

Establishing an HTTP Connection:

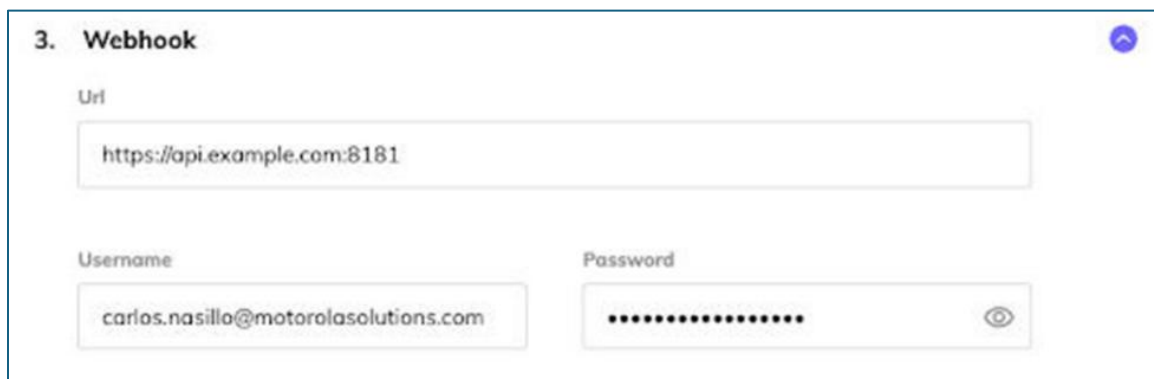
- In the Configuration section, find **Webhook** from the list of options.

2. Select Webhook to expand.



The screenshot shows a 'Configuration' page with a subtitle 'Edit site name, notification email and settings.' and a 'Save & Done' button. A list of six settings is displayed, each with a dropdown arrow on the right. The third item, '3. Webhook', is highlighted with a red rectangular border. The other items are '1. Name & Time', '2. Monitoring Station SMTP', '4. Single Image Algorithm', '5. Alarm Alerts via Email', and '6. Arm/Disarm state change'.

3. Under **URL**, enter the fully qualified endpoint URL:
<https://integration.boldgroup.io/Calipsa/signal>
4. Enter your username and password.
 - a. **Username**: This is a username mutually agreed upon between Bold and the central station.
 - b. **Password**: This is a password mutually agreed upon between Bold and the central station.



The screenshot shows the '3. Webhook' configuration form. It has a title '3. Webhook' and a close button in the top right. There are three input fields: 'Uri' with the value 'https://api.example.com:8181', 'Username' with the value 'carlos.nasillo@motorolasolutions.com', and 'Password' which is masked with dots and has an eye icon to toggle visibility.

Mapping Keywords

To successfully integrate Calipsa and Manitou, first specify the request method, then map the Calipsa key names with Webhook parameter names.

Under Key Mapping, select **POST** as the Request Method.

2. Webhook

Url

Username Password

Key Mapping [See documentation](#)

Request Method ☐ GET ☒ POST

Calipsa key name Webhook parameter name

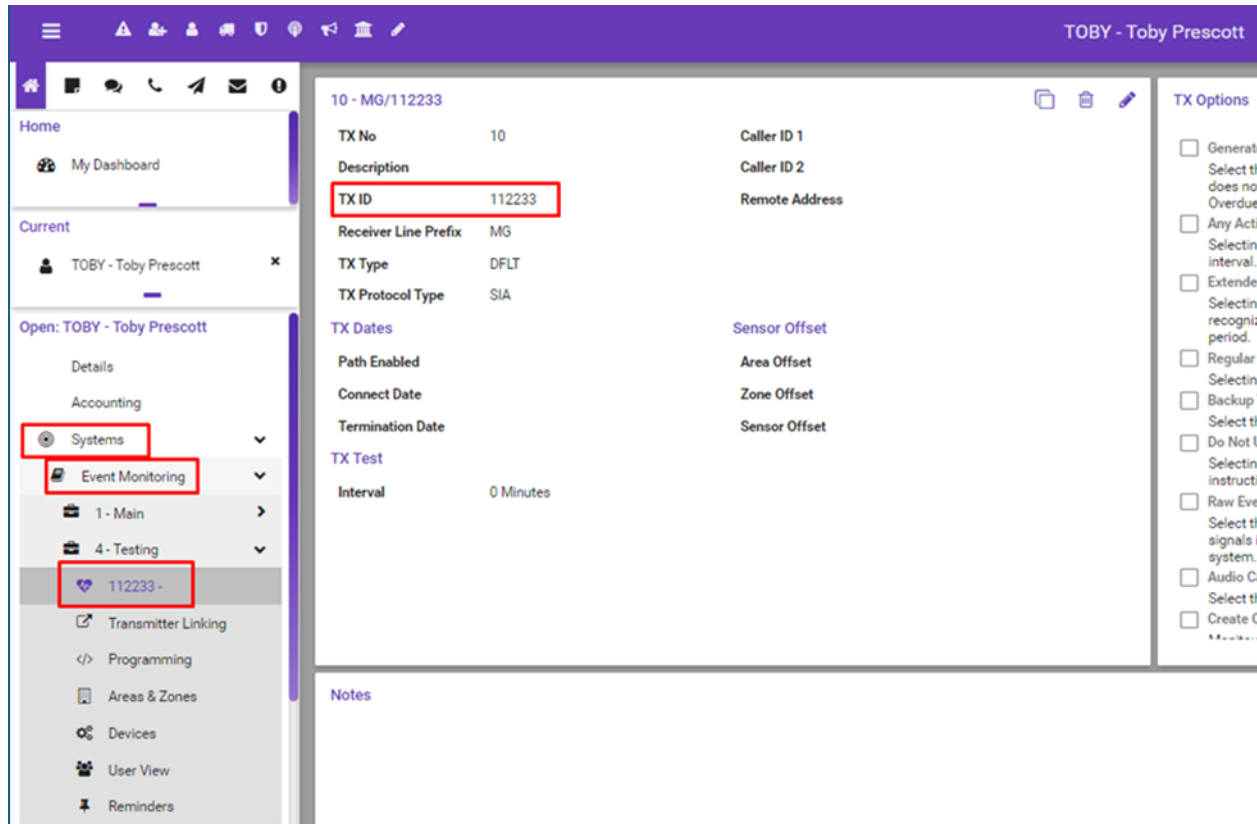
1. →

Payload (YAML)

```
Accountid: "112233"
Event: "BA"
Area: "1"
Zone: "1"
Comment: (&('People:'"$$.counts.person', Vehicles:'"$$.counts.vehicle', Camera:'"$$.camera.name))
Username: ( $.credentials.username )
Password: ( $.credentials.password )
Uri: ( $.snapshot.url )
```

- CSID: This is a tenant ID mutually agreed upon between Bold and the central station.
- AccountId: This should be the Manitou TXID or Stages XMIT number for the account.
- Event: "BA"
- Area: "1"
- Zone: "1"
- Comment: (&('People:'"\$\$.counts.person', Vehicles:'"\$\$.counts.vehicle', Camera:'"\$\$.camera.name))
- Username: (\$.credentials.username)
- Password: (\$.credentials.password)
- Uri: (\$.snapshot.url)

Where to find the AccountID in the Manitou Web Client



Testing the HTTP Connection

Click **Test Connection** to test the connection between Calipsa and your endpoint.

If the connection is successful, there is a success message alongside the status code.

The screenshot shows a configuration interface with a section labeled "6. Select parameter". Below this is a "Payload (YAML)" field containing the following text:

```
camera: $.camera.id
object types:
  vehicles: $.counts.vehicle
  people: $.counts.person
```

At the bottom of the interface, there is a green dot followed by the text "Status: 200". To the right of this text are two buttons: "Test Connection" and "Save".

If the connection is unsuccessful, due to a failed connection or error, the interface displays the status code. There is a tooltip with more information regarding the error.

The screenshot shows a configuration interface with two mapping sections:

- 4. counts.vehicle → n_vehicles
- 5. Custom field → my_param my_value

Below these mappings is a button labeled "+ Add new mapping". At the bottom of the interface, there is a red dot followed by the text "Status: 500". To the right of this text are two buttons: "Test Connection" and "Save".

A tooltip is displayed over the "Status: 500" text, containing the following information:

Status code 500: request to
https://api.example.com:8181/?
site=00000000-0000-4000-8000-
000000000002&camera_id=00000000
-0000-4000-8000-
000000000001&number_of_people=3&
n_vehicles=1&my_param=my_value
failed, reason: getaddrinfo
ENOTFOUND api.example.com

Below the status and tooltip, there is a list of three items, each with a dropdown arrow:

- 4. Single Image Algorithm
- 5. Alarm Alerts via Email
- 6. Arm/Disarm state change

Using Webhooks

Once a Webhook is configured, you will start receiving alert notifications only for TRUE alarms, for example: person or vehicle.

Even if the Webhooks feature executes a call to your endpoint, we cannot guarantee that your endpoint will be available or may respond in a timely manner.

Transmitter Setup in Manitou

You need to set up a new Transmitter Type for the Calipsa Video. Navigate to Maintenance > Transmitter Types and add a new transmitter. Make sure it is marked as Video Capable and in the Video Type drop down, select Calipsa Video.

The screenshot shows the 'Transmitter Types' configuration window in the Manitou software. The window is titled 'Transmitter Types' and has a blue header. On the left, there is a sidebar with a list of transmitter types, including 'CALIPSA - Caplipsa', 'CHECKVIDEO - CheckVideo', 'CLSS - Honeywell CLSS', 'DPLT - Default Transmitter', 'DOOR-SENTRY - Door SENTRY', 'ELEVATOR - Elevator Alarm', 'FIRE-SENTRY - Fire Alarm', 'NOTIFYME - Bold Notify', 'OPENEYE - OpenEye', 'RESIDIO - Residio', 'RSI VIDEO - RSI VIDEO', 'RSPNDR - Rapndr Transmitter', 'SALIENT - Salient Transmitter', 'SENTRYAI - Sentry AI', 'SENTRYDEMO - demo', and 'SUREVIEW - SureView Transmitter'. The 'CALIPSA - Caplipsa' type is selected and highlighted in yellow. The main area of the window is titled 'CALIPSA - Caplipsa (Event Monitoring)' and contains the following fields and options:

- Protocol Type:** A dropdown menu set to 'None'.
- Reverse Command Protocol:** A dropdown menu set to 'None'.
- Base:** A table with three groups, each having a 'Base' column with radio buttons for 'Decimal' (selected) and 'Hexadecimal', and 'Min' and 'Max' columns with input fields. The values are 0 for all.
- Separator:** A column with input fields.
- Transmitter ID Input Mask:** A text input field with a 'CLEAR' button.
- Raw Event Programming:** A checked checkbox.
- Monitored Transmission Path:** An unchecked checkbox.
- Generate Late to Test only when Closed:** An unchecked checkbox.
- Web Capable:** An unchecked checkbox.
- Audio Type:** A dropdown menu set to 'None'.
- Video Type:** A dropdown menu with 'Calipsa Video' selected and highlighted in yellow.
- Audio Capable:** An unchecked checkbox.
- Create Call Session (No Listen-In):** An unchecked checkbox.
- Drop Listen-In if no alarm:** An unchecked checkbox.
- Video Capable:** A checked checkbox.

At the bottom of the window, there is a status bar with the date '7/14/2026 09:28:51', the time 'Mountain Time (US & Ca', and a 'CLEAR' button.

Save the transmitter type.

Create or edit a customer to add a new transmitter. On the customer, add the created transmitter and give it a unique Transmitter ID:

BCAL - John Jett

1 - Test Account 1 MG/223344

Transmitter No: 1, Description: Test Account 1, Transmitter ID: 223344, Receiver Line Prefix: MG, Transmitter Type: CALIPSA, Transmitter Protocol Type: , Transmitter Dates: , Sensor Offset: , Path Enabled: , Connect Date: , Termination Date: , Transmitter Test Interval: 0 Minutes

Transmitter Options:

- ☐ Generate Restore Overrides
- ☐ Any Activity Satisfies Test
- ☐ Extended Signaling
- ☐ Regular Activity Expected
- ☐ Backup Transmitter
- ☐ Do Not Use Dealer Programming
- ☐ Raw Event Programming
- ☐ Audio Capable
- ☐ Create Call Session (No Listen-In)
- ☐ Drop Listen-In if no alarm
- ☒ Video Capable
- ☐ Monitored Transmission Path
- ☐ Generate Late to Test only when Closed
- ☐ Encrypted
- ☐ Add-On Module

Notes

Alarm Progress Problem for 'Unknown Event' of priority 4 for monitoring group 0

Once an alarm comes in for this customer on this transmitter from Calipsa, you will see a Video alarm notification:

(BCAL) John Jett - BA (Burglary Alarm)

John Jett - 4050 Lee Vance Drive Suite 250, Colorado Springs, Colorado 80918

Alarm Details:

- Priority: 4
- System: 1 - Camera
- FEP/Receiver/Line: 1 - Area 1
- Alarm Time: 07/14/2026 09:26:11
- Transmitter: 1 - Test Account 1 (MG/223344)
- Point ID: People:1, Vehicles:0, Camera: Pelco Serix Pro 4 Dome - SRXP4-SV10-EMD

Action Pattern - G4 (1/18):

- 0 CALL THE CUSTOMER
- 0 CALL THE AHJ
- 0 SET: @COUNTER = 0
- 0 LABEL: RECALL_1
- 0 CONTACT COMPANY KEYHOLDER
- 0 IF PRIOR ACTION COMPLETED
- 0 ELSE
- 0 END IF
- 0 CLOSE THE ALARM

Customer Activity Log:

Date	Time	Log Description	User ID	Workstation
07/14/2026	09:26:11	ALARM - Burglary Alarm (BA) People:1, Vehicles:0, Camera: Pelco Serix Pro 4 Dome - SRXP4-SV10-EMD S: 1 A: 1 RL: MG TX ID: 223344 Key: BA DA: 1		
09:26:11		BINARY - URL		
09:26:46		ALLOCATED - Burglary Alarm (BA) - Manual		
09:26:46		VIEWED - Burglary Alarm (BA) - Response [35 Secs]		
07/14/2026	09:24:26	VIEW - Customer Opened for View		
07/10/2026	12:46:24	VIEW - Customer Opened for View		

Alarm Progress Problem for 'Unknown Event' of priority 4 for monitoring group 0

You can use this to launch VCC and see the alarm images that have come from Calipsa:

