SAP Interface Integration Certification

SAP Interface Scenarios:
IOT Gateway Edge Device 1.0

IOT-GW-EDGE-DEVICE 1.0

Test Procedure

SAP Integration and Certification Center
icc@sap.com

Document Version 1.3
August 16, 2017

THE BEST RUN SAP

Document Details

Name	Objective	Audience	Description
IOT Gateway Edge Device 1.0 IOT-GW-EDGE-DEVICE 1.0 Certification Procedure	SAP Interface Integration	SAP Partners	Specification for a Hardware Interface to SAP Cloud Platform Internet of Things Gateway Edge Certification.

For any info on this document please contact:

Name	Email ID
SAP Integration and Certification Center	icc@sap.com

Change Log

Version	Date	Author	Description
1.0	June 20, 2017	Hemachandran, Sujit	Initial document
1.1	August 16, 2017	Dan Tauro	Added Section 3.2 Security Questions.
1.2	October 26, 2017	Dan Tauro	Minor adjustments
1.3	November 21, 2017	Dan Tauro	Modified procedure for New Software Release
1.3a	December 5, 2017	Dan Tauro	Minor adjustments
1.4	March 1, 2018	Dan Tauro	Graphics updated

Document Release

Version	Date	Approved By	Description
1.00	June 20, 2017	IOT Certification core team	To be used for certification process and amendment for certification agreements

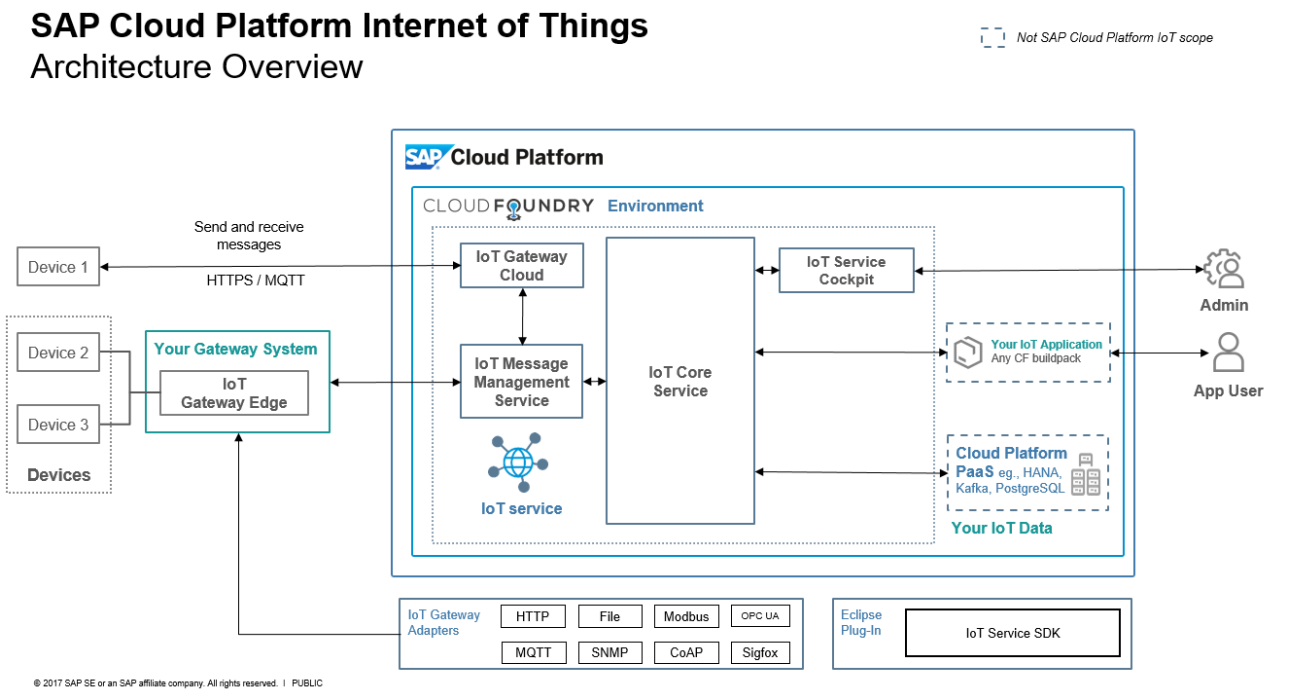
www.sap.com/contactsap

IOT GATEWAY EDGE CERTIFICATION PROCEDURE: INTRODUCTION

The Internet of Things service connects devices to the SAP Cloud Platform to provide scalable ingestion of IoT data and device management. The respective services provide a secure connection to remote devices using a broad variety of IoT protocols and manage the device lifecycle from onboarding to decommissioning.

The Internet of Things service collects and processes sensor data at scale already at the edge or in the cloud and stores it on the SAP Cloud Platform for use by other applications. Moreover, the Internet of Things service provides a multi-tenant architecture allowing role-based access to device data through easy-to-use APIs.

The Internet of Things Gateway provides adapters for network convergence and syntactic protocol normalization. The Internet of Things Gateway acts as a virtual gateway that brings devices and assets online, managing the connectivity with devices according to the specific communication protocol that the devices implement. The Internet of Things Gateway component is responsible for collecting data from a sensor and sending commands to the network on behalf of other Internet of Things Core Service modules.



Partner will supply the hardware for IoT Gateway Edge. The version of Gateway tested must be the latest released version. Please note the “Validity of Certification section. The Gateway can either be downloaded from the Service Market Place or can be supplied by the certification team. To download from Service Market Place, use this link. search for IOT SERVICES EDGE

The “Device” is simulated via Paho MQTT Simulator by Eclipse. The IOT Core services and IOT Service cockpit etc. are part of the SAP Cloud Platform and are therefore supplied by SAP.

This certification comprises of the following processes. The Device sends sensor data to the IoT Gateway Edge. The Gateway Edge device formats and forwards the data to the SAP Cloud Platform. The IoT Admin person can view the sensor data. The data is now ready for other applications to consume the data.

This document presents a certification plan for the IOT Gateway Edge. Certification allows manufacturers of Edge Devices to demonstrate successful implementation of the IOT Gateway Edge software on their hardware devices. This certification may not be taken to imply any valuation of an IOT Edge Hardware platform. Rather, the certification guarantees only that the tested functionality is correctly executed. Further,

no implication is made as to the performance of the Gateway device, its suitability for uses other than utilization of the tested functionality, or its quality and utility relative to other hardware platforms.

This certification does not test any custom developed software including drivers and external IO.

Prerequisites:
Oracle Java Version 8 JRE for windows JVM for Linux
TCP/IP wired or Wi-Fi.
Gateway Edge latest GA release
Gateway Edge Device must be reachable from an external network
SAP NOTE with Hardware Minimums SAP NOTE 0002387440
INFOZIP is required on Linux Environments.

Validity of Certification

Validity of Certification
Certification is release dependent and valid for the following combination: the specific version of IoT Gateway Edge listed on the certificate, in connection with a specific device model and the operating system originally tested against.

Certification is valid for two years, if all elements of the above combination remain under general maintenance: IoT Gateway Edge version from SAP, device model from partner, and OS version.

If the SAP IoT Gateway Edge version that partner certified against goes out of maintenance during the initial two year validity period of the certification, SAP will offer to partner a free of charge re-certification against the newer version of IoT Gateway Edge. Please refer to SAP NOTE 0002387440 for details.

Further Information:
You can find the official documentation on the SAP HELP PORTAL. HELP.SAP.COM-SAP CLOUD PLATFORM INTERNET OF THINGS. Installation and of course test procedure for the Gateway is available as part of this document.

1 SETUP OF IOT GATEWAY EDGE FOR MQTT PROTOCOL

Prerequisites	You need an instance of the SAP Cloud Platform Internet of Things Service. You need the host name (referred to as **<HOST_NAME>** in the following) which you can use to access the system. Java must be installed to launch Paho client and IOT Gateway Edge. JAVA_HOME operating system variable set home of directory of JRE/JVM
Notes	Basic authentication credentials must be used as follows: name = <`user`>, for example `max` password = <`password`>
URL Scheme	Internet of Things Service Cockpit: `https://trial.canary.cp.iot.sap/iot/cockpit/` Internet of Things API Service: `https://trial.canary.cp.iot.sap/iot/core/api/v1/doc/`
References	User Guide for the Internet of Things Service Cockpit on the SAP Help Portal (Logon required). Glossary
Tool Downloads	Paho Client (Linux/ Windows/ macOS) OpenSSL (Windows)

Step	Description	Additional Data
Setting Up the Internet of Things Gateway Edge		
1.	***Open the terminal (macOS) or command line tool CMD (Windows) and change the directory to the path of the extracted ZIP file Internet of Things Gateway Edge.***	***The directory must contain the following files: build.bat or build.sh (executable).***
2.	***Launch build.bat (Windows) or build.sh (macOS) in the extracted folder.*** ***Note*** ***To launch build.bat on Windows an installation of Java Development Kit (JDK) is required.***	***For Windows:*** ***build.bat MQTT*** ***For Mac:*** ***./build.sh MQTT*** ***A new file config_gateway_mqtt.xml is created in the /config folder.***
3.	***Open the config_gateway _mqtt.xml with a text editor.***	

Step	Description	Additional Data
4.	***Enter the <HOST_NAME> for the connectionString and for the two address elements in the coreBundles by replacing 127.0.0.1*** ***In this case use "trial.canary.cp.iot.sap"***	***Sample Code*** ***<cnf:connectionString>failover:(nio+ssl://sample.cp.iot.sap:61616?daemon=true&soTimeout=60000)</cnf:connectionString>*** ***<cnf:cxf lan="true">*** ***<cnf:address dev="core">sample.cp.iot.sap</cnf:address>*** ***<cnf:cxf lan="false">*** ***<cnf:address dev="core">sample.cp.iot.sap</cnf:address>***

Step	Description	Additional Data
5.	***Set the uri parameter in the<cnf:transportConnector> tag to the IP of the system where the Internet of Things Gateway Edge is running.*** ***Note*** ***The server binds only to the uri given in<cnf:transportConnector>tag. Specify one of your local IP addresses here. The address you bind the server to and the address you access the server can be different, depending on your network topology, for example, reverse proxies.*** ***Note*** ***The default port for the MQTT API is 61618 (if necessary change it by setting the value in the uri).***	***Sample Code*** ***<cnf:transportConnector name="mqtt" uri="mqtt://192.168.1.1:61618?transport.soTimeout=60000"/>*** ***Note*** ***In case the Internet of Things Gateway Edge is running on localhost, leave it at 127.0.0.1 . For Linux systems set this to the local IP.***

Step	Description	Additional Data
6.	***Optional:*** ***Add attribute gatewayAlternateId to the<cnf:gateway> tag.***	***Sample Code*** ***<cnf:gateway gatewayAlternateId="1122334455667788">*** ***Note*** ***In case of problems on gateway startup due to gateway alternate Ids being used multiple times in the Internet of Things Service Cockpit, the atewayAlternateId of the network to be created can be changed by adding this attribute. Set the attributes value to a valid alphanumeric string.***
7.	***Save your changes to the file.***	
Downloading Certificate		
1.	***Log on to the Internet of Things Service Cockpit with your user credentials.***	
2.	***Choose (Show/hide information about the current user) in the upper right corner.***	***The system displays the Name, Tenant, Role and a Certificate Download of your user.***
5.	***Choose Download.***	***The system starts to download a ZIP file, which is named certificate-<user>.zip and contains the certificates.***

Step	Description	Additional Data
6.	***Extract the certificate-<user>.zip file inside a folder certificates of the configfolder of the extracted Internet of Things Gateway Edge.***	***Create the "config/certificates" directory if it does not exist.***
7.	***Open the pswd.properties file in the certificates folder with a text editor.***	
8.	***Enter your user password as password.***	***password = <password>*** A password will be provided during certification
9.	***Save your changes to the file.***	
Starting the Internet of Things Gateway Edge		
1.	***Open the terminal (macOS) or command line tool CMD (Windows) and change the directory to the path of the extracted ZIP file Internet of Things Gateway Edge.***	***The directory must contain the following files: gateway.bat (Windows) or gateway.sh (macOS/Linux) (executable)***

Step	Description	Additional Data
2.	***Launch gateway.bat (Windows) or gateway.sh (mac OS) located in the root of the extracted folder.***	***For Windows:*** ***gateway.bat*** ***For Mac/Linux:*** ***./gateway.sh*** ***Note*** ***You must be connected to public Internet. Most corporate networks do not work due to port and protocol restrictions.*** ***If the Internet of Things Gateway Edge is started successfully, you see the following message Initialization successfully finished.***

2 SEND MQTT DATA VIA PAHO CLIENT

In this step, we will send the data from Device Simulator that supports MQTT protocol. We have already on-boarded this simulator device during previous steps. Once we send the data, it would be received by Internet of Things Gateway Edge, which will send the data to IOT Core Services and data would be visible in the IoT services cockpit and vis APIs.

1.	Open the Paho client.	
2.	Choose in the **Connections** tab to create a new connection.	The system opens a new tab with the connection details.
3.	Choose the **MQTT** tab of the connection (default).	
4.	Add the **Server URI** which contains the IP by which the server, where the Internet of Things Gateway Edge is running, can be accessed from outside the network. Note In case the Internet of Things Gateway Edge is running on localhost, use 127.0.0.1 .	Add the **Server URI** as follows:tcp://<IP_GW_EDGE>:61618
5.	Choose **Connect**.	The status should be **Connected**.

6.	Enter the **Topic** in the **Publication** section. For the purposes of certification use: **measures/ICCMQTTDevice**	Topic: measures/<DEVICE_ALTERNATE_ID> Enter the <DEVICE_ALTERNATE_ID> as a string. For example: measures/44556677 Note The Alternate ID string can be composed of any printable ASCII characters, with the following exceptions: +, <,>, #, *, ., \, /,& and the blank space character. Including any of the above characters in the provided Alternate ID will prevent the device creation from completing successfully. A new device should be created automatically in the Internet of Things Service Cockpit with the same Alternate ID as inserted here. It should include a sensor with Alternate ID 1234567890 and a Temperature configuration.
7.	Enter the **Message** in the **Publication** section. For the purposes of certification use: { "capabilityAlternateId": "1", "sensorAlternateId": "0", "measures": [["NN.N"]] }	Use This message: Sample message: { "capabilityAlternateId": "1", "sensorAlternateId": "0", "measures": [["45"]] } In this JSON sample: • The Capability Alternate ID 1 is related to a temperature capability of a sensor with Alternate ID 0. • The measure can be adjusted to any numeric temperature value.
8.	Choose **Publish**.	A message is sent to the SAP Cloud Platform Internet of Things Service using the Internet of Things Gateway Edge (MQTT).
9.	Change the Temperature and send again.	

3 CONSUME AND VIEW SENSOR DATA

1.	Log on to the Internet of Things Service Cockpit with your user credentials.	You can access the Internet of Things Service Cockpit at https://trial.canary.cp.iot.sap/iot/cockpit. For more information, please refer to the Internet of Things Service Cockpit documentation.
2.	Choose **Devices**.	All devices are listed.
4.	Search and select the device.	
5.	In the device detail page, choose the **Data Visualization** tab.	
6.	Select a **Sensor** from the dropdown list.	Select Sensor 0

7.	Select a **Capability** from the dropdown list.	Select Temperature
8.	Select the **Properties** from the dropdown list you would like to visualize in the chart.	Select Temperature
	You have the following options for the chart: • □ (Refresh chart): refreshes the view manually. • □ (Legend): explains the meanings of all visual elements in the chart. • □ (Zoom In) • □ (Zoom Out) • □ (Open Full Screen) You have the following options to refresh the view: • To refresh the view manually, choose □ (Refresh chart). • To refresh the view automatically, turn **Auto Refresh**to **ON**. If turned on, it updates the chart automatically every second. Tip You can filter the values to see only specific number of recent values (100, 50, 30, 10) in the chart. You can see the information about each data point by selecting them in the chart.	You should see the numbers you published in the Paho Client.

3.1 Security Questions

This Security-related questionnaire needs to be answered. This information is recorded in the Test Report but not in the certificate.

Security Questionnaire:

What level of user privileges does the owner/operator of the device have on the device, and what level of access does your company have once deployed? i.e. a limited privileged user, administrative access, super user/root access?

How does the firmware upgrade mechanism operate, and what level of involvement by your company does this require? Please document whether the device features automatic updates, is the owner/operator able to modify the firmware and/or its source code made available?