IoT Platform
Service Details Instruction Manual
(Version 5.1_0)

<Revision History>

Version No.	Description	Date
Version 1.0	First version	2016/10/07
Version 1.1	Review and Edits for launch on K5 environment in UK	2016/11/01
Version 1.2	Error Correction (method of acquiring necessary technical information; supporting status of MQTT/MQTTS when granting operating permission)	2016/12/01
Version 1.2	Error correction	2017/01/12
4_1.0	Added details regarding enhanced functions (1) Added notes on P/G permissions, protocol restrictions and client certificates to access code settings in 2.3.7 (2) Added the following to Service Portal screen functions in 2.4.3 "Error log storage" "CORS function" "Client certificate" (3) Changed the name of item (2) in 2.3.6.2 and 2.3.6.3 from system version to API version	Internal version (Not released)
4_2.0	Deleted section on enhanced features of version 4_1.0 2.4.2 Added Windows 10 to the list of Service Portal operating environments 2.10 Added "Error Log Storage" 2.11 "CORS Support" 2.12 "Client Certificates" Changed the manual name from "FUJITSU Cloud Service K5 IoT Platform Service Details Instruction Manual" to "IoT Platform Service Details Instruction Manual" 3.1 Changed guidelines for the frequency of service use	2017/8/1
4_2.1	Modified section 3.1 Response for Uses that Exceed Usage Guidelines Added section 3.8 DoS measure Added section 4.8 Deletion of Event Setting	2017/10/11
5.0_0	Added explanation of BSON in Terms Added section 2.3.6 csv/text/binary(under 256Kbyte) data for JSON form is available. Moved contents of Section 2.13.3 and 2.13.4 to Section 2.5.3 and 2.5.5 respectively. Added 2.3.7.4 is Issue client certificate the customer made is available. Other minor changes	2017/11/15
5.0_1	Deleted section 2.3.6.2 TLS 1.1 of SSL support	2018/1/9
5.1_0	Version upgrade	2018/3/17

2

Preface

Thank you for considering the "FUJITSU Cloud Service K5 IoT Platform Service (hereafter, this service)".
This "FUJITSU Cloud Service K5 IoT Platform Service Details Instruction Manual (hereafter, this manual)" is intended for customers considering or implementing this service. We ask for your understanding regarding the following matters.

1   Customers considering this service are kindly requested to utilize   this manual to assist in making their decision to implement this service only.
2. This manual and the contents therein are not to be disclosed or provided to any third parties.
3   Copying or reproducing the contents of this manual without the permission of the provider is prohibited.

This manual contains important information to be used in implementing this service.
Customers signing up to a service contract are asked to thoroughly read this manual prior to using this service.
Please handle this manual with care and store it in a safe place.
Customers opting to not use this service are responsible for promptly disposing of this manual.

*Windows and Internet Explorer are registered trademarks of Microsoft Corporation.

The contents of this manual may change without notice.

<Terms>

Term	Description	Notes
IoT	An abbreviation of "Internet of Things" This refers to "things" connected to a network via an Internet protocol (Internet language)".	
REST	An abbreviation of REpresentational State Transfer This refers to a software design format where design principles optimized for linking multiple software instances are adapted for the web. *A caller interface (referred to as a "RESTful API") sends messages written in XML to a specific URL via HTTP(s). For this service, replies are provided in JSON format.	
MQTT	An abbreviation of Message Queuing Telemetry Transport MQTT is a light communications protocol on the TCP/IP network suited to frequently sending and receiving short messages between multiple subjects. The use of MQTT is now very common in M2M networks and the IoT (Internet of Things) field. At a minimum, the header is only two bytes in size, significantly reducing the amount of communications traffic, CPU load and energy consumption required, compared to sending the same communications via HTTP.	
Dynamic resource controller (DRC)	Dynamic Resource Controller Provides distributed control processing based on proprietary wide-area distribution technologies. This function assists in the optimal collection of data from a limited number of resources based on traffic fluctuation during data collection.	
BSON	Data exchange format mostly used as data storage and network forwarding format of Mongo DB.	
Resource	The collection unit for IoT data	
Resource data	One piece of data	
Access code	Authorization information for resources	

4

- Contents -

Chapter 1   FUJITSU Cloud Service K5 IoT Platform

1.1. Overview

This is an IoT-dedicated cloud service responsible for:

- sending, receiving and storing data for the large number of devices required by IoT-enabled solutions,
- event processing to make judgments and perform defined actions on a real time basis,
- and managing the data distribution functionality to allow for stable and efficient data collection.

- Data management function

    A website (Service Portal) is provided to customer administrators responsible for data management.

- Data collection function

    Stores data to this service. A transfer function to transfer data to external services is also available.

- APIs provided

    APIs are provided for data management/collection/use.
    Compatible with HTTP(s) REST and MQTT protocols (with TLS).

- Authorization management

    An API request authorization function is provided. This allows for authorization management per resource.

- Event function

    Set conditions for data registered for this service to perform actions when these conditions are met.
    Type of actions supported include: API startup action and Email notification action

- Dynamic resource controller (distributed control)

    This function allows for efficient data collection with a limited amount of IT resources.

- Access restriction function

    This function restricts access to IP addresses specified by the customer. Access to both the Service Portal and access codes can be restricted.
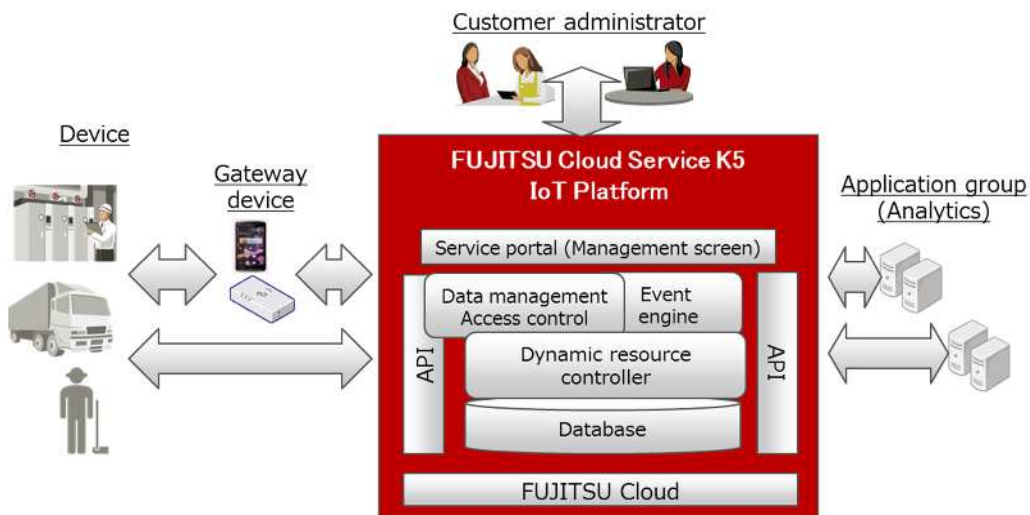
Figure 1.1 Service overview

4

1.2. Features

- IoT systems can be configured in a short period of time

  Customers are not required to configure the infrastructure environment as this uses a cloud service. As basic functions required for IoT are bundled, customers can concentrate on developing their business applications utilizing IoT data from the platform. A standard interface is provided to simplify the application development process.

- Compatible with a wide range of sensors/devices

  The light "MQTT" protocol, designed to reduce communications overhead and battery consumption, is a supported standard. It is also compatible with the conventional HTTP REST, enabling business with a wide variety of sensors and devices.

- Secure data management

  As access permissions can be set for each data group (resource) stored by the sensors/devices/gateways, data can be restricted to a single company (or business unit), or can be shared between multiple companies including your customers and suppliers in a secure manner.
  Encryption for data transport is provided by HTTP(s) and MQTT with TLS to ensure that sensor/ device/ gateway provided data is secure as well as access to the data from external analytics and business applications.

- Support for stable data collection

  Proprietary overall optimization technologies (wide area distribution technologies) of Fujitsu are used to collect data generated from sensors and other devices to ensure efficient and stable data collection even when fluctuations in data traffic, etc. are experienced.

1.3. Scope of Service

The scope of this service focuses on the Cloud Service IoT Data use layer, as depicted in the middle portion of the diagram below.   This service does not extend to:

- groups of devices and sensors providing the data (bottom layer of diagram),
- the networks necessary for data transport
- or the "analysis platforms" and "customer/partner applications" which consume the IoT data (top layer).
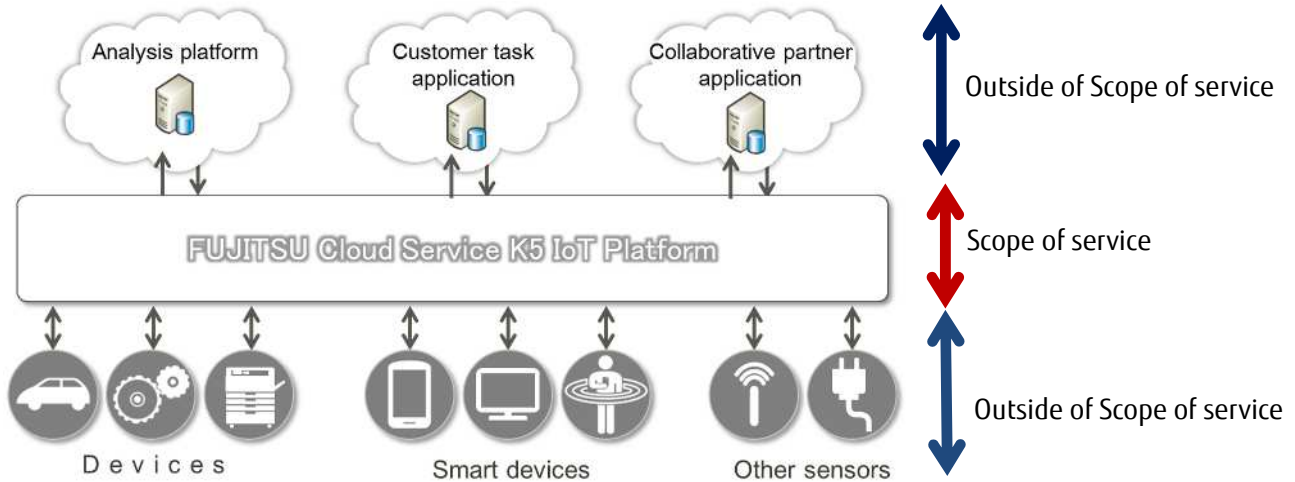
Figure 1.3 Scope of service

1.4. Documentation

Details pertaining to documents concerning this service are as follows.

Manual name	Description
FUJITSU Cloud Service K5 IoT Platform Service Details Instruction Manual	Describes service specifications. (This manual)
IoT Platform Service Portal Operating Manual	A manual concerning web interface functionality (hereafter, the Service Portal).
IoT Platform User Guide	A manual used to support API usage during application design and development.
IoT Platform API Reference	An API reference manual provided for this service.

Table 1.4 Documentation

6

Chapter 2   Service Specifications

2.1.   Multi-tenant

A specific area will be setup in our cloud service for each customers use, as shown in the below diagram.   As this shared service is supporting multiple customers, a best effort approach is utilized for the overall service.

Multiple tenants can be created in the customer area.
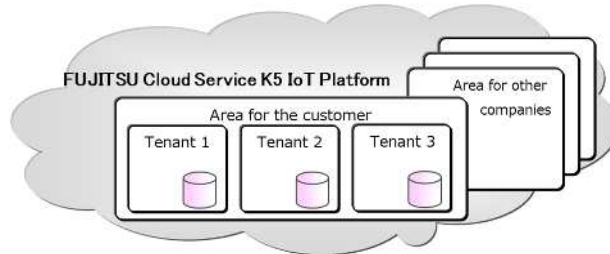
Figure 2.1 Multi-tenant

2.2.   Feature Highlights

2.2.1.   Data Collection

Users create "resources", which serve as units of registered data storage within the tenant. "Access codes" granting permissions to the resource must be created and assigned to the resource.

Access codes are assigned (provided) to those using the API to approve and run the requests the access code corresponds to.   Users of the API may be devices/sensors or analytics/business applications, each would require an access code granting them the appropriate permissions.

<Permission types>
C: Permission to create resources, access codes, etc.
R: Permission to reference (or read) data
U: Permission to register (or update) data
D: Permission to delete resources, access codes, events, etc.
L: Permission to acquire a list of resources, access codes, events, etc.
P: Permission to register data under a specific resource directory
G: Permission to reference data under a specific resource directory

2.2.1.1.   Data collection preparation

Operations can be performed from the Service Portal, or with the API.
*API operations can be performed for "resources", "access codes", and "events".
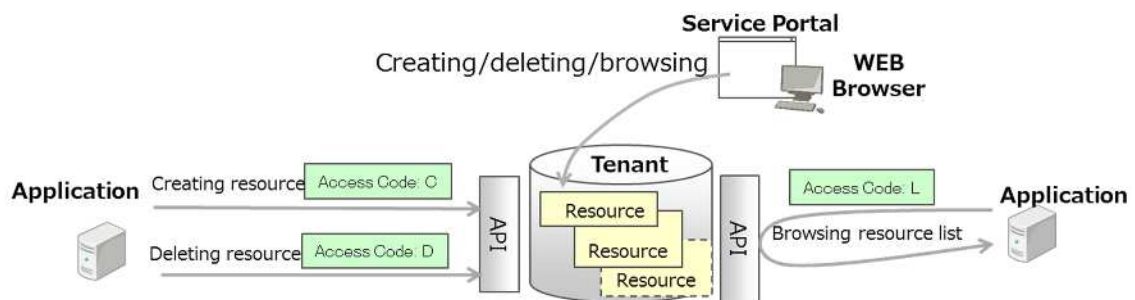
Figure 2.2.1.1 Managing resources

7

2.2.1.2. Collecting and using data

Data can be registered and browsed with an API.
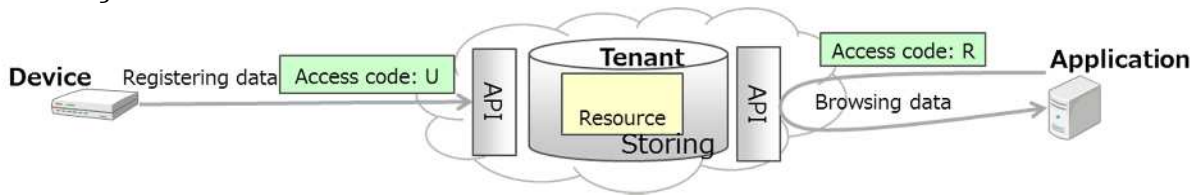
Figure 2.2.1.2-1 Storing data

A special type of resource, a "resource(transfer)" allows data to be transferred to other services without the need to store the data with this service.

Figure 2.2.1.2-2 Transferring data

2.2.2. Event Function

Set conditions to extract data as events to perform actions when extraction conditions are met based on data registration/update triggers. These actions can be configured to send email notifications, or invoke a specific API.
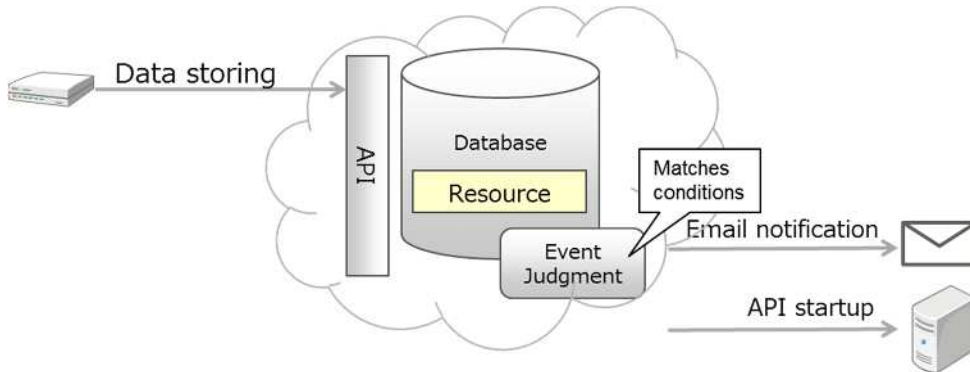
Figure 2.2.2 Event functionality

2.2.3. Access Restrictions

Restrictions can be set for IP addresses accessing this service.
You can restrict access to resources by adding access restrictions to both the Service Portal and access codes.
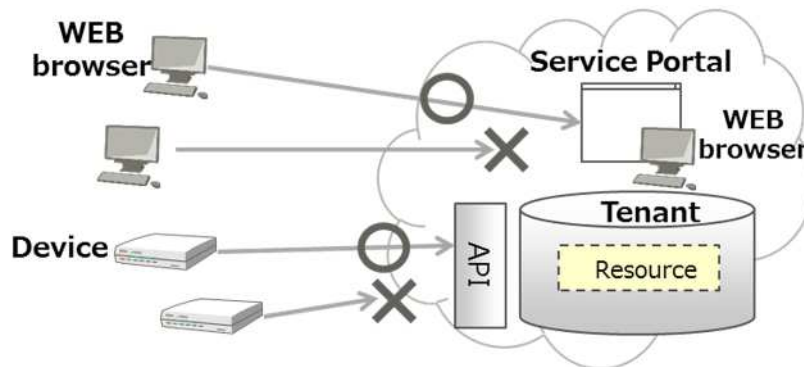
Figure 2.2.3 Access restrictions

2.2.4. Dynamic Resource Controller

This provides recommend resources (recommendations) for use during data collection as a means of controlling data collection based on cloud load. This allows data collection to be optimized (ex: distributed filtering) based on the level of IT resources available to the customer.
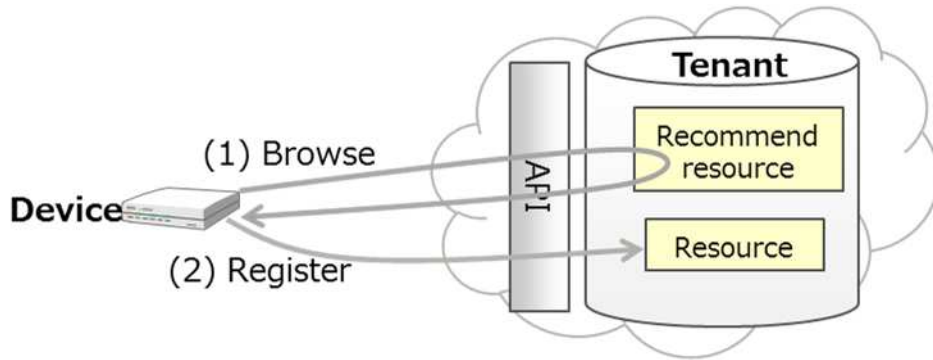
Figure 2.2.4 Dynamic resource controller

2.3. Definitions

2.3.1. Tenant ID

A unique code used within this service to identify tenants within a customer area.

<Definition>

Format	Alphanumeric character
No. of characters	10 (fixed)

2.3.2. Administrator Account

A website (hereafter, Service Portal) account used to manage data provided for each customer.

<Definition> E-mail address

Format	E-mail address
Registration limit	No restrictions

(Note)

The administrator account has operating permissions for all tenants within a customer area.

If you prefer to split administrator accounts by tenant, you will need to submit another application under a separate   customer identifier.

2.3.3. Administrator Password

The password policy for administrator account passwords is as follows.

<Definition>

Usable character types	At least one of each of the following four character types must be used. Upper and lower case alphabetical characters, numbers, symbols (eight symbols: #,@,-,(,),:,.,_)
No. of characters	8 to 15
Period of initial password validity	No restrictions
Period of password validity	No restrictions

9

2.3.4. MQTT Account

The tenant ID is used as the account for using MQTT.

2.3.5. MQTT Password

The MQTT password policy is as follows.
   <Definition>

Usable character types	At least one of each of the following four character types must be used. Upper and lower case alphabetical characters, numbers, symbols (eight symbols: #,@,-,(,),:,.,_)
No. of characters	8 to 12
Period of initial password validity	No restrictions
Period of password validity	No restrictions

2.3.6. Resources

Data storage units are referred to as "resources", and data groups within a resource are defined as "resource data".

2.3.6.1. Type of resources and supported data format

Type of resources and their details is described below.

	Type of resource	Supported data format for registration	Use in this service	
			Process when registering	Process when browsing
1	Resource_JSON	JSON	Stored in BSON format	Output in JSON format (Note2)
		CSV Text Binary(256Kbyte or less)	Stord in BSON format after converting to JSON.(Note1)	Output in JSON format
2	Resource_Binary	Bynary	Stored in Binary format	Output in Binary format
3	Resource (Transfer)_JSON	JSON	Transferred in JSON format	-
		CSV Text Binary(256Kbyte or less)	Treansferred after convertingto JSON format.(Note1)	-

Table 2.3.6.1 Type of resource

(Note1) **How to** convert each data to JSON format
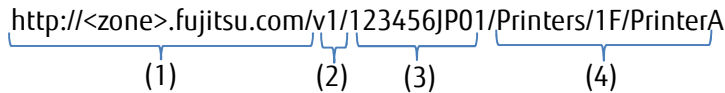
	Data format	Conversion method
	CSV	CSV is converted as one JSON data. #No rules/regulation in the format. (CSV conforms to RFC4180.) Upper N line can be deleted.
	Text	Text is converted as one JSON data.
	Binary (256Kbyte or less)	It is converted as one JSON data after encoding the binary data in Base64.

(Note2) Duplecation of names (alternative of comments) in the JSON format will be deleted.

2.3.6.2. REST API URI
<Definition>

http://<zone>.fujitsu.com/v1/123456JP01/Printers/1F/PrinterA

           (1)   (2)   (3)   (4)

Character strings linking the following four items with a "/ (slash)" denote resources in a HTTP URI.
 (1) baseURI
   To be notified when applied for the service.   In the above example, the BaseURI is
   "http://<zone>.fujitsu.com"
   *When using SSL (HTTPS), http becomes https. *SSL supports TLS 1.2
 (2) API version
   To be notified when applied for the service.   In the above example the System Version is depicted by "v1"
 (3) Tenant ID
   To be notified when applied for the service.   In the above example Tenant-ID is "123456JP01".
 (4) Resource path
   Character string named by the customer. Can be written in a hierarchical structure.
   In the above example, the resource path is "Printers/1F/PrinterA"

<Definition>
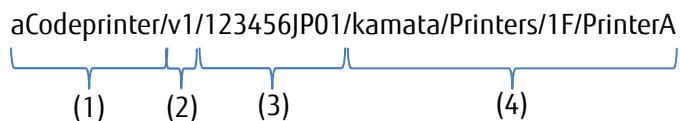
Usable characters	Upper and lower case alphabetical characters, numbers, symbols (three symbols: - (hyphen), _ (underscore), / (slash)) *Single-byte characters only *Available symbols cannot be used as the first character. *"-", "_", and "/" cannot be used after "/", such as "/-", or "/_". *_fwd/ is automatically added to the start of any transfer resources created. *_bin/ is automatically added to the start when selecting binary data.
No. of characters	1 to 128 characters *For transfer resources, _fwd/ is included in the maximum of 128 characters. *For binary data, _bin/ is included in the maximum of 128 characters.
Restriction	Unique to a tenant

(Additional note) The access code must be set for the header when using HTTP.

2.3.6.3. MQTT topic
<Definition>

aCodeprinter/v1/123456JP01/kamata/Printers/1F/PrinterA

      (1)   (2)   (3)   (4)

Character strings linking the following three items with a "/ (slash)" denote resources in a MQTT.
 (1) Access codes
   Refer to Chapter 0 (described later)
 (2) API version
   Refer to 2.3.6.2 (2)
 (3) Tenant ID
   Refer to 2.3.6.2 (3)
 (4) Resource path
   Refer to 2.3.6.2 (4)

2.3.7. Access Codes

Access codes are codes that show operating permissions granted to configure resource, access code and event settings.

While these can be created from the Service Portal or with the API, <u>the initial access code must be configured from the Service Portal.</u>

<Definition>

Usable characters	Upper and lower case alphabetical characters, numbers, *Single-byte characters only
No. of characters	3 to 48 characters
Restriction	Unique to a tenant

A Resource needs to be specified while setting Access code. Further details of access code setting is as following.

2.3.7.1. Operating permission

The type and details concerning operating permissions granted are as below.

Operating permission	Content	Subject of operation	Corresponding protocol
Create (C:Create)	Permission to create resources Enable items **under** a specified resource (Note 1)	Resources Access codes Events	HTTP/HTTPS
Browse (R:read)	Permission to refer to data stored in a resource Enable items for the specified resource only	Resource data	HTTP/HTTPS MQTT/MQTTS (Note 2)
Update (U:update)	Permission to register data to resources Permission to update data stored in a resource (MQTT/MQTTS not supported) Permission to delete data stored in a resource (MQTT/MQTTS not supported) Enable items for the specified resource only	Resource data	HTTP/HTTPS MQTT/MQTTS
Delete (D:delete)	Deletion permissions Enable items **under** a specified resource (Note 1)	Resources Access codes Events	HTTP/HTTPS
Acquire lists (L:list)	Permission to acquire a list of resources under a specified resource Enable items **under** a specified resource (Note 1)	Resources Access codes Events	HTTP/HTTPS
Update group (P:put)	Permission given to multiple resources under a resource URL (directory) for which U permissions have been set	Resource data	HTTP/HTTPS MQTT/MQTTS
Browse group (G:get)	Permission given to multiple resources under a resource URL (directory) for which R permissions have been set	Resource data	HTTP/HTTPS MQTT/MQTTS

(Note 1) In the instance that two permissions set conflict with one another, the permission that takes precedence shall apply.

(Note 2) MQTT/MQTTS is not supported when acquiring lists of data where the update time is specified for binary data.

Table 2.3.7.1 List of operating permissions

2.3.7.2. Combinations of operating permissions

Permissions can be combined in units of "CDL", "L", "R", and "U".

2.3.7.3. Protocol Control

Protocol permissions can be set to permit access.

Not restrict protocol	Setting not to restrict protocol
Restrict protocol	Setting not to restrict protocol in combinations of HTTP/HTTPS/MQTT/MQTTS.

2.3.7.4. Client Certificate

The client certification can be done by registering the client certificate issued by the service portal or arranged by the customer to the accesscode. Client ceritification can be used only for HTTPS protocol. (HTTP/MQTT/MQTTS is not supported)

2.4. Service Portal

You can configure the settings needed to use this service from the Service Portal screen (WEB-IF).
*Refer to the "IoT Platform Service Portal Operating Manual" for more details.
*You can switch between tenants when using the Service Portal if the Service Portal URL is the same when multiple tenant agreements are signed. However, this option is not available if the URL is different.

2.4.1. Conditions of Use

The conditions of use for the Service Portal are as follows.

	Item	Condition	Notes
1	Means of use	WEB browser	-
2	Access	Internet	-
3	Compatible languages	Japanese/English	The default language is based on your region. This can be set after logging in.

Table 2.4.1 Conditions of use for the Service Portal

2.4.2. Tested Operating Environment

The following Service Portal operation checks have been performed. Functions under conditions other than those described below are not guaranteed.

	Compatible OS	Browser	Notes
1	Windows 7/8/8.1/10	Internet Explorer 11 *When Enhanced Protected Mode is on	Operation not confirmed for Enterprise Mode/Edge Mode

Table 2.4.2 Service Portal operation check

2.4.3. Management Function

Functions provided with the Service Portal are as follows.

	Management function	Content	Notes

1	Account	Create and delete accounts for Service Portal use Reissue passwords	-
2	Resources	Create/change/delete resources, batch registration Resource data auto-deletion settings (set number of days from 1 to 9,999) * Users can reference data for the date and time set + a maximum of one day Display/search/download resource lists	-
3	Access codes	Create/change/delete access codes, batch registration Display/search/download access code lists Register client certificate	-
4	Events	Create/change/delete events Display/search events	-
5	Logs	Display/search/download the Search Portal use history Display monthly use summaries Display monthly usage amount screens Download timestamped use logs (to confirm fees) Display system log screens (to confirm internal system requests that may have been terminated with an error)	-
6	Access restrictions	Create/change/delete Service Portal access restriction conditions Create/change/delete access code access restriction conditions	-
7	Distribution settings	Configure/change/delete settings to use the dynamic resource controller Enable/disable distribution policies	-
8	Common settings	Display/change the MQTT password Turn error log storage ON/OFF Turn the CORS function ON/OFF * CORS: A means of permitting access via a server (Confirmed running on Internet Explorer 11/HTTP. CORS support depends on the web browser in use)	-
9	Client certificate	Issue client certificate	-

Table 2.4.3 Management function overview

2.4.3.1. Purpose of system logs

System logs for this service are primarily provided as a means of determining whether requests have been canceled during application development work performed by the customer according to internal service processes.

	Item	Content
1	Purpose	Confirm the following Event transfer results (API/E-mail) MQTT results
2	Reference conditions	Screen display only
3	Log display conditions	The 5000 most recent logs pertaining to the tenant concerned held in the system for the past two days, including the date logs are referenced. *This does not guarantee that logs are kept for two days.

Table 2.4.3.1 Management function overview

2.5. API

You can perform operations for resource, access code and event settings using an API.

Request authorization is provided by adding an access code with the necessary permissions for the resource into the API.
Refer to the "IoT Platform User Guide" for more information on API details and supported protocols, etc.

2.5.1. HTTP REST Interface

Compatible with HTTP and HTTPS. The interface provided is described below.

	Operation	Method name	Relation to access code
Management	Create resource	POST	Permitted with C
	Update resource	PUT	Permitted with C
	Delete resource	DELETE	Permitted with D
	Create resource/access code	POST	Permitted with C
	Update access code	PUT	Permitted with C
	Delete access code	DELETE	Permitted with D
	Create event	POST	Permitted with C
	Update event	PUT	Permitted with C
	Delete event	DELETE	Permitted with D
	Reference resource list	GET	Permitted with L
	Reference access code list	GET	Permitted with L
	Reference event list	GET	Permitted with L
Data	Register resource data (JSON)	PUT	Permitted with U or P
	Browse resource data (JSON)	GET	Permitted with R or G
	Update resource data (JSON)	PUT	Permitted with U or P(Note)
	Delete resource data (JSON)	DELETE	Permitted with D
	Transfer resource data (JSON)	PUT	Permitted with U
	Register resource data (Binary)	PUT	Permitted with U or P (Note)
	Browse resource data (Binary)	GET	Permitted with R or G
	Browse resource data lists (Binary)	GET	Permitted with R or G
	Delete resource data (Binary)	DELETE	Permitted with D

(Note) Updates for the same time setting will store data as multiple data items.* Binary data will be overwritten when registered for the same time.

Table 0 REST IF list

2.5.2. MQTT Interface

Compatible with MQTT and MQTTS. The interface provided is described below.

	Operation	Control Packet name	Relation to access code
Data	Registering resource data (JSON)	PUBLISH	Permitted with U or P
	Browsing resource data (JSON)	SUBSCRIBE + PUBLISH (Note)	Permitted with R or G
	Delete resource data (JSON)	Not supported	
	Transfer resource data (JSON)	PUBLISH	Permitted with U
	Register resource data (Binary)	PUBLISH	Permitted with U or P
	Browse resource data (Binary)	SUBSCRIBE + PUBLISH (Note)	Permitted with R or G
	Delete resource data (Binary)	Not supported	

(Note) PUBLISH from this service after SUBSCRIBE from the client

Table 2.5.2 MQTT IF list

2.5.3. Restriction to Request

The restrictions that apply to request are as described below.

	Type of request	Maximum data capacity	Other restrictions
1	Browsing lists	-	1,000 items per request
2	Registering resource data (JSON)	16 Mbytes for JSON-format resources, and 16 Mbytes for BSON-format resources	-
3	Browsing resource data (JSON)	16 Mbytes for JSON-format resources	Up to the maximum data capacity, or 1,000 items
4	Registering resource data (JSON) (Transfer)	16 Mbytes for JSON-format resources	-
5	Registering resource data (binary)	100 Mbytes for Binary-format resources	-
6	Browsing resource data (binary)	100 Mbytes for Binary-format resources	Only one data item can be acquired with each request
7	Browsing resource data lists (binary)	-	Up to 1,000 items
8	Data transferred with the Event function (JSON)	256Kbyte for JSON-format resources	-

Table 2.13.3 Request restrictions

2.5.4. Relationship between Registering Resource Data with HTTP-IF, and MQTT-IF

When registering data to a resource with HTTP-IF, the service will publish to subscribing clients for MQTT-IF for the corresponding resource.
However, JSON batch registration APIs(=bulk)/binary data are not supported.

*Binary data may be supported in the future with feature enhancement.

2.5.5. Handling Data with the Same Timestamp

Time can be distinguished upto the millisecond (3digit).

(1) JSON data format

Multiple data entries will be registered when registering multiple data items for the same resource at the same time. Please be aware that times will be specified in the following manner when multiple data entries with the same timestamp exist.

	Operation	Result	Notes
1	Update	One data entry with the specified timestamp will be subject to updates	The data set for updates is not determined in a definite manner
2	Browse	All data with the specified timestamp is returned	-
3	Delete	All data with the specified timestamp is deleted	-

Table 2.5. 5(1) Handling data with the same timestamp (JSON)

(2) Binary data format

Data entries will be overwritten when registering multiple data items for the same resource at the same time.

2.6. Data Transfer Destination Settings

You can transfer data to other services without storing this data with this service by selecting "resource (transfer)" as the resource type when creating a resource (transfer destination IF only supports HTTP and HTTPS). The following transfer destination settings can be configured.

*You can also acquire data with MQTT Subscribe without configuring these settings (without transferring data) (refer to 2.5.4).

	Item	Settings	Notes
1	URI	Free entry	Only single-byte, maximum of 254 characters
2	Method	Select from screen	NULL/POST/PUT/GET/DELETE/HEAD/OPTIONS/TRACE
3	Authentication ID	Free entry	Only single-byte, maximum of 20 characters * Only supports Basic authentication
4	Authentication password	Free entry	Only single-byte, maximum of 20 characters * Only supports Basic authentication
5	Header name	Free entry	Only single-byte, maximum of 20 characters. Maximum of 10.
6	Header name	Free entry	Only single-byte, maximum of 512 characters. Maximum of 10.

Table 2.6 Setting items of destination API

2.7. Event Function

Set detection conditions for data in a resource, and what actions to perform when such data is detected.

2.7.1. Available Operations

The operations available for resources subject to the event function are as follows.
*Events cannot be set for "Resource(Transfer)" type resources.

	Operation	Available operation for event	Notes
1	Registering resource data	Available	-
2	Browsing resource data	Not available	-
3	Updating resource data	Available	-
4	Deleting resource data	Not available	-

Table 2.7.1 Available operations for event functions

2.7.2. Detection Condition Settings

The following items can be set as detection conditions.

*Remove detection is a function used to prevent actions from being performed for the same event after being detected once.
   When this condition is not set the pre-defined action will always be performed when detection occurs.

*Detection conditions cannot be set for Resource_Binary (binary data).

	Item	Settings	Notes
1	Target resource	Select using the screen search function	Maximum of one
2	Target period	Select the year, month, date, hour, minute and second on the screen/free entry	-
3	Data position	Freely enter the target position in the data	Enter in the JSONPath format
4	Character types detected	Select whether the data is a number or character string	-
5	Detection value	Free entry	(Note 1)
6	Detection judgment conditions	Select on the screen	(Note 2)
4	Character types removed from detection	Select whether the data is a number or character string	-
5	Values removed from detection	Free entry	(Note 1)
6	Detection removal judgment conditions	Select on the screen	(Note 2)

(Note 1) If the character type is "numbers", only single-byte numbers can be entered
*If the character type is "numbers" [Match/Does not match/Or more/Or less/Under/More] can be used, and if the character type is "character strings" [Full-text match/Partial match] can be used.

Table 2.7.2 Detection condition settings

2.7.2.1. Email notification settings

The following items can be set for email actions.

	Item	Settings	Notes
1	Email address	Free entry	E-mail address format only Only single-byte, maximum of 254 characters
2	Subject	Free entry	Single-byte/full-width, 0 to 256 characters
3	Body text	Free entry	Single-byte/full-width, 1 to 140 characters

Table 2.7.2.1 Email notification items

(Additional note) When sending email notifications, the following information is added as an attachment file (JSON-format text).
Event ID/Resource path when the event occurred/Resource update timestamp/Data entity
*However, only data sizes up to 10 MBs are permitted. Email notifications will not be sent if this is exceeded.

2.7.2.2. API startup settings

The following items can be set for API startup actions (startup IF only supports HTTP and HTTPS).

	Item	Settings	Notes
1	URI	Free entry	Only single-byte, maximum of 254 characters
2	Method	Select from screen	POST/PUT/GET/DELETE/HEAD/OPTIONS/TRACE
3	Authentication ID	Free entry	Only single-byte, maximum of 20 characters *Only supports Basic authentication
4	Authentication password	Free entry	Only single-byte, maximum of 20 characters *Only supports Basic authentication
5	Header name	Free entry	Only single-byte, maximum of 20 characters. Maximum of 10.
6	Header name	Free entry	Only single-byte, maximum of 512 characters. Maximum of 10.
7	Body	Free entry	Single-byte/full-width, maximum of 1,024 characters, Japanese input allowed

Table 2.7.2.2 API startup settings

2.7.3. Data Attachment When Issuing Events

This shows whether the resource data triggering the event is attached when event conditions are met.

	Event trigger	Action	Result
1	Registering resource data (JSON)	Email notification	Attach resource data as a file
		API startup	Add resource data to the Body section. However, the size limit for resource data is 10 MBs. *While the maximum data capacity when registering resource data is 16 MBs, events will not trigger when over 10 MBs.
2	Register resource data (Binary)	Email notification	No resource data file attachment.
		API startup	Resource data not added to the Body section.

Table2.7.3 Overview of when resource data is attached when an event occurs

2.8. Access Restriction Function

You can set the range of IP addresses (including single IP addresses) permitted access.
The following settings can be configured.

2.8.1. Service Portal Access Restrictions

The IP addresses permitted access can be set for users.

	Item	Settings	Notes
1	Permitted IP address	Free entry	Starting IP address ~ Ending IP address
2	No. of IP address range settings	Maximum of five	-
3	Eligible users	Select from screen	-

Table 2.8.1 Service Portal access restriction settings

2.8.2. Resource Access Restrictions

The IP addresses permitted access to access codes can be set as a means of restricting access to resources.

* However, as MQTTS IF is not supported, a disconnection will occur when attempting to use the corresponding access code with an MQTTS request.

	Item	Settings	Notes
1	Permitted IP address	Free entry	Starting IP address ~ Ending IP address
2	No. of IP address range settings	Maximum of five	-
3	Access codes to restrict access to	Select from screen	-

Table 2.8.2 Access code access restriction settings

2.9. Dynamic Resource Controller Function (Distribution Function)

This service collects service load analytic data by type of measurement and compares these values with conditions set by the customer (edge computing conditions) to provide recommendations to the customer. Customers can develop applications to optimally collect data within the IT resources available using these recommendations.

Distribution conditions can be configured as a distribution policy. Available settings are as shown below.
Set one distribution policy per tenant, and three recommend resources for storing recommendations for each distribution policy. Different edge computing conditions can be set for each recommend resource.

	Item	Settings	Notes
1	Enable/disable	Select from screen	Switch between enabling/disabling the distribution policy. [Note] API charges will be incurred as recommendations and load measurements are written to resources. Disable the distribution policy when not in use to prevent charges incurred. While load resources and recommend resources are written based on a recommend cycle, recommend resources are only written to when changes are made to recommendations and notification character strings.
2	Recommend cycle	Free entry	1 to 1,440 minutes
3	Calculating period	Free entry	1 to 1,440 minutes *Value must be the same as or longer than the recommend cycle
4	Load resource	Select from screen or free entry	Set resources and access codes for writing the load for the customer tenant.

Table 2.9-1 Distribution policy settings

	Item	Settings	Notes
1	Enable/disable	Select from screen	Switch between enabling/disabling each recommend resource within the distribution policy.
2	Recommend resource	Select from screen or free entry	Set resources and access codes for writing recommendations for the customer tenant.
3	Type of measurement	Select from screen	TPS (transaction/second)/BPS (bit/second)
4	Edge computing conditions, or resolutive conditions for such	Fixed	Numerical values only
5	Edge computing conditions, or resolutive conditions for such	Free entry	Single-byte numerals, maximum of 10 digits.
6	Inequality sign for edge computing condition detection judgments, or resolutive condition detection judgments for such	Select from screen	NULL/match/no match/or more/or less/less than/more than
7	Notification character string when edge computing conditions are met, or when resolutive conditions for such are met	Free entry	Maximum of 10 characters, Japanese allowed

Table 2.9-2 Recommend resource settings

2.10. Error Log Storage Function

The error log storage function stores error information to the error collection resource "_error" when requests are lost due to issues within the service and the transmission destination. Reference this resource to confirm the occurrence/causes of errors.

<Target>
    Event function (Email sending errors, API startup errors)
    MQTT/MQTTS internal errors
    Forwarding errors

2.11. CORS Support

Normally you will not have direct access to APIs for this service from your browser as Javascript does not allow connections other than to the web server for the download source. However, CORS (Cross-Origin Resource Sharing) support is provided as a means of allowing access to such APIs. CORS function settings are described below.

	Item	Settings	Notes
1	Enable/disable	Select from screen	—

Table 2.11-1　CORS settings

2.12. Function for Issuing Client Certificate

This service can be used to issue client certificates.

2.13. Notes (Specification Restrictions)

2.13.1. Character Codes Used With APIs

Only TF-8 characters are supported.

2.13.2. Time

Coordinated Universal Time +00:00 (UTC) is used.

2.13.3. Guideline about data size that can be accumulated in one resource (JSON data)

★Important★
While an upper limit to the amount of data that can be stored to a single resource applies, as the performance when retrieving JSON data is inversely proportional to the amount of data stored within a single resource, make sure to take this into consideration when designing resources according to your performance needs. In general it is assumed that resources will be created for each continuous piece of data (device). However, consider splitting resources up into multiple resources when it is likely that - due to the number of days data is to be collected - a large volume of data is to be collected from a single device. For example, expanding the body from which data is retrieved by storing data collected from multiple devices onto a single resource may prevent data from being acquired due to timeout issues. Refer to the "IoT Platform User Guide" for more information.

2.13.4. [MQTT Only] QoS

While MQTT QoS levels 0, 1, and 2 are accepted, data arrival is not guaranteed when disconnecting a session. Processing errors within the system after data is received may also prevent the arrival of data.

2.13.5. [MQTT Only] Behavior When a Cut Connection Occurs

Please be aware that retain may disappear when the MQTT connection is cut due to server maintenance or for some other reason.

2.13.6. [MQTT Only] Chargeable messages

Number of API usage and SSL usage of below messages are chargeable.
- CONNECT
- PUBLISH

(Message from Client to IoT-PF, or message from Iot-PF to Client)
- SUBSCRIBE
- PINGREQ

2.13.7. Other Matters

The current specifications take precedence for all other matters not expressly written in this manual.

Chapter 3   Restrictions

3.1.   Response for Uses that Exceed Usage Guidelines

Please contact us via our sales department regarding data registration or reference frequency if you might exceed any one of the following guidelines for use concerning the following as we may not be able to prepare a usage environment that suits your needs.

Please be noted that, system restriction will be in effect in case of peak frequency of communications continues to exceed usage guideline for a certain time. In such case, system will return error response (in case of HTTP/HTTPS), or discard data (in case of MQTT/MQTTS) for any request.

.

<Guidelines for use>

Single-communication data size		256 Kbytes
Frequency of communications (peak)	Data system API	Depending on service contract
	Management system API*	1 time/second
No. of registered resources		10,000
Data storage size within one resource		100 Mbytes
No. of simultaneous connections		1,000

*Indicates an API that creates, updates, deletes or refers a resource, access code or event.

3.2.   Prohibition of Excessive, Intensive Use

Excessive, intensive use is prohibited. Further access may be denied in instances of intensive use that may cause grave damage to this service (including cases which your usage constantly exceeds the guideline mentioned in Section 3.1).

3.3.   Notes for Using the Event Function/Transfer Function

The following restrictions apply to events and transfers occurring when registering data.
<Events>
Event requests may be canceled due to the response performance of the API set for the transmission destination.
<Transfers>
Requests may be canceled due to the response performance of the API set for the transfer destination.
*For example, when the number of data registration requests exceeds the response performance of destination where the event is set.
*Please pay particular attention to deteriorating performance issues when transmitting communications with SSL.

3.4.   Data Guarantee

This service does not backup data or implement disaster recovery measures. Please be aware that Fujitsu cannot guarantee the recovery of customer data lost. You are kindly requested to employ the appropriate measures using your own applications to ensure data security. Further, please note that Fujitsu cannot migrate data under any circumstances whatsoever.

3.5.   Data Reachability

Request received responses may be lost after being returned by this service. When attempts are made to send

transfer and event to the transmission destination set, the request sender cannot confirm whether such requests were successful / failed.

3.6. Potential for Changes to API Query Specifications

It is possible indeed that queries targeting large amounts of stored full-text data may incur increased charges or be restricted in the future (narrow down searches to 10,000 records by specifying indexes, etc. is recommended). Please be aware of this when developing applications. *The current index only pertains to the time and resource. Indexes cannot be specified in-application.

3.7. Deleting Data

Fujitsu will delete all appropriate data after the service contract is canceled.
Delete any data you prefer to delete prior to canceling this service

3.8. DoS Measure

Number of access from same network segment (/24) is limited to 300 requests per second.

Chapter 4   Explanation of Important Matters

4.1.   Service Provision Times

While this service is in operation 24 hours a day, 365 days a year, this service may be stopped during periods of scheduled or emergency maintenance. System maintenance may take several hours, during which the service will be unavailable (you may not be able to store data during these times). Maintenance times cannot be changed at the customer's request.

4.1.1.   Scheduled Maintenance

Generally, we will contact you two weeks before a scheduled shutdown is to occur.

4.1.2.   Emergency Maintenance

Emergency maintenance may be performed when system failures occur, which will involve prior short notice or after-action notice. Failure reports cannot be submitted in these circumstances.

4.2.   Scope of Support

Please be aware that Fujitsu cannot provide support for any issues which may arise with communications equipment and information collection devices prepared by the customer. Please seek support from the contact point at purchase for these devices.

4.2.1.   Information Required When Using the Support Desk

You are kindly requested to have the following information on hand when contacting the support desk.

	Item	Information
1	Contract service name	FUJITSU Cloud Service K5 IoT Platform
2	Customer identifier	A 15 character identifier used to identify your company
3	Customer's company name	Customer's company name
4	Name of the person in charge at the customer company	Name of the person in charge at the customer company
5	Contact phone number	The phone number which Fujitsu can contact
6	Content of inquiry	(1) Type of use (inquiry or failure report) (2) Content *Please include as detailed information as possible when contacting us regarding issues. Include details such as the "time of occurrence", the "tenant ID", and the "operating procedures".

4.3. Suitability of Data Stored

As the content of information collected and stored using this service is selected by the customer, it is the customer's responsibility to acquire the necessary permissions, etc. from the end user with regard to the collection of information.

Further, recent developments have seen overseas countries move to introduce laws and regulations prohibiting the transfer of data, particularly data that constitutes personal information, outside the region. It is the customer's responsibility to check and comply with such laws and regulations.
(We do not recommend storing personal information and confidential information with this service)

4.4. Access Code Management

It is the customer's responsibility to manage access codes and administrator account passwords. If this information becomes known to others, it may result in unreasonable charges and data leaks due to access of this service in an unintended manner.

4.5. Viewing of Customer Data

While the contents of customer data is referenced when this service is used to execute APIs to manipulate data and to provide event functions, this data is only used to provide these functions and is not used for any other purpose.

4.6. Charges When Using the Dynamic Resource Controller

API charges will apply according to volume written to recommend resources and load resources when using the dynamic resource controller. Please be aware that charge amounts will be based on the distribution policy set by the customer. You can prevent charges incurred by disabling the distribution policy to stop the use of this function.

4.7. Use of Stored Data

Information collected during the period this service is in use shall be used by Fujitsu without the consent of, or compensation to, the customer for the purpose of improving the quality of this service and the functions provided, and to publish the results of statistics collected. On the other hand, customer data itself will not be used by Fujitsu without prior consent.

Information acquisition location	Target data
Servers Communications devices	Information regarding communications (time, access counts, volume of communication) Server performance information (load, state of resource use) Server system logs Logs for the applications/middleware making up this service Frequency and content of Service Portal use/type and parameters of APIs used (including internal APIs) and usage counts/amount of disc use, etc.

4.8. Deletion of Event Setting

Please do not register an email address in the event function setting that does not exist (or is not able to receive email). Please be noted that, in such case the event setting will be deleted.

All Rights Reserved, Copyright©FUJITSU LIMITED 2016-2018