Create Pipelines

Cisco Edge Intelligence pipelines

In Cisco Edge Intelligence local manager dashboard, we create pipelines to define the data progression. Creating a pipeline involves defining:

1. One/multiple source asset type
2. One data destination
3. A data transformation method, in the form of a data rule or a data logic

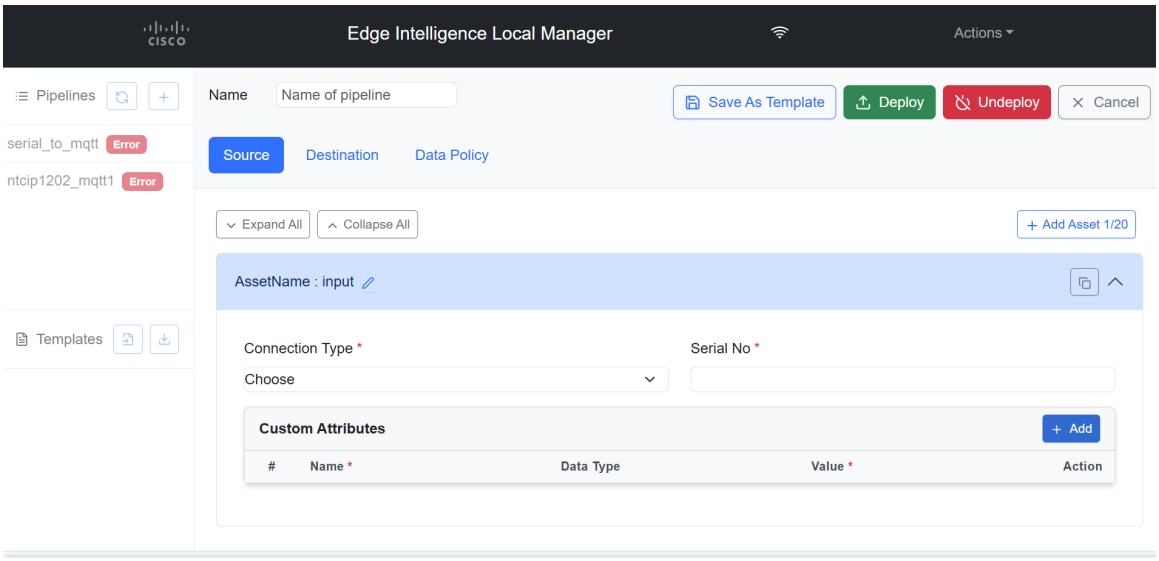
To create a pipeline in the Cisco Edge Intelligence local manager GUI, in the **Pipelines** area of the left pane, click the plus (+) sign button. At the top of the page, enter a name for the pipeline. Ensure that each pipeline name for the Cisco Edge Intelligence must be unique, in compliance with the following recommendations.

- Do not use special characters for a pipeline name, as special characters are removed during internal processing. We recommend using the CamelCase naming convention.

  For example, use `WaterSensorSalinityJ2345` instead of `Water Sensor-Salinity_J2345`.

- Avoid ending a pipeline name with the letter `s` to indicate a plural form, as this name can cause internal naming conflicts.

  For example, use `ColdStoragePlc` instead of `ColdStoragePlcs`.



Add Source

Adding Asset Type Details

Procedure

In the **Source** tab, complete the following fields.

Field	Description
Asset Name	Click the pencil icon to enter a name for the asset. This name gives a significant value to the data logic.
Connection Type	From the drop-down list, choose one of the following protocols: • MQTT • Modbus – Serial • Modbus – TCP/IP • OPC-UA • Serial • RSU • NTCIP1202 • NTCIP1203 • NTCIP1204

Field	Description
Serial Number	Enter a serial number for the chosen source type.

Custom Attribute Configuration	You can add custom attributes along with each asset type-specific attribute. Add the following details to configure the custom attribute:
	a. **Name**: Enter a name for the custom attribute.
	b. **Data Type**: From the drop-down list, select a data type, string, double, encrypted string, or file.
	c. **Value**: Enter a custom attribute value.
	If the Data Type is selected as **File**:
	• There can be only one attribute type **File** for a given asset type.
	• The max size of the uploaded file should be 12 KB.
	• The file can be of any type - ASCII or binary.
	• If the asset is part of a data rule policy and the destination is configured to send the custom attribute to the northbound destination, the base64 equivalent of the file contents will be sent.
	• If the asset is part of a data logic policy, a custom attribute value is available in the data logic script as a byte array (UInt8Array), and it can be converted to the original format for access.
	• For example, if the custom attribute "reference_data" was of **File** type and the uploaded file was as ASCII file, the following code shows how to convert the value available as UInt8Array into ASCII text.
	`function on_update() {`
	`...`
	`var file_contents = new TextDecoder().decode(input.reference_data);`
	`// Converts UInt8Array to ASCII`
	`...`
	`}`
	Click **Add** to add more custom attributes to any asset configuration

Note
Cisco Edge Intelligence local manager have the provision to configure the multiple assets under a single pipeline. You can configure upto 20-assets type details and run the deployment.

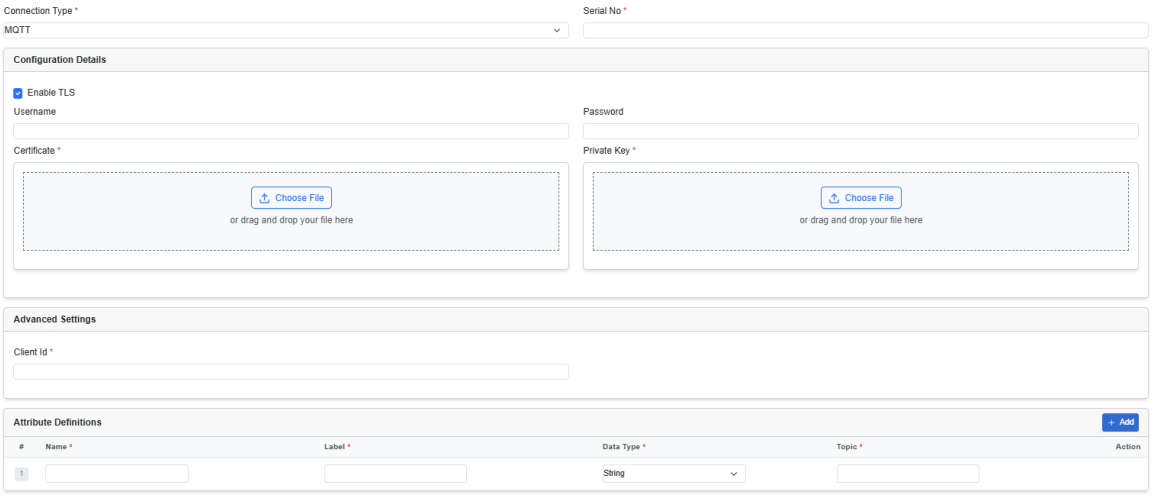
If you want to duplicate an existing asset details with a different serial number, click copy-paste icon next to the asset name.

Configure MQTT asset type

The MQTT asset type enables and configures the Cisco Edge Intelligence MQTT Server. You can publish data to the EI Agent from an MQTT client on the following ports after deploying this to an EI Agent:

- Port 8883 for TLS configurations
- Port 1883 for non-TLS configurations

In the **Source** tab, from the **Connection Type** drop-down list, choose **MQTT**. Then, fill out the following fields.



Field	Description
Configuration Details	
Enable TLS	Choose this checkbox to enable TLS. When you choose to enable TLS, additional fields are displayed to allow the upload of certificate and private key files. The MQTT server that is deployed on the EI agent, uses these certificates and private keys to authenticate the MQTT clients connecting to it.
Username	Enter a username. The connecting MQTT Clients (sensors) will use this username for authentication at the MQTT Server which will be spawned on the EI Agent.
Password	Enter the Password. The connecting MQTT Clients (sensors) will use this password for authentication at the MQTT Server which will be spawned on the EI Agent.

Field	Description
Advanced Settings	
Client ID	Add a client ID to publish data. (Topic-based device or sensor identity detection is not supported). The client ID, specified in the MQTT client connection, differentiates various MQTT connections to Cisco Edge Intelligence.
Attribute Definitions	The data model explains how data is represented in the asset, and what MQTT topics the asset should be updated from. To define a data model, add the following details: 1. **Name**: Enter a name for the data model 2. **Label**: Enter a label for the data model 3. **Data Type**: From the drop-down menu, select a measurement entity (string, integer, float, long, or boolean) for the MQTT topic. 4. **Topic**: Enter the MQTT topic over which the measurement is sent by the transmitting MQTT client. For example, `sensors/tempXY/temp`. Click **Add** to add more data model attributes to the configuration

Note The MQTT topic used to publish sensor data and the data format should match the **data model** JSON file.

MQTT data model example:

```
{
    "apiVersion": 1.0,
    "connectionType": "MQTT",
    "fields": {
      "temperature": {
        "category": "TELEMETRY",
        "label": "Temperature",
        "description": "Outside temperature sensor XY | Temperature",
        "datatype": "Float",
        "topic": "sensors/tempXY/temp"
       },
       "humidity": {
         "category": "TELEMETRY",
         "label": "Humidity",
         "description": "Outside temperature sensor XY | Humidity",
         "datatype": "Float",
         "topic": "sensors/tempXY/hum"
       },
       "attr1": {
         "category": "ATTRIBUTE",
         "label": "Attribute 1",
```

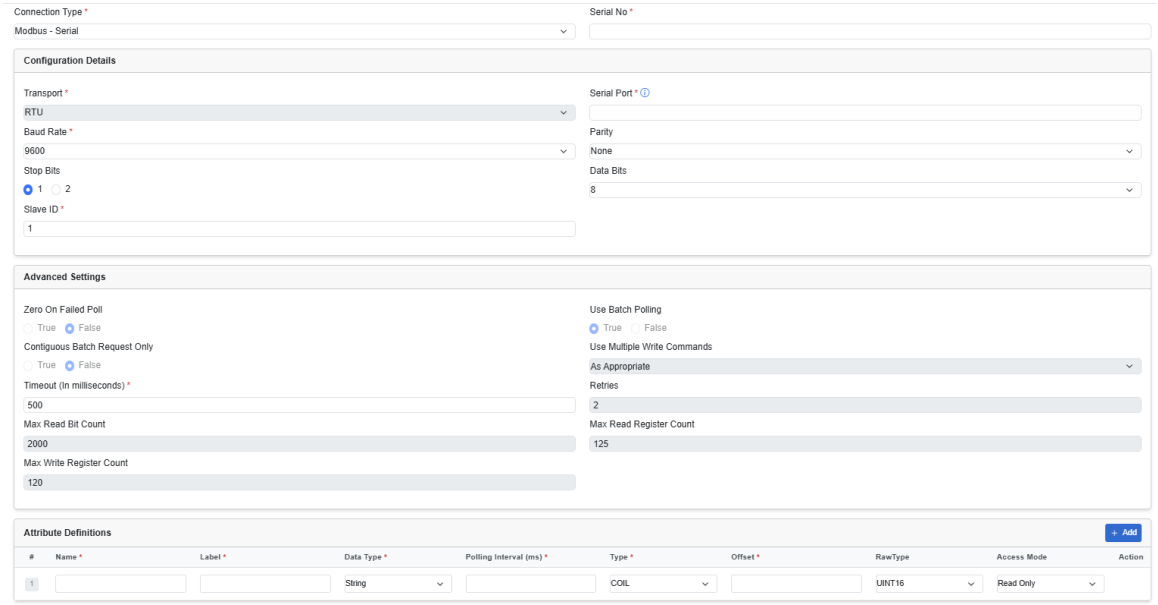
```
        "datatype": "Float",
        "description": "My Attribute 1",
        "required": true,
        "defaultValue": 12.9
      },
      "attr2": {
        "category": "ATTRIBUTE",
        "label": "Attribute 2",
        "datatype": "String",
        "description": "My Attribute 2",
        "required": false,
        "defaultValue": null
      },
      "encrypted_attr3": {
        "category": "ATTRIBUTE",
        "label": "New Attribute",
        "datatype": "EncryptedString",
        "description": "My Attribute 3",
        "required": true,
        "defaultValue": null
      }
    }
}
```

MQTT topic and sensor data used by MQTT Client example:

```
MQTT Client Topic: sensors/tempXY/hum
MQTT Client Data: 50.0
```

Configure Modbus-Serial asset type

From the **Device Type** drop-down list, choose **MODBUS-Serial**. Then enter the required details in the following fields.



Field	Description
Configuration Details	

Field	Description
Transport	This field is not editable. It has a default value set for RTU.
Serial Port	Enter a port number. For example, `/dev/ttyS0`.
Baud Rate	Enter a baud rate.
Parity	From the drop-down list, choose **None**, **Odd**, or **Even**.
Stop Bits	This value can be either 1 or 2. Choose the required radio button.
Data Bits	From the drop-down list, choose a value 5–9.
Slave ID	This refers to the unique identifier assigned to a Modbus secondary device (such as a sensor or PLC) on a serial network. Modbus protocol requires each secondary device to have a unique ID (1–247) to distinguish it on a shared bus. This ID ensures that the Modbus primary (such as the Cisco EI agent) sends requests to the correct device and processes its responses.
Advanced Settings	
Zero or Failed Poll	The value if there is no response from the asset. This field is not editable.
Use Batch Polling	To request batch responses from the asset. This field is not editable.
Contiguous Batch Request Only	To request contiguous batch responses from the asset. This field is not editable.
Use Multiple Write Commands	This field is not editable.
Timeout	The time in which to receive the data before it is reset. The default value is 500.
Retries	The number of times the server requests for retransmission of data. This field is not editable.
Max Read Bit Count	The maximum number of bits that the server reads in one read request. This field is not editable.
Max Read Register Count	The maximum number of registers that the server reads in one read request. This field is not editable.
Max Write Register Count	The maximum number of registers that the server writes in one write request. This field is not editable.

Field	Description
Attribute Definitions	A data model explains how data is represented in the asset. You can create a data model using a JSON file. Select one of the following: 1. **Name**: Enter a name for the data model. 2. **Label**: Enter a label value. 3. **Data Type**: From the drop-down list, select a measurement entity (string, integer, float, long, or boolean) for the MODBUS serial data. 4. **Polling Interval (ms)**: Enter a value to define the fastest rate at which the server must test and debug. 5. **Type**: From the drop-down list, choose a data type for industrial control of factory devices. The available choices are **COIL**, **HOLDING**, **DISCRETE**, and **INPUT**. 6. **Offset**: Enter a value to reference a specific register within the function. 7. **RawType**: From the drop-down list, choose the value type for storing binary data or byte strings. 8. **Access Mode**: From the drop-down list, choose an access mode. The available choices are **Read Only**, **Read & Write**, and **Write Only**. Click **Add** to add more data model attributes to the configuration

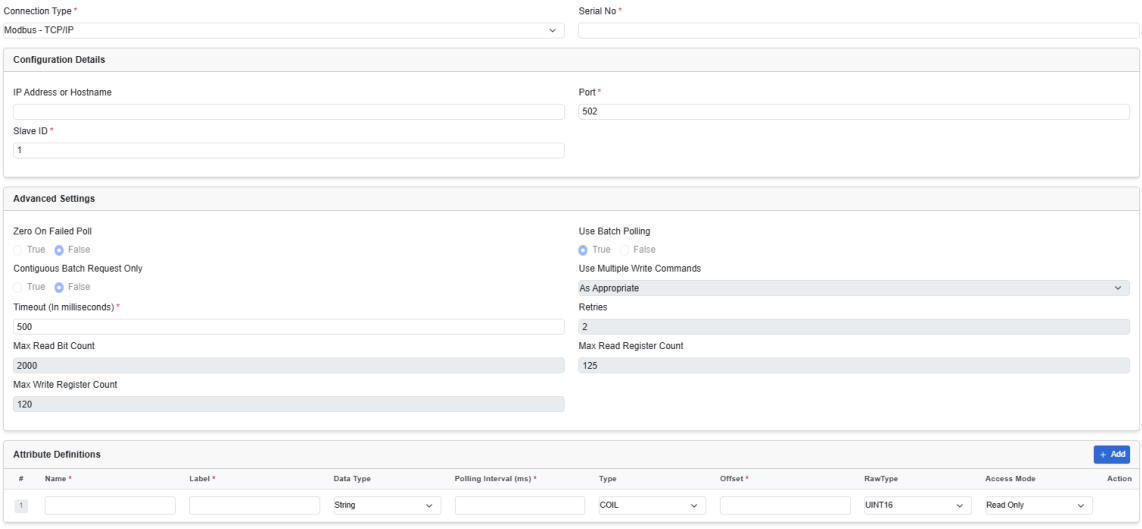
Modbus_serial data model example:

```
{
  "apiVersion": 1,
  "connectionType": "MODBUS_SERIAL",
  "fields": {
    "pressureInPascal": {
      "label": "MetrLabeModb1",
      "pollingInterval": 50,
      "offset": 12,
      "type": "HOLDING",
      "datatype": "Float",
      "rawType": "VARCHARSTRING",
      "description": "",
      "access": "Write"
    },
    "TemperatureInDegrees": {
      "label": "Temperature",
      "pollingInterval": 41,
      "offset": 56,
      "type": "DISCRETE",
      "datatype": "String",
      "rawType": "INT16",
```

```
      "description": "",
      "access": "ReadWrite"
    },
    "HumidityInDegrees": {
      "label": "Humidity",
      "pollingInterval": 20,
      "offset": 45,
      "type": "COIL",
      "datatype": "Int",
      "rawType": "FLOAT64",
      "description": "Humidity Value ",
      "access": "Read"
    }
  }
}
```

Adding Asset Types for Modbus TCP Connection Type

After you select the MODBUS-TCP/IP, complete the following additional fields by adding the details on it.



Field	Description
Configuration Details	
IP Address or Host Name	Enter an IP address or hostname.
Port	Enter a port number.
Slave ID	This refers to the unique identifier assigned to a Modbus secondary device (such as a sensor or PLC) on a serial network. Modbus protocol requires each secondary device to have a unique ID (1–247) to distinguish it on a shared bus. This ID ensures that the Modbus primary (such as the Cisco EI agent) sends requests to the correct device and processes its responses.
Advanced Settings	

Field	Description
Zero on Failed Poll	The value if there is no response from the asset. This field is non-editable.
Use Batch Polling	To request batch responses from the asset. This field is non-editable.
Contiguous Batch Request Only	To request contiguous batch responses from the asset. This field is non-editable.
Use Multiple Write Commands	This field is non-editable.
Timeout	The time set to receive the data before it is reset. The default value is 500.
Retries	The number of times the server requests for retransmission of data. This field is non-editable.
Max Read Bit Count	The maximum number of bits that the server reads in one read request. This field is non-editable.
Max Read Register Count	The maximum number of registers that the server reads in one read request. This field is non-editable.
Max Write Register Count	The maximum number of registers that the server writes in one write request. This field is non-editable.

Field	Description
Attribute Definitions	A data model explains how data is represented in the asset. You can create a data model using a JSON file. Enter the following details: 1. **Name**: Enter a name for the data model. 2. **Label**: Enter a label value. 3. **Data Type**: From the drop-down menu, select a measurement entity (string, integer, float, long, or boolean) for the MODBUS-TCP/IP data. 4. **Polling Interval**: Enter a value to define the fastest rate at which the server should test and debug. 5. **Type**: From the drop-down menu, choose a data type for industrial control of factory devices. The available choices are **COIL**, **HOLDING**, **DISCRETE**, and **INPUT**. 6. **Offset**: Enter a value to reference a specific register within the function. 7. **RawType**: From the drop-down menu, choose the value type for storing binary data or byte strings. 8. **Access Mode**: From the drop-down list, choose an access mode. The available choices are **Read Only**, **Read & Write**, and **Write Only**. Click **Add** to add more data model attributes to the configuration

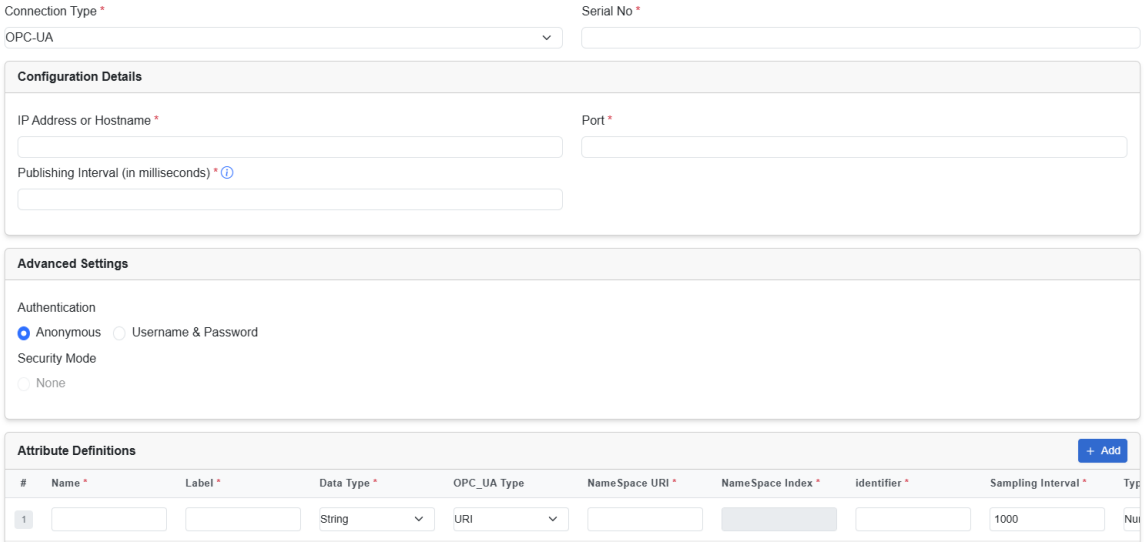
The following is an example of a data model for Modbus-TCP/IP source type.

```
{
  "apiVersion": 1,
  "connectionType": "MODBUS_TCP",
  "fields": {
    "desired_temp": {
      "label": "Desired Temperature",
      "datatype": "Int",
      "description": "WO",
      "rawType": "UINT16",
      "type": "HOLDING",
      "pollingInterval": 5000,
      "offset": 5,
      "category": "TELEMETRY",
      "access": "Write"
    },
    "temp_to_display": {
      "label": "Temperature to be displayed",
      "datatype": "Int",
      "description": "RW",
      "rawType": "UINT16",
```

```
      "type": "HOLDING",
      "pollingInterval": 5000,
      "offset": 100,
      "category": "TELEMETRY",
      "access": "ReadWrite"
    },
    "temp": {
      "label": "Current Temperature",
      "datatype": "Int",
      "description": "RO",
      "rawType": "UINT16",
      "type": "HOLDING",
      "pollingInterval": 5000,
      "offset": 1,
      "category": "TELEMETRY",
      "access": "Read"
    }
  }
}
```

Configure OPC-UA asset type

After you select the asset type OPC-UA, enter the required details in the following fields:



Field	Description
Configuration Details	
IP Address or Host Name	Enter an IP address or hostname.
Port	Enter a port number.

Field	Description
Publishing Interval	This is the requested publishing frequency from the OPC-UA Server. The interval must be greater than or equal to 1000ms. **Note** The OPC-UA server publishing frequency is independent of the metric-specific sample interval. In case the sampling interval (in the following attribute table) of an individual metric is smaller than the publishing interval, the OPC-UA server queues up and send all the sampled values for a metric between the last publish and the current publish.
Advanced Settings	
Authentication	Choose an authentication type: • **Anonymous**: The OPC-UA client inside the EI Agent does not authenticate at the OPC-UA server. Use this authentication type if your OPC-UA server does not have authentication that is enabled for connecting clients. • **Username & Password**: Enter the username and password that the EI Agent must use to authenticate at the OPC-UA server.
Security Mode	This field is non-editable. The default value is **None**.

Field	Description
Attribute Definitions	A data model explains how data is represented in the asset. 1. **Name**: Enter a name for the data model. 2. **Label**: Enter a label for the data model. 3. **Data Type**: From the drop-down menu, select a measurement entity (string, integer, float, long, or boolean) for the OPC-UA data. 4. **OPC_UA Type**: From the drop-down menu, choose **URI** or **INDEX**. 5. **NameSpace URI**: Enter a value to identify the naming authority that defines the identifiers of Node IDs. **Note** This field is editable if you select **URI** under **OPC_UA Type**. 6. **NameSpace Index**: Enter a value to identify the naming authority that defines the identifiers of Node IDs. **Note** This field is editable if you select **INDEX** under **OPC_UA Type**. 7. **Identifier**: Enter a value that is unique across different naming authorities. 8. **Sampling Interval**: Enter a value to indicate the fastest rate at which the server should sample its underlying source for data changes. 9. **Type**: From the drop-down menu, choose the data type for the identifier. The available choices are **Numeric** and **String**. Click **Add** to add more data model attributes to the configuration

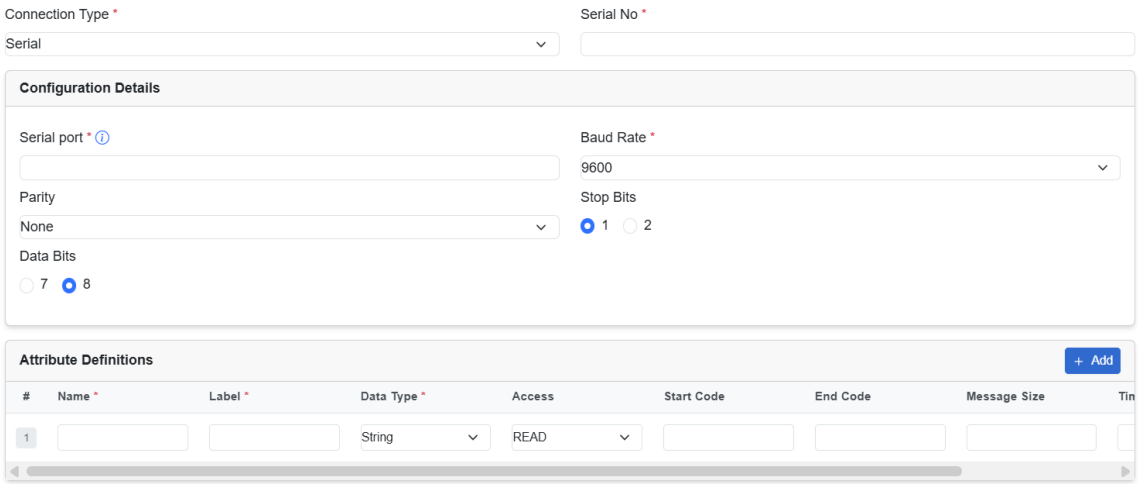
The following is an example of a data model for OPC-UA source type.

```
{
  "apiVersion": 1,
  "connectionType": "OPC_UA",
  "fields": {
    "temperature": {
      "label": "Temperature",
      "description": "",
      "datatype": "Float",
      "nodeId": {
```

```
          "namespaceUri": "2",
          "identifier": "2",
          "type": "numeric"
        },
        "samplingInterval": 1000,
        "category": "TELEMETRY"
      }
    }
  }
}
```

Configure Serial asset type

After you select the asset type **Serial**, enter the required details in the following fields.



Field	Description
Configuration Details	
Serial Port	Enter a port number. For example, `/dev/ttyS0`
Baud Rate	From the drop-down menu, choose 9600, 19200 or you can add a new custom value on it.
Parity	From the drop-down menu, choose **None**, **Odd**, or **Even**
Stop Bits	Choose the radio button for **1** or **2**.
Data Bits	From the drop-down menu, choose **7** or **8**.

Field	Description
Attribute Definitions	A data model explains how data is represented in an asset. 1. **Name**: Enter a name for the data model. 2. **Label**: Enter a label for the data model. 3. **Data Type**: From the drop-down menu, choose **String** or **Binary**. If you select **Binary**, the data is delivered in binary form 1. a. For a data logic policy, the data is delivered as a binary buffer in the data logic script in the *on_update()* function. b. For a data rule policy, the data is sent to the northbound destination in the base64 format. 4. **Access**: From the drop-down menu, choose read, write, or read and write. 5. **Start Code**: Enter the marker that indicates the start of a stream of bytes. 6. **End Code**: Enter the marker that indicates the end of a stream of bytes. 7. **Message Size**: This is the size, in bytes, between the start code and the end code. 8. **Timeout**: Enter a time, in milliseconds, within which to receive data, before it is reset. This is enabled only for **READ** and **READWRITE** access modes. This field is mandatory only if the message size is configured.

Common errors and troubleshooting

Errors can easily occur when configuring a serial port. For example:

- The wiring must be accurate. For example, see the Cisco IR829 installation guide.
- The serial relay service should be configured correctly for the Guest OS. For example, see the Cisco Catalyst IR1101 documentation and Cisco Catalyst IR1800 documentation.
- The physical serial port must be correctly exposed to IOx through the local manager.

To troubleshoot a serial interface:

- Make sure that serial port is configured in propagate mode at the IOS level. A current workaround is to use just the 0x prefix as the StartCode to specify an empty StartCode.
- For testing interface options only:
  - Use a data model with a fixed message size of 1 byte and no start code.

- Verify that there is some data that is coming in to ensure that the connection is working.
- Once this is done, the actual data model can be defined.

Serial Connector data model

A serial connector asset type has a reduced data type.

The following combinations are allowed:

- One read attribute
- One read plus one write attribute
- One read-write attribute

Read attribute allows the following configuration combinations:

- Message Size and Timeout
- StartCode and Message Size and an optional Timeout
- StartCode and EndCode and an optional Timeout

Start-/End-Code prefix handling:

- Prefix 0x allows to specify hex encoded binary data. For example, 0x1310 -> CR+LF)
- **Prefix** allows to specify **as-is**

Serial data model example:

```
{
  "apiVersion": 1,
  "connectionType": "SERIAL",
  "fields": {
    "data_string1": {
      "label": "My Data String",
      "datatype": "String",
      "description":    "serial read attribute",
      "access": "READ"
      "startCode": "$",
      "endCode": "0x0a",
      "messageSize":""
    }
  }
}
```

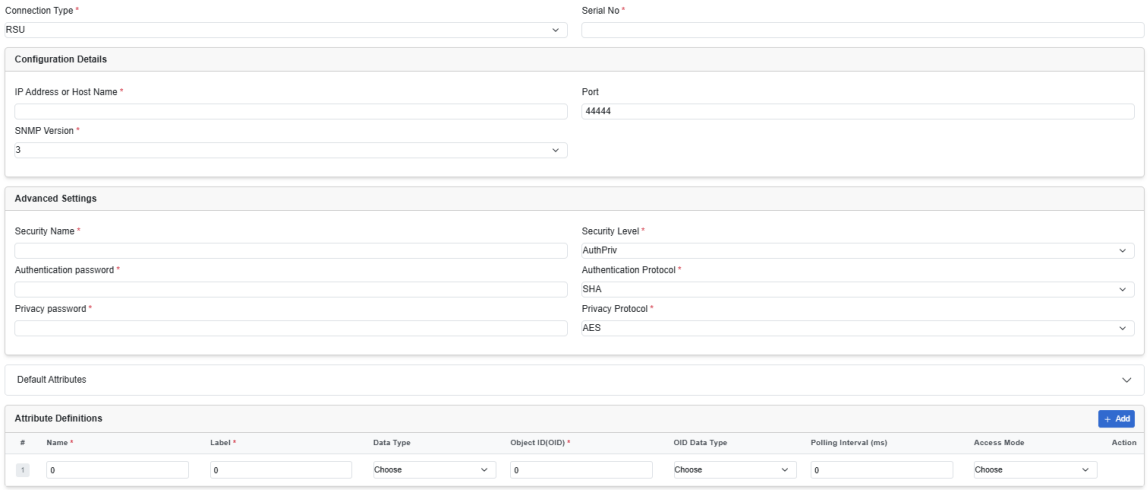
RSU asset type settings

The RSU asset type supports a set of static attributes in addition to the regular configurable attributes. Static attributes are always available and not required to be configured.

- The static attributes have a JSON string content and reflect incoming DSRC messages, except storeAndRepeatMessage and broadcastImmediately static attributes.
- The storeAndRepeatMessage must be set as an array of message objects. All previous messages will be overwritten by the new array.
- The current array of messages can be obtained by reading the attribute.

- The basic configuration for this asset type includes the host, port, and SNMP version.
- Advanced settings like community or authentication data must be set depending on the SNMP version.

In the **Source** tab, from the **Device Type** drop-down list, choose **RSU**. Then, fill the following fields.



Field	Description
Configuration Details	
IP Address or Host Name	Enter the IP address or hostname.
Port	Enter the port number.
SNMP Version	Select a version from the drop-down list from 1, 2c and 3. 3 is the most secure version.
Advanced Settings	Complete these fields based on the selected SNMP Version.
Default Attributes	It shows the default attributes that are specific to RSU. Even if you will not add any additional attributes, it runs for the agents.

Field	Description
Attribute Definitions	A data model explains how data is represented in an asset. 1. **Name**: Enter a name for the data model. 2. **Label**: Enter a label for the data model. 3. **Data Type**: From the drop-down list, choose **String**, **Integer**, **Float**, **Long**, or **Boolean**. 4. **Object ID (OID)**: OID address is used to uniquely identify managed devices and their statuses. 5. **OID Data Type**: OID is the data type for the object. **String** or **Integer**. 6. **Polling Interval (ms)**: This indicates the fastest rate at which the Server should test and debug. Select a unit from the up-down menu. 7. **Access Mode**: From the drop-down list, choose read, write, or read and write. Click **Add** to add more attributes to the asset configuration.

NTCIP1202, NTCIP1203, NTCIP1204 asset type settings

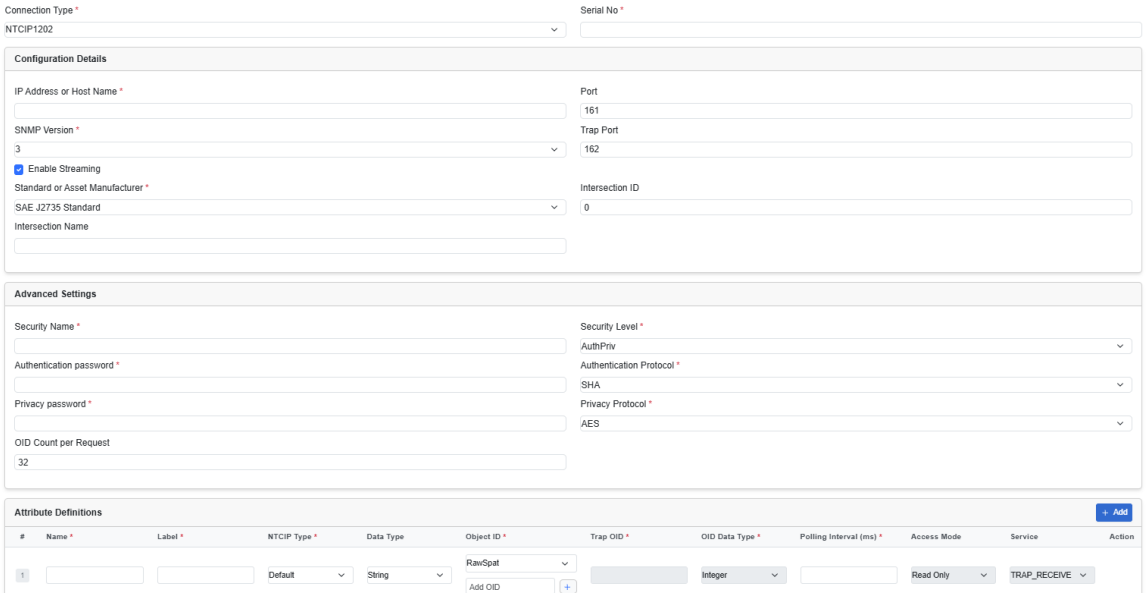
Cisco Edge Intelligence - local manager supports three NTCIP devices. Use the Asset Type for the correct connection type.

- NTCIP 1202—Actuate Signal Controller
- NTCIP 1203—Dynamic Message Sign
- NTCIP 1204—Road Weather Information System

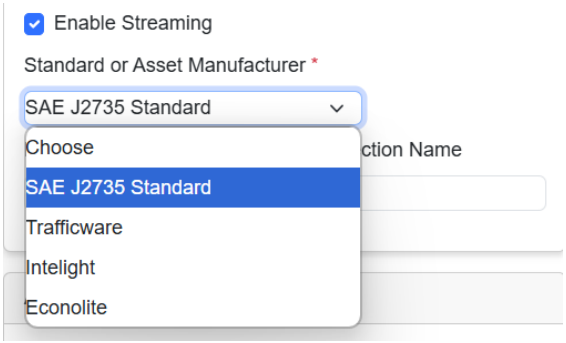
The basic configuration for all these three asset types include the host, port, and SNMP version.

Advanced settings like community or authentication data must be set depending on the SNMP version.

Each NTCIP asset type supports a set of static attributes in addition to the regular configurable attributes.



Field	Description
Configuration Details	
IP Address or Host Name	Provide the IP address or Host Name.
SNMP Version	Select a version from the drop-down list from 1, 2c and 3. 3 is the most secure version.
Port	Provide a NTCIP connector port number. **Note** NTCIP1202 port number should never match Trap port number, and vice versa.
Trap Port (Applicable only for device type: NTCIP1202)	Provide Trap port number. **Note** Trap port number should never match NTCIP1202 port number, and vice versa.

Field	Description
Enable Streaming (Specific to device type: NTCIP1202)	Choose this checkbox to enable Streaming. When you choose to enable Streaming, an additional field **Standard or Asset Manufacturer** protocol is displayed. NTCIP 1202 allows the streaming of data using standard and Asset manufactured protocols. The different protocols are: Standard protocol: • SAE J2735 Standard Asset manufactured protocols • Trafficware • Intelight • Econolite 
Intersection ID (Specific to device type: NTCIP1202)	Intersection ID is optional and depends on the user's specific use case. You can choose to configure this field if required for their particular scenario. For example, in traffic use cases, this information is mandatory.
Intersection Name (Specific to device type: NTCIP1202)	Intersection Name is optional and depends on the user's specific use case. You can choose to configure this field if required for their particular scenario.
Advanced Settings	The specific Advanced Setting details vary based on the SNMP Version. Provide the appropriate authentication information accordingly.

Field	Description
Attribute Definitions	A data model explains how data is represented in an asset. 1. **Name**: Enter a name for the data model. 2. **Label**: Enter a label for the data model. 3. **NTCIP Type**: From the drop-down list, choose **Default** or **trap**. 4. **Data Type**: From the drop-down list, choose **String**, **Integer**, **Float**, **Long**, or **Boolean**. 5. **Object ID**: From the drop-down list, choose **RawSpat**, **NTCIP-1211 SRM**, and **SAE J2735 SRM**. Bottom to that add OID. OID address is used to uniquely identify managed devices and their statuses. **Note** This field is applicable if you select **Default** under **NTCIP Type**. 6. **Trap OID**: Enter an ID for Trap NTCIP type. **Note** This field is applicable if you select **Trap** under **NTCIP Type**. 7. **OID Data Type**: OID is the data type for the object. **String** or **Integer**. 8. **Polling Interval (ms)**: It indicates the fastest rate at which the Server tests and debug. Select a unit from the up-down menu. 9. **Access Mode**: From the drop-down list, choose read, write, or read and write. **Note** This field is applicable if you select **Default** under **NTCIP Type**. 10. **Service**: From the drop-down list, choose TRAP_RECEIVE. **Note** This field is applicable if you select **Trap** under **NTCIP Type**.

Add data destinations

In the **Destination** tab, define where configured data policies must send data to.

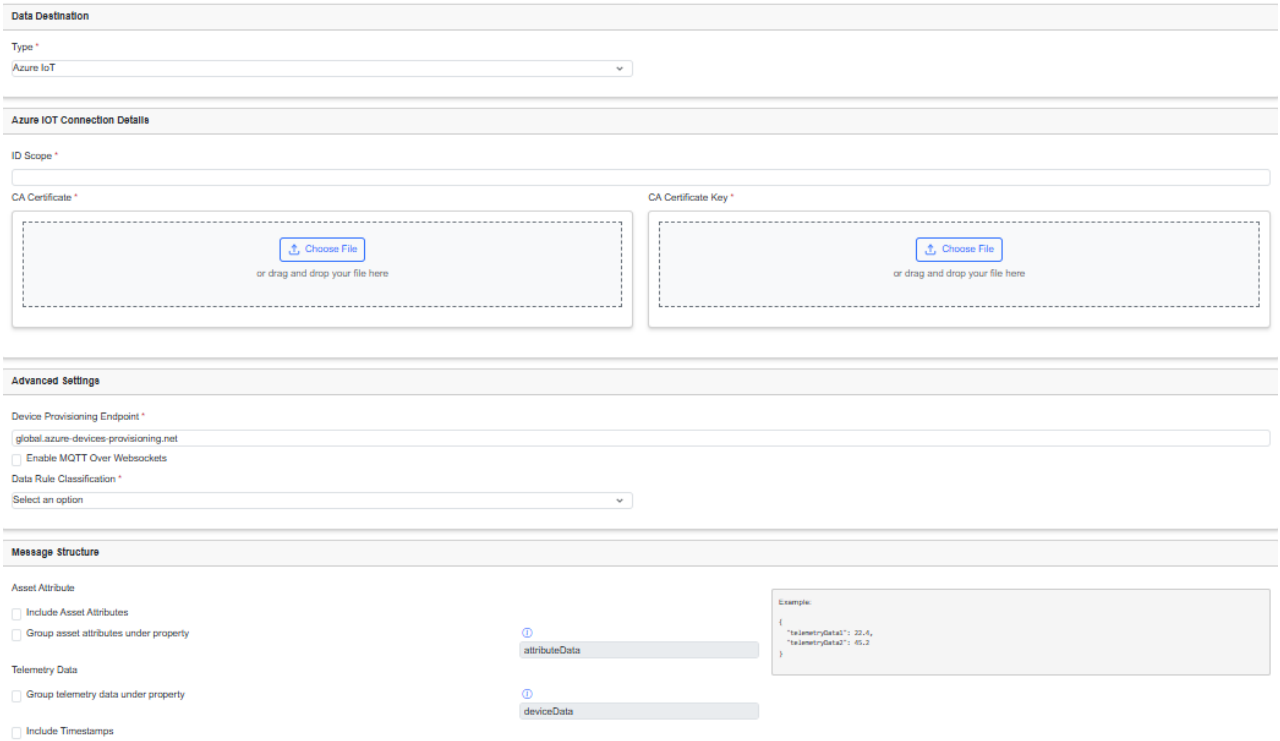
The supported destinations are MQTT servers, AWS IoT server, and Azure IoT Hub. From the **Type** drop-down list, choose the destination. Then, configure the connection settings for the chosen destination.

Before you configure a data destination in the pipeline, ensure that you have set up the servers or hubs. You must have the required identifying information ready to complete the destination configuration.

Add a Microsoft Azure IoT Hub destination

Procedure

In the **Destination** tab, from the **Type** drop-down list, choose **AZURE IoT**, and enter the required details in the following fields.



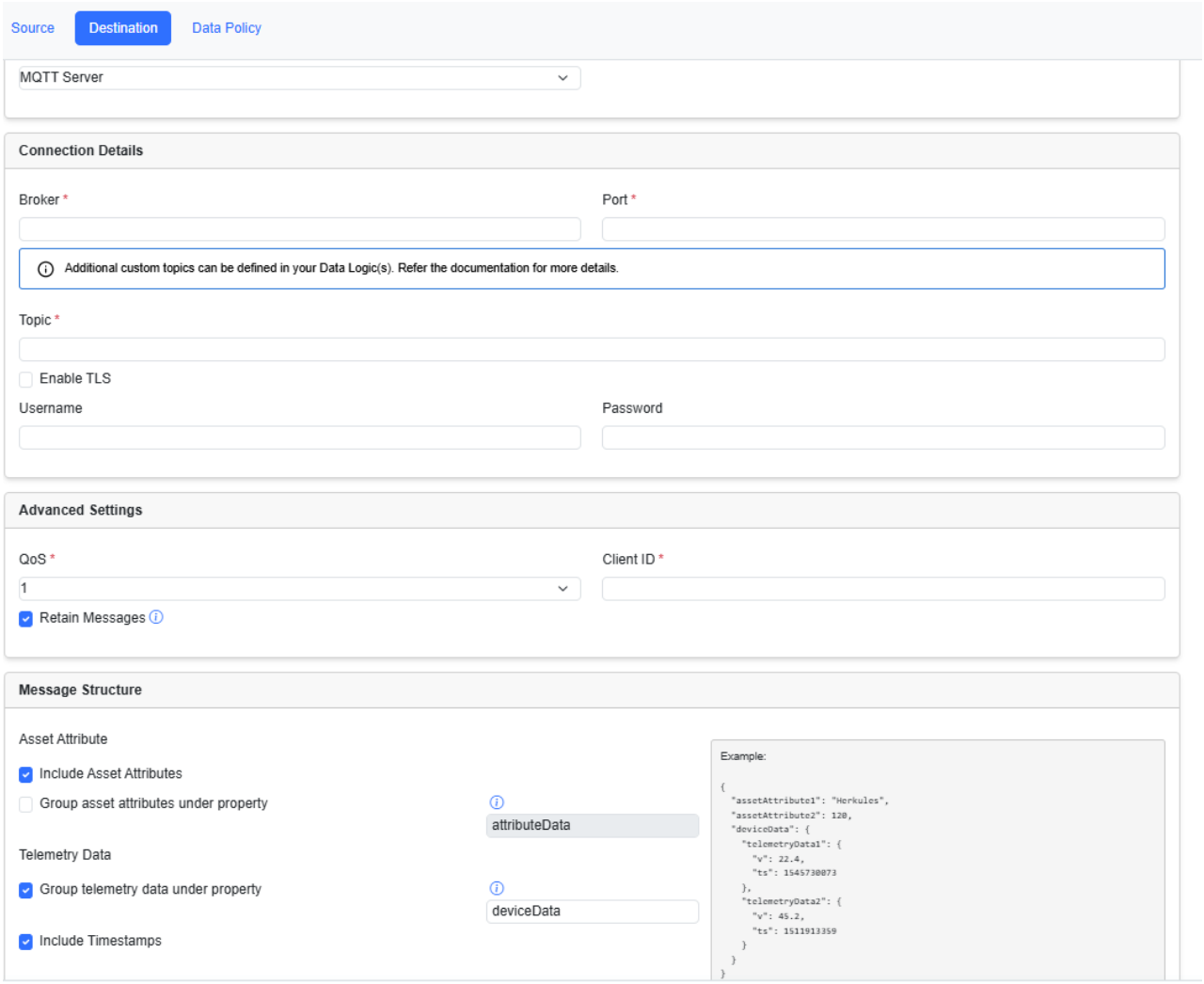
Field	Description
Azure IoT Connection Details	
ID Scope	Enter the ID Scope that is displayed in the **Azure Device Provisioning Service Overview** page.

Field	Description
CA Certificate	Upload the intermediate CA Certificate file that you have configured in your Azure Device Provisioning Service. **Note** The status of this CA certificate in the Azure Provisioning Service must be marked as trusted, or device creation (and therefore metric sending) is not allowed by Azure.
CA Certificate Key	Upload the unencrypted private certificate key file that belongs to the intermediate CA certificate that you uploaded. The private key must be in PKCS8 format, and must not include a passphrase. To convert an existing key, use the command: `openssl pkcs8 -topk8 -inform PEM -outform PEM -nocrypt -in azure-iot-test-only.intermediate.key.pem -out azure-iot-test-only.intermediate.pkcs8.pem`
Advanced Settings	
Device Provisioning Endpoint	Enter the **Global Device Endpoint** value from the Azure IoT Hub Device Provisioning Service.
Enable MQTT over WebSockets	Check this check box to enable the browser to leverage all MQTT features.
Data Rule Classification	From the drop-down list, choose **DEVICE_PROPERTY** or **TELEMETRY**.
Message Structure	Choose the required options in this area to customize the structure of the device-to-cloud message. You can choose **Include asset attributes**, **Group asset attributes under property** in the Asset Attributes section or choose **Group telemetry data under property**, **Include Timestamps** in the Telemetry Data section. The data can be sent in a flat structure or can be grouped with a key. Customization does not apply if the chosen data policy is of the type Device Properties.

Add an MQTT Server destination

Procedure

In the **Destination** tab, from the **Type** drop-down list, choose **MQTT Server** and enter the required details in the following fields.



Field	Description
Connection Details	
Broker	Enter the URL or IP address of your MQTT broker.
Port	Enter the port number used by the broker.

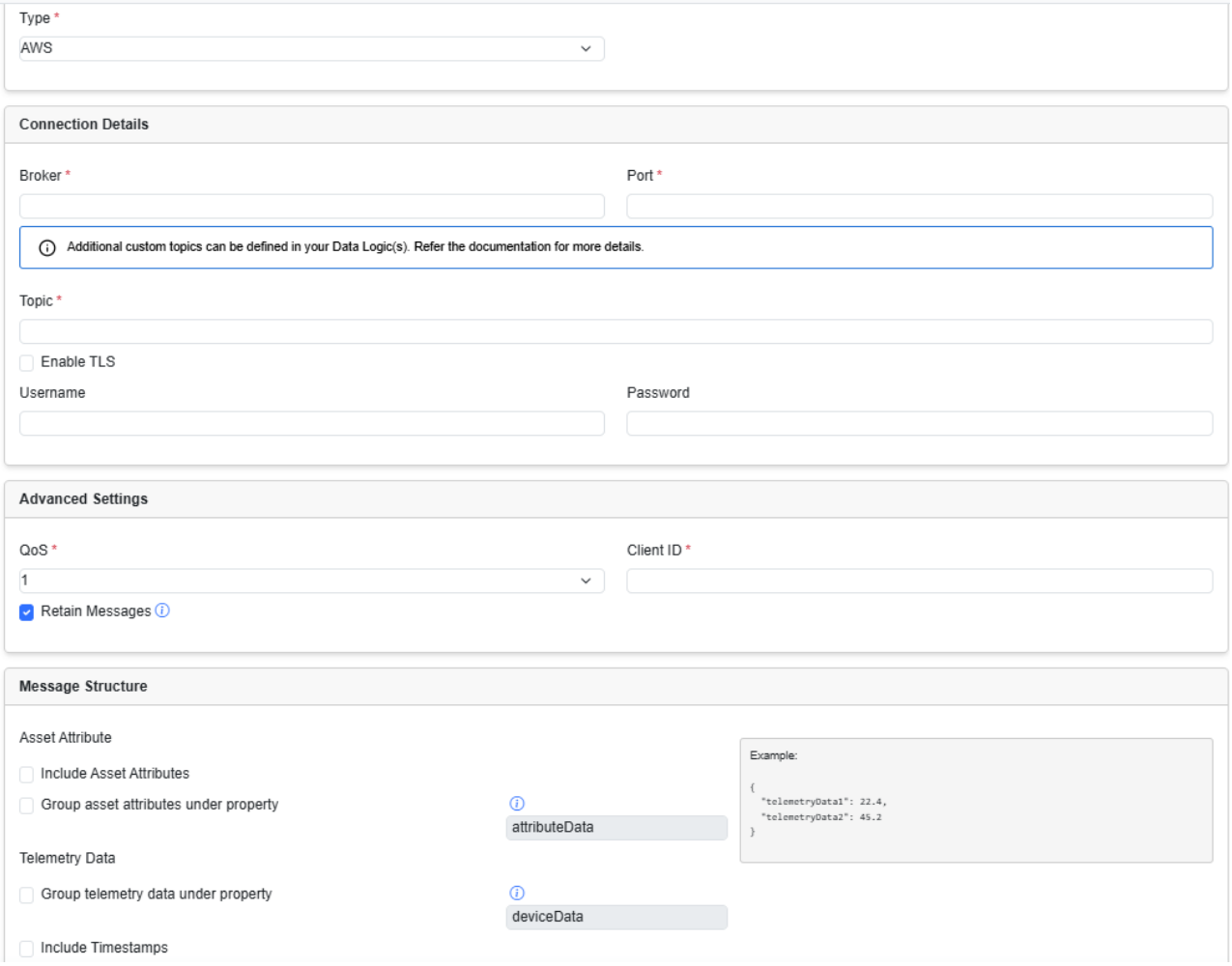
Field	Description
Topic	Enter the topic to which device states and other data are published. For example, cisco/edge-intelligence/telemetry/%deviceSerialNumber%/%deviceSerialNumber%. The example topic matches the device or asset instance serial number that is configured previously in the source tab. **Note** MQTT topic has a restricted number of characters that can be used in a topic name. For example, # or + cannot be part of a topic name. Topic names are URL-encoded to ensure that they do not violate MQTT specifications. URL-encoding also allows northbound applications to decode a topic easily to get to the original contents.
Enable TLS	Check the TLS check box to enable the protocol. When you choose TLS, the following fields are displayed: • **Verify Peer**: Check this checkbox to allow peer verification. When you select this option, the **Certificate** field is displayed where you can upload a CA certificate. • **Enable X.509**: Check this check box to use X.509 certificates. When you select this option, two fields are displayed where you can upload a CA certificate and a private key. Enabling the use of X.509 certificates allows you to turn on configure MQTT brokers (like Mosquitto) to require certificates for authentication. You can also use X.509 client certificates instead of usernames and passwords to ensure that only trusted assets are allowed to send data to a cloud MQTT broker. **Note** • The private key must be PKCS8-compatible. • The generated certificate for each asset contains the CN - Serial Number of the asset. • X.509 certificates can be used with the username and password authentication method, or as the only authentication method.
Username	Enter the username to connect to the MQTT destination broker.
Password	Enter the password to connect to the MQTT destination broker.

Field	Description
Advanced Settings	
QoS	From the drop-down list, choose **0**, **1**, or **2**.
Client ID	Enter a Client ID. The Client ID field is not URL-encoded because there are no restrictions in MQTT specifications about allowed characters.
Retain Messages	Check this check-box to retain messages on the broker for new subscribers.
Message Structure	Choose the required options in this area to customize the structure of the device-to-cloud message. You can choose **Include asset attributes**, **Group asset attributes under property** in Asset Attributes section or choose **Group telemetry data under property**, **Include Timestamps** in Telemetry Data section. The data can be sent in a flat structure or grouped with a key. Customization does not apply if the chosen data policy is of the type Device Properties.
Cloud to Network Device	
Enable cloud to data logic commands	Use the cloud to data logic commands to send a command (with payload) from a cloud app to a data logic on an edge device. The data logic script parses the command. This feature provides bi-directional communication between the cloud and edge, allowing the application to send a command and receive a response. For example, a cold storage unit connected to an edge device can send commands to: • Set the temperature on the cold storage unit • Initiate a defrost action on the cold storage unit To enable cloud to data logic commands, enter the following topic values: **a.** **Command Topic**: Enter the syntax and variables in the format, *cisco/edge-intelligence/**commands**/variable*. **b.** **Response Topic**: The response topic must use the format *cisco/edge-intelligence/**responses**/variable*. Responses are optional. If a script doesn't send a response, nothing is published to the topic.

Add an AWS Server destination

Procedure

From the **Destination** tab, from the **Type** drop-down list, choose **AWS** and enter the required details in the following fields.



Field	Description
Connection Details	
Broker	Enter the URL or IP address of your AWS broker. This info can be found from the AWS IoT **Settings** page
Port	Enter `8883`.
Topic	Enter a topic to which device states and other data are published.

Field	Description
Enable TLS	For AWS destinations, you must enable the TLS protocol. When you choose TLS, the following fields are displayed: • **Verify Peer**: Do not choose this option. • **Enable X.509**: Check this check box to use X.509 certificates. When you select this option, two fields are displayed where you can upload a CA certificate and a private key.
Username	Do not enter any value in this field.
Password	Do not enter any value in this field.
Advanced Settings	
QoS	From the drop-down list, choose **1**.
Client ID	Enter a Client ID.
Retain Messages	For AWS destination type, do not choose the **Retain Messages** option. This option retains messages on the broker for new subscribers.
Message Structure	Choose the required options in this area to customize the structure of the device-to-cloud message. You can choose to include asset attributes, include timestamps, group asset attributes, or group telemetry data in the device-to-cloud messages. The data can be sent in a flat structure or can be grouped with a key. Customization does not apply if the chosen data policy is of the type Device Properties.
Cloud to Network Device	

Field	Description
Enable cloud to data logic commands	Use the cloud to data logic commands to send a command (with payload) from a cloud app to a data logic on an edge device. The data logic script parses the command. This feature provides bi-directional communication between the cloud and edge, allowing the application to send a command and receive a response. For example, a cold storage unit connected to an edge device can send commands to: • Set the temperature on the cold storage unit • Initiate a defrost action on the cold storage unit To enable cloud to data logic commands, enter the following topic values: **a.** **Command Topic**: Enter the syntax and variables in the format, *cisco/edge-intelligence/**commands**/variable*. **b.** **Response Topic**: The response topic must use the format *cisco/edge-intelligence/**responses**/variable*. Responses are optional. If a script doesn't send a response, nothing is published to the topic.

About Data Policies

Data Policies define how data is sent from edge assets to a destination. There are two types of policies:

- **Data Rule**: Data is sent from Assets to a destination without transformation.
- **Data Logic**: Data is transformed before being sent to a destination. Data Logic scripts are developed using Microsoft VS Code and embedded UI editor.

Restriction Make sure to configure Data Logic when you have configured multiple Source type. Proceeding only with Data Rule, will pop-up an error while deployment.

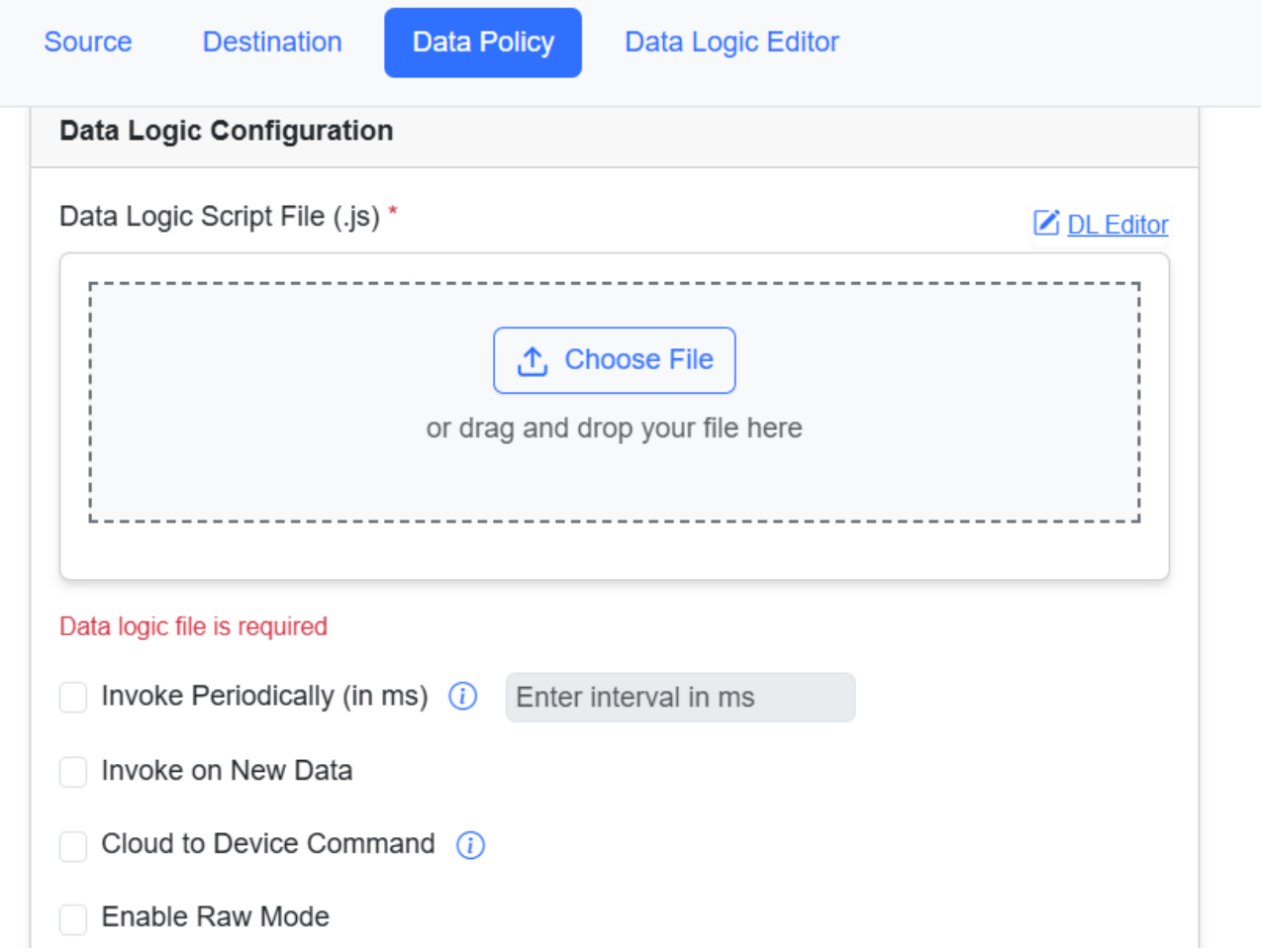
Create a Data Logic

Data logic is used to transform data from connected assets before it is delivered to a destination. Unlike Data Rules that send all the raw data for an Asset Type, Data Logic allows you to aggregate or average data, send only data that exceeds certain value, detect anomalies, and more.

Data Logic is developed and debugged using JavaScript in Microsoft Visual Studio (VS Code) and embedded UI editor. Scripts are synchronized to Cisco IoT where they can be deployed to EI Agents running on Edge Devices.

Procedure

Step 1 From the **Data Policy** tab, select **Data Logic** checkbox.

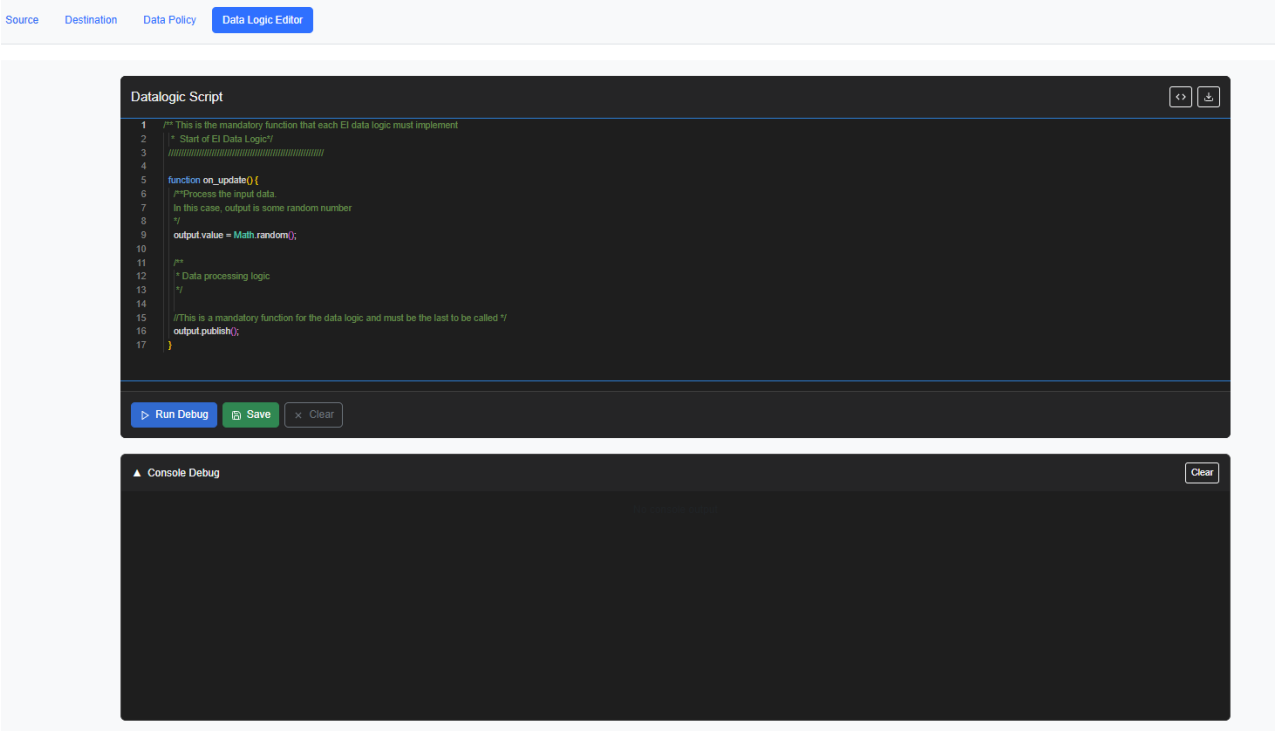


Note
Clicking upon **Data Logic** radio button the **Data Logic Editor** tab appears next to Data Policy.

Step 2 To add a data logic script, click **Choose File** to select precreated new script (example: **LogicExample.js**) from your local drive.

Step 3 To review or to create a new data logic script, click **DL Editor**.

- It helps to verify and validate the existing script file by clicking **Run Debug**.
- You can write a new script and validate it.



Step 4 After you upload a script file, the new download and delete icon appears. It helps to check/validate what uploaded from other agents. Another user can also check an existing pipeline and can download it.

Step 5 From the following run-time options, select when the script will be run.

- **Invoke Periodically (in ms)**: when you tick the checkbox, it enables the ms interval. Enter the interval time, in ms. For example, if you enter 500, the Data Logic script will be called every 500 ms. Enable this option if needed.
- **Invoke on New Data**: The script is called when data changes.
- **Cloud to Device Command**: This function is called when you receive a command from the cloud.
- **Enable Raw Mode**: A default output JSON data model is automatically created when a Data Logic script is created.
- (Optional) In the **Output Logic Data Model**, you can modify the default format of the Output Data Logic Model script (in JSON) and specify the output model with custom names.

  Valid categories: TELEMETRY, PROPERTY, ATTRIBUTE

  Valid types: string, int, binary, boolean, double

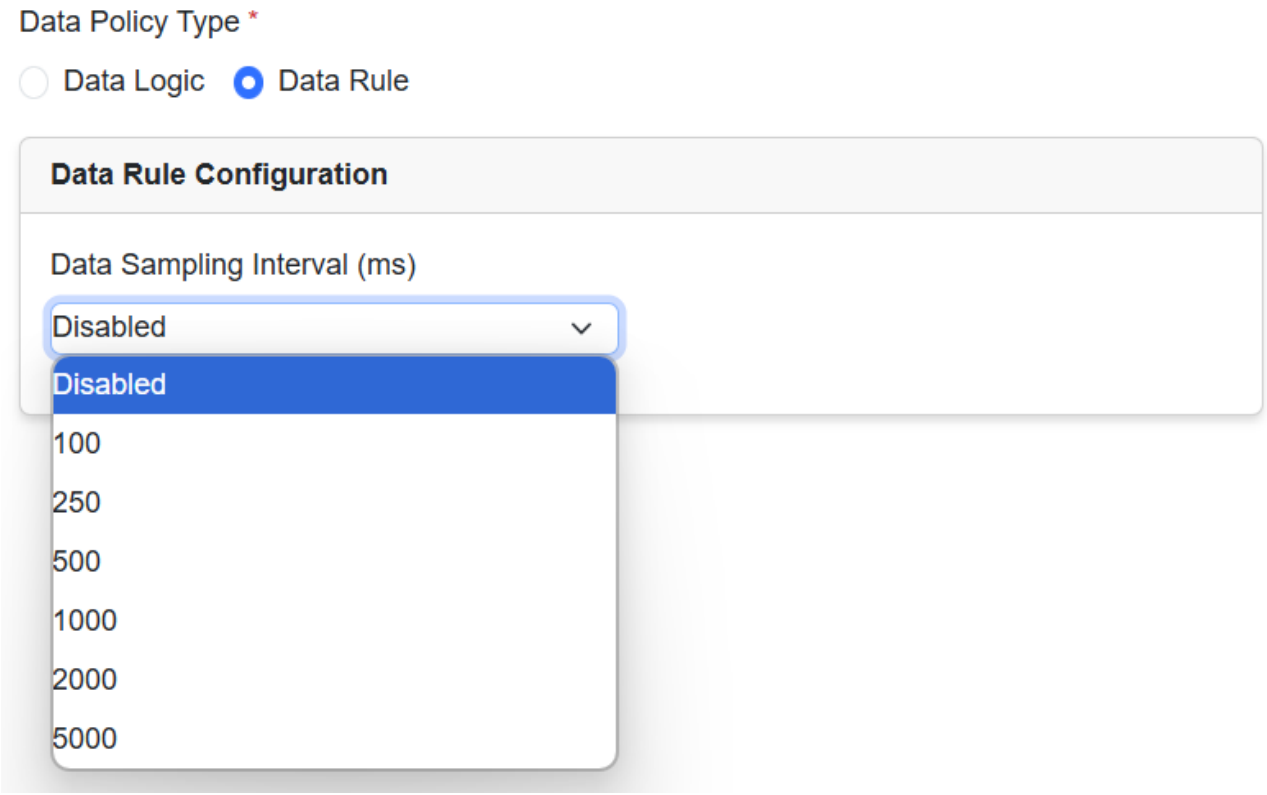
Create a Data Rule

Data rules define the flow of data, from connected assets to data destinations, without transformation.

Procedure

Step 1 From the **Data Policy** tab, select **Data Rule** checkbox.

Step 2 To configure the Data Rule, select a data from **Data Sampling Inerval (ms)** drop-down list.



Deploy or undeploy pipelines

When deployed, a pipeline runs on the Cisco network device where the EI agent is installed.

Procedure

Step 1 To deploy a pipeline:

a) Create a pipeline.

b) Click **Deploy**.

The deployed pipeline is listed in the **Pipelines** area of the Cisco Edge Intelligence page.

Step 2 To undeploy a pipeline, in the **Pipeline** section, select a pipeline and click **Undeploy**.

When you undeploy a pipeline, it is entirely removed from Cisco Edge Intelligence. If you wish to retain a copy of the configuration, save the pipeline configuration as a template before you undeploy the pipeline.

View health status

To track the health status of an EI agent, select a pipeline from the list of pipelines.

Procedure

Step 1 From the left pane, click any **Pipeline** which you want to view the details.

Step 2 Click **Health Status** tab. A combined list log of pipeline overview, source status, and destination status appears for the EI agent.

Step 3 Click on any status tab to preview each log report.

Column Header	Description
Health Status	Displays the overall health of the data pipeline, indicating errors in source or destination connections.
Pipeline Status	Shows the current status of the data pipeline. For example, Error and so on.
Source Status	Indicates the connection status (online or offline) of the source asset.
Destination Status	Reflects the status (online or offline) of the data destination.