



ADVANCED
NETWORK DEVICES

Configuring M2M in InformaCast Fusion

Version 2.0

6/2/2025

© 2025 ADVANCED NETWORK DEVICES

3820 NORTH VENTURA DR.

ARLINGTON HEIGHTS, IL 60004

U.S.A

ALL RIGHTS RESERVED

Proprietary Notice and Liability Disclaimer

The information disclosed in this document, including all designs and related materials, is the valuable property of Digital Advanced Network Devices and/or its licensors. Advanced Network Devices and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

The Advanced Network Devices product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by Advanced Network Devices.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of Advanced Network Devices is prohibited.

Static Electric Warning



TROUBLESHOOTING AND ADDITIONAL RESOURCES

User Support: <https://www.anet.com/user-support/>
Technical Resources: <https://www.anetd.com/user-support/technical-resources/>
AND Legal Disclaimer: <https://www.anetd.com/legal/>

OVERVIEW

Machine-to-Machine (M2M) technology enables high-functioning communication over the network between AND devices and InformaCast. This utilizes Simple Network Management Protocol (SNMP) messages from device to device for the purpose of reading or writing information on the device.

For AND devices, this enables a wide array of functionality with InformaCast, such as:

- Reading the input of a device over the network and acting from it
- Remotely activating the output of a device
- Setting button light indication states

This application note will cover the configuration of both your InformaCast server and the AND devices for M2M operation.

CONFIGURING THE AND DEVICE

Since M2M utilizes SNMP, the AND device will need to be configured to utilize SNMP. For this, SNMP communities and an SNMP trap manager will need to be set up.

To configure AND devices with InformaCast, alter the global InformaCast configuration file which it automatically serves to devices on the network.

1. Using an FTP client like WinSCP or FileZilla, access your InformaCast server using SFTP. The default username is "admin" with no password.
2. Navigate to the following directory: /data/d_{version}/usr/local/singlewire/InformaCast/web/resources/
3. Locate and edit the global configuration file "InformaCastSpeaker.cfg"
4. Add the following lines of configuration within the top level <InformaCastSpeakerConfiguration> tags:

```
<SNMP
  read_community="readcomm"
  write_community="writecomm"
>
<TrapManager
  addr="10.20.30.40"
  pdu_version="1"
  community="informacomm"
/>
</SNMP>
<GPIO
  snmp_trap_for_input_gpio0="1"
  snmp_trap_for_input_gpio1="1"
  pulse_ms_output_gpio0="5000"
/>
```

5. Change each of the read_community, write_community, and community variables to the name of the SNMP communities you will be using. Change the addr variable to the IP of your InformaCast server.
6. Save the file, then reboot each AND device to allow them to search for and retrieve the new configuration file.

CONFIGURING INFORMACAST

With SNMP communities and trap settings defined on the device, InformaCast's M2M communication can be utilized.

Each device which will utilize M2M will need to be configured as a contact closure within InformaCast. To do this, open the InformaCast web application and navigate to Recipients > M2M > Contact Closures. Click "Create Contact Closure" to create a new contact closure for a device. On the next page, give the contact closure a name and description, then enter the IP address of the device and the desired SNMP community name. The SNMP community name must match the name defined for the write community and trap manager community defined on the device. Click "Save" to create the contact closure. As an IP is required for this configuration, we recommend setting up a DHCP reservation for the device.

UTILIZING AN INPUT FROM A DEVICE

To trigger an action in InformaCast from a device input, add an input port to this contact closure. On the Contact Closure Details page, locate the "Input Ports" section and click "Create Input Port."

Configure the input port as follows:

- Name: Whatever you wish
- Monitoring Status: ACTIVE
- Time Schedule: Always On
- Port Identifier (OID):
 - For input GPIO0: 1.3.6.1.4.1.39866.3.1.4.10.1.3.1
 - For input GPIO1: 1.3.6.1.4.1.39866.3.1.4.10.1.3.2
- Port Switch On/Off (OID Value): 1
- Message Template: The message template you wish to trigger when the button is pressed
- Device Groups: The Device Groups to send the above message template to
- Distribution Lists: The Distribution Lists to send the above message template to

Save the Input Port by clicking the "Save" button.

ACTIVATING THE OUTPUT OF A DEVICE

To remotely activate the output of a device from InformaCast, first configure an output port on this contact closure. On the Contact Closure Details page, locate the "Output Ports" section and click "Create Output Port."

Configure the output port as follows:

- Name: Whatever you wish
- Monitoring Status: ACTIVE
- Time Schedule: Always On
- Port Identifier (OID):
 - For Output GPIO0: .1.3.6.1.4.1.39866.3.1.4.11.1.22.1
 - For Output GPIO1: .1.3.6.1.4.1.39866.3.1.4.11.1.22.2
- Field Type: Integer
- Port Switch On/Off (OID Value): 1

Save the Output Port by clicking the “Save” button.

Next, in order to activate this output port, it will need to be added to a device group, which will be added to a message template.

To create the device group, navigate to Recipients > Device Groups, then click “Create Device Group.” Give the device group a name, then in the “Filters” section, locate the “Individual Devices” section. Click on the text box in this section and type the name of either the contact closure or output port. Select the matching “M2M Output Port: {Contact Closure}: {Output Port}” from the list to add it to the device group. Several output ports may be added to the same device group.

To add this device group to a message template, navigate to Notifications > Message Templates and either create or edit an existing message template. In the “Recipients” section, select the button for “Device Groups” and select the device group you just created from the list.

Whenever this message template is triggered, InformaCast will address each M2M output port in any device group assigned to the message template by sending an SNMP trap with the configured details.

RESET EMERGENCY STATE (STOP BLINKING)

AND IP panic buttons have a light indicator visible on the device which indicates whether or not the button has been pressed. This “emergency indication” is intentional, and designed to be obvious that the button has been activated. When the situation has cleared though, one may want to reset this blinking of the button. This can be done in a similar way to configuring an Output Port on a contact closure. Since InformaCast addresses Output Ports by sending an SNMP trap, this can be utilized to address the related OID for the emergency state and reset it.

Begin by creating a contact closure, then on the Contact Closure Details page, locate the “Output Ports” section and click “Create Output Port.”

Configure the output port as follows:

- Name: Whatever you wish
- Monitoring Status: ACTIVE
- Time Schedule: Always On
- Port Identifier (OID): .1.3.6.1.4.1.39866.3.1.3.27.1.0
- Field Type: Integer
- Port Switch On/Off (OID Value): 2

Save the Output Port by clicking the “Save” button.

Next, in order to activate this SNMP trap, this output port will need to be added to a device group, which will be added to a message template. This is done in the same way as described at the top half of this page. Please refer to that section to finalize this implementation.

PERMANENTLY SETTING AN OUTPUT

Activating the output of a device is most easily done with the previously discussed method, as this uses the device's output "pulse" to activate the output for a configured amount of time. We can establish further functionality though by permanently setting the state of the output to either active or inactive.

Begin by creating a contact closure, then on the Contact Closure Details page, locate the "Output Ports" section and click "Create Output Port."

To create the SNMP trap that will permanently set the output to active, configure the output port as follows:

- Name: Whatever you wish
- Monitoring Status: ACTIVE
- Time Schedule: Always On
- Port Identifier (OID):
 - For Output GPIO0: .1.3.6.1.4.1.39866.3.1.4.11.1.21.1
 - For Output GPIO1: .1.3.6.1.4.1.39866.3.1.4.11.1.21.2
- Field Type: Integer
- Port Switch On/Off (OID Value): 11

An additional output port will need to be created to set the output to inactive.

To create the SNMP trap that will permanently set the output to inactive, configure the output port as follows:

- Name: Whatever you wish
- Monitoring Status: ACTIVE
- Time Schedule: Always On
- Port Identifier (OID):
 - For Output GPIO0: .1.3.6.1.4.1.39866.3.1.4.11.1.21.1
 - For Output GPIO1: .1.3.6.1.4.1.39866.3.1.4.11.1.21.2
- Field Type: Integer
- Port Switch On/Off (OID Value): 0

Save the Output Port by clicking the "Save" button.

Next, in order to activate this SNMP trap, each of these output ports will need to be added to a device group, which will be added to a message template. This process is detailed in the "Activating the Output" section.

Associate the device group containing the permanent active SNMP trap to the message that you wish to activate the output. Associate the device group containing the permanent inactive SNMP trap to the message that you wish to deactivate the output.