

IoT Platform Service Portal Operating Manual
(Version 7.0_0)

<Revision History>

Version No.	Description	Date
Version 1.0	First version	2016/10/07
Version 1.1	Error corrections and supporting launch of IoT Platform on UK K5	2016/11/01
Version 1.2	Error corrections (deleting definition of Customer ID, changing definition of Tenant ID, changing title of this manual and other related documents)	2016/12/01
Version 1.2	Correction of cross reference error	2017/01/12
Version 4_1.0	Support for V4.0 1.5 Added Windows 10 to the user environment. Removed Windows 8. 4.6 Added note on resources used for resource collection. 4.7 Added access code permissions (G, P). Added sections on specifying an access protocol and client certificate settings. 4.9 Segmented usage log output items. 4.13 Added section on the certificate generator function. 4.14 Added CORS settings and error collection settings to the section on common settings.	Internal Version (Not published)
Version 4_1.1	Added note that screen images showing functions scheduled to be provided from July 2017 were dummy images.	Internal Version (Not published)
Version 4_2.0	Deleted all other notes on functions to be provided from July 2017 other than the images.	2017/4/24
Version 4_2.1	Replaced images 4.10.4. Corrected description provided for changing users.	2017/6/1
Version 5.0_0	Changed Version No. only.	2017/10/20
Version 5.1_0	Changed Version No. only.	2018/3/17
Version 7.0_0	4.7.5 Added note regarding access code controlling when 101 or more resources linked to one access code.	2018/9/15

Preface

Thank you for considering the "IoT Platform". This "IoT Platform Service Portal Operating Manual (hereafter, this manual)" is intended for customers considering or implementing this service. We ask for your understanding with 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 trademarks or registered trademarks of Microsoft Corporation in the United States of America and other countries.

The contents of this manual may change without notice due to changes to the specifications of this service provided.

Disclaimers

- We do not accept any responsibility for unexpected malfunctions or for unforeseen charges occurring due to the user performing operations not listed in this manual of this service.

- We do not accept any responsibility in the unlikely event that the use, or inability to use, this service causes damage to the user (including, but not limited to, damages caused by a suspension of work, damage to/loss of data, or accident-related damages, and including the potential for liability claims from a third party).

● <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). When using this service, replies are sent back in JSON format, not XML.	
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.	
Resources	The collection unit for IoT data	
Resource data	One piece of data	
Access codes	Authorization information for resources	
CORS	Meaning Cross-Origin Resource Sharing. Web server determines a controlling method to cross-domain access, enabling safe communications between domains.	

- Contents -

Chapter 1	Introduction.....	8
1.1	Purpose of this Manual	8
1.2	Available Documents.....	8
1.3	Features	8
1.4	Preparations Required for the Customer.....	8
1.5	User Environment.....	8
Chapter 2	IoT Platform.....	10
2.1	What IoT is all about.....	10
2.2	Service Overview	10
2.2.1	Data Collection	10
2.2.2	Event Function.....	11
2.2.3	Access Restrictions.....	11
2.2.4	Dynamic Resource Controller	11
2.2.5	Service Portal Functions.....	12
Chapter 3	Definitions and Concepts Of This Service	13
3.1	Tenant ID.....	13
3.2	User.....	13
3.3	Resources	13
3.4	Transferring data with Resource(Transfer)_JSON.....	14
3.5	Access Codes	15
3.6	Events	16
3.6.1	Judgment Conditions	16
3.6.2	Actions after an event is Detected	16
3.6.3	Cancel Event Settings.....	17
3.7	Writing Data.....	18
3.8	Referencing Written Data	19
3.9	API.....	20
3.9.1	HTTP REST Interface	20
3.9.2	MQTT Interface.....	22
3.10	Access Restrictions.....	23
3.11	Dynamic Resource Controller (DRC)	24
3.12	ID and Password for MQTT Connections.....	24
3.13	Regions and Times	25
3.14	Languages	25
3.15	Client Certificate	25
3.16	CORS.....	25
Chapter 4	Screen Descriptions	26
4.1	Basic Settings Procedure	26
4.2	Using CSV Files	27
4.3	Login Screen.....	27
4.4	Selecting Tenant.....	29
4.4.1	Editing Comments	29
4.5	Home Screen	30
4.5.1	Main Screen.....	30
4.5.2	Select a Tenant ID.....	30
4.5.3	Select Password Change	31
4.5.4	Language Settings.....	32
4.5.5	Select Version Information.....	32
4.5.6	Select Operating Manual	32
4.5.7	Logging Out.....	33

4.6	Resource Screen	33
4.6.1	Add All Resources.....	34
4.6.2	Add Resources.....	35
4.6.3	Downloading Resources.....	37
4.6.4	Searching for Resources	38
4.6.5	Changing Resource Settings.....	39
4.6.6	Delete All Resources.....	41
4.7	Access Code Screen.....	43
4.7.1	Batch Add Access Codes.....	44
4.7.2	Adding Access Codes.....	45
4.7.3	Searching for Access Codes	47
4.7.4	Downloading Access Codes.....	48
4.7.5	Changing Access Code Settings.....	48
4.7.6	Batch Delete Access Codes.....	54
4.8	Event Screen.....	55
4.8.1	Add Events (Judgement Settings)	57
4.8.2	Add Events (Action Settings)	60
4.8.3	Searching for Events	62
4.8.4	Changing Event Settings.....	62
4.8.5	Batch Deleting Events.....	64
4.9	Log Screen.....	64
4.9.1	Usage Screen	64
4.9.2	Operation Log Screen.....	66
4.9.3	Usage Log Screen.....	68
4.9.4	System Log Screen	69
4.10	User Screen.....	73
4.10.1	Adding Users	73
4.10.2	Changing Password.....	75
4.10.3	Searching for Users	75
4.10.4	Changing Users.....	76
4.10.5	Batch Deleting Users	77
4.11	Access Control Screen	78
4.11.1	Service Portal Access Control Screen	78
4.11.2	Access Code - Access Control Screen.....	87
4.12	Distribution Screen.....	95
4.12.1	tps/bps Distribution Settings Screen	95
4.13	Generate Certificate Screen	101
4.13.1	Generate Certificate Screen (Create New Certificate).....	101
4.13.2	Create Certificate (Certificate Signature)	103
4.14	Common Screen	105
4.14.1	MQTT Screen	105
4.14.2	CORS Setting Screen.....	106
4.14.3	Error Correction Setting Screen.....	106
Chapter 5	Example of Settings Using the Service Portal	109
5.1	Sample Data.....	109
5.2.1	Login	112
5.2.2	Add Resources.....	113
5.2.3.	Generate Certificates.....	115
5.2.4.	Add Access Codes.....	116
5.2.5.	Integrating APIs into the Application.....	118
5.2.6.	Event Function (Email) Settings	118

5.2.7.	Email Receipt Confirmation When an Event (Email) Occurs.....	124
5.2.8.	Event Function (Call API) Settings.....	124
5.2.9.	Access Control Settings	129
5.2.10.	Distribution Settings	132
5.2.11.	MQTT Settings.....	134
5.2.12.	CORS settings.....	136
5.2.13.	Error Collection Settings.....	137
Chapter 6	List of Error Messages.....	139
Chapter 7	Appendix.....	152
7.1	Notes on the CSV Format.....	152
7.1.1	Overview of the CSV Format Used for Resources.....	152
7.1.2	Overview of the CSV Format Used for Access Codes.....	154
7.2	Notes on the Sorting Policy	155
7.3	Event Function Notification Messages.....	157
7.4	Cautions When Accessing the Login URL.....	158

Chapter 1 Introduction

1.1 Purpose of this Manual

This manual describes the operations of the web interface (hereafter, Service Portal) when using the IoT Platform service (hereafter, this service).

1.2 Available Documents

The following documents are available concerning the use of this service.

Manual name	Description
IoT Platform Service Details Instruction Manual	Describes service specifications.
IoT Platform Service Portal Operating Manual	A manual describing the Service Portal. (This manual)
IoT Platform User Guide	A manual used to support API usage during application design with this service, including specific examples.
IoT Platform API Reference	An API reference manual used for application design using this service.

1.3 Features

Configuring settings from the web

You can configure settings to use this service via your web browser.

Configuring settings from the Internet

You can configure settings regarding this service from anywhere provided you have an Internet connection.

Configuring settings from various devices

You can configure settings regarding this service from not only desktop PCs but also the devices including tablet PCs.

Configuring settings regarding the collection and browsing of data

You can configure the default settings regarding the collection and browsing of data provided with this service. Configuring these settings will allow you to connect to devices compatible with the general work application using REST (HTTPs) and/or MQTT(s) protocols.

1.4 Preparations Required for the Customer

A customer user ID and password is required to utilize this Service Portal. You will be notified of this information after service contract. The following information is required to log in.

- Service Portal URL
- Customer and Tenant ID
- Service Portal user ID
- User ID password (initial)

1.5 User Environment

Please prepare the following operating environment for accessing the Service Portal.

- Connection to the Internet

- A terminal to be connected to the Internet

Table 1.5. Tested user environments

	Item	Requirements	Notes
1	Compatible OS	Windows 7 SP1 (32 bit version, 64 bit version) Windows 8.1 (32 bit version, 64 bit version) Windows 10 (32 bit version, 64 bit version)	Only available in Japanese and English on Windows
2	Browser	Internet Explorer 11	
3	Screen size	PC: 1024×768 or higher (recommended) Tablet devices: 1920×1200 or higher	

Chapter 2 IoT Platform

2.1 What IoT is all about

IoT refers to utilizing the vast amounts of information gained from people and things, connected to the Internet, in the creation of new services benefiting from the information and knowledge provided.

2.2 Service Overview

A customer specific area will be setup in our cloud service to use this service. You can apply to have multiple tenants within a customer area.

2.2.1 Data Collection

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

Access codes are utilized by the API to approve and run the requests the access code corresponds to.

<Permission types>

C: Permission to create resources, access codes, etc.

R: Permission to reference (read) data

U: Permission to register (update) data

D: Permission to delete resources, access codes, events, etc.

L: Permission to acquire a list of resources, access codes, events, etc.

G: Permissions to refer to all resources under the resource

P: Permissions to update and delete all resources under the resource

2.2.1.1 Data collection preparation

Most operations can be performed from the Service Portal, or with the API.

*API operations can only be performed for "resources", "access codes", and "events".

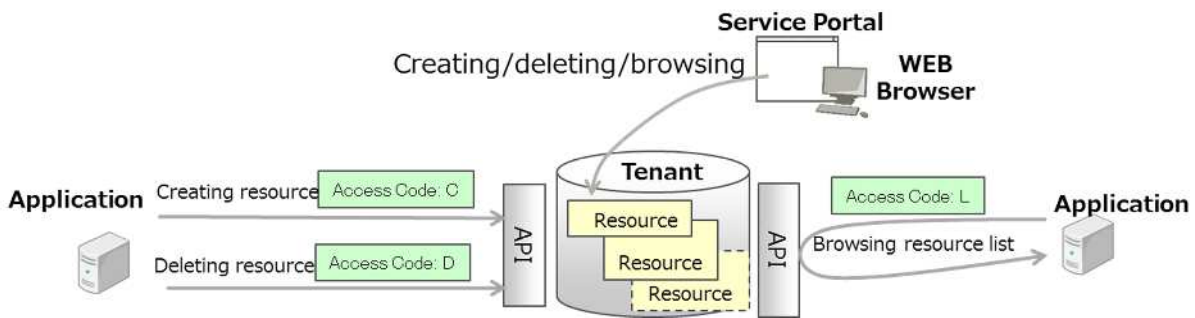


Figure 2.2.1.1 Managing resources

2.2.1.2 Collecting and using data

Data can be registered and browsed with an API.

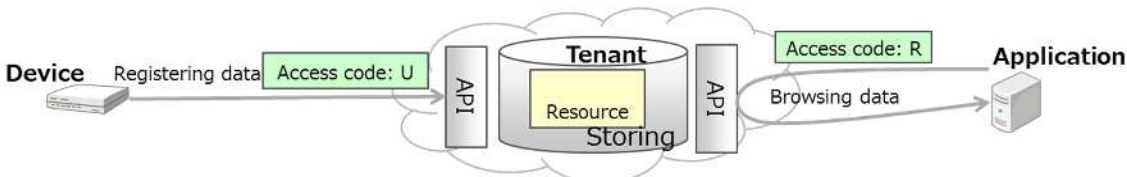


Figure 2.2.1.2-1 Storing data

Data can be transferred to other services without the need to store the data with this service.

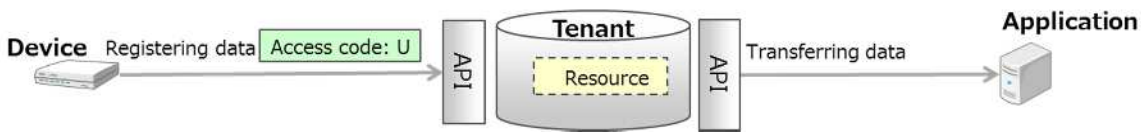


Figure 2.2.1.2-2 Transferring data

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 start up a specific API.

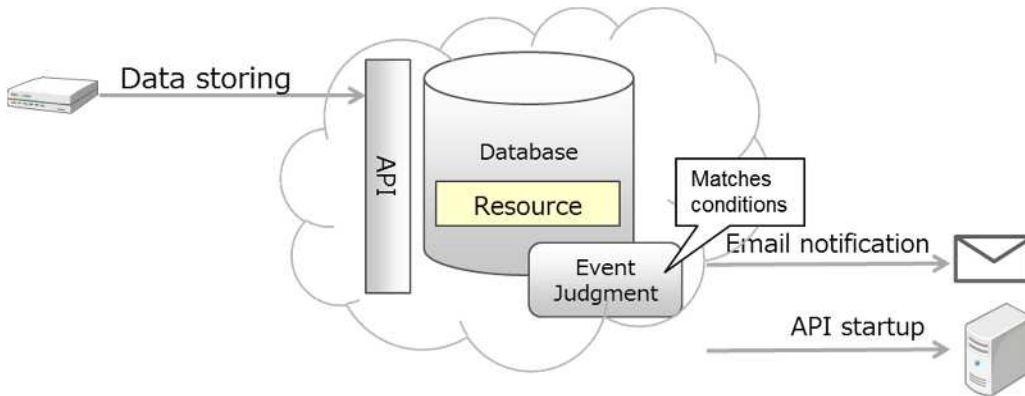


Figure 2.2.2 Event functionality

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.

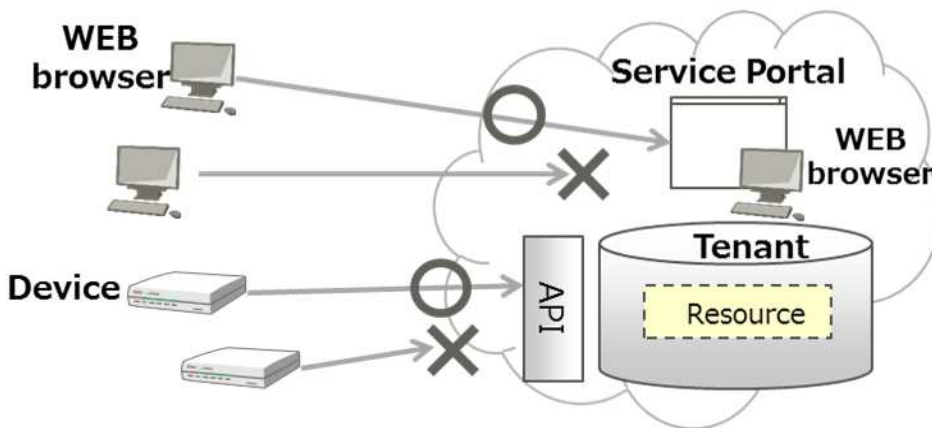


Figure 2.2.3 Access restrictions

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.

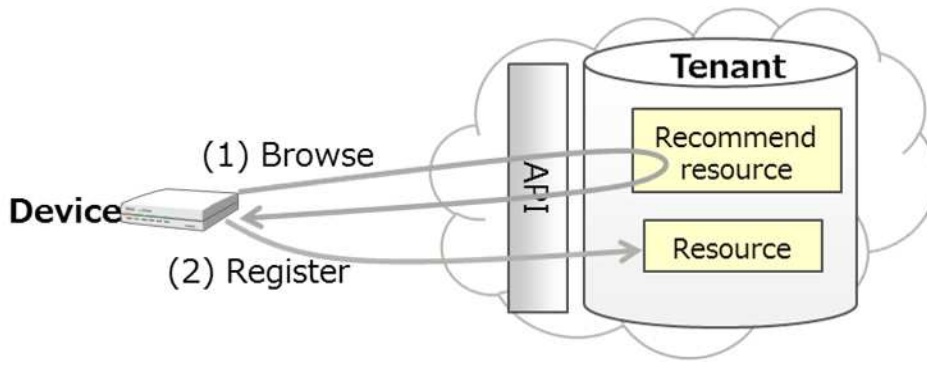


Figure 2.2.4 Dynamic resource controller

2.2.5 Service Portal Functions

Functions provided with the Service Portal are as follows.

Table 2.2.5 Service Portal Menu

	Management function	Content	Notes
1	User account	- Add and delete accounts for Service Portal use - Reissue passwords	Refer to Chapter 3.2 and 4.10
2	Resources	- Add/change/delete resources, batch add - Display/search/download resource lists	Refer to Chapter 3.3 and 4.6
3	Access codes	- Add/change/delete access codes, batch add - Display/search/download access code lists	Refer to Chapter 3.5 and 4.7
4	Events	- Add/change/delete events - Display/search events	Refer to Chapter 3.6 and 4.8
5	Logs	- Display/search/download the customer search portal use history - Display monthly use summaries - Display monthly usage amount screens - Download timestamped use logs - Display system log screens	Refer to Chapter
6	Access restrictions	- Add/change/delete IP addresses from which the Service Portal can be accessed - Add/change/delete IP addresses associated with an access code	Refer to Chapter 4.11
7	Distribution settings	- Enable/disable the distribution control function - Configure the load status calculation cycle, and the recommend cycle - Configure load status acquisition resources - Configure recommend resources - Add/change/delete edge computing conditions	Refer to Chapter 4.12
8	Client certificate	- Generate client certificates	Refer to Chapter 14.13
9	Common settings	- Configure MQTT passwords - Configure CORS - Configure error correction	Refer to Chapter 14.14

Chapter 3 Definitions and Concepts Of This Service

This chapter describes the definitions used for and concepts of this service.

3.1 Tenant ID

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

3.2 User

This is the administrator at the customer's company responsible for managing tenants included in the contract. Users can be created freely from the Service Portal. User operating permissions are shared by all users, allowing use to all of the Service Portal functions described in this manual.

[Note] Relationship between tenants and users

The relationship between tenants and users is as follows.

- Users can access all tenants under the same customer identifier.
- Users cannot access tenants under a different customer identifier.

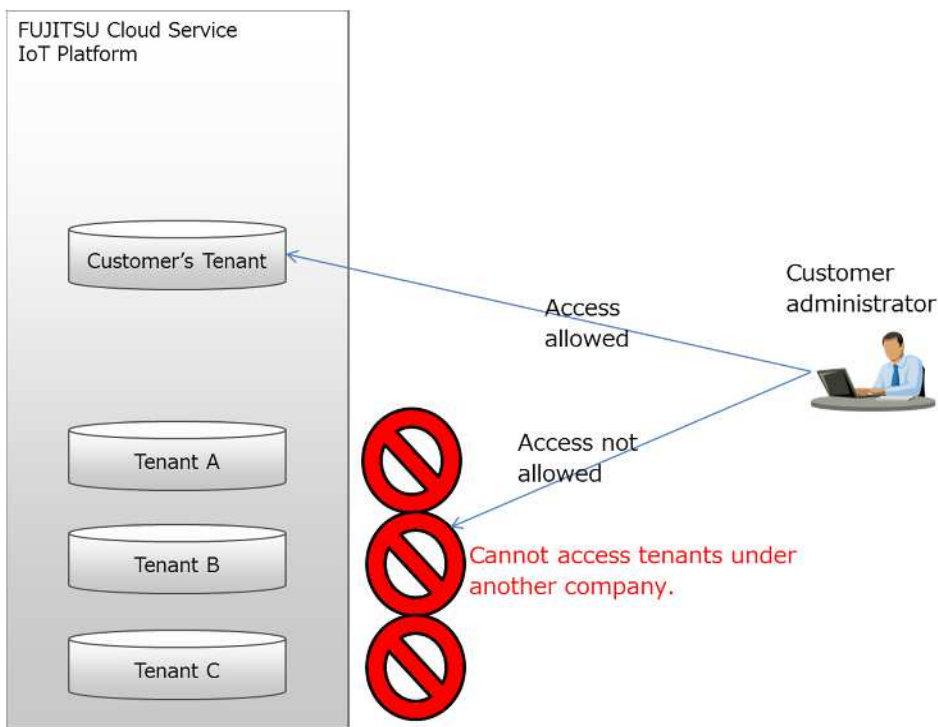


Figure 3.1 Tenants and users

3.3 Resources

This service defines "resources" as "spaces used for the collection of data".

This service manages resources in "resource paths", which are structured in a similar manner to directories and files.

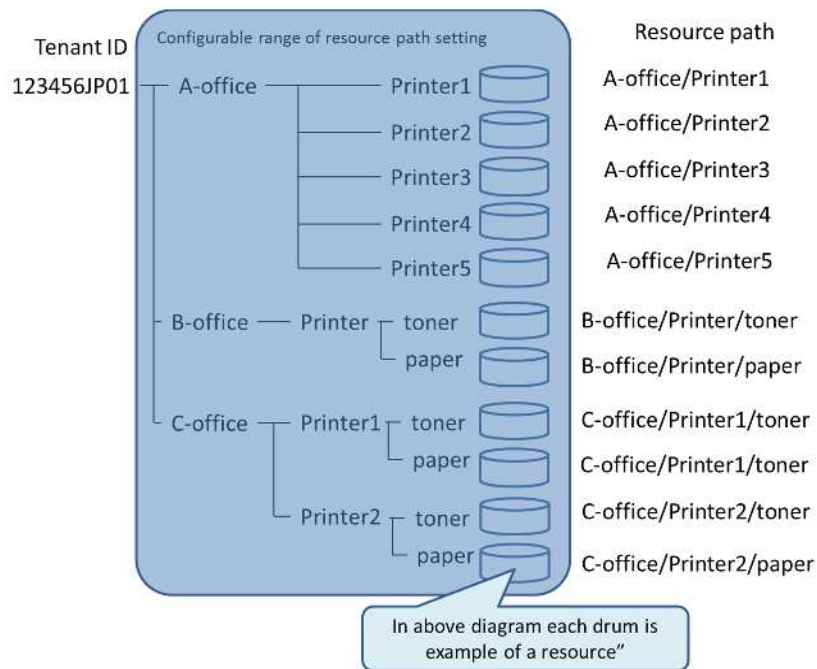


Figure 3.2 Resource Path Example

Resource paths are structured in the following manner.

- Each resource path within the same tenant is unique
- Resource paths are named with any given character string of up to 128 characters

3.4 Transferring data with Resource(Transfer)_JSON

This service allows for the creation of (transfer) resources to store data on other services, without storing data within this service. As with regular resources, resources (transfer) are controlled by "resource path", and these resource paths have the same specifications as that for regular resources, with the exception of the unique character string (`_fwd`) added to the beginning of the resource path.

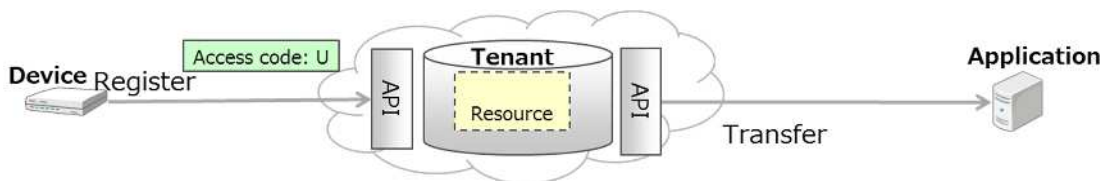


Figure 3.3 Resource (transfer) management



Note

Binary data cannot be transferred.

3.5 Access Codes

This service allows you to configure permissions (access codes) for the use of data within a resource in order to prevent use by unspecified persons. You can assign permissions to register, update, delete and list resources (CDL), permissions to register data (U) and reference data (R), and permissions to list (L) resources via an API, for each resource. By setting U permissions, users can register, update and delete data, and by setting R permissions, users can reference data. Assigning L permissions enables users to reference resources in a resource list. By setting CDL permissions, users can register, update and delete resources, register and delete access codes for resources, and register and delete events for resources, in addition to actions allowed with L permissions. By setting G permissions, users can refer to data for all resources under the resource. By setting P permissions, users can register, update, and delete data for all resources under the resource.

You can write data to a resource and reference data in a resource by adding access codes to an API call from the customer's application.

Refer to the "IoT Platform User Guide" for more information.

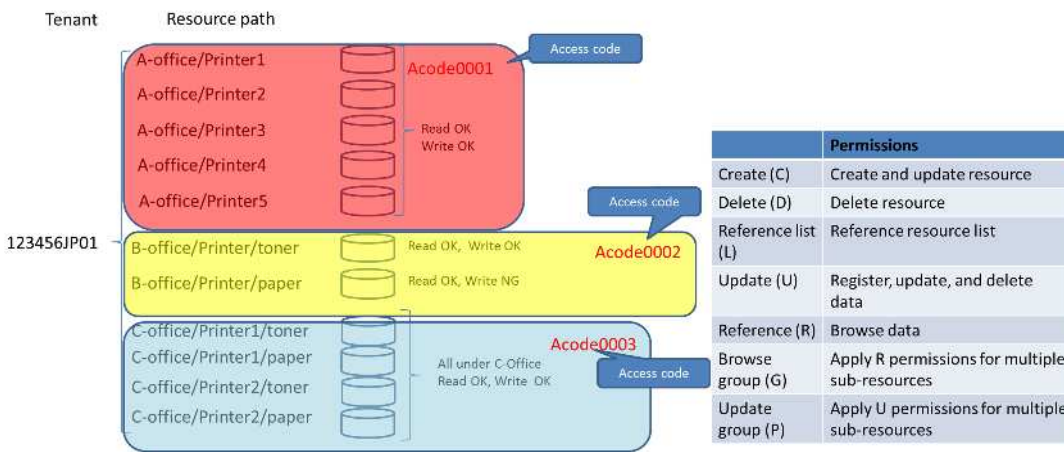


Figure 3.4 Relation between resource and access code

In the above example: OK indicates the right/permission is granted, while NG indicates "Not Granted"

Access code specifications are as follows.

- All access codes within the same tenant are unique
- Access codes must be added after the resource has been added. Access codes cannot be added without adding a resource
- Permissions for multiple resources can be configured with a single access code
- Access code values can be set freely by the customer

You can set access codes for resources (transfer) in a similar manner to regular resources. You can use a resource (transfer) to transfer data by adding access codes to an API used to call data from the customer's application.

U or P permissions are required to use a resource (transfer) to transfer data. Resources (transfer) cannot be accessed when only R or G permissions have been granted.

Refer to the "IoT Platform User Guide" for more information.

3.6 Events

This service can use an event function to perform actions when there is a change in the data.

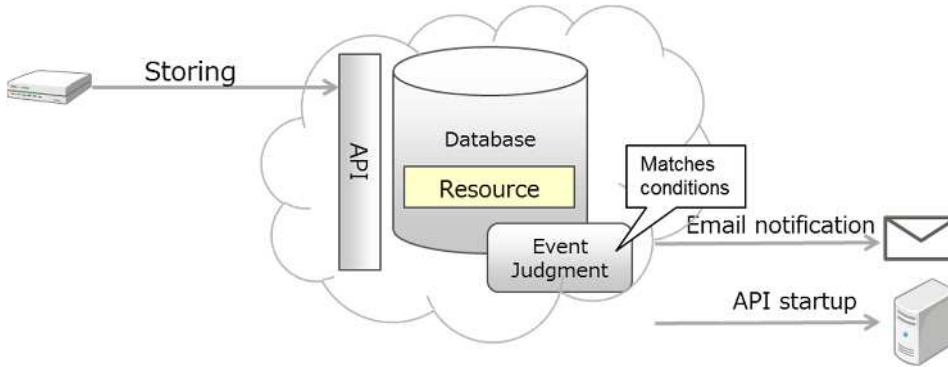


Figure 3.5 Event function



Note

Events cannot be set for resources (transfer).

3.6.1 Judgment Conditions

The judgment conditions for events set by this service's event function are as follows.

1. When data is written for the specified resource
2. When the system detects that the status of written data in the specified data position(*) changes to one of the following statuses

Character string

- Perfect match with set character string
- Contains set character string

Numerical values

- Value found in the data > Set value
- Value found in the data < Set value
- Value found in the data = Set value
- Value found in the data >= Set value
- Value found in the data <= Set value

(*) The data position is specified in JSONPath format.

You can also set a time range for detecting statuses 1. and 2. described above.

The system judges an event to have occurred when the conditions for status 1. or 2. described above are met within the time range specified (when time ranges are used).



Note

Judgment conditions cannot be specified when the resource data is in a binary format.

3.6.2 Actions after an event is Detected

The possible actions after an event is detected with this service's event function are as follows.

1. A notification is sent to the specified email address.
2. The specified REST API is called.

3.6.3 Cancel Event Settings

You can select between having this service's event function continue or invalidated after initial trigger, even when status continues to meet the event criteria. The "continue to judge events" setting is configured by default. With this default setting, if an event judgment setting is validated when the temperature reaches 30 degrees centigrade or more, as long as the temperature remains at (or above) 30 degrees centigrade, the system will continue to judge this as an event.

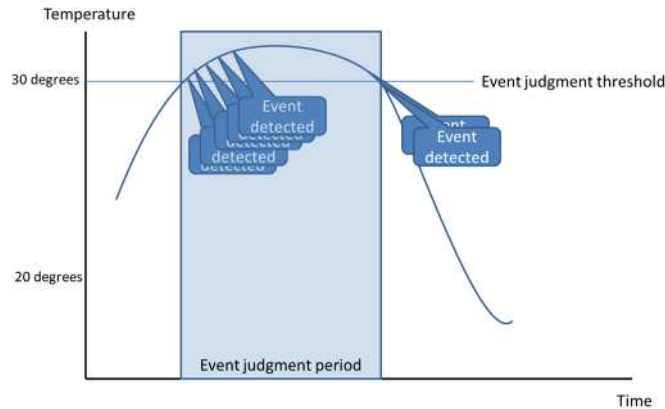


Figure 3.6. Actions when an event is detected

Continuing to have the system perform actions may not be ideal in situations that are "collecting constantly changing data at short intervals" - such as when collecting data at the above-mentioned temperature - as the state where the threshold is exceeded will continue to persist. "Cancel event settings" can be configured to prevent this by disabling the event judgment function once an event is detected.

[E.g.]

The case below shows an example of the following event settings:

- Judge events when temperatures reaching 30 degrees centigrade and over or more
- Cancel events when the temperature drops to 20 degrees centigrade or below

In this instance, while a temperature that reaches 30 degrees centigrade is initially detected as an event, this will disable the event judgment function while the temperature remains at 30 degrees centigrade following this, meaning that further events will not be detected even if a state of 30 degrees centigrade or more persists. Further, as event judgment functionality will no longer be disabled once the temperature drops to 20 degrees centigrade or below, events will start being detected again from this point. The figure below presents this as an image.

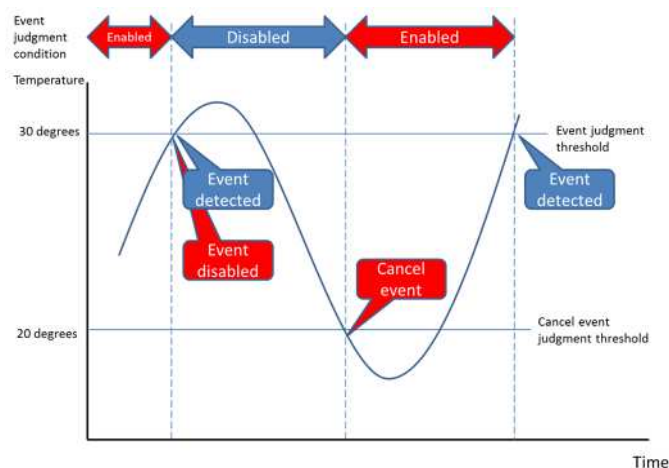


Figure 3.7. Relationship between event judgments and disabled events

*Do not perform cancel event settings for the following cases.

- When you intend to set data writing for a specific resource only as the target of event judgments
- When you intend to set same content data writing for data within a resource as the target of event judgments

3.7 Writing Data

You can write data using this service by adding a resource. The general procedure for writing data is as follows.

1. Use the Service Portal or an API to add a resource. (Step (1) in the figure below)
2. Use the Service Portal or an API to grant access permissions for the resource. (Step (1) in the figure below)
You will be able to write data by granting writing permissions for the resource.
3. Add an API call to the application to write data to the resource. (Step (3) in the figure below) Refer to the "IoT Platform User Guide".
4. Write data to this service by calling the API used to write data to the resource from the application. (Step (4) in the figure below)

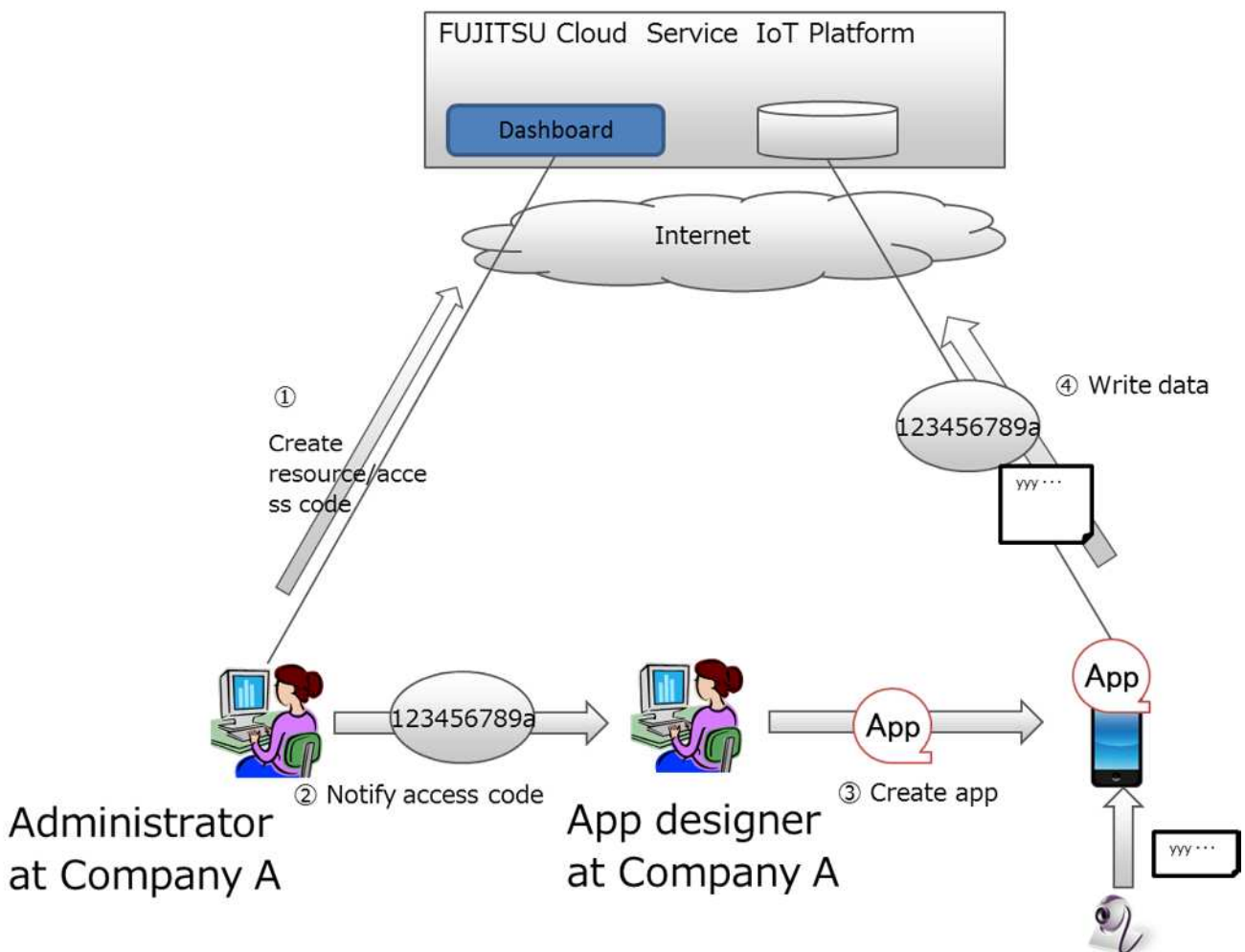


Figure 3.8. Steps taken to write data

3.8 Referencing Written Data

This service can be used to reference data written using the steps outlined in Chapter 3.8. You can also specify which data to reference by setting search conditions. The general procedure for referencing data is as follows.

1. Add an API call to the application you prefer to use for referencing resource data. Reference permissions must be set for the corresponding resource when the access code is set. Refer to the "IoT Platform User Guide" for more information.
2. You can reference data from this service by calling APIs used to reference data written to a resource from the application.

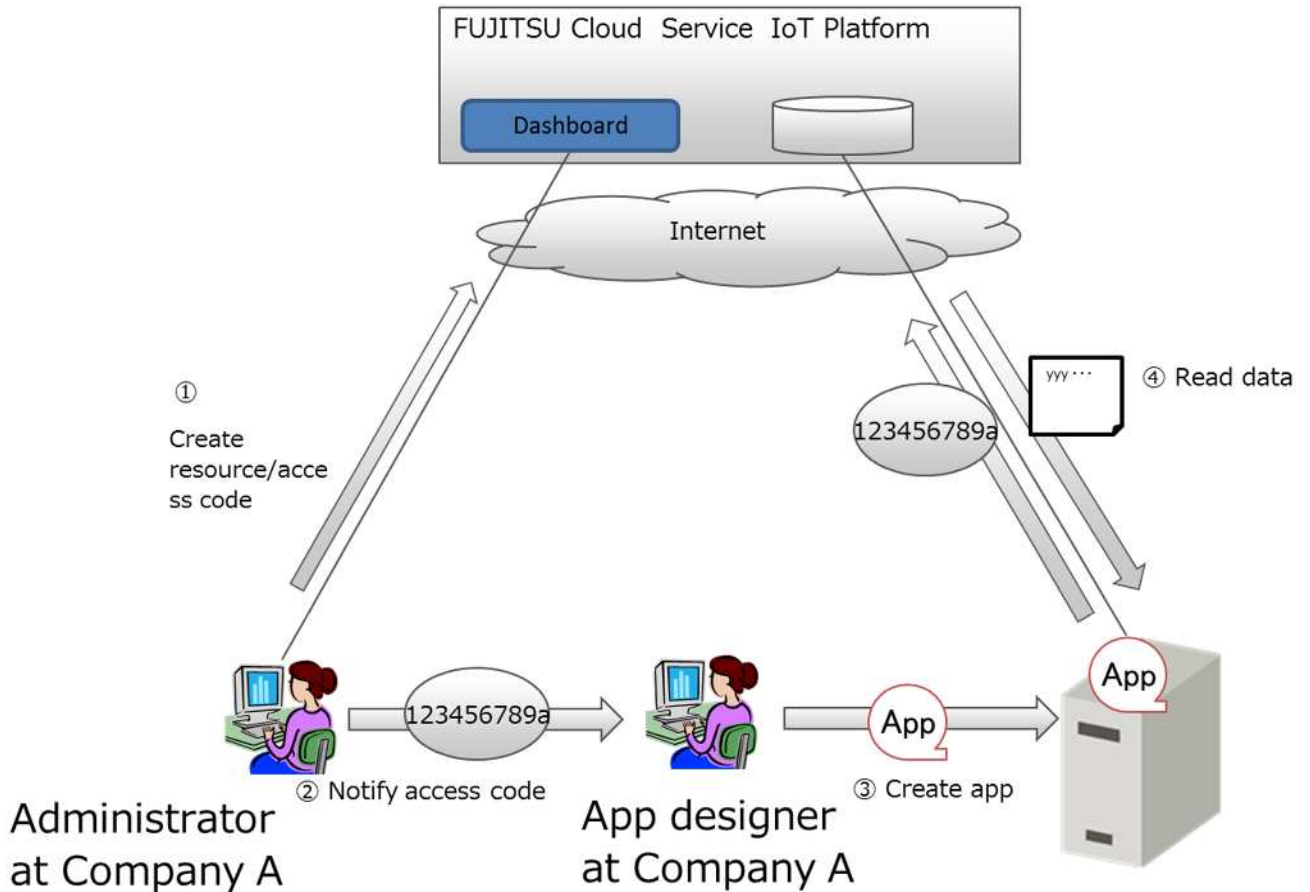


Figure 3.9. Steps to reference data

3.9 API

APIs enabling users to interact with resources, access codes, events, and the data in a resource have been made available with this service.

Refer to the "IoT Platform User Guide" for more information.

3.9.1 HTTP REST Interface

Compatible with http and https.

The interface provided is described below.

Data groups within a resource are written as resource data.

Table 3.9.1 REST Interface (IF) list

- Resource related

	Operation	Option	Method name	Relation to access code
1	Register resource	-	POST	Permitted with C
2	Referencing Resource Metadata	Specify field to acquire Specify number of acquired data items	GET	Permitted with L
3	Updating Resource Metadata	-	PUT	Permitted with C
4	Delete resource	-	DELETE	Permitted with D

- Resource data related (if the data format is JSON)

	Operation	Option	Method name	Relation to access code
1	Registering resource data	Registration timestamp RETAIN flag Bulk Insert flag	PUT	Permitted with U Permitted to all resources with P
2	Browsing resource data	Specify field to acquire	GET	Permitted with R Permitted to all resources with G
3	Retrieving resource data	Specifying time/date Specifying the range of times/dates Specify field to acquire Specify number of acquired data items	GET	Permitted with R Permitted to all resources with G
4	Updating resource data	Registration timestamp after update	PUT	Permitted with U Permitted to all resources with P
5	Deleting resource data	Specifying time/date Specifying the range of times/dates	DELETE	Permitted with U Permitted to all resources with P



Note

The following restrictions apply to resources (transfer).

- Only PUT method support provided. GET and DELETE are unavailable for use.

- U permissions must be granted to access resources. Users with only R permissions cannot access said resources.

- The binary data format cannot be used.

- Resource data related (if the data format is binary)

	Operation	Option	Method name	Relation to access code
1	Registering resource data	Registration timestamp	PUT	Permitted with U Permitted to all resources with P
2	Browsing resource data	—	GET	Permitted with R Permitted to all resources with G
3	Retrieving resource data	Specifying time/date Specifying the range of times/dates Specify number of acquired data items	GET	Permitted with R Permitted to all resources with G
4	Deleting resource data	Specifying time/date Specifying the range of times/dates	DELETE	Permitted with U Permitted to all resources with P



Note

Binary resource data cannot be updated.

Memo

This section provides an explanation of resource-related and resource data-related options that can be specified.

- Registration timestamp

Specify the data and time data is registered. When left blank, this will be set to the date and time the service receives a request.

- RETAIN flag

Specify whether to retain the registration data on the MQTT broker side.

- Bulk Insert flag

Specify whether or not to run a bulk insert(*).

*Data registered with multiple JSON objects in a JSON array will be stored and managed as separate data items.

- Specify time/date

Specify the target to be retrieved/deleted by date and time.

- Specifying the range of times/dates

Specify the target to be retrieved/deleted by a range of times/dates.

- Specify field to acquire

Specify the field to acquire. Only fields specified will be acquired.

- Specify number of acquired data items

You can specify the number of items to acquire, and the number of data items retrieved as search results to skip.

The maximum number of items that can be acquired at once is 1,000.

- Registration timestamp after update

Update the data registration timestamp at the date and time specified.

- Access code-related

	Operation	Option	Method	Notes
--	-----------	--------	--------	-------

			name	
1	Register access code	-	POST	
2	Reference access code information	Specify resource path Specify number of acquired data items	GET	
3	Update access code information	-	PUT	
4	Delete access code	-	DELETE	

Memo

This section provides an explanation of access code-related options that can be specified.

- Specify resource path

Specify the resource path for resources corresponding to the access code to be referenced as a condition, and return only those access codes that meet the conditions set as search results.

- Event-related

	Operation	Option	Method name	Notes
1	Register event	-	POST	
2	Reference event	Specify event ID Specify number of acquired data items	GET	
3	Update event	-	PUT	
4	Delete event	-	DELETE	

Memo

This section provides an explanation of event-related options that can be specified.

- Specify event ID

Specify the event ID for events to be referenced as a condition, and return only those events that meet the conditions set as search results. When omitted, all events pertaining to the tenant will be search targets.

3.9.2 MQTT Interface

Compatible with MQTT and MQTTS.

The interface provided is described below.

Data groups within a resource are written as resource data.

Table 3.9.1 MQTT Interface (IF) list

- Resource data related (if the data format is JSON)

	Operation	Option	Control Packet name	Relation to access code
1	Registering resource data	Registration timestamp	PUBLISH	Permitted with U Permitted to all resources with P
2	Browsing resource data	-	SUBSCRIBE	Permitted with R

			+PUBLISH(*)	Permitted to all resources with G
--	--	--	-------------	-----------------------------------

- Resource data related (if the data format is binary)

	Operation	Option	Control Packet name	Relation to access code
1	Registering resource data	-	PUBLISH	Permitted with U Permitted to all resources with P
2	Browsing resource data	-	SUBSCRIBE +PUBLISH(*)	Permitted with R Permitted to all resources with G

(*) PUBLISH from this service after SUBSCRIBE from the client (cannot be specified as an option)

Memo

- Registration timestamp
Specify the data and time data is registered. When left blank, this will be set to the date and time the service receives a request.

3.10 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.

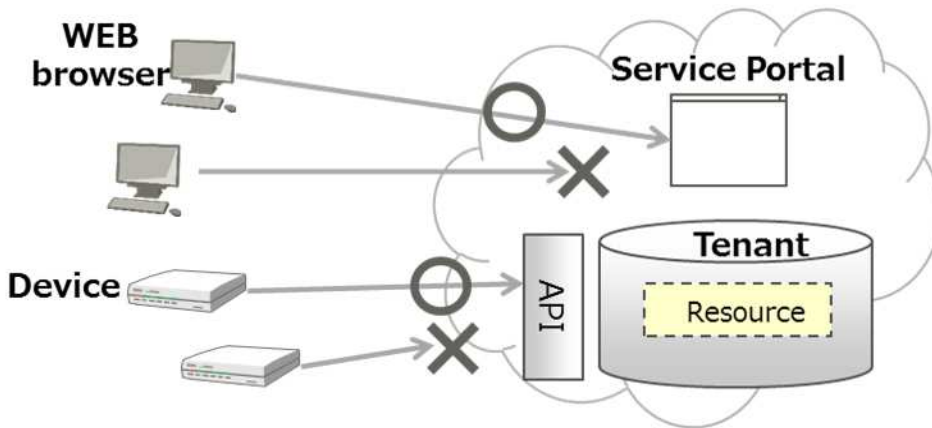


Figure 3.10. How access restrictions work

3.11 Dynamic Resource Controller (DRC)

This service uses the dynamic resource controller (distributed control) function (hereafter, DRC) to enable the use of proprietary overall optimization technologies (distributed service platform technologies) of Fujitsu 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.

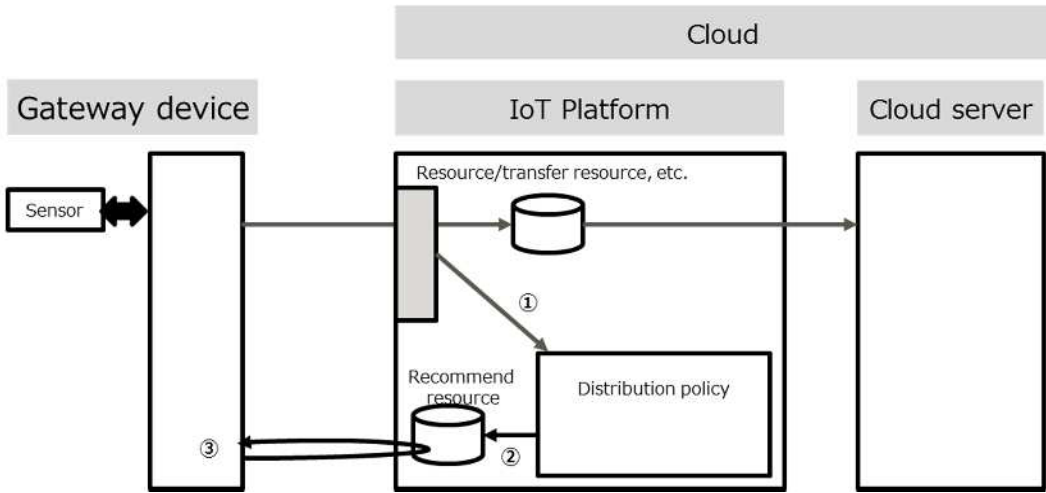


Figure 3.11. Visual representation of the DRC

This service collects service load information 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. The process flow for using the DRC is as follows.

- The distribution policy is used to monitor the load placed on this service.
- Recommend resources are flagged as recommended based on a pre-defined distribution policy.
- Processes are modified based on the rewritten recommend resources.

The gateway device, cloud solution and sensor shown in the diagram shall be prepared by the customer. This enables processes to be modified based on system load, allowing for stable system operation.

3.12 ID and Password for MQTT Connections

- MQTT connection account

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

- MQTT password

The MQTT password policy is as follows. (note: MQTT password can be set and changed within the service portal)

<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 limit
Period of password validity	No limit

3.13 Regions and Times

- Regions

This service can be used in multiple regions.

Users can ascertain which region is active for the system they are logged into from the region code displayed next to the tenant ID at the top of the Service Portal screen.

- System times, on-screen dates and times and API dates and times

System times for this service are set to Coordinated Universal Time (UTC), regardless of which region the service is provided. Date and time information and log output times displayed on the Service Portal screen, and times specified with an API are all displayed, output and specified, based on system times.

3.14 Languages

Users can select the language in which item names, messages, etc. appear on the Service Portal screen, choosing from Japanese or English.

Language settings are saved when creating/modifying users and when users change language settings by themselves. The Service Portal screen will automatically appear in the language set when next logging in.

3.15 Client Certificate

In this service, users can set the client certificate as an authorization function to access to the access code. You can generate the certificate on the screen of the Service Portal.

3.16 CORS

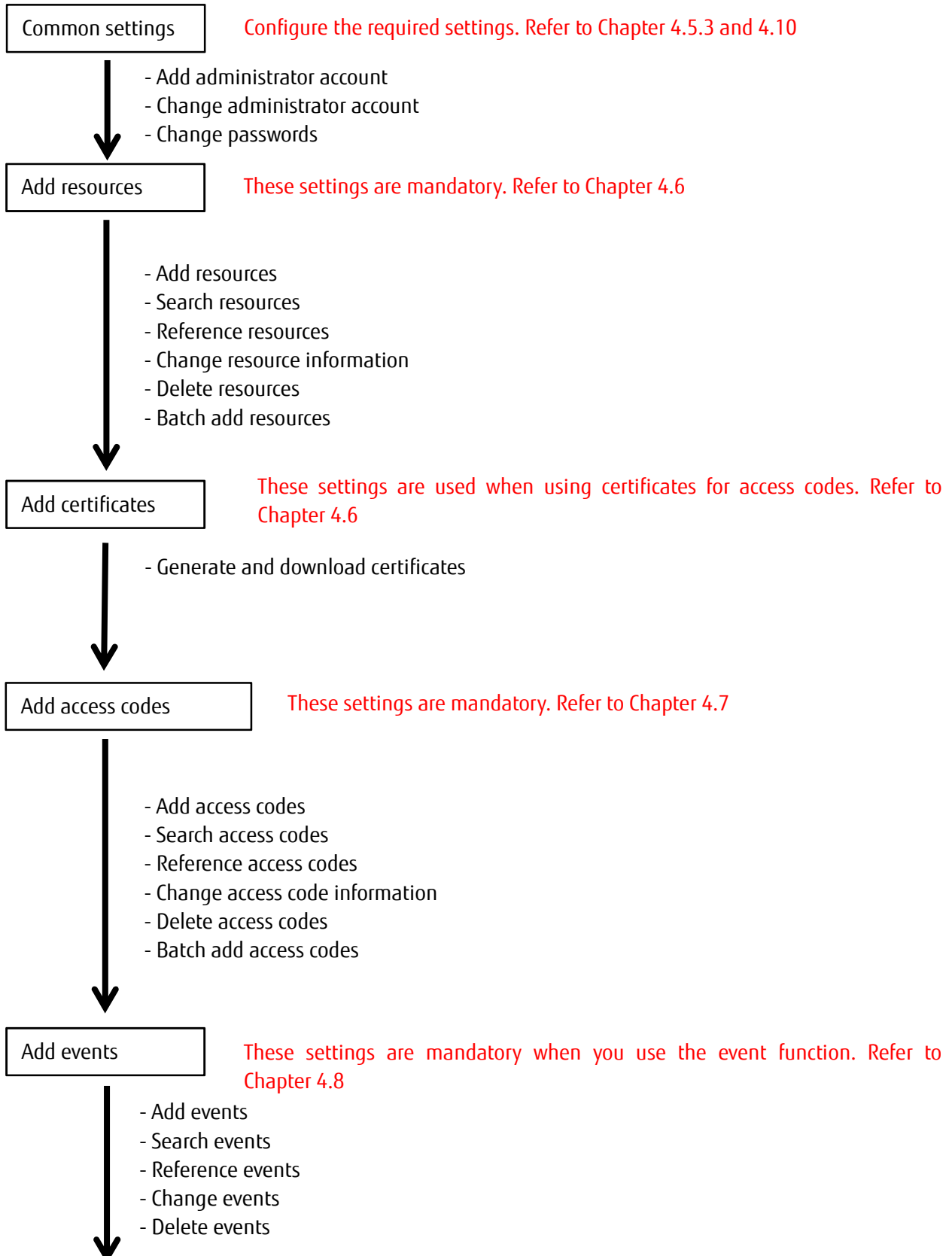
By using Cross-origin Resource Sharing (CORS), this service provide you to send an HTTP request to the domains other than the domain which you installed this service. You can switch activate and deactivate CORS on the Service Portal screen.

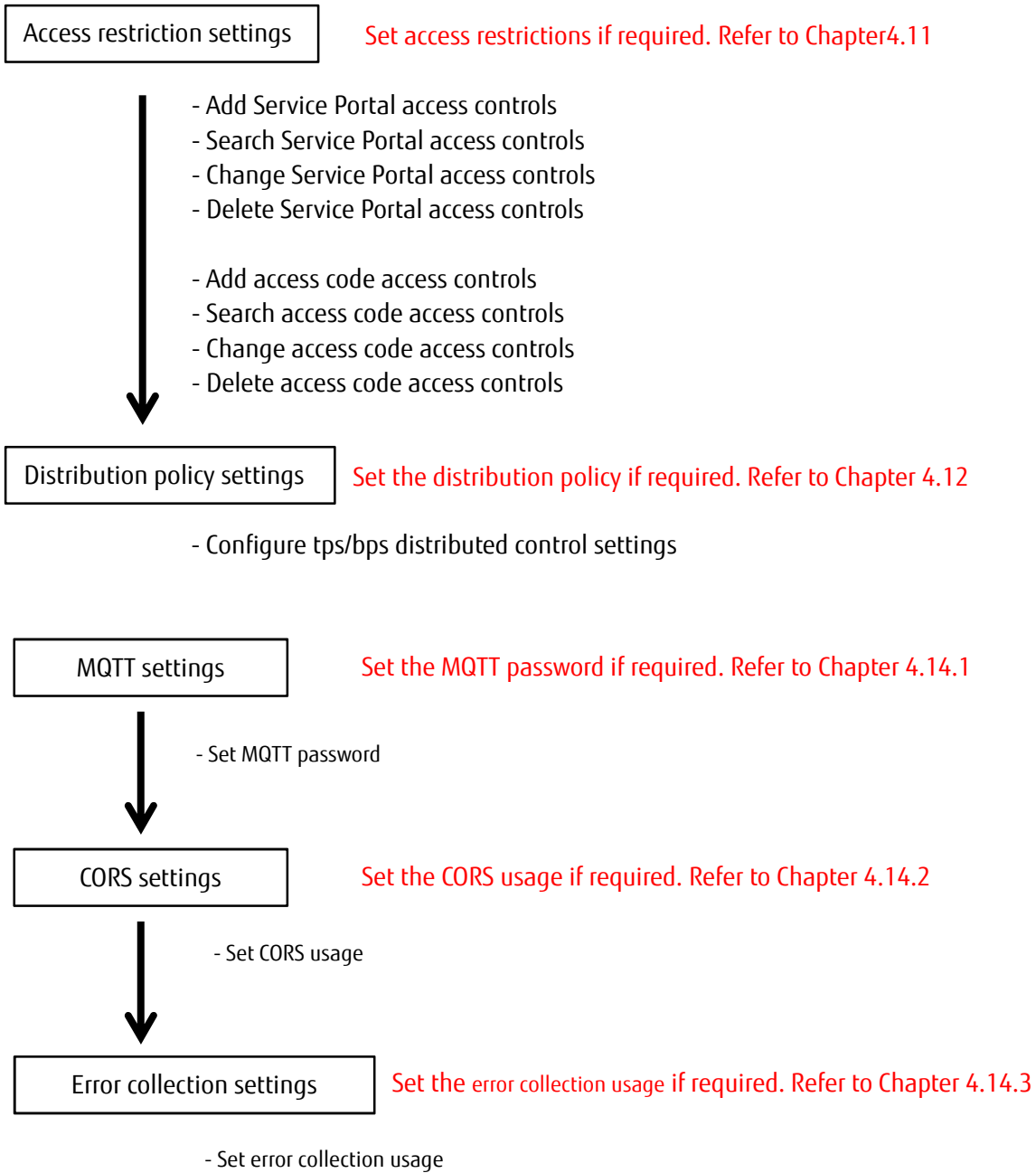
Chapter 4 Screen Descriptions

This chapter describes how to use the Service Portal.

4.1 Basic Settings Procedure

A flowchart showing the setting procedures that will need to be configured when starting to use the service is provided below.





4.2 Using CSV Files

We recommend preparing a preliminary list of resources and access codes before adding them to the system. Batch adding resources and access codes by uploading CSV files saves you time and effort when using the system for the first time, or when modifying a number of resources and access codes. Refer to Chapter 5.2.2 and 5.2.44 for more details.

4.3 Login Screen

The following screen will appear when accessing the login URL.

Memo

- The login URL will appear when configuring service use settings from the FUJITSU Cloud Service K5 PaaS Portal screen.

1. Enter the user ID into (1).
2. Enter your password into (2).
3. Click the Login button shown as (3).



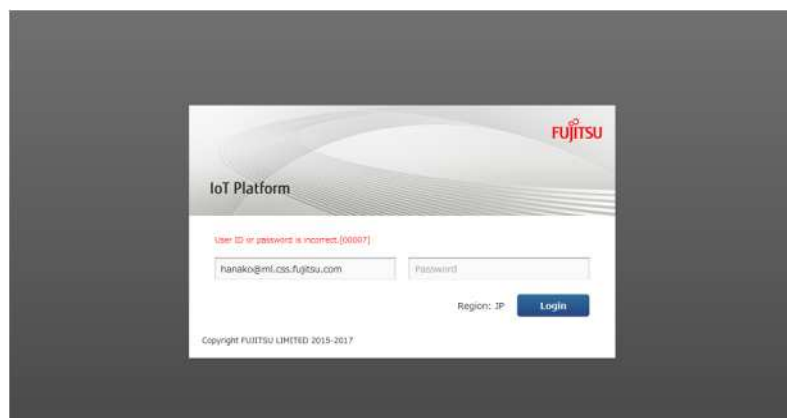
Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
User ID	Text	Single-byte alphanumeric characters	Yes	-	-	E-mail address format
Password	Text	Single-byte alphanumeric characters Alphanumeric characters	Yes	8 to 15	-	The character types allowed are as follows Upper and lower case alphabetical characters, numbers, # @ - () : . _

Memo

- The region of the system you are logging into is fixed based on your login URL.
- The language appeared in the Login screen can be changed via your browser's language settings. Pages will appear in Japanese when your browser's language settings are set to Japanese. It will appear in English when these settings are set to any other language.
- The language appeared in the pages after logging in can be set for each user logging in. Refer to Chapter 4.10 for more details.

The screen will show the following when the user ID and password do not match.



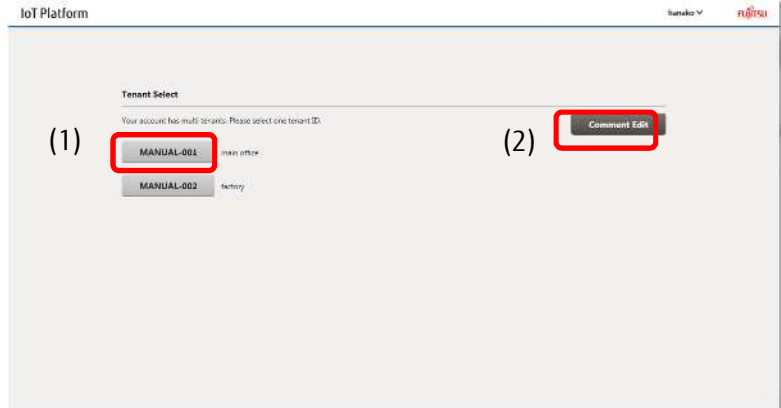
If you have forgotten your password, have another customer administrator within the same tenant reset the
All Rights Reserved, Copyright©FUJITSU LIMITED 2016-2018

password. Refer to Chapter Chapter 13.14.10.4 (1) for more details.

4.4 Selecting Tenant

The following screen will appear when you have logged in successfully and there are multiple tenants included in the customer's contract.

1. Select the tenant you prefer to use by clicking the Tenant Select button shown as (1) in the figure. After clicking this, you will proceed to the Home screen described in Chapter 4.5.



Click the Comment Edit button shown as (2) in the figure to edit comments appearing at the right of the Tenant Select button.

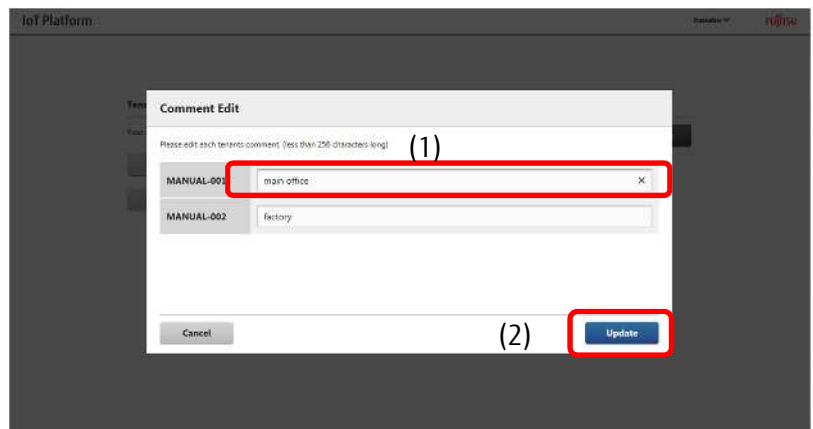
Memo

This screen will not appear when only one tenant is included in the customer's contract. In this instance, you will proceed directly to the Home screen described in Chapter 4.5.

4.4.1 Editing Comments

The following screen will appear when the Select Comment button is clicked.

1. Enter the Comment in the area shown as (1) in the figure.
2. Click Update shown as (2) in the figure.



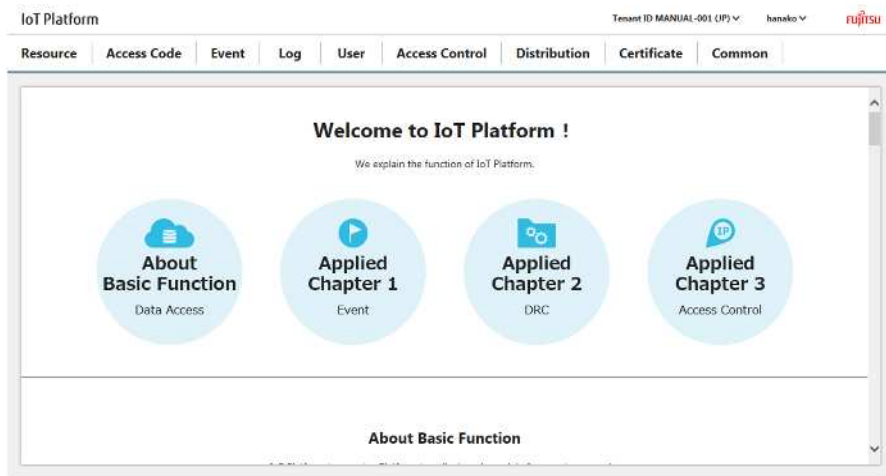
Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Comment	Text	Optional	-	Up to 256	-	

4.5 Home Screen

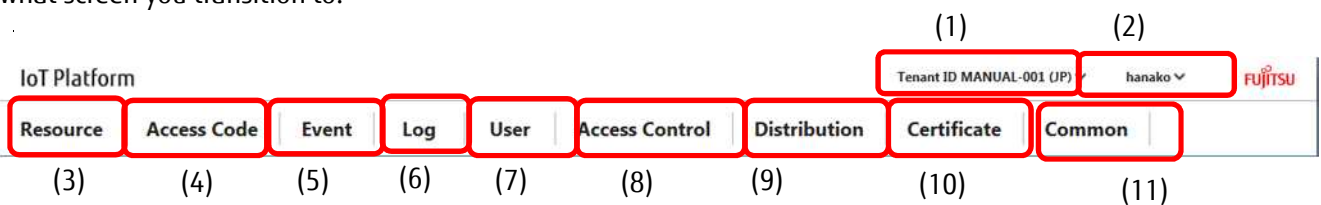
The following screen will appear when you have successfully logged in.

An overview of the service functions available appears on the Home screen. Click an image to jump to a brief description of each of the functions available.



4.5.1 Main Screen

This section covers the "Main screen" which always appears at the top of the screen after logging in, regardless of what screen you transition to.



Number	Entry name	Description	Notes
(1)	Select a Tenant ID	Selects the tenant ID. The region code will appear after the tenant ID in parentheses.	Refer to Chapter 4.5.2
(2)	Select User	Users are able to select "Change Password/Language Settings/Version Information/Operating Manual/Logout".	Refer to Chapter 4.5.3 to 4.5.7
(3)	Resource	Opens the Resource screen.	Refer to Chapter 4.6
(4)	Access Code	Opens the Access Code screen.	Refer to Chapter 4.7
(5)	Event	Opens the Event screen.	Refer to Chapter 4.8
(6)	Log	Opens the Log screen.	Refer to Chapter 4.9
(7)	User	Opens the User screen.	Refer to Chapter 4.10
(8)	Access Control	Opens the Access Control screen.	Refer to Chapter 4.11
(9)	Distribution	Opens the Distribution screen.	Refer to Chapter 4.12
(10)	Certificate	Opens the Certificate screen.	Refer to Chapter 4.13
(11)	Common	Opens the Common screen.	Refer to Chapter 4.14

4.5.2 Select a Tenant ID

When multiple tenants are included in a customer's contract, you will be able to click the Select Tenant ID pull-down menu to show "Tenant Select".

"Tenant Select" will appear. Click Tenant Select to proceed to the screen in Chapter 4.4.

Memo

Nothing will appear when clicking Select Tenant ID when only one tenant is included in the customer's contract.

4.5.3 Select Password Change

This section describes the process used to change passwords to log into the Service Portal.

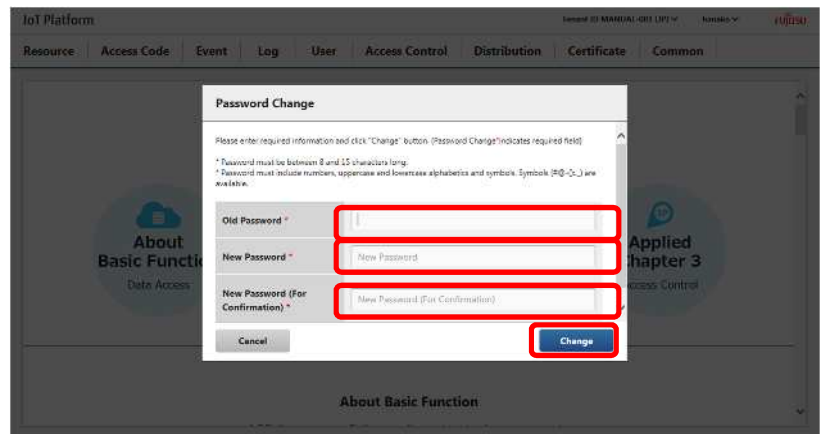
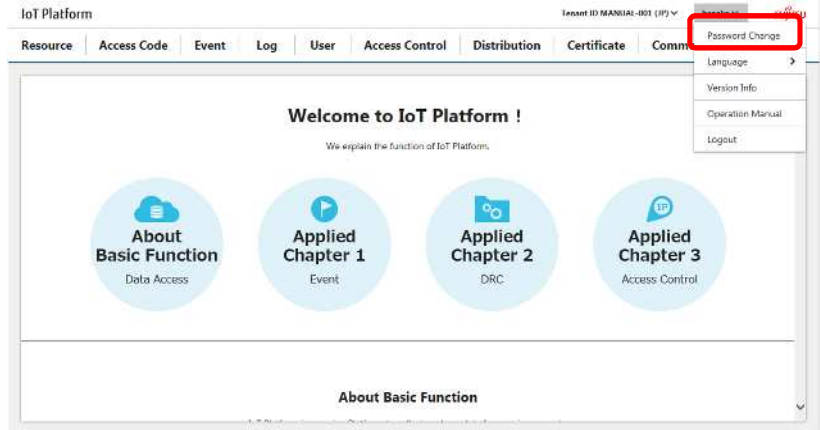
1. Select "Password Change" from the user name pull-down menu on the Home screen to move to the Password Change screen.

2. Enter your old password.

3. Enter your new password.

4. Enter your new password again (for confirmation).

5. Click Change.



Notes on input parameters

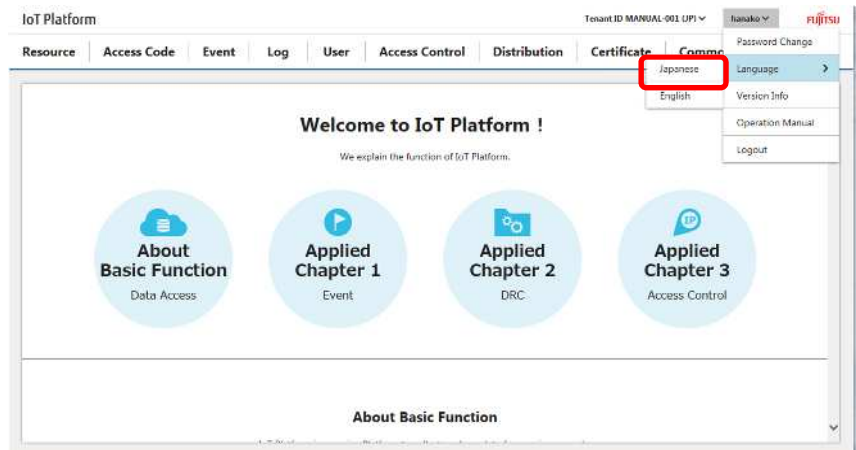
Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Old password	Text	Single-byte alphanumeric characters Alphanumeric characters	Yes	8 to 15	-	The character types allowed are as follows Upper and lower case alphabetical characters, numbers, # @ - () : . _
New password	Text	Single-byte alphanumeric characters Alphanumeric characters	Yes	8 to 15	-	The character types allowed are as follows Upper and lower case alphabetical characters, numbers, # @ - () : . _

New password (for confirmation).	Text	Single-byte alphanumeric characters Alphanumeric characters	Yes	8 to 15	-	The character types allowed are as follows Upper and lower case alphabetical characters, numbers, # @ - () : . _
----------------------------------	------	--	-----	---------	---	--

4.5.4 Language Settings

This section describes how to change the language display for the Service Portal.

Select the language from the Language pull-down menu under the user name.
You can select from Japanese or English.



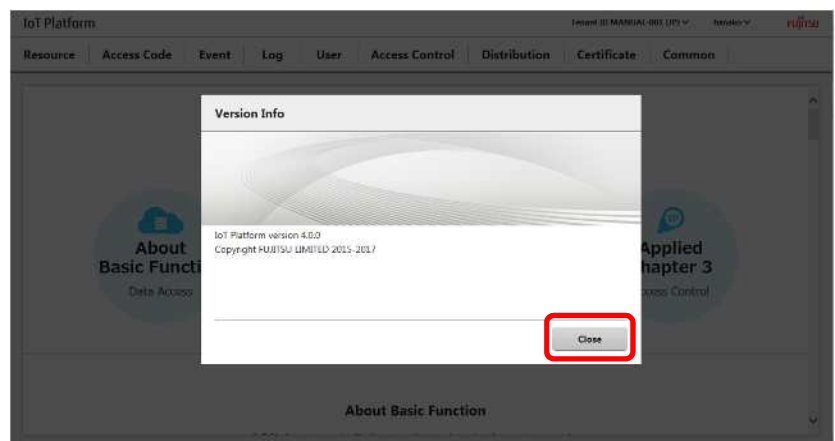
Memo

Language setting changes in Language will be saved, and the screen will appear in the language selected when you next log in.

4.5.5 Select Version Information

The following screen will appear when you select Version Info from the user name pull-down menu.

Click Close to return to the previous screen.

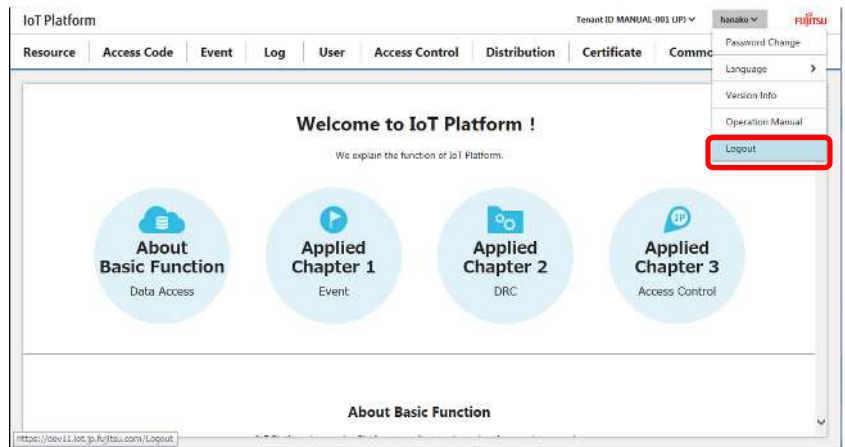


4.5.6 Select Operating Manual

This operating manual will appear on the device you are logged into when you select Operation Manual from the user name pull-down menu.

4.5.7 Logging Out

Log out by selecting Logout from the user name pull-down menu in the Main screen.

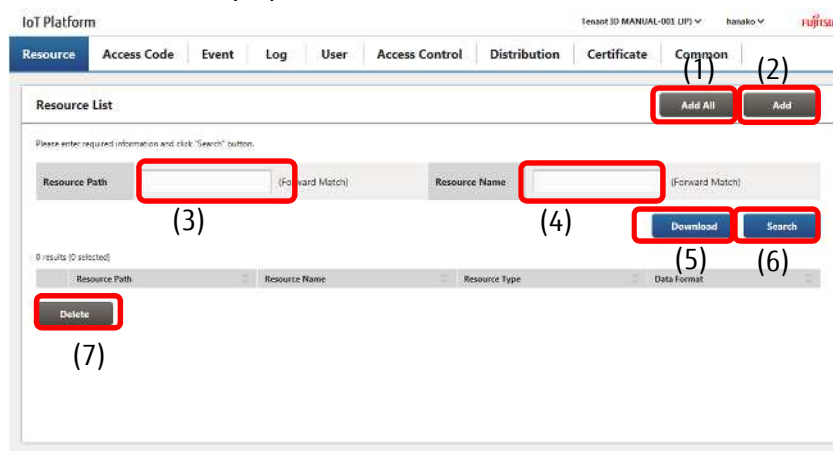


Note

- Make sure to log out before closing the browser screen.

4.6 Resource Screen

Click Resource on the Main screen to display the Resource screen.



Number	Entry name	Description	Notes
(1)	Add all	Batch adds all resources.	Refer to Chapter 4.6.1
(2)	Add	Adds the resource.	Refer to Chapter 4.6.2
(3)	Resource path	Set when searching for resources.	Refer to Chapter 4.6.4
(4)	Resource name	Set when searching for resources.	Refer to Chapter 4.6.4
(5)	Download	Downloads configured resource information.	Refer to Chapter 4.6.3
(6)	Search	Retrieves resources.	Refer to Chapter 4.6.4
(7)	Delete	Use when deleting batches of resources.	Refer to Chapter 4.6.6

Notes on input parameters

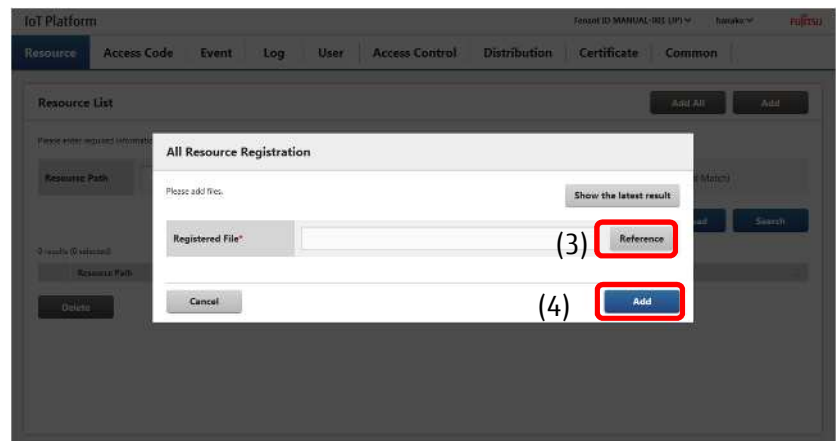
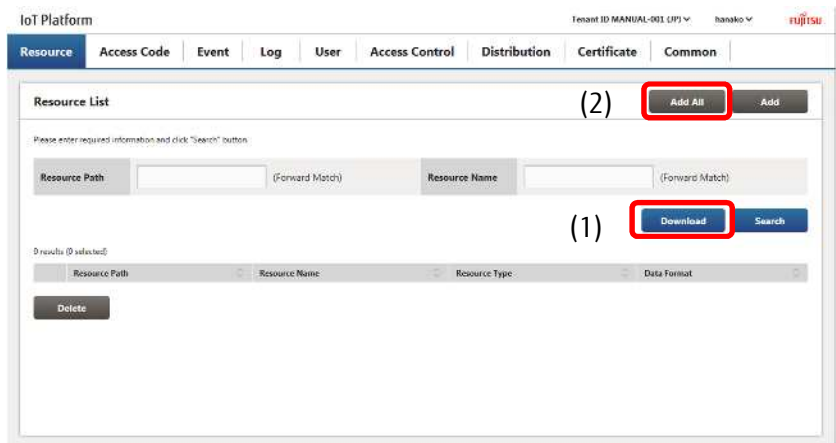
Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				

Resource path	Text	Single-byte alphanumeric characters	-	Up to 128	-	Usable characters Numbers, upper and lower case alphabetical characters, - (hyphen), _ (underscore), / (slash) Refer to 4.6.4
Resource Name	Text	Optional	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters @ - () : . _ Refer to 4.6.4

4.6.1 Add All Resources

You can add resources as a batch using CSV files.

1. Click Download shown as (1) in the figure to download a CSV template to your device.
2. Edit the CSV file.
3. Click Add All shown as (2) in the figure.
4. Click Reference shown as (3) in the figure and select the edited CSV file.
5. Click Add shown as (4) in the figure.



Memo

- The name of the downloaded file will be in resource_YYYYMMDDHHMMSS.csv format.
- You can download the CSV template only without a resource being added by downloading the CSV template before a resource is added.
- You can also add access codes without downloading by editing a CSV file with the same formatting as the template from the PC in use.
- A maximum of 100 resources can be added at a single operation using the Add All function. Add resources in multiple batches when you are adding 100 or more resources.

- Resources cannot be added if a resource with the same resource path and resource name is already in use within the same tenant ID.
- You can only add new resources when downloading and editing a CSV file. Existing resources cannot be modified.
- Refer to Chapter Chapter 17.1 for more information about the CSV format.

[1] Display previous results / Show the latest result

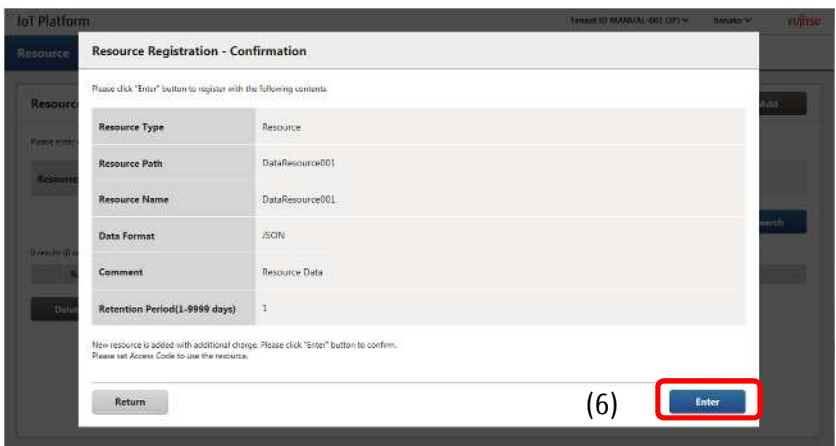
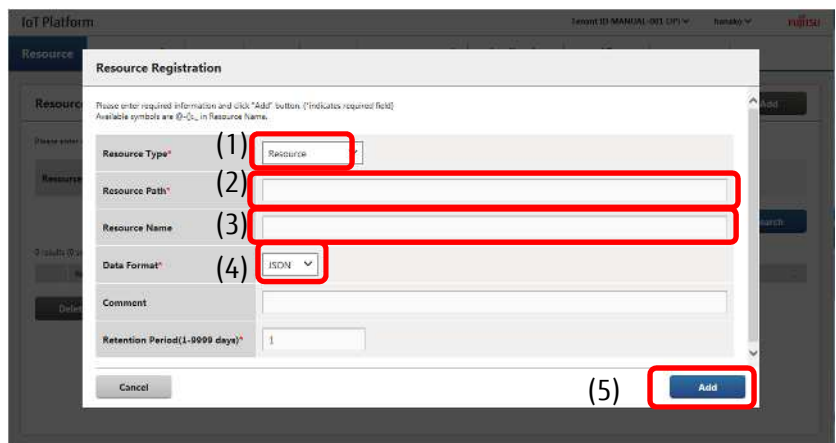
Click "Display Previous Results / Show the latest result" on the All Resource Registration screen to output a log of previous operations.

4.6.2 Add Resources

The following screen will appear when you click Add on the Resource screen described in Chapter 4.6. This menu is used when you prefer to add a single resource only. First, select the resource type from (1) in the screenshot shown below. If "Resource" is selected as the resource type, an entry field for the resource to be used for data storing will appear. If Resource (Transfer) is selected, an entry field for the data transfer resource will appear. Examples below explain settings for each type of resource.

- For data storing resources

1. Select Resource from the pull-down menu shown as (1) in the figure.
2. Enter the resource path into the field shown as (2) in the figure.
3. Enter the resource name into the field shown as (3) in the figure.
4. Select the data format from the pull-down menu shown as (4) in the figure.
5. Click (5) Add.
6. A Confirmation screen will appear after clicking Add. Click Enter shown as (6) in the figure to add the resource.



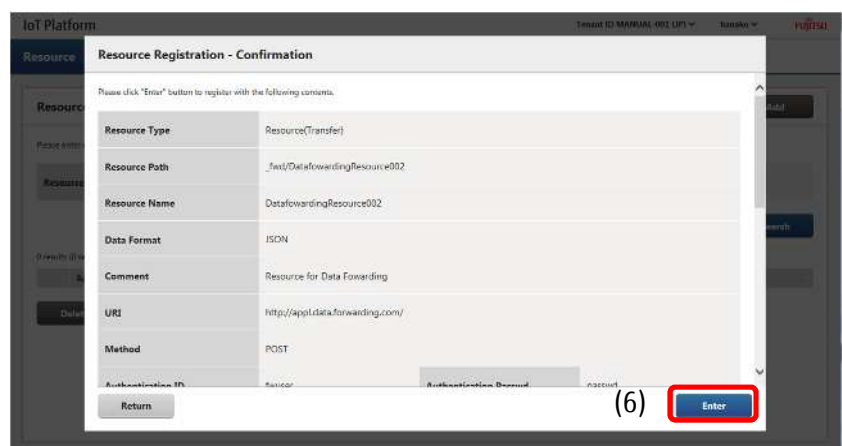
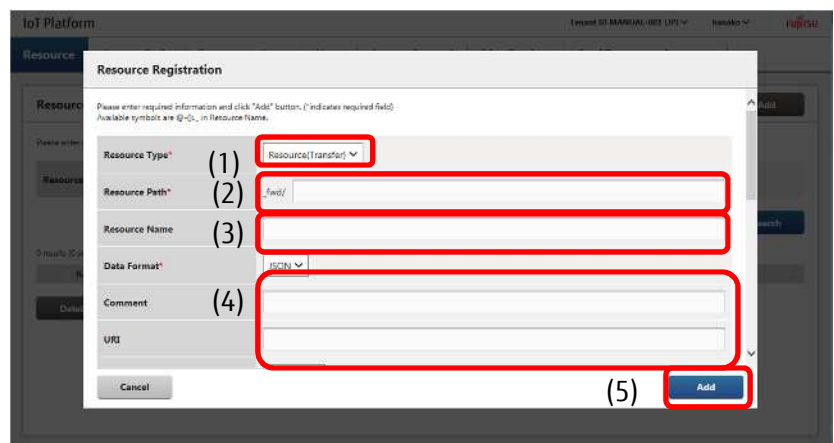
Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Resource type	Pull-down	-	Yes	-	Resource	Select from Resource and Resource (Transfer)
Resource	Text	Single-byte	Yes	Up to 128	-	Usable characters

path		alphanumeric characters				Numbers, upper and lower case alphabetical characters, - (hyphen), _ (underscore), / (slash)
Resource Name	Text	Single- and double-byte characters Alphanumeric characters Symbols	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters @ - () : . _
Data format	Pull-down	-	Yes	-	JSON	Select from JSON and Binary
Comment	Text	Optional	-	Up to 256	-	
Retention period	Text	Single-byte numerals	Yes	Up to 4	1	Unit: Days Data added will be deleted once the set retention period has elapsed.

- For data transfer resources

1. Select Resource (Transfer) from the pull-down menu shown as (1) in the figure.
2. Enter the resource path into the field shown as (2) in the figure.
3. Enter the resource name into the field shown as (3) in the figure.
4. Enter transfer destination details and set the data to be transferred into the fields shown as (4) in the figure (several fields can be completed by scrolling through the form).
5. Click (5) Add.
6. A Confirmation screen will appear after clicking Add. Click Enter shown as (6) in the figure to add the resource.



Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Resource type	Pull-down	-	Yes	-	Resource	Select from Resource and Resource (Transfer)
Resource	Text	Single-byte	Yes	Up to	-	Usable characters

path		alphanumeric characters		128 (*1)		Numbers, upper and lower case alphabetical characters, - (hyphen), _ (underscore), / (slash)
Resource Name	Text	Single- and double-byte characters Alphanumeric characters	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters @ - () : . _
Data format	Pull-down	-	Yes	-	JSON	JSON only
Comment	Text	Optional	-	Up to 256	-	
URI	Text	Single-byte alphanumeric characters	-	Up to 256	-	
Method	Pull-down	-	-	-	(NULL)	Select from (NULL)/POST/PUT/GET/DELETE/HEAD/OPTIONS/TRACE
Authentication ID	Text	Single-byte alphanumeric characters	-	Up to 20	-	
Authentication password	Text	Single-byte alphanumeric characters	-	Up to 20	-	
Header names 1 to 10	Text	Single-byte alphanumeric characters	-	Up to 20	-	
Header values 1 to 10	Text	Single-byte alphanumeric characters	-	Up to 512	-	

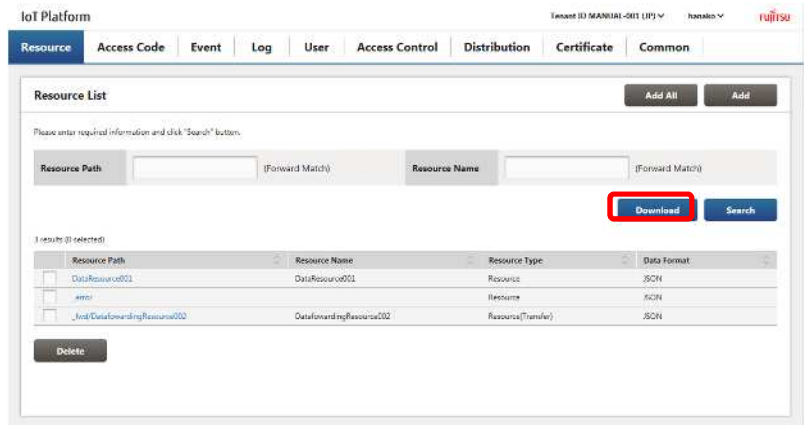
Memo

- Resources cannot be added if a resource with the same resource path is already in use within the same tenant.
- Resource paths that start with an underscore (_), or have an underscore (_) immediately after a slash (/) cannot be specified.
- _bin/ is automatically added to the start of resource paths when the resource type selected is resource, and the data format is binary.
- _fwd/ is automatically added to the start of resource paths when the resource type selected is resource (transfer).
- (*1) The maximum number of characters for resource paths is 128, including the _bin/ and _fwd/ strings at the start.
- It may take up to five minutes before you are able to access APIs using settings configured when adding or changing resources/access codes.

4.6.3 Downloading Resources

You can download information regarding resources registered to one of your tenants. This function can be used to download all resources retrieved with the Search key.

Click Download to download information regarding tenant resources.



Memo

- Clicking Download without performing a search will download all files that include any resources found within all tenants. Click something other than Resource in the Main screen, and then click Resource in the Main screen again to return to the results retrieved from the search performed.

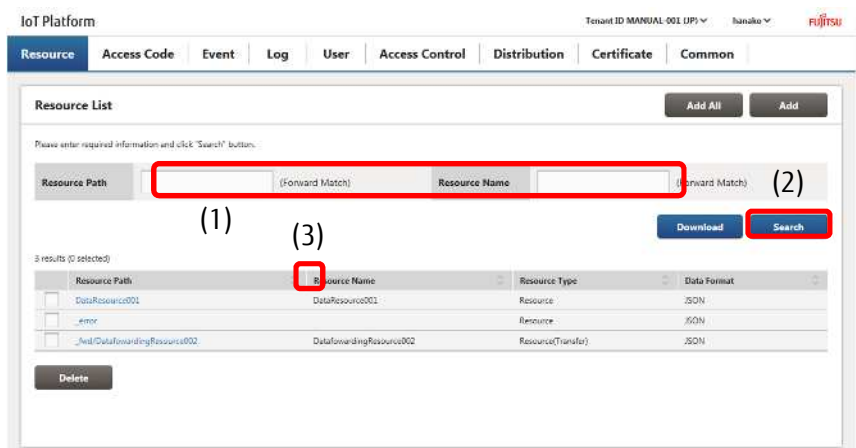
Note

- Attempting to download all resources when there are many resources registered may result in long download times. It is recommended that you use search conditions to narrow down the resources being downloaded to avoid this.

4.6.4 Searching for Resources

You can search for resources from the Resource screen. This is mainly used to modify resources or delete unnecessary resources. You can also opt to download resource information for resources matching the search conditions set only.

1. Enter the resource path or resource name that you prefer to search for as a prefix match into the area shown as (1) in the figure.
2. Click Search shown as (2) in the figure to display the search results.



- Click (3) to sort the search results. Refer to Chapter 7.2 for more information about the display order for sorting.

Memo

- Resource paths and resource names can be searched for based on prefix matches.
- Up to 100 search results can be displayed. Please be aware that only the first 100 search results will appear when performing searches that return over 100 matches.

4.6.5 Changing Resource Settings

You can change resource settings for resources that you have added.

1. Search for the resource you prefer to change from the Resource screen. Refer to Chapter 4.6.4 for more information on searching.

2. Click the resource path shown as (1) in the figure for the resource settings you prefer to change.

3. Enter the new resource name into (2) when you prefer to change the resource name.

4. Enter a new comment into (3) when you prefer to change the comment.

*You can also change other input items, as required. Refer to 4.6.2 for further details on input items.

5. Click Update shown as (4) in the figure.

6. The Resource Update/Confirm screen will appear. Check that everything is correct and click Enter.

IoT Platform

Tenant ID MANUAL-001 (JP) | harako | FUJITSU

Resource | Access Code | Event | Log | User | Access Control | Distribution | Certificate | Common

Resource List

Please enter required information and click "Search" button.

Resource Path (Forward Match) | Resource Name (Forward Match)

Download | Search

3 results (0 selected)

Resource Path	Resource Name	Resource Type	Data Format
DataResource001	DataResource001	Resource	JSON
_error		Resource	JSON
/v1/databwarding/resource002	DatabwardingResource002	Resource (transfer)	JSON

Delete

IoT Platform

Resource Update

Please enter required information and click "Update" button.
Available symbols are @, #, % in Resource Name.
Please use Access Code attached to corresponding resource in [Access Code] of MQTT Topic.

Resource Type: Resource

Resource Path: DataResource001

Resource Name (2): DataResource001

Data Format: JSON

Comment (3): Resource Data

Retention Period(1-9999 days)*: 1

REST URI: http://api.dev11.iot.jp.fujitsu.com/v1/MANUAL-001/DataResource001

MQTT Topic: <Access Code>/v1/MANUAL-001/DataResource001

Cancel | Update (4)

IoT Platform

Resource Update - Confirmation

Please click "Enter" button to update with the following contents.
Please use Access Code attached to corresponding resource in [Access Code] of MQTT Topic.

Resource Path: DataResource001

Resource Name: DataResource001

Data Format: JSON

Comment: Resource Data

Retention Period(1-9999 days): 10

REST URI: http://api.dev11.iot.jp.fujitsu.com/v1/MANUAL-001/DataResource001

MQTT Topic: <Access Code>/v1/MANUAL-001/DataResource001

Return | Enter

Note

- The resource path and data format cannot be changed.
- To change the resource path and data format, you must first delete the corresponding resource and add it again with the new path.
- The error collection resource "_error" added by the system when creating a tenant cannot be updated or deleted.

[1] Deleting a single resource

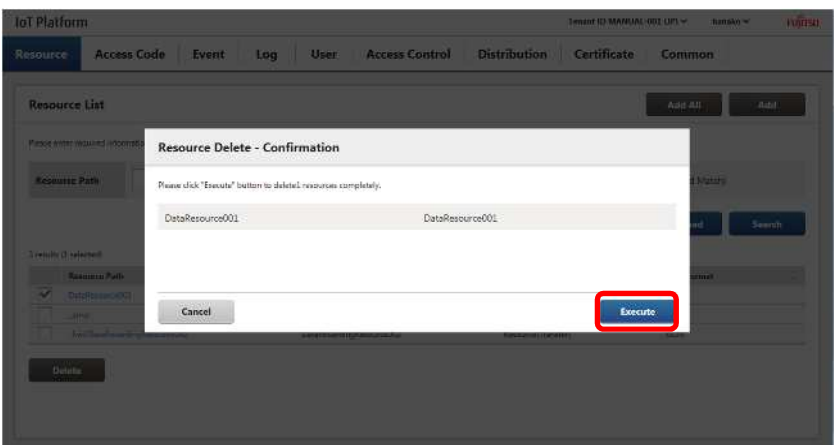
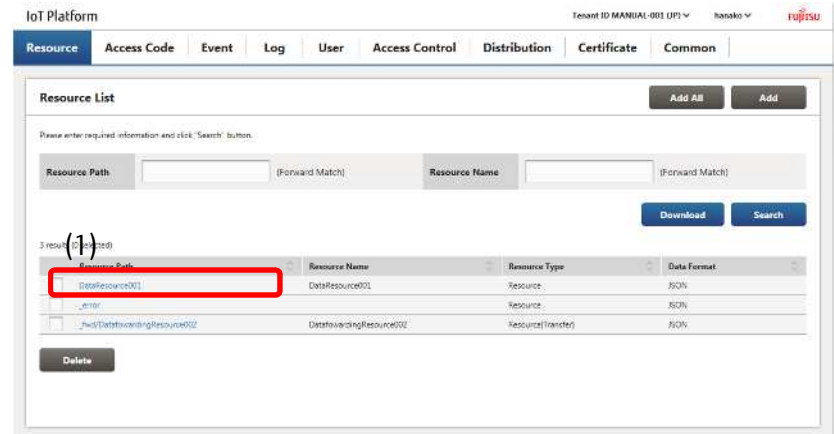
This section describes the procedure to delete a single resource. If an access code is tied to the resource you prefer to delete, you will need to delete the access code first before proceeding. Refer to Chapter 4.7.5 (5) for more details.

1. Search for the resource name you prefer to delete from the Resource screen. Refer to Chapter 4.6.4 for more information on searching.

2. Click the resource path shown as (1) in the figure for the resource name you prefer to delete.

3. Click Delete shown as (2) in the figure on the Resource Update screen.

4. Click Execute after confirming the contents of the Confirmation screen when it appears.



Memo

- You can also delete resources using the method described in Chapter 4.6.6.



Note

- Deleting resources will delete both the resource and all data written to the resource.
- Once deleted, resources and the data written to the resource cannot be recovered. Customers are responsible for using caution in checking the contents of resources being deleted before deleting them.
- The error collection resource "_error" added by the system when creating a tenant cannot be deleted. Clicking the Delete button on the "_error" Update Resource screen will not delete the resource.

4.6.6 Delete All Resources

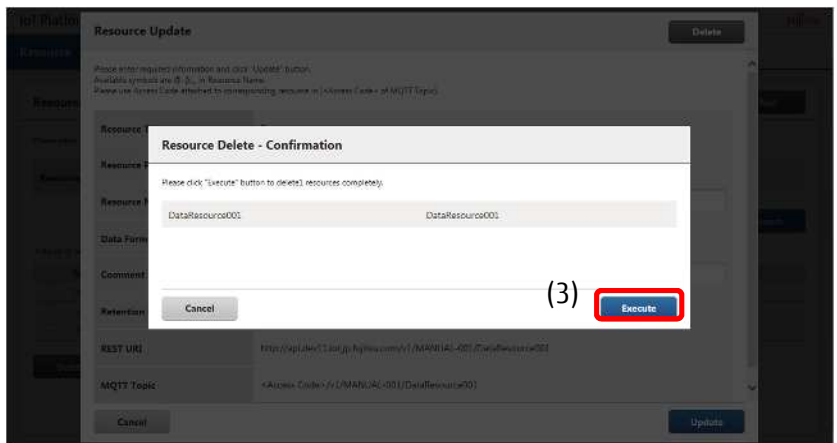
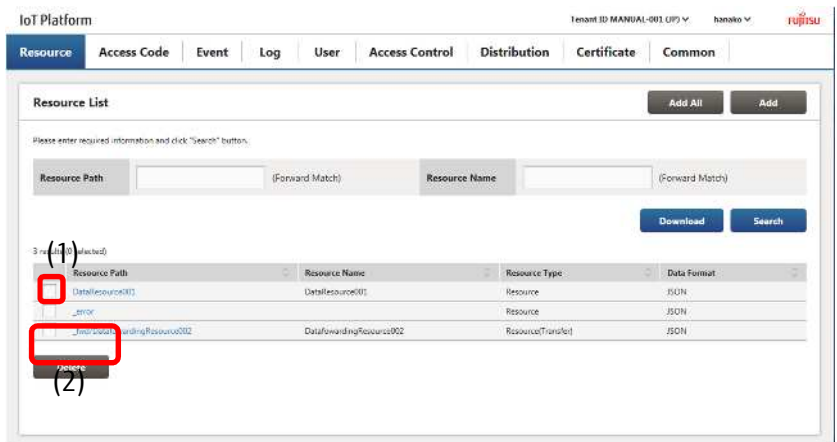
Follow the procedure below to delete multiple resources as a batch. If an access code is tied to the resource you prefer to delete, you will need to delete the access code first before proceeding. Refer to Chapter 4.7.6 for more details.

1. Search for the resource name you prefer to change from the Resource screen. Refer to Chapter 4.6.4 for more information on searching.

2. Select the check box next to the resource you prefer to delete, shown as (1) in the figure. Select multiple check boxes when you prefer to delete multiple resources.

3. Click (2) Delete.

4. Click (3) Execute after confirming the contents of the Confirmation screen when it appears.



Memo

- You can also delete resources using the method described in Chapter 4.6.5 (1).



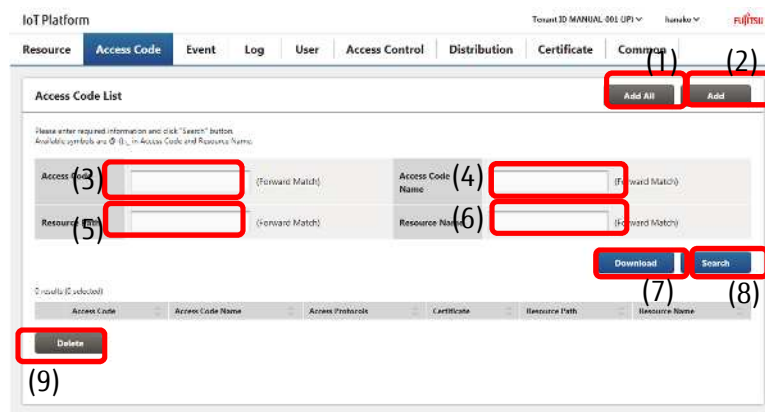
Note

- Deleting resources will delete both the resource and all data stored to the resource.
- Once deleted, resources and the data written to the resource cannot be recovered. Customers are responsible for using caution in checking the contents of resources being deleted before deleting them.
- The error collection resource "_error" added by the system when creating a tenant cannot be deleted.

Selecting the "_error" check box and attempting to delete the resource will fail to delete the "_error" resource.

4.7 Access Code Screen

Click Access Code in the Main screen to display the Access Code screen.



Number	Entry name	Description	Notes
(1)	Add all	Batch adds access codes.	Refer to Chapter 4.7.1
(2)	Add	Adds an access code.	Refer to Chapter 4.7.2
(3)	Access Code	Set when searching for access codes.	Refer to Chapter 4.7.3
(4)	Access Code Name	Set when searching for access codes.	Refer to Chapter 4.7.3
(5)	Resource path	Set when searching for access codes.	Refer to Chapter 4.7.3
(6)	Resource Name	Set when searching for access codes.	Refer to Chapter 4.7.3
(7)	Download	Downloads configured access code information.	Refer to Chapter 4.7.4
(8)	Search	Retrieves access codes.	Refer to Chapter 4.7.3
(9)	Delete	Use when deleting batches of access codes.	Refer to Chapter 4.7.6

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes (Usable characters)
	Input method	Character type				
Access Code	Text	Single-byte alphanumeric characters	-	3 to 48	-	Numbers, upper and lower case alphabetical characters Refer to 4.7.3
Access Code Name	Text	Refer to Notes	-	3 to 48	-	Numbers, upper and lower case alphabetical characters, Double-byte characters, @ - () : . _ Refer to 4.7.3
Resource path	Text	Single-byte alphanumeric characters	-	Up to 128	-	Numbers, upper and lower case alphabetical characters, - (hyphen), _ (underscore), / (slash) Refer to 4.7.3
Resource Name	Text	Refer to Notes	-	Up to 32	-	Numbers, upper and lower case alphabetical characters, Double-byte characters, @ - () : . _ Refer to 4.7.3

4.7.1 Batch Add Access Codes

You can add access codes as a batch using CSV files.

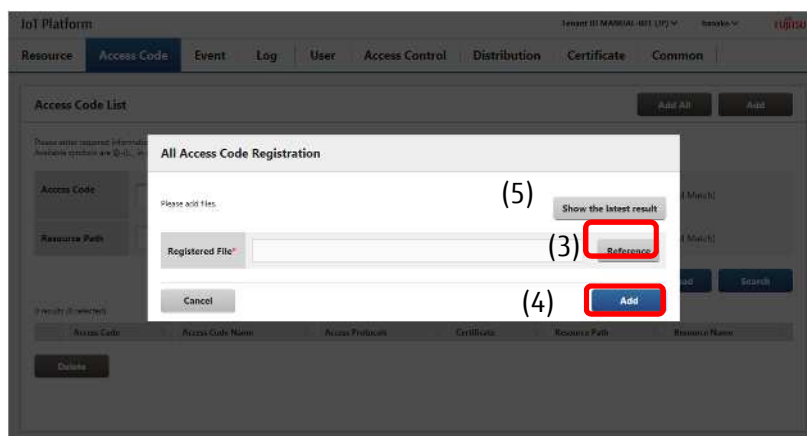
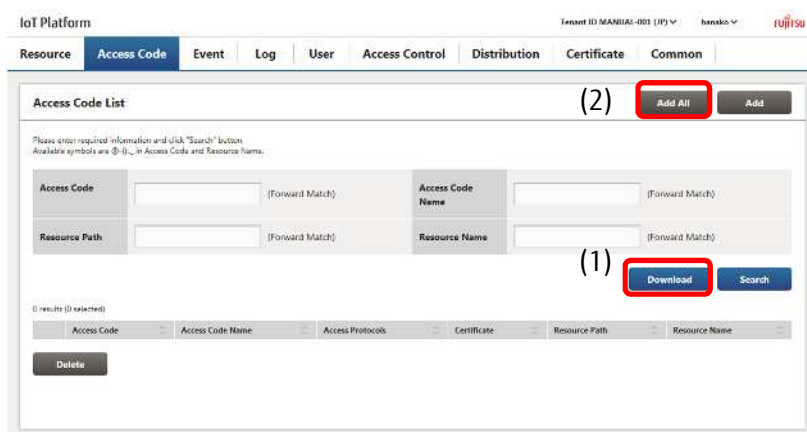
1. Click Download shown as (1) in the figure to download a CSV template to your device.

2. Edit the CSV file.

3. Click Add All shown as (2) in the figure.

4. Click Reference shown as (3) in the figure and select the edited CSV file.

5. Click (4) Add.



Memo

- The name of the downloaded file will be in access_code_YYYYMMDDHHMMSS.csv format.
- You can download the CSV template only without an access code being added by downloading the CSV template before an access code is added.
- You can also add access codes without downloading by editing a CSV file with the same formatting as the template from the PC in use.
- A maximum of 100 access codes can be added at a single operation using the Add All function. Add access codes in multiple batches when you are adding 100 or more access codes.
- Multiple resource paths can be assigned to a single access code by adding them on lines to the right as shown in the CSV Image in Chapter 7.1.2.
- Configure access codes and access code names so that they do not repeat addition completed values.
- Make sure to assign R or G access permissions for access codes set for events.
- You cannot set certificates for access codes when adding access codes as a batch.
- Refer to Chapter Chapter 17.1 for more information about the CSV format.

[1] Display previous results / Show the latest result

Click "Display Previous Results" on the All Resource Registration screen to output a log of previous downloads .

4.7.2 Adding Access Codes

The following screen will appear when you click Add on the Access Code screen described in Chapter 4.7. This menu is used when you prefer to add a single access code only.

1. Enter the access code in the field marked as (1) in the figure.

2. Enter the access code name in the field marked as (2) in the figure.

3. To specify an access protocol, select Specify in the area marked as (3) in the image, and select the check box next to the corresponding access protocol. Select Do not specify to not specify an access protocol.

4. To set a certificate, click the Browse button in the area marked as (4) in the image, and select a certificate file.

5. Select the resource that you prefer to grant the permissions that this access code gives.

5-1. Enter the resource path or the resource name as the search keyword in the field marked as (5) in the figure.

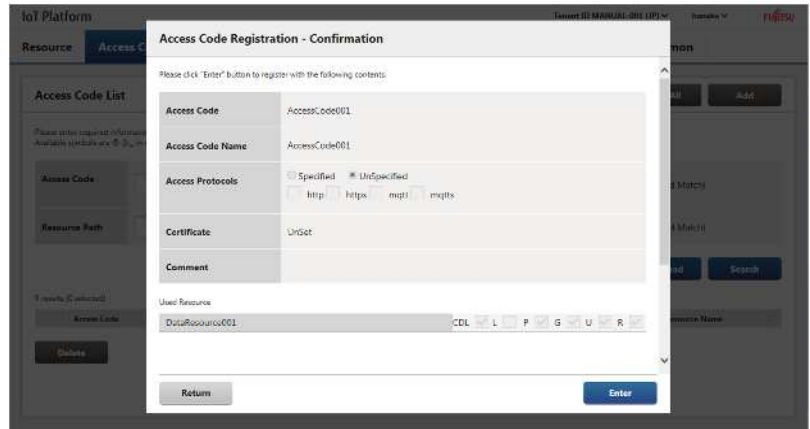
5-2. Click Search shown as (6) in the figure to display resource paths matching the search conditions at the bottom of the screen.

5-3. Select the check box for the resource you prefer to grant permissions for shown as (7) in the figure, and then click (8) for Add to add the resource to the Used Resources List at the bottom of the screen.

6. You can set permissions for registering, updating, deleting and listing (CDL) via an API, and permissions for listing (L), updating/deleting (P) all sub-resources, referencing all sub-resources (G), registering data (U), and referencing data (R) via an API.

* You can grant CDL, L, P, G, U, and R permissions for multiple resources at once by selecting the Select All check box in the Used Resources List.

9. Confirm the contents of the Add/Confirm screen when it appears, and then click Enter.



Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Access Code	Text	-	Yes	3 to 48	-	Usable characters Numbers, upper and lower case alphabetical characters
Access Code Name	Text	Single- and double-byte characters Alphanumeric characters	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters, @ - () : . _
Access protocol	Radio button	-	-	-	Do not specify	Select from Do not specify and Specify
Access protocol (types)	Check box	-	Yes	-	HTTP,HTTPS, MQTT,MQTTS	This can only be selected when Do not specify is selected for the access protocol. Multiple access protocols can be selected from HTTP, HTTPS, MQTT, MQTTS
Certificate	Text	Refer to Notes	-	-	-	All characters that can be used in a file path are available for use
Comment	Text	Optional	-	Up to 256	-	
Resource path	Text	Refer to Notes	-	Up to 128	-	Usable characters Numbers, upper and lower case alphabetical characters, - (hyphen), _ (underscore), / (slash)
Resource Name	Text	Refer to Notes	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters, @ - () : . _

Memo

- You can display the resource name by clicking the resource path in the Add screen.
- Make sure to assign R or G access permissions for access codes set for events.
- Assign CDL access permissions to add resources under a resource via an API, and to update and delete resources added via an API.
- L access permissions cannot be selected if CDL access permissions are selected.
- CDL access permissions cannot be selected if L access permissions are selected.
- Access codes cannot be added if the same access code is already in use within the scope of the same tenant ID.
- It may take up to five minutes before you are able to access APIs using settings configured when adding or changing resources/access codes.
- Access codes set for a load resource or recommend resource on the Distribution screen (Chapter 4.12) cannot be deleted if Distribution settings are enabled.
In this case, disable Distribution settings first to delete the access code.



Note

- Please specify the certification which is generated on Generate Certificate Screen.

4.7.3 Searching for Access Codes

You can search for access codes from the Access Code screen. This is mainly used to edit access codes and to delete unnecessary access codes.

1. Enter the access code or access code name, or the resource path or resource name you prefer to search for into the fields shown in (1) in the figure.

2. Click Search shown as (2) in the figure to display the search results at the bottom of the screen.

- Click (3) to sort the search results. Refer to Chapter 7.2 for more information about the display order for sorting.

Access Code	Access Code Name	Access Protocols	Certificate	Resource Path	Resource Name
<input type="checkbox"/> AccessCode001	AccessCode001	Unspecified	UnSet	DataResource001	DataResource001
<input type="checkbox"/> ForwardingAccess001	ForwardingAccess	Unspecified	UnSet	_fw01/DataforwardingResource001	DataforwardingResource001

Memo

- All search keys are compatible with prefix-match searching.
- Up to 100 search results can be displayed. Please be aware that only the first 100 search results will appear when performing searches that return over 100 matches.



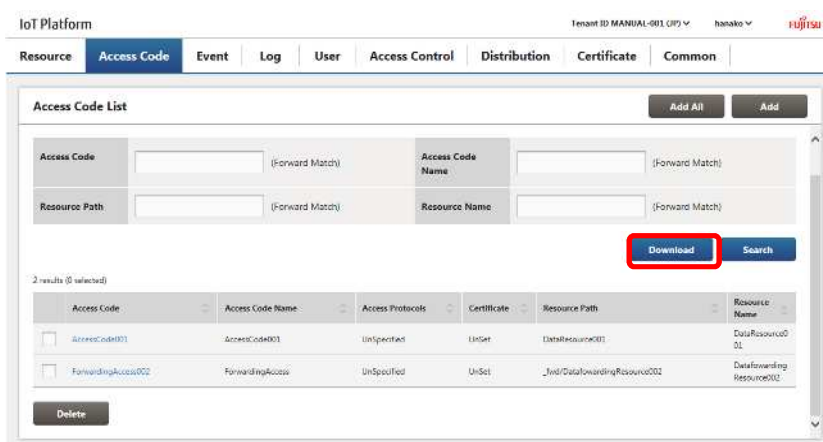
Note

- Avoid entering only an underscore (_) into the access code or access code name fields and pressing the Search button as doing so will retrieve all access codes in the search results.

4.7.4 Downloading Access Codes

You can download information regarding access codes registered to one of your tenants. This function can be used to download all resources retrieved with the Search key.

1. Perform searches using the access code searching procedure described in Chapter 4.7.3.
2. Click Download.



Memo

- Clicking Download without performing a search will download all files that include any access codes found within all tenants. Click something other than Access Code in the Main screen, and then click Access Code in the Main screen again to return to the results retrieved from the search performed.

! Note

- The certificate set for an access code cannot be downloaded when downloading access codes.

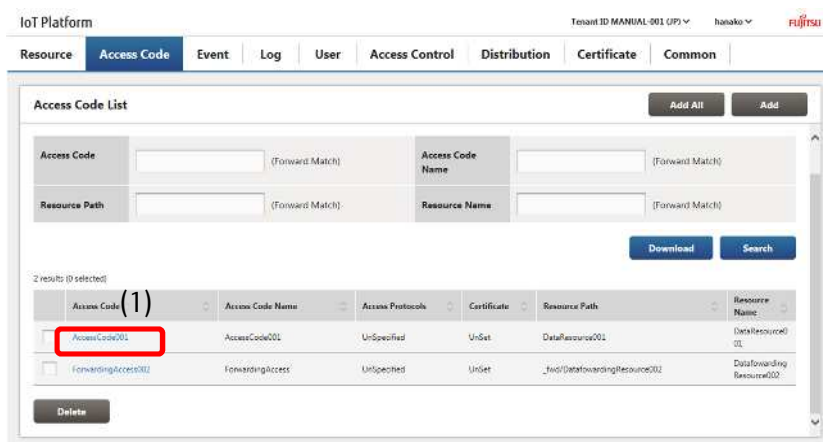
4.7.5 Changing Access Code Settings

Display the Access Code Information Update screen by clicking the link for the access code you prefer to change settings for after searching for the access code.

The access code cannot be deleted if it has been assigned to event settings. In this instance you must first delete the event settings before deleting the access code.

1. Search for the access code you prefer to change settings for from the Access Code screen. Refer to Chapter 4.7.3 for more information on searching.

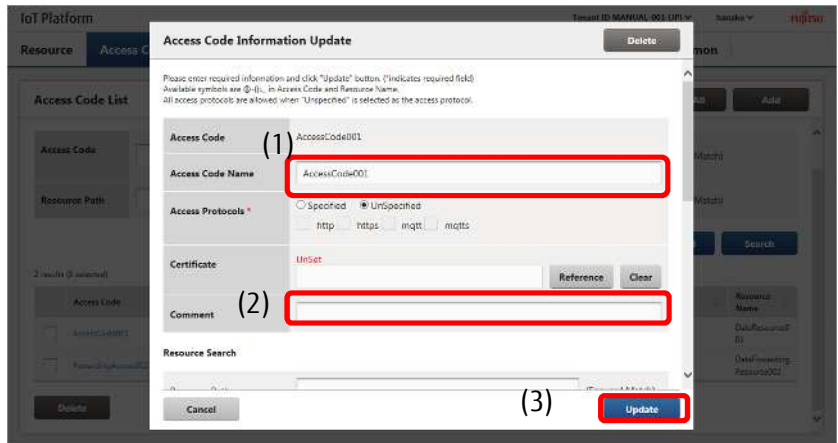
2. Click the access code you prefer to change settings for, shown as (1) in the figure, to proceed to the Access Code Information Update screen. The following provides a description of the changes and operation procedures that can be performed in the Access Code Information Update screen.



[1] Change the access code name

1. Change the access code name in the field marked as (1) in the figure. You can also change the comment in (2) if necessary.

2. Click Update shown as (3) in the figure.



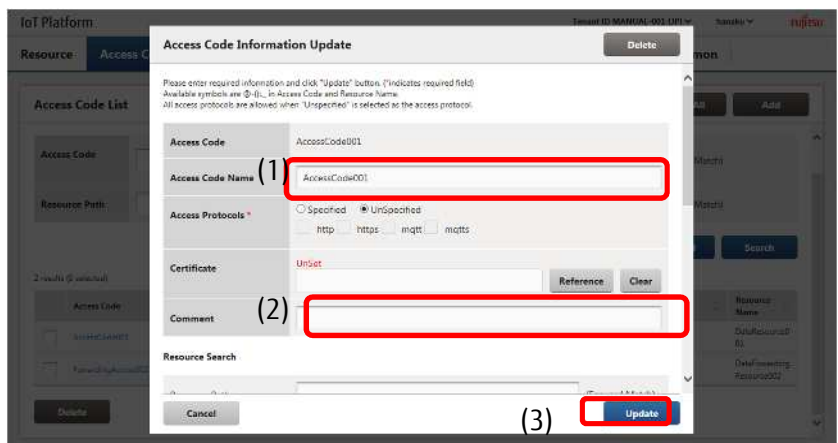
Note

- Access code values cannot be changed. To change access code values, delete the relevant access code first, and then add a new access code with the new values.

[2] Change the access protocol

1. Change the selection in the area marked as (1) in the image, or change the access protocol selected in the area marked as (2) in the image.

2. Click Update shown as (3) in the figure.

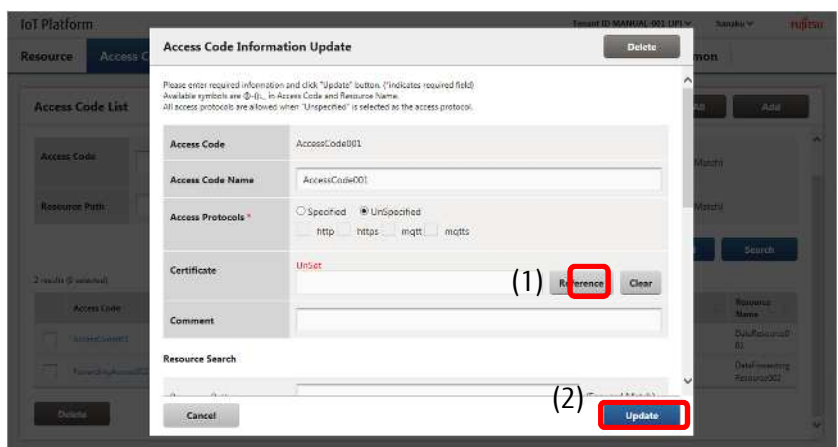


[3] Change the certificate

- If a certificate has not been set "Unset" will appear in the Certificate field.

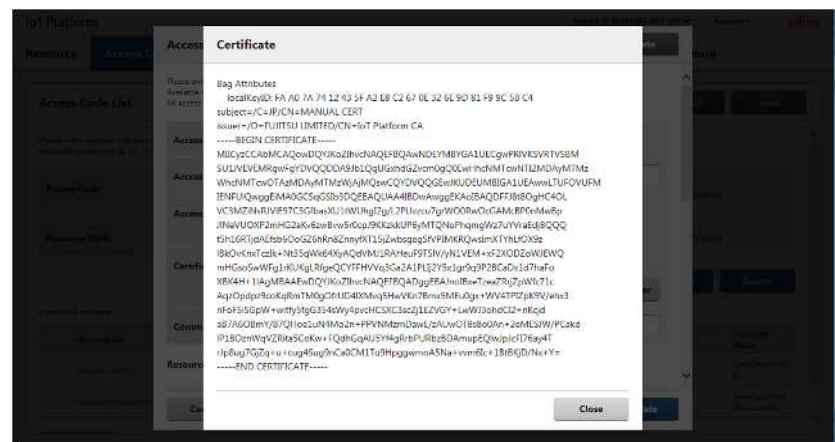
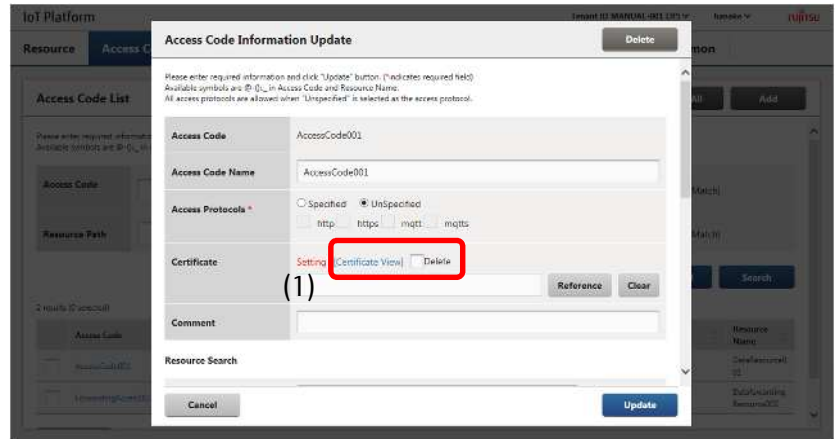
1. To set a certificate, click the Browse button in the area marked as (1) in the image, and select a certificate file.

2. Click Update shown as (2) in the figure.



- If a certificate has been set "Setting" will appear in the Certificate field. The "Reference" link and Delete check box will also appear.

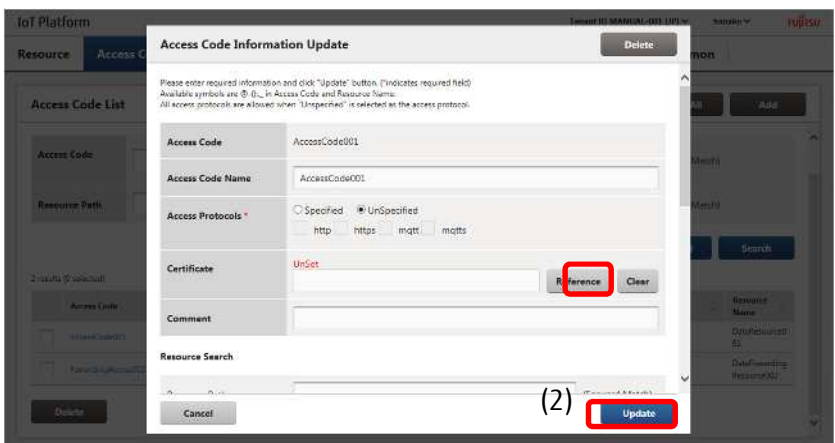
Click "Reference" (1) to display the currently set certificate.



- Changing certificates

1. To change certificates, click the Reference button in the area marked as (1) in the image, and select a certificate file.

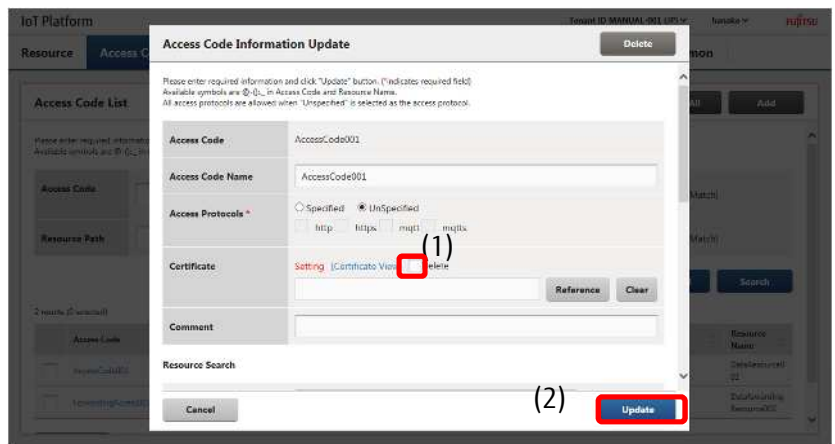
2. Click Update shown as (2) in the figure.



- Deleting certificates

1. Select the Delete check box shown as (1) in the figure to delete a certificate.

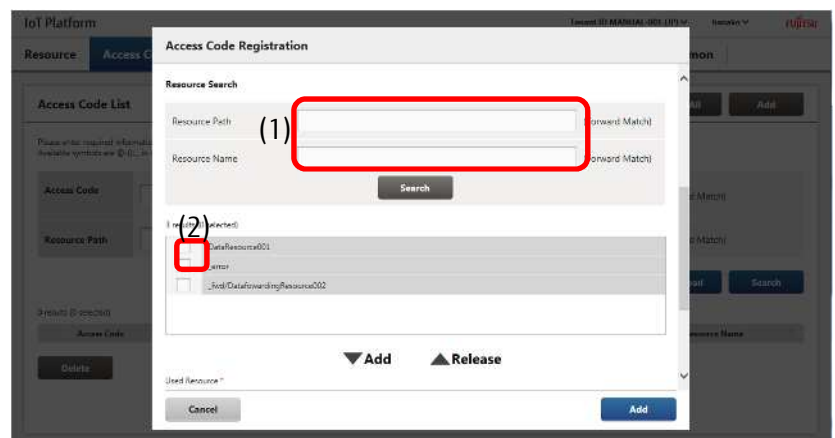
2. Click Update shown as (2) in the figure.



[4] Add resources tied to the relevant access code

1. Add resource paths/resource names as search keys in the fields provided in (1) to search for the resources you prefer to add.

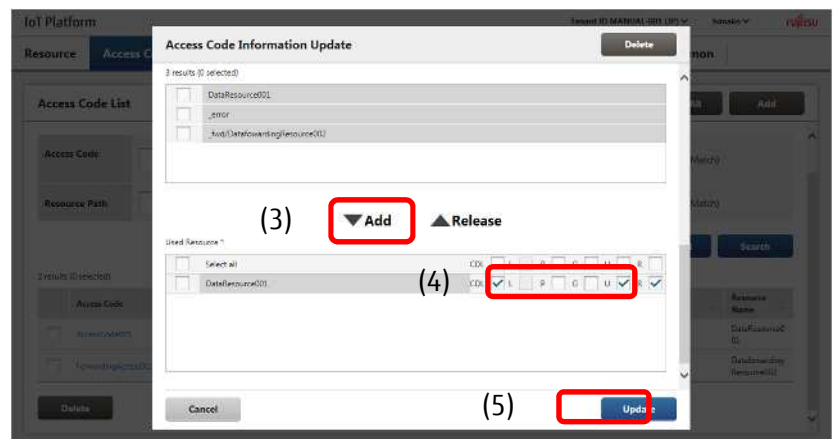
2. Resource paths that match the search keys added will appear at the bottom of the screen. Select the resources you prefer to add by selecting the check boxes shown as (2) in the figure.



3. Click (3) Add to add new resources to the Used Resource List.

4. Assign the access permissions for the resources you have added using the check boxes shown as (4) in the figure.

5. Click Update shown as (5) in the



Memo

- Search for resource paths and resource names as prefix-match searches.

⚠️ Note

Access code setting can not be changed/edited from service portal when 101 or more resources are linked to one access code. In such case, please use following method A) or B) for changing the access code setting .

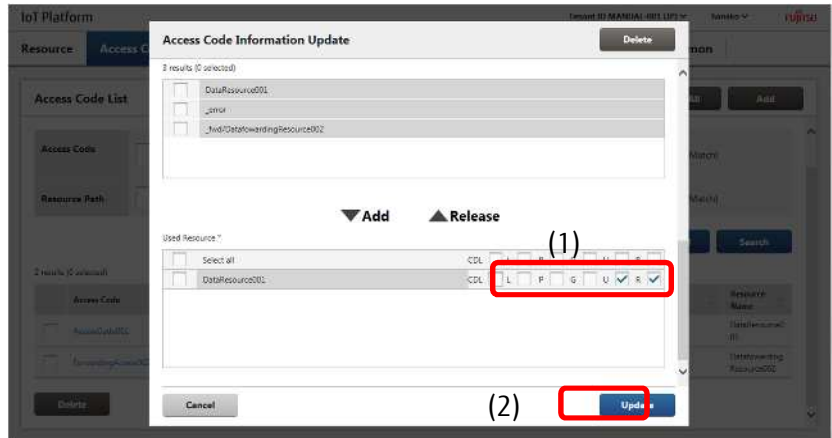
- A) Use "Controlling Access Codes (REST)" API. (Refer to "IoT Platform API Reference")
- B) Change the access code setting using following steps (Download, Edit, Delete, Upload).

1. Download Access Codes. (refer to section 4.7.4)
2. Edit the downloaded CSV file.
3. Delete the Access Code from service portal which need to be changed.(refer to section 4.7.6)
4. Batch add Access Codes by uploading the CSV file edited in step2. (refer to section 4.7.1)

[5] Changing access permissions for resources which have already been assigned an access code

1 . Select the resource you prefer to change access permissions for from the resources in use at the bottom of the screen, and then select or deselect the check boxes shown as (1) in the figure to change access permissions.

2. Click Update shown as (2) in the figure.

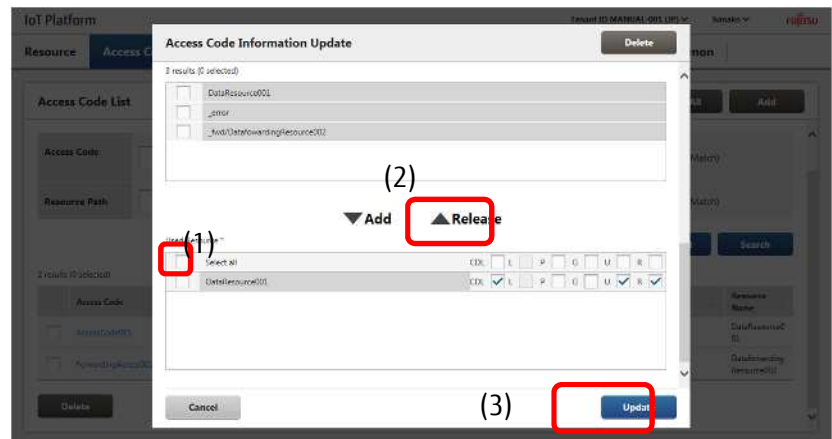


[6] Removing resources which have been assigned an access code

1 . Select the resource you prefer to remove from the Used Resource list by selecting the check box shown as (1) in the figure.

2. Click (2) for Release to delete the selected resource from the Used Resource list.

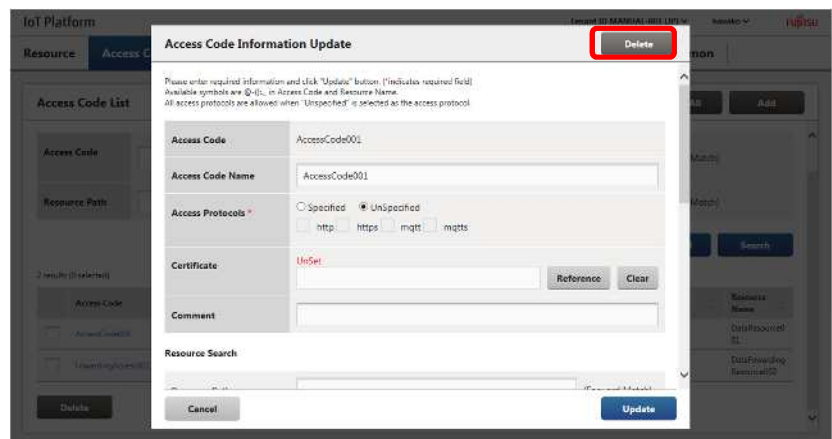
3. Click Update shown as (3) in the figure.

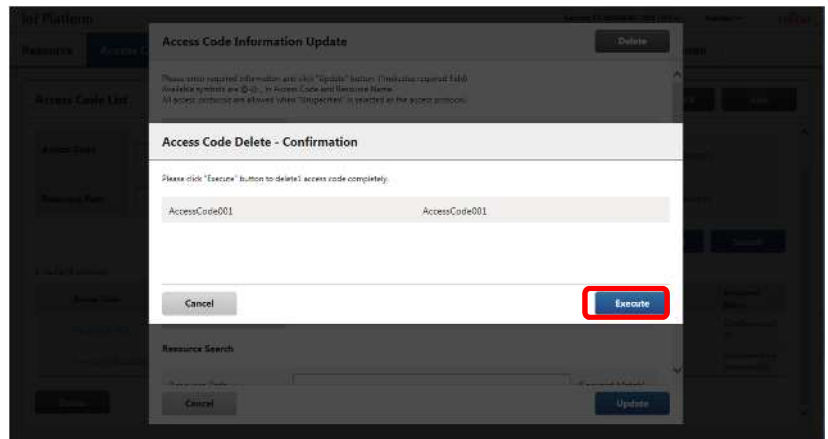


[7] Deleting access codes from the Access Code Information Update screen

1 . Click Delete.

2. The Access Code Delete - Confirmation screen will appear. Check that everything is correct and click Execute.





Note

- Once deleted, access code information cannot be recovered. Customers are responsible for using caution in checking which access code to delete before deleting them.

4.7.6 Batch Delete Access Codes

Follow the procedure below to delete multiple access codes in a batch. Access codes cannot be deleted if they have been assigned to event settings.

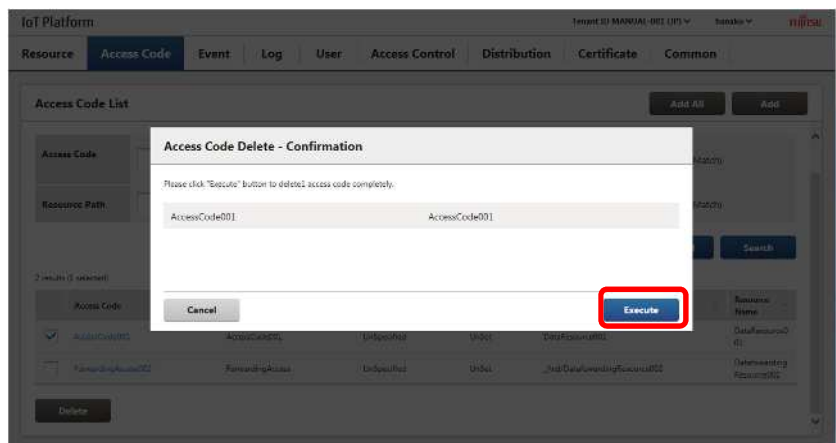
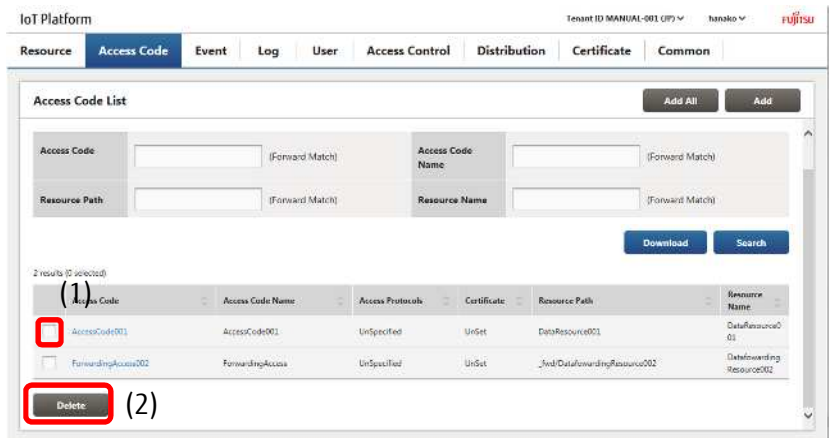
In this instance you must first delete the event settings before deleting the access code.

1. Search for the access code you prefer to delete from the Access Code screen. Refer to Chapter 4.7.3 for more information on searching.

2. Select the check box (1) next to the resource you prefer to delete. Select multiple check boxes when you prefer to delete multiple resources.

3. Click (2) Delete.

4. Click Execute after confirming the contents of the Confirmation screen when it appears.



Memo

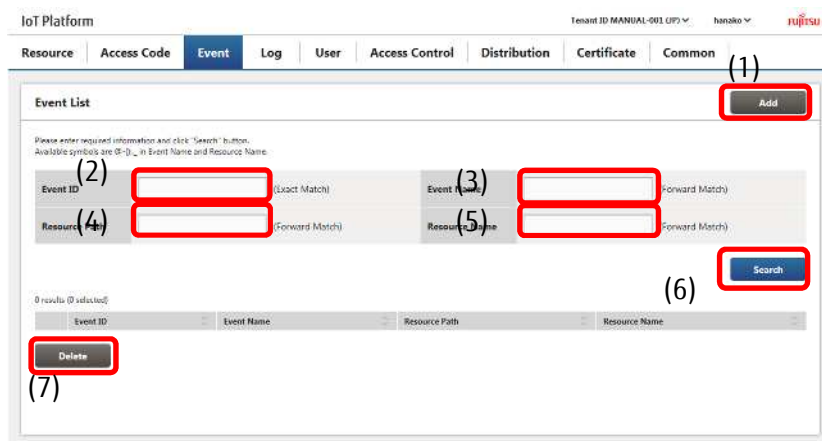
- You can also delete access codes using the method described in Chapter 4.7.5 (5).

⚠️ Note

- Access codes cannot be deleted if they are associated with a permitted IP address with the access code access control function. The association with the permitted IP address must be removed before deleting the access code.
- Deleted access code information cannot be retrieved. Customers are responsible for using caution in checking which access code to delete before performing the deletion.

4.8 Event Screen

Click Event in the Main screen to display the Event screen.

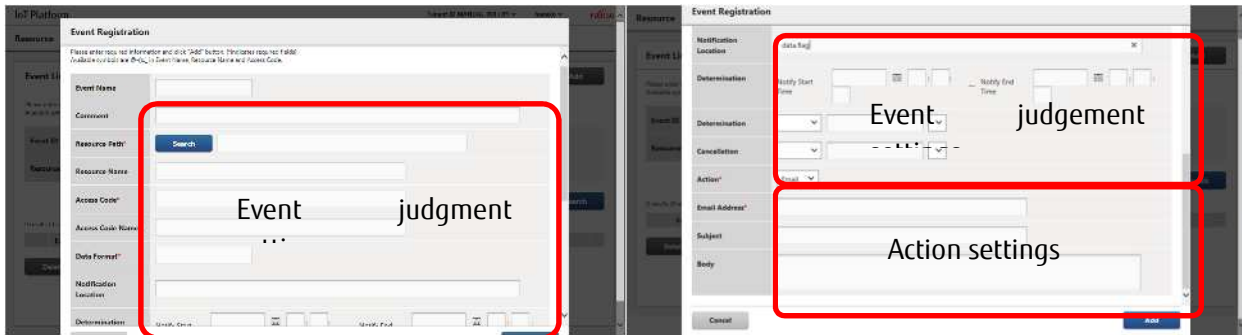


Number	Entry name	Description	Notes
(1)	Add	Adds an event.	Refer to Chapter 4.8.1
(2)	Event ID	Set when searching for events.	Refer to Chapter 4.8.3
(3)	Event name	Set when searching for events.	Refer to Chapter 4.8.3
(4)	Resource path	Set when searching for events.	Refer to Chapter 4.8.3
(5)	Resource Name	Set when searching for events.	Refer to Chapter 4.8.3
(6)	Search	Searches for events.	Refer to Chapter 4.8.3
(7)	Delete	Use when deleting batches of events.	Refer to Chapter 4.8.5

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Event ID	Text	Single-byte alphanumeric characters	-	Up to 12	-	
Event name	Text	Refer to Notes	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters @ - () : . _ Refer to 4.8.3
Resource path	Text	Single-byte alphanumeric characters	-	Up to 128	-	Usable characters Numbers, upper and lower case alphabetical characters, - (hyphen), _ (underscore), / (slash) Refer to 4.8.3
Resource Name	Text	Refer to Notes	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters @ - () : . _ Refer to 4.8.3

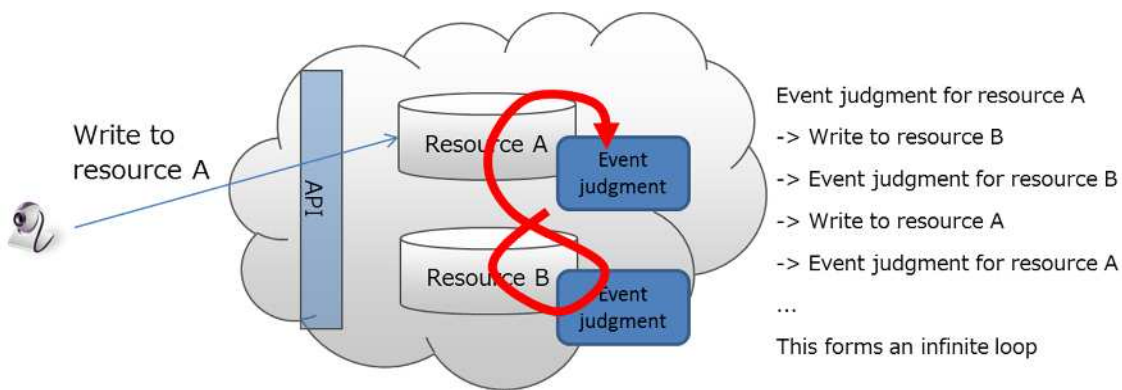
The Event Registration screen will appear when you click Add on the Event screen described in Chapter 4.8.



While this service allows both event judgment and action settings to be configured on the same screen, the process for configuring event settings and action settings is described separately in this manual.

Note

- While you will not incur event charges for adding events, you will incur charges for the number of events registered to a resource each time an API for writing data to a resource is called. Please use caution when setting events to avoid unnecessary charges.
- You may be charged with a large usage bill if event settings are configured so that actions are performed on a loop. Avoid configuring settings in the following manner.
 - Call the API to write to resource B belonging to a tenant when data is written to resource A.
 - Call the API to write to resource A belonging to a tenant when data is written to resource B.



Note

- Events cannot be set for resource (transfer) type resources.

4.8.1 Add Events (Judgement Settings)

[1] Writing data to a specific resource

This section describes the procedure to use when you prefer to set event judgment conditions to when data is written to a specific resource.

1. Enter the event name in the field shown as (1) in the figure. Enter a comment if necessary.

2. Set the resource for the target of event judgment settings.

2-1. Click Search next to the resource path shown as (2) in the figure.

2-2. Enter the resource path or the resource name as the search keyword in the field marked as (3) in the figure.

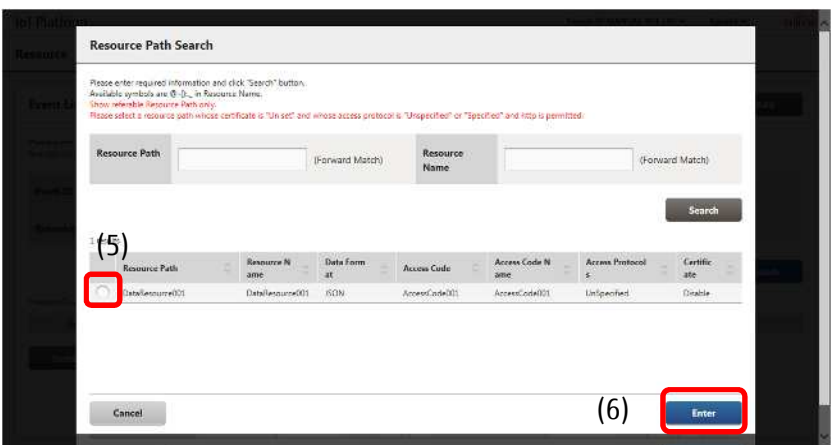
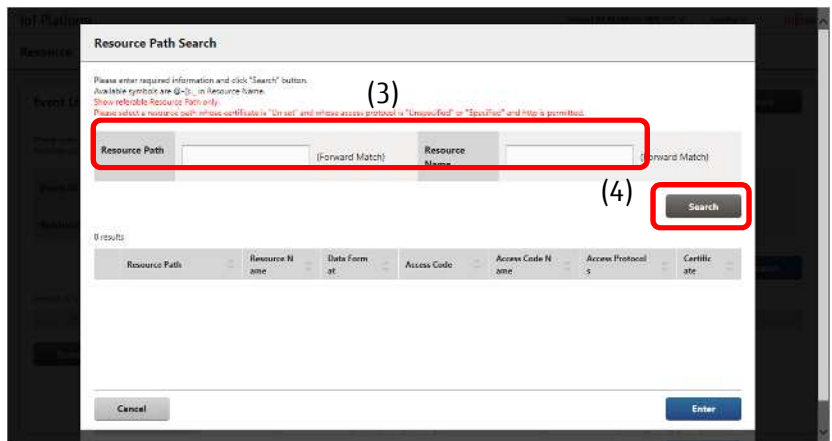
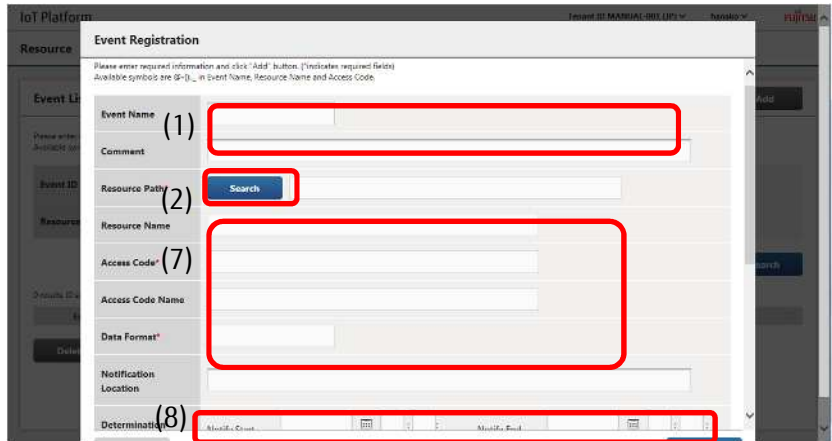
2-3. Click Search shown as (4) in the figure to display resource paths matching the search conditions, and the access codes associated with said resources, at the bottom of the screen.

2-4. Select a combination of resources for the target of event judgment settings and access codes by clicking a check box shown as (5) in the figure.

2-5. Click (6) Enter to return to the Event Registration screen and automatically fill out the fields shown as (7) in the figure.

2-6. Set the event monitoring time range, shown as (8) in the figure, if necessary.

Next, configure the action settings. Refer to Chapter 4.8.2 for more details.



Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Event name	Text	Full- and single-byte characters Alphanumeric characters	-	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters, @ - () : . _
Comment	Text	-	-	Up to 256	-	
Resource path	Text	Single-byte alphanumeric characters	Yes	Up to 128	-	Entered by searching.
Resource Name	-	-	-	-	-	Entered automatically from resource path settings.
Access Code	-	-	-	-	-	
Access code name	-	-	-	-	-	
Data format	-	-	-	-	-	
Extraction condition (time)	Text or calendar	Single-byte numerals	-	-	-	Entered in YYYY/MM/DD HH:MM:SS format

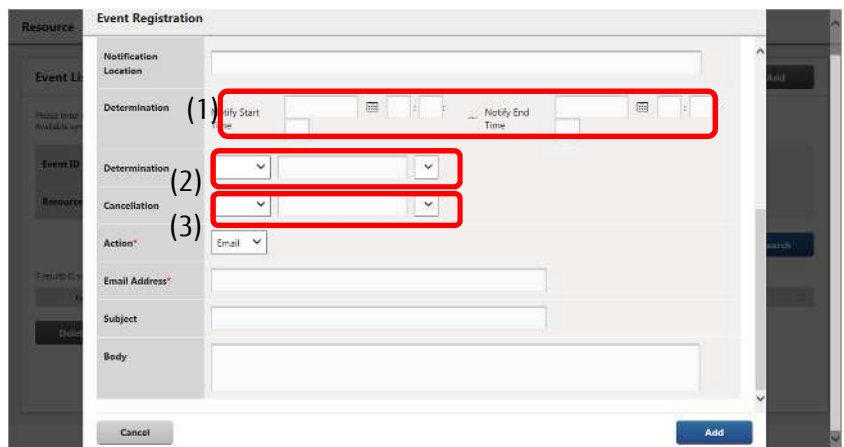
Memo

- Resources without an access code cannot be selected.
- Resources with an access code, but without an R permission, or not under the resource with a G permission, cannot be selected. If without permissions, modify the access code settings from the access code menu (Chapter 4.7.5 (3)).
- The error collection resource "_error" added by the system when creating a tenant cannot be selected.

[2] Judgments based on data content

This section describes the procedure to use when you prefer to set event judgment conditions to cases when data is written to a specific resource, combined with when data content changes to a specific status.

1. Perform the operation described in Chapter 4.8.1 (1).
2. Set the data position in the field shown as (1) in the figure. Input this in JSONPath format.
3. Set the search conditions in the field shown as (2) in the figure.
4. Set resolatory conditions in the field shown as (3) in the figure if necessary. Refer to Chapter 3.6.3 for more information about resolatory condition specifications.



Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Data path	Text	Refer to Notes	-	Up to 1902	-	Refer to Chapter 3.6.1
Extraction condition (type)	Pull-down	-	-	-	-	Selectable from a numerical value/character string
Extraction condition (value)	Text	Single-byte alphanumeric characters	-	Up to 64	-	Usable characters Numbers, upper and lower case alphabetical characters,
Extraction condition (condition)	Pull-down	-	-	-	-	If "Numerical value" is selected as the detection condition (type) Select from match/no match/or more/or less/less than/more than. If "Character string" is selected as the detection condition (type) ->Selectable from perfect match/partial match
Resolutive condition (type)	Pull-down	-	-	-	-	Selectable from a numerical value/character string
Resolutive condition (value)	Text	Single-byte alphanumeric characters	-	Up to 64	-	Usable characters Numbers, upper and lower case alphabetical characters,
Resolutive condition (condition)	Pull-down	-	-	-	-	If "Numerical value" is selected as the detection condition (type) Select from match/no match/or more/or less/less than/more than. If "Character string" is selected as the detection condition (type) ->Selectable from perfect match/partial match



Note

- Data content-based judgments are unavailable for use if the resource entered into the resource path is in a

binary data format.

- Detection condition fields and resolatory condition fields cannot be entered if the resource entered into the resource path is in a binary data format.
- If the resource path field is changed to a resource path with a binary data resource, any content input into detection condition fields and resolatory condition fields will be deleted.

4.8.2 Add Events (Action Settings)

The settings described in this chapter are provided as an extension from the Add Event (Judgment Settings) described in Chapter 4.8.1.

[1] Email settings

1 . Select the action contents shown as (1) in the figure.

Select Email.

2. Set the email address to send emails to in the field shown as (2) in the figure.

3. Set the subject line in the field shown as (3) in the figure.

4. Set the text of the email in the field shown as (4) in the figure.

5. Click Add to finish configuring Add Event settings.

Input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Action	Pull-down	-	Yes	-	-	Selectable from Email/Call API
Email address	Text	Single-byte alphanumeric characters	Yes	Up to 254	-	E-mail address format
Subject	Text	Optional	-	Up to 256	-	
Body	Text	Optional	-	Up to 140	-	When left empty, this service will automatically insert an "Event Occurs" message when sending emails.

A notification message will be sent as an attachment to the email address specified. Refer to Chapter 7.3 for more information about the contents of the notification message.

[2] API caller settings

1 . Select the action contents shown as (1) in the figure.

Select the API caller here.

2. Set the calling destination URI in the field shown as (2) in the figure.

3. Set the HTTP method in (3).

4. Set the authentication ID and password in the fields shown as (4) in the figure if the calling destination is compatible with Basic Authentication.

5. Set the HTTP headers and header values if necessary in the fields shown as (5) in the figure. (Up to ten variations acceptable.)

6. Set the HTTP body value if necessary in the field shown as (6) in the figure.

7. Click Add to finish configuring Add Event settings.

Input parameters

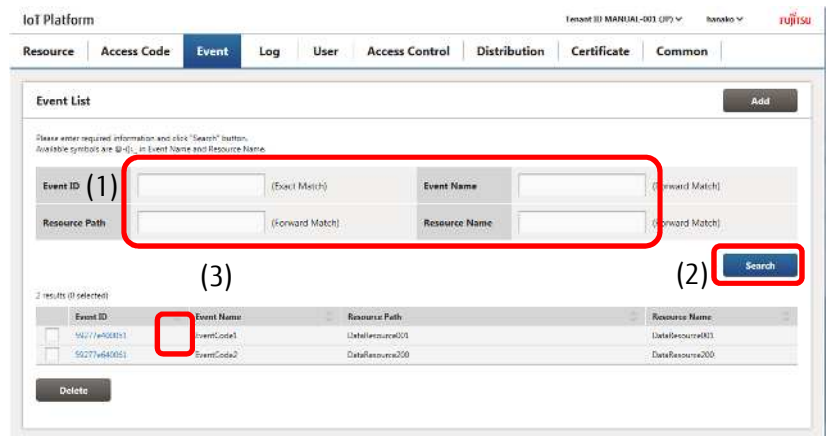
Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
URI	Text	Single-byte alphanumeric characters	Yes	Up to 256	-	-
Method	Pull-down	-	Yes	-	-	Selectable from GET/POST/PUT/DELETE/HEAD/OPTIONS/TRACE
Authentication ID Authentication password	Text	Single-byte alphanumeric characters	-	Up to 20	-	
Field name Field value	Text	Single-byte alphanumeric characters	-	Up to 20 Up to 512	-	

Body	Text	Single-byte alphanumeric characters	-	Up to 1024	-	This service will automatically apply a notification message (refer to Chapter 7.3) if nothing is set for the body. A notification message will not be applied if a value is set.
------	------	-------------------------------------	---	------------	---	---

4.8.3 Searching for Events

This section describes the process of searching for events to change event settings and display a list of events.

1. Enter the search keys into the fields shown as (1) in the Event screen, and then click (2) Search to display the search results at the bottom of the screen.



- Click (3) to sort the search results.

Refer to Chapter 7.2 for more information about the display order for sorting.



Note

- Avoid entering only an underscore (_) into the event name, resource path or resource name fields and then pressing the Search button, as doing so will retrieve all events in the search results.

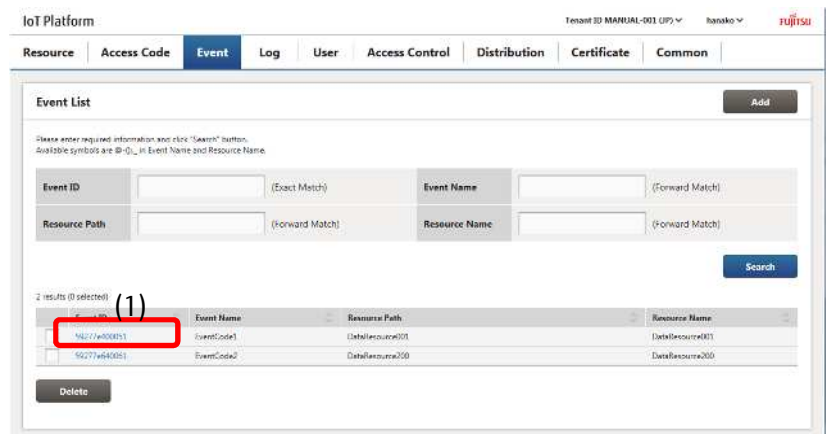
4.8.4 Changing Event Settings

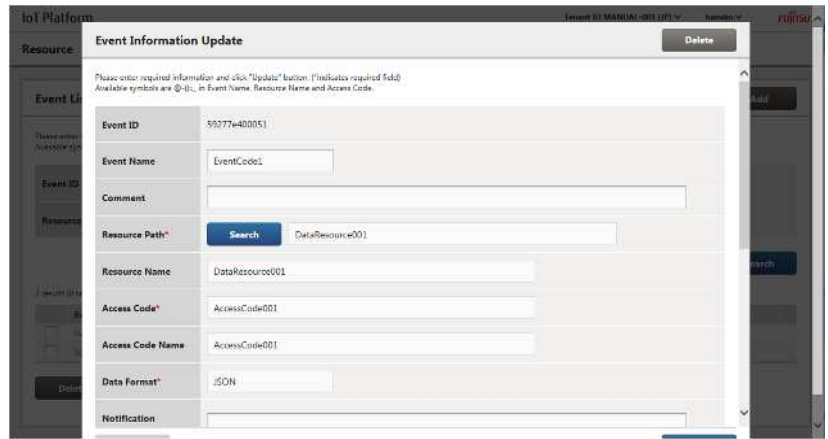
1. Display the event that you prefer to reconfigure using the Search Events function described in Chapter 4.8.3.

2. Click the event ID (1) of the event you prefer to change.

3. When the Event Information Update screen appears, select the settings you prefer to modify.

*Refer to Chapter 4.8.1 and 4.8.2 for more information about parameter settings.





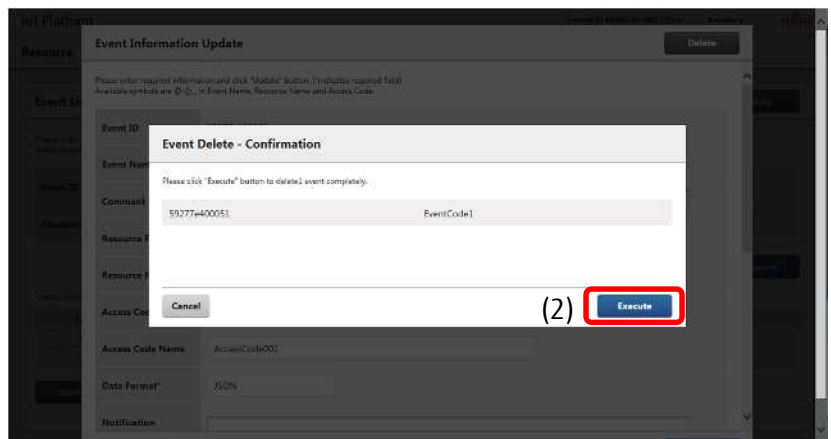
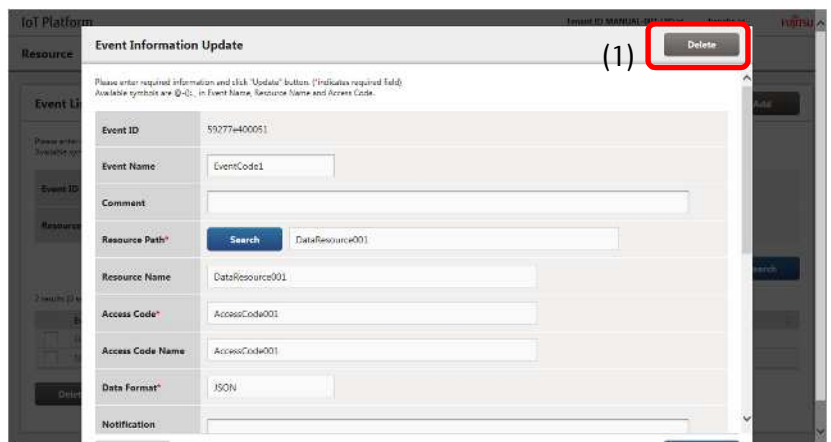
[1] Deleting events

1. Display the event that you prefer to delete using the Search Events function described in Chapter 4.8.3.

2. Click the event ID of the event you prefer to delete.

3. When the Event Information Update screen appears, click (1) for Delete.

4. Click OK (2) after confirming the contents of the Confirmation screen when it appears.



- Once deleted, event information cannot be recovered. Customers are responsible for using caution in checking which event to delete before deleting them.

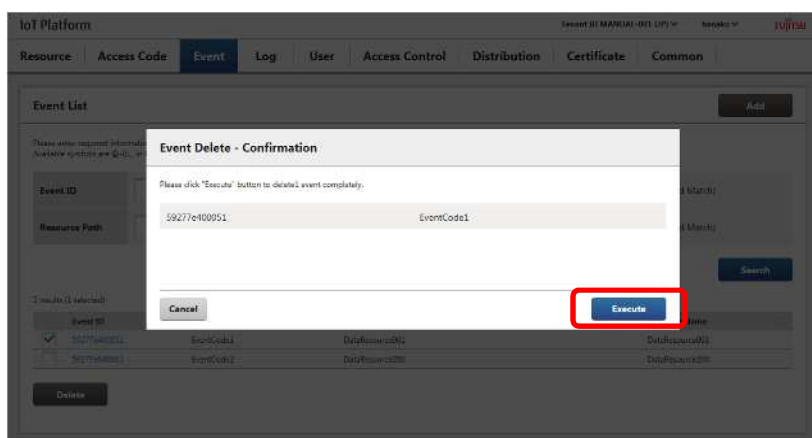
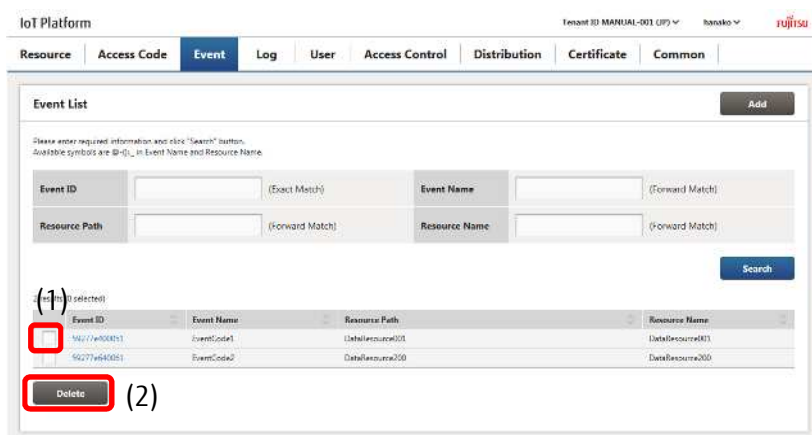
4.8.5 Batch Deleting Events

1. Display the event that you prefer to delete using the Search Events function described in Chapter 4.8.3.

2. Select the check box (1) to the left of the event you prefer to delete. Select multiple check boxes to delete multiple events at once.

3. Click (2) for Delete.

4. Click Execute after confirming the contents of the confirm deletion screen when it appears.



Note

- Once deleted, event information cannot be recovered. Customers are responsible for using caution in checking which event to delete before deleting them.

4.9 Log Screen

Click Log in the Main screen to display the Log screen.

The Log screen consists of four screens, Usage, Operation Log, Usage Log, and System Log.

4.9.1 Usage Screen

[1] Download monthly usage amounts

Downloads a usage amount log for the month specified. Downloads results up to previous three months.

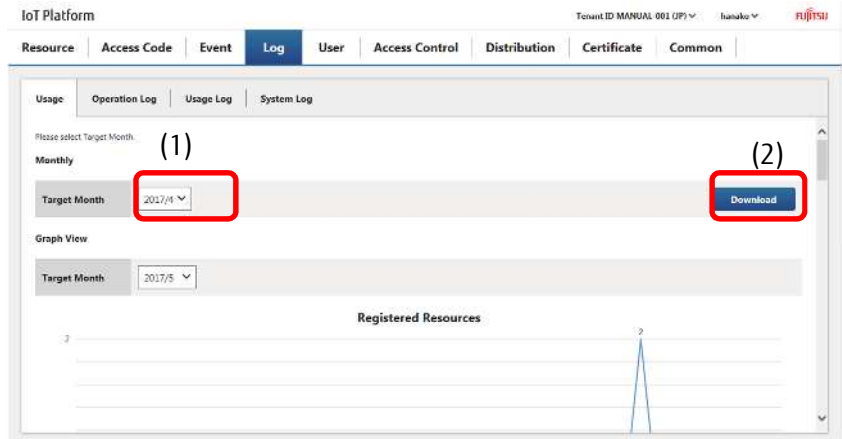
The content shown in a monthly usage amount log is as follows.

- Number of resources (history of resources registered by day)
- Amount of disk use (in MB) (history of disk space used by day)
- Amount of Normal API use (cumulative one month total)
- Amount of Light API use (cumulative one month total)
- Amount of API Bulk use (cumulative one month total)
- Amount of Normal SSL use (cumulative one month total)
- Amount of Light SSL use (cumulative one month total)

- Amount of SSL Bulk use (cumulative one month total)
- Amount of Event use (cumulative total for the month)
- Communication volume (cumulative total for the month)

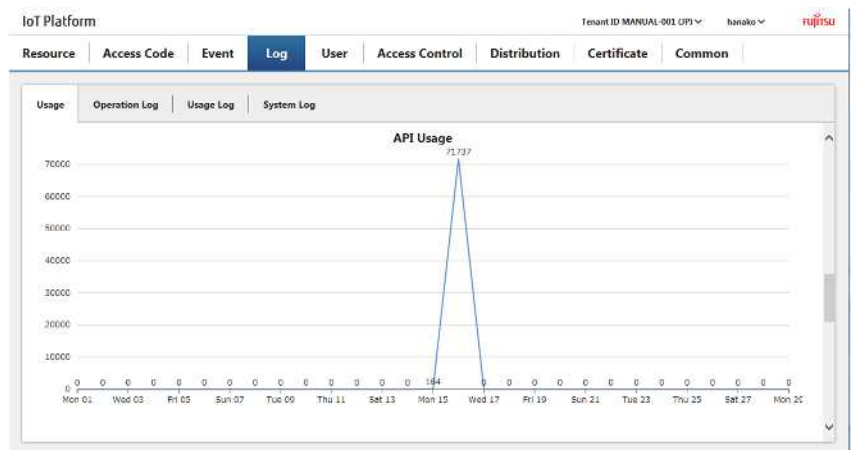
1. Specify the usage amount month you prefer to download in the field shown as (1) in the figure in the Usage Amount screen. You can either directly input this date, or click the calendar icon to select it.

2. Click (2) to specify the folder to save to on the device in use and save.



[2] Display graphs

Display graphs tracking usage amounts by day for the specified month. Results for the past year can be displayed. The following is displayed on the graphs.



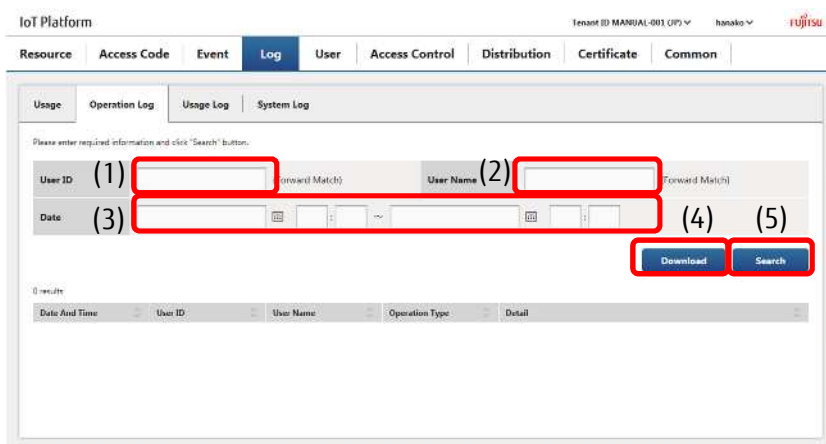
- Number of resources
- Amount of disk use
- Amount of API use
- Amount of SSL use
- Amount of Event use
- Communication volume

Memo

- The API usage amount displays the total number of uses for Normal API, Light API and API Bulk use.
- The SSL usage amount displays the total number of uses for Normal SSL, Light SSL and SSL Bulk use.

4.9.2 Operation Log Screen

Click the Operation Log tab in the Log screen to display the Operational Log screen. The operation log refers to an operational history of all user operations, covering all access to the Service Portal for tenants under customer management, and all Service Portal operations. These logs can be used to check a history of operations for errors pertaining to resource, access code, event or other settings.



Number	Entry name	Description	Notes
(1)	User ID	Set when searching for operational logs.	Refer to [2]
(2)	User name	Set when searching for operational logs.	Refer to [2]
(3)	Date	Set when searching for operational logs.	Refer to [2]
(4)	Download	Downloads the operational log.	Refer to [1] and [3]
(5)	Search	Searches for operational logs.	Refer to [2]

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
User ID	Text	-	-	Up to 256	-	
User name	Text	-	-	Up to 32	-	
Date	Text/calendar	-	-	-	-	Usable characters: Numerical values

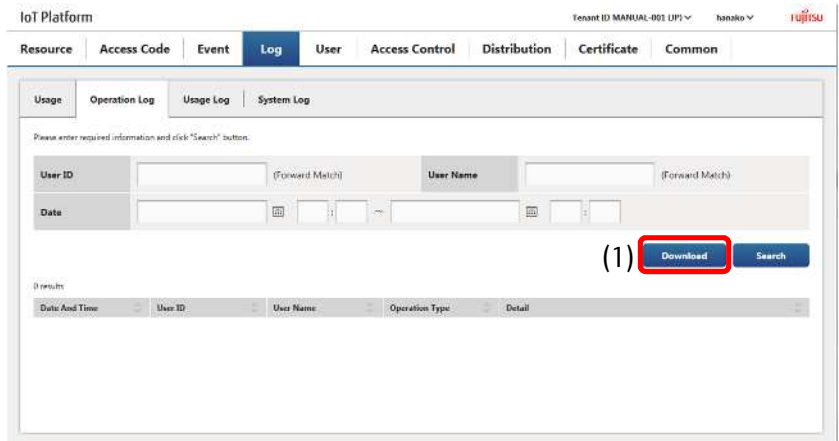
Memo

- Search results are output in Coordinated Universal Time (UTC). The format used is YYYY/MM/DD HH:MM+00.

[1] Batch download operational logs

1. Click (1) without performing a search from the main Operation Log screen.

2. Specify the folder to save to on the device in use and save.



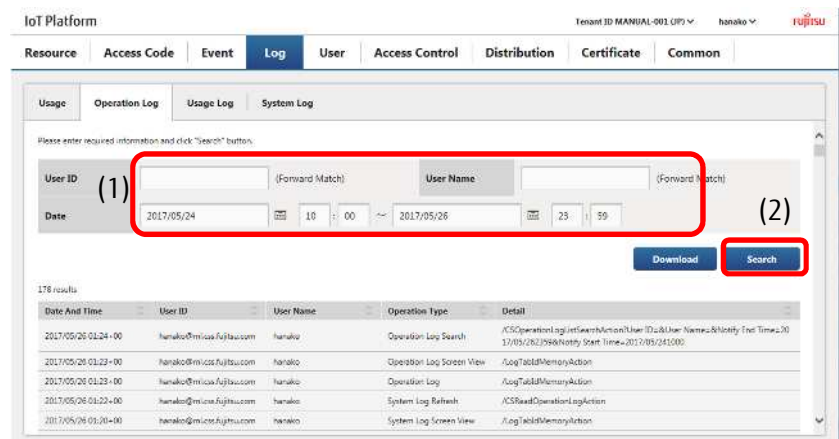
Memo

- Up to 92 days of operational logs for all users within a tenant can be downloaded.
- Clicking Download without performing a search will download all files including any operational logs found within all tenants. Click any parts other than Log in the Main screen, and then click Log in the Main screen again to return to the results retrieved from the search performed.

[2] Searching for operational logs

1. Enter the user ID, user name, or the date that you prefer to search for in the fields provided in (1) on the main Operation Log screen. Enter the user ID or user name as prefix searches.

2. Click (2) for Search to display the search results.



- Clicking Search without setting any of the fields shown as (1) in the figure will display the operation logs of all relevant users for up to 92 days.

Memo

- If over 1,000 search results are returned, only the first 1,000 results will be displayed.

! Note

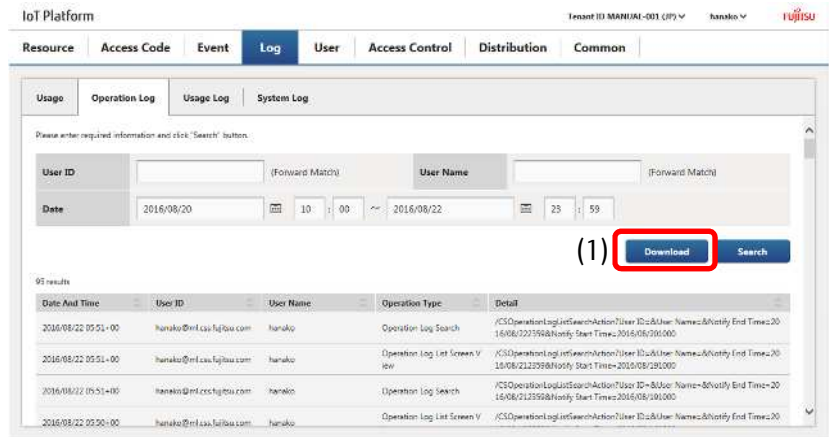
- Avoid entering only an underscore (_) into the user ID or user name fields and then pressing the Search button, as doing so will retrieve all logs in the search results.

[3] Downloading from operational log searches

You can download a file containing only the search results displayed by selecting Download from an operational log search result screen.

1. Click (1), having performed a search from the main Operational Log screen.

2. Specify the folder to save to on the device in use and save.



4.9.3 Usage Log Screen

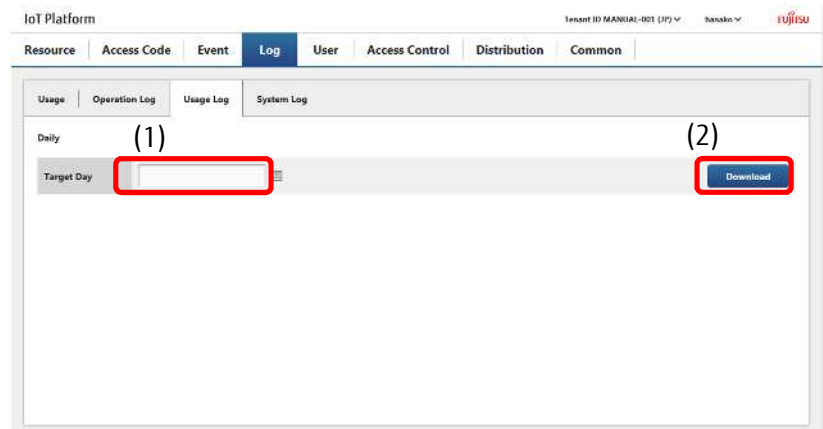
Click the Usage Log tab in the Log screen to display the Usage Log screen. You can download usage amount logs recorded by day as of the date specified. You can download logs by day up to previous 92 days.

The content shown in a usage amount log is as follows.

- Number of resources
- Amount of disk use (in MB)
- Amount of Normal API use (in no. of times used)
- Amount of Light API use (in no. of times used)
- Amount of API Bulk use (in no. of times used)
- Amount of Normal SSL use (in no. of times used)
- Amount of Light SSL use (in no. of times used)
- Amount of SSL Bulk use (in no. of times used)
- Amount of event use (in no. of times used)
- Communication volume (in MB)
- Use trace logs

1. Specify the date for the log you prefer to download in the field shown as (1) in the figure in the main Usage Log screen. You can either directly input this date, or click the calendar icon to select it.

2. Click (2) to specify the folder to save to on the device in use and save.



[1] Using the Usage Log screen

This section describes the Usage Log format and how to reference information concerning charges from the Usage Log.

1. Log format

The Usage Log outputs one line for each use, namely API or event use. Each of the following items is output on each line, separated by single-byte spaces.

Entry name	Description	Notes
Timestamp	Outputs the timestamp the log was output in RFC3339 format. API use: Timestamp of the API use request Event use: Timestamp of event judgment	Output example: 2016-02-01T11:52:08.586808+09:00
Tenant ID	Outputs the ID of the tenant used.	
Destination	Outputs the source IP address sending the API request.	
Use code	Outputs the code used for access.	For API use: Access code For event use: Tenant ID
Message	Outputs a user-defined message for each log.	

2. Confirming charge-related information

- API usage amount

You can count the number of API uses within a period output to a log by extracting uses with a transmission type of 1 (denoting API use) from the Usage Log and counting the number of lines. You can also reference the SSL use code for the extracted log to determine whether SSL is used for each API use.



Note

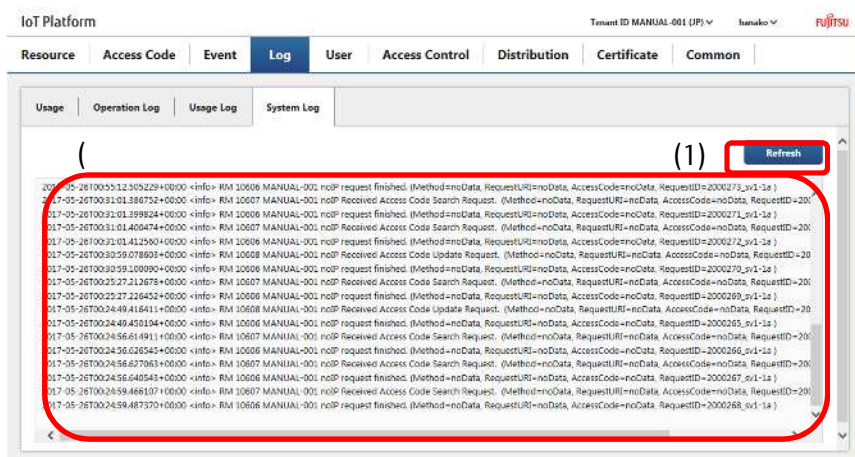
- The Usage Log is intended for customers to check API usage amounts to confirm the grounds for fees charged. Other log details irrelevant to the above shall not be disclosed.

4.9.4 System Log Screen

Click the System Log tab in the Log screen to display the System Log screen.

Refer to the System Log to confirm error details when internal service processing errors occur for processes that are performed by tenants under the customer 's control that are approved (2,000K received).

- Execution of event actions (Email, API)
- Transferring resources
- MQTT requests

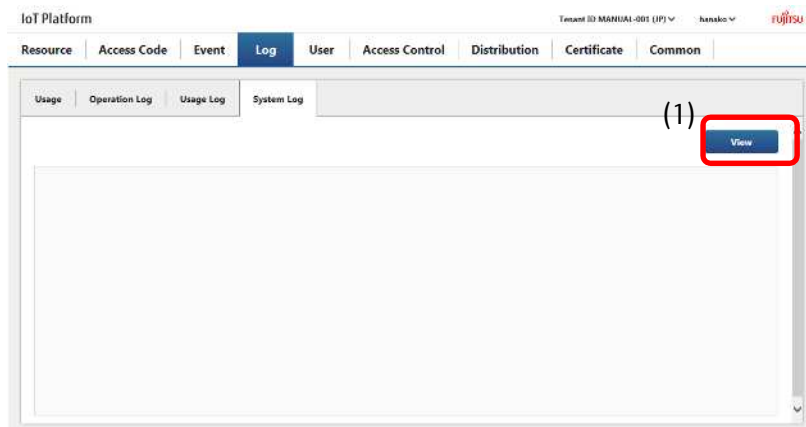


Number	Entry name	Description	Notes
(1)	View/refresh	View/refresh the System Log.	View is for the initial System Log screen display.
(2)	System Log display area	Display the System Log.	An empty border will be shown for the initial System Log screen

		display.
--	--	----------

[1] View/refresh the System Log.

1 . Display the System Log screen and click (1) View. The System Log will appear.



*The scroll bar for the System Log display area will move to the bottom when the System Log is displayed. The View button will also change to the Refresh button.

2. Click Refresh once the System Log is displayed to show the most recent log information.

Memo

- It may take several moments to display the System Log when it contains many line entries.
- If the System Log has over 5,000 entries, only the first 5,000 entries will be displayed.

[2] Using the System Log

This section describes the System Log format and how to reference various information from the System Log.

- System Log format

One line is output in the System Log for each event action or other process performed. Each of the following items is output on each line, separated by single-byte spaces.

Entry name	Description	Notes
Timestamp	Outputs the timestamp the log was output in RFC3339 format.	Output example: 2016-02-01T11:52:08.586808+09:00
Log level	Outputs the log level.	Displays one of the following. <emerg>,<err>,<warning>,<info> Refer to log level details for more details.
Component abbreviations	Outputs component names for the log output origin in two-character abbreviated format.	AO: Authorized DM: Data management EJ: Event judgment ET: Event transmission IP: IP filter MP: MQTT parser MX: MQTT-Proxy PP: Pre-process FW RM: REST parser (management) RT: Transfer resource judgment SV: Service Portal RD: REST parser (data)

		TS: Transfer resource transmission
Message ID for basic functions	Outputs unique five digit decimal messages.	
Tenant ID	Outputs the tenant ID for the tenant executing the process.	The following may be output as special tenant IDs. - Tenant IDs with an asterisk (*) at the end This shows processes performed while the authorization process has not been performed. Tenant IDs specified in API requests and other requests will be output. - iotpf This shows processes not initiated by the user, such as process initialization processes.
Sender IP	Outputs the IP address of the API publisher.	The following may be output as special sender IPs. - noIP Processes not initiated by the user, such as process initialization processes.
Message content	Outputs a user-defined message for each log.	

Log level details

Log level	Content	Notes
warning	- Warning Warning is output when a process has only completed in part due to an error occurring during the requested process.	
info	- Information Shows application actions.	

(1) Confirming a log of event actions performed (API) from the System Log

Process

1. Search for the resource path accessed from the System Log detailing events close to the time when the resource was accessed.
2. Search for the component abbreviation "ET" representing event actions performed from the search results returned in step 1.
3. When the API is successfully called, "Success to send transmissionData" will appear in the <info> log level.
Starting with this, information on the calling destination URL and related resource paths, etc. will also appear.
*When calling the API fails, "Failed to send transmissionData" will appear in the <warning> log level.
4. The request ID (ReqID) is output to the above-mentioned log, allowing you to search the System Log with this ID to retrieve a series of log information detailing processes from when a resource is accessed, to when an executed process completes.

Log example:

```
2016-02-23T10:52:33.428322+09:00 <info> ET 10506 SMPAPL-001 Success to send Transmission Data to
http://sampleapp1.iot.jp.fujitsu.com/WebApl/AccessServlet. (ReqID=93942, ResourcePath=test,
AccCode=) (ReqId=93942, ResourcePath=test, AccessCode=)(EventTransmissionForHttp.java:164)
2016-02-23T10:52:33.429069+09:00 <info> ET 10502 SMPAPL-001 Success to transmit event(http).
Event Trigger Info(56cbb9f70011, test, create). Event Operational
Info(http://sampleapp1.iot.jp.fujitsu.com/WebApl/AccessServlet, POST) (ReqId=93942,
ResourcePath=test, AccessCode=)(ReceiveEvt.java:251)
```

(2) Confirming a log of event actions performed (Email) from the System Log

Process

1. Search for the resource path accessed from the System Log detailing events close to the time when the resource was accessed.
2. Search for the component abbreviation "ET" representing event actions performed from the search results returned in step 1.
3. When the email is successfully sent, "Success to transmit event." will appear in the <info> log level.
*When email sending fails, "Fail to transmit event(smtp)" will appear in the <warning> log level.
4. The request ID (ReqID) is output to the above-mentioned log, allowing you to search the System Log with this ID to retrieve a series of log information detailing processes from when a resource is accessed, to when an executed process completes.

(3) Confirming the transfer of resources (transfer) from the System Log

Process

1. Search for the resource path accessed from the System Log detailing events close to the time when the resource was accessed.
2. Search for the component abbreviation "TS" representing resource (transfer) processes from the search results returned in step 1.
3. When the transfer process is successful "Success to send Transmission Data" will appear in the <info> log level. Starting with this, the transfer address URL will be output.
4. The request ID (ReqID) is output to the above-mentioned log, allowing you to search the System Log with this ID to retrieve a series of log information detailing processes from when a resource is accessed, to when an executed process completes.

Log example:

```
2016-02-23T10:58:23.004101+09:00 <info> TS 10406 SMPAPL-001 180.43.8.247 Success to send
Transmission Data to http://sampleapp1.iot.jp.fujitsu.com/WebApl/AccessServlet. (ReqID=94330,
ResourcePath=_fwd/image, AccCode=imageAccessCode) (Normal) (ResourceSendForHTTP.java:150)
```

(4) Confirming data added by MQTT requests from the System Log

Process

All Rights Reserved, Copyright©FUJITSU LIMITED 2016-2018

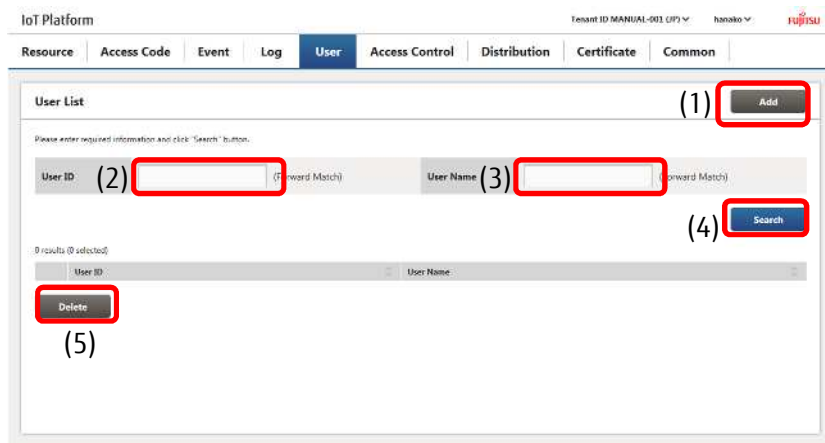
1. Search for the resource path accessed from the System Log detailing events close to the time of data being sent with MQTT.
2. Search for the component abbreviation "TS" representing data added from the search results returned in step 1.
3. When the data is successfully added, "Add of resource data succeed." will appear in the <info> log level.

Log example:

```
2016-02-23T10:57:39.110570+09:00 <info> DM 30001 SMPAPL-001 180.43.8.247 Add of resource data
succeed.[DataLength=19] (ReqId=1010326, ResourcePath=test, AccessCode=)
(MongoDbManage.go:155)
```

4.10 User Screen

Click User in the Main screen to display the User screen.



Number	Entry name	Description	Notes
(1)	Add	Adds a user.	Refer to Chapter 4.10.1
(2)	User ID	Set when searching for users.	Refer to Chapter 4.10.3
(3)	User name	Set when searching for users.	Refer to Chapter 4.10.3
(4)	Search	Deletes a user.	Refer to Chapter 4.10.3
(5)	Delete	Deletes a user.	Refer to Chapter 4.10.5

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
User ID	Text	Single-byte alphanumeric characters	-	Up to 254	-	E-mail address format Refer to Chapter 4.10.4 and 4.10.3
User name	Text	-	-	Up to 32	-	Refer to Chapter 4.10.4 and 4.10.3

4.10.1 Adding Users

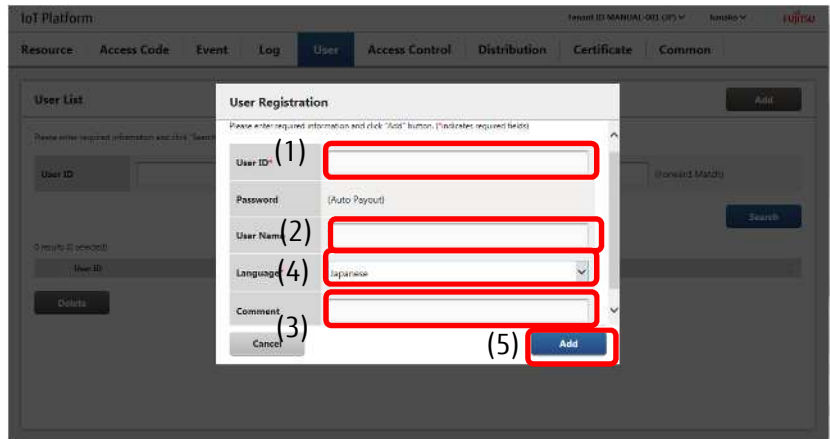
You can add users by clicking Add on the User screen. This section describes how to use the User Registration screen.

1. Enter the user ID into the field shown as (1) in the figure. Make sure to enter in an email address format.

2. Enter the user name into the field shown as (2) in the figure. Enter a comment if necessary into the field shown as (3) in the figure.

3. Select the language the screen after login appears for the login user in the field shown as (4) in the figure.

4. Click (5) Add.



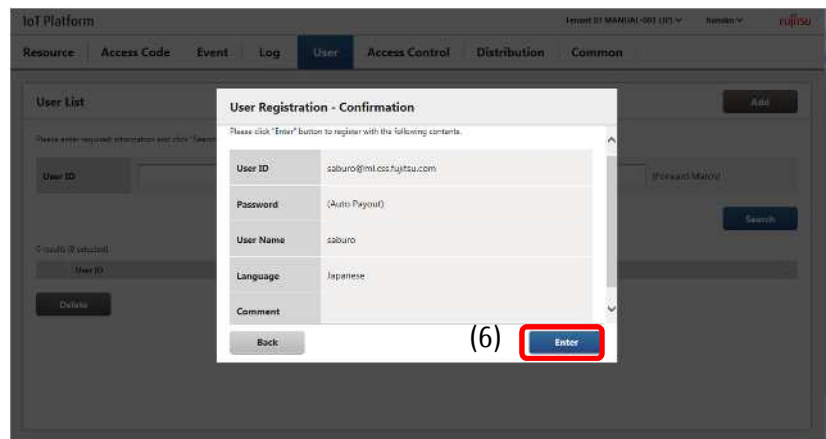
Notes on input parameters

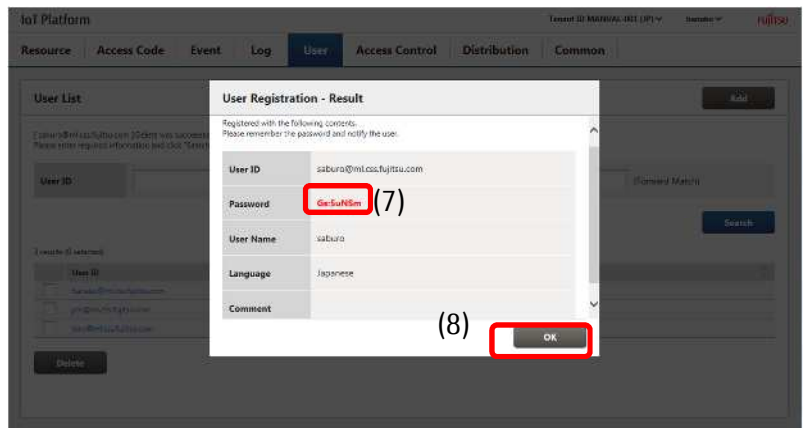
Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
User ID	Text	Single-byte alphanumeric characters	Yes	Up to 254	-	E-mail address format
User name	Text	Optional	-	Up to 32	-	
Language	Pull-down	-	Yes	-	Japanese	Select from Japanese and English
Comment	Text	Optional	-	Up to 256	-	

5. If there are no problems when the User Registration - Confirmation screen appears, click (6) to continue.

6. Take a note of the password for the user added which appears in the field shown as (7) in the figure.

7. Click (8) OK. Notify the added user of the password appearing in the field shown as (7) in the figure.





Memo

- Reset the password if you have forgotten the password noted down. Refer to Chapter 4.10.4 (1) for more details.

4.10.2 Changing Password

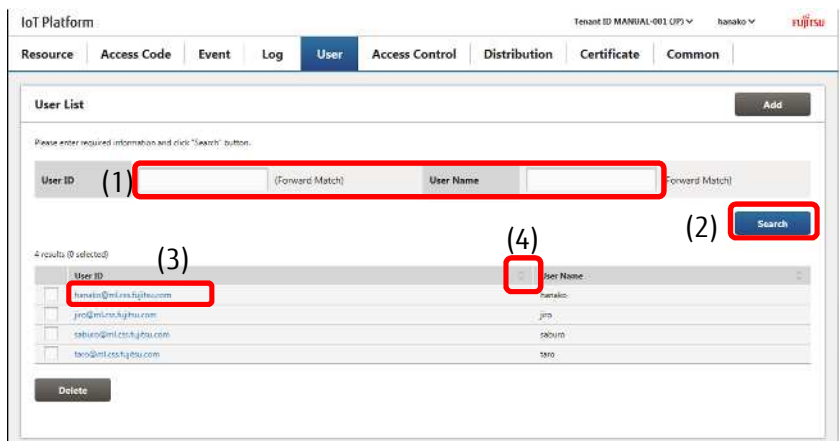
Passwords can be changed from the Main screen. Refer to Chapter 4.5.3 for more details.

4.10.3 Searching for Users

1. Enter the user ID or user name of the user you prefer to search for as a prefix-match in the fields provided in (1) in the figure.

2. Click (2) to display the users matching the search keys entered at the bottom of the screen.

3. Click the user ID in (3) to display the User Information Update screen.



- Click (4) to sort the search results. Refer to Chapter 7.2 for more information about the display order for sorting.



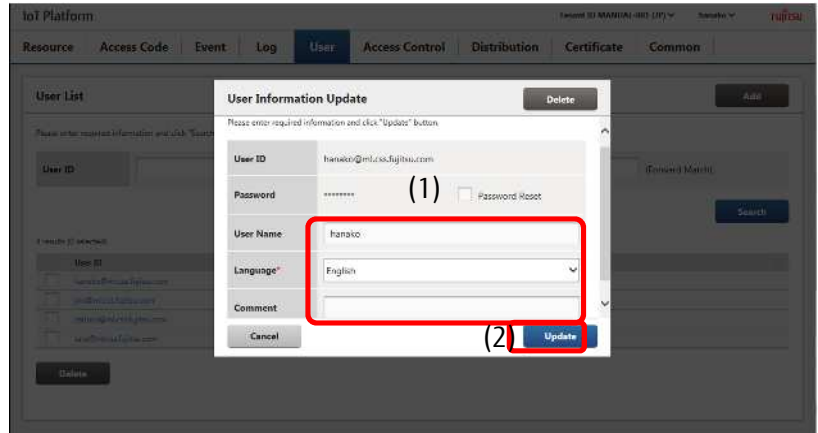
- Avoid entering only an underscore (_) into the user ID or user name fields and then pressing the Search button, as doing so will result in all users being retrieved in the search results.

4.10.4 Changing Users

1 . Display the User Information Update screen for the user you prefer to change by following the procedure described in 4.10.3.

2. Edit the user name, language and comment in the fields shown as (1) in the figure.

3. Click (2) Update to display the update confirmation screen. Click (3)



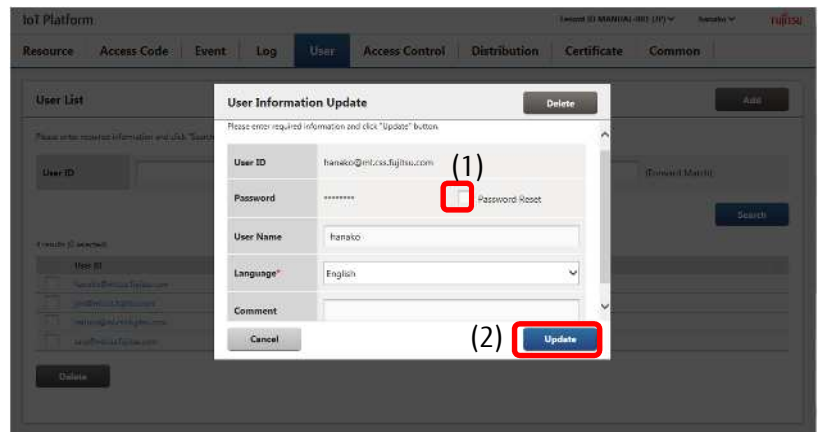
[1] Resetting passwords

You can reset a password if you have forgotten it. Ask a system administrator at your company to reset the password.

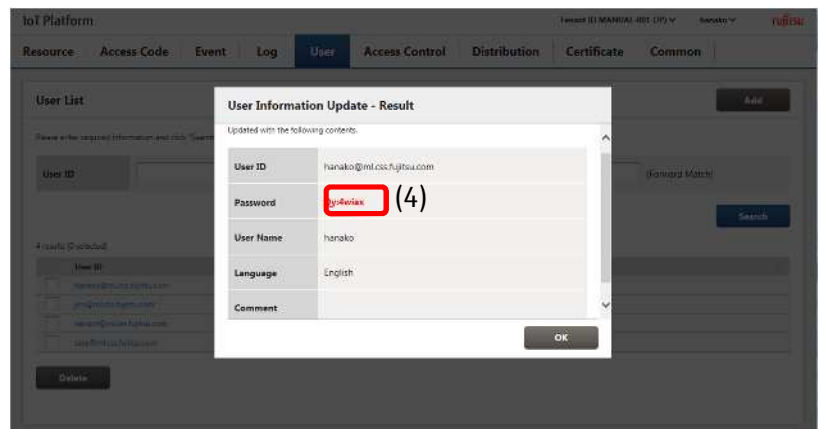
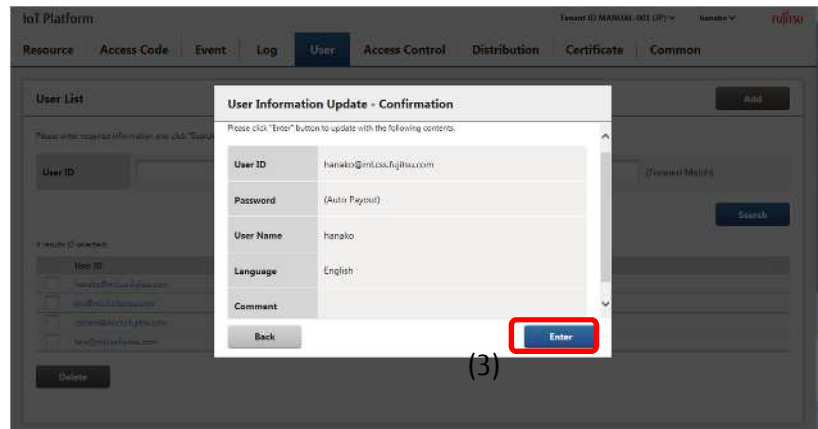
1 . Display the User Information Update screen for the user you prefer to reset the password for by following the procedure described in 4.10.3.

2. Select the (1) Password Reset check box, and then click (2) Update.

3. When the User Information Update - Confirmation screen appears, click (3) Enter to reset the password.



4. The reset password will appear in the field shown as (4) in the figure in the User Information Update - Confirmation screen. Notify the user of the reset password.

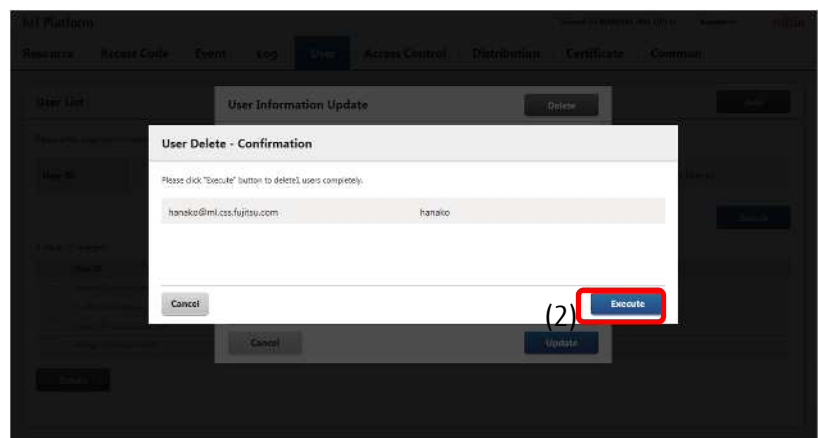
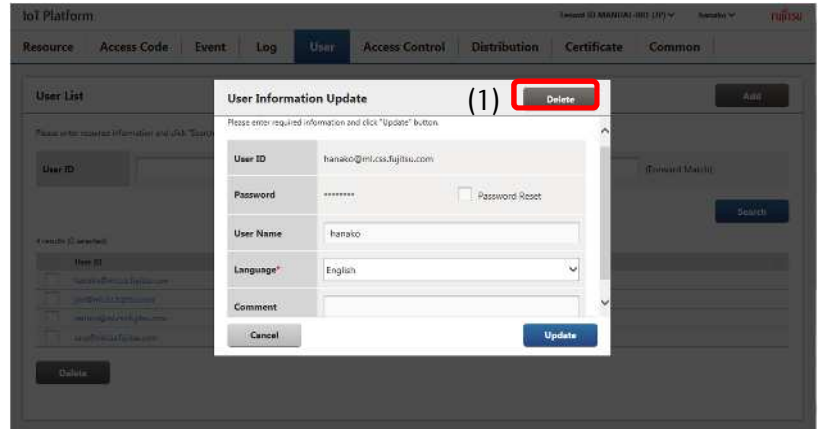


[2] Deleting users

1 . Display the User Information Update screen for the user you prefer to delete by following the procedure described in 4.10.3.

2. Click (1) for Delete.

3. When the User Delete - Confirmation screen appears, click (2) Execute to delete the user.

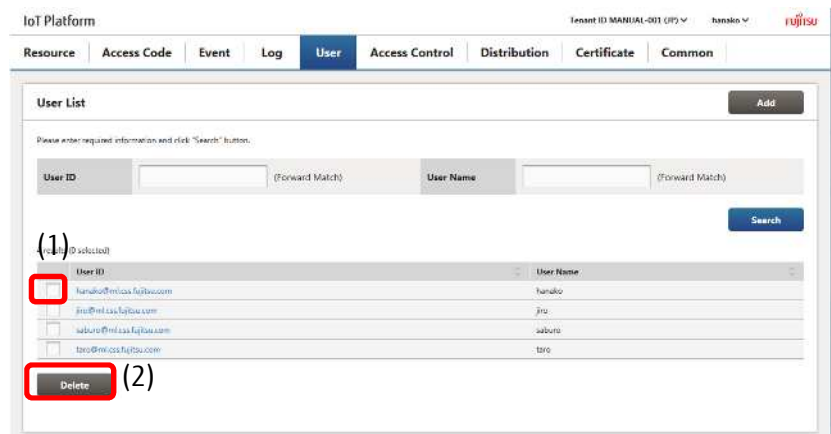


4.10.5 Batch Deleting Users

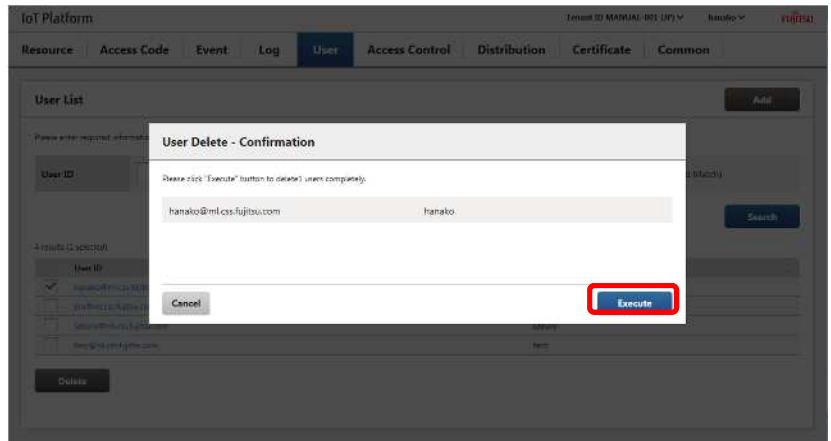
1 . Display the users you prefer to delete by searching for the users using the procedure described in 4.10.3.

2. Select the check box of the users you prefer to delete, shown as (1) in the figure, and then click (2) Delete.

3. When the User Delete - Confirmation screen appears, click (3) Execute to delete the user.



(3)



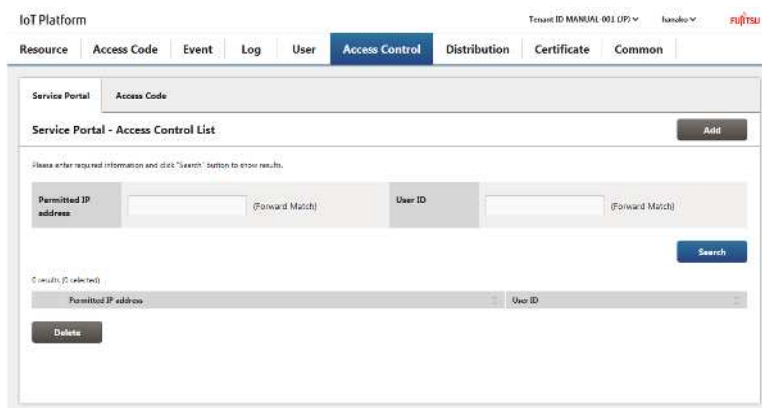
Note

- Users subject to Service Portal access control cannot be deleted. Remove those users from Service Portal access control in order to delete them. Refer to Chapter 4.11.1 for more information about Service Portal access control.

4.11 Access Control Screen

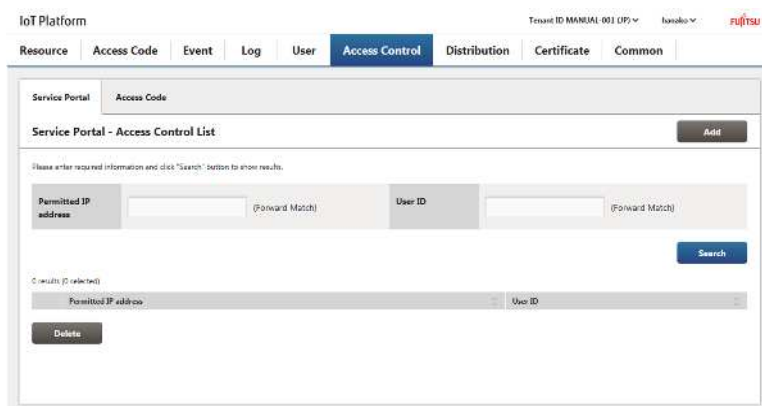
Click Access Control in the Main screen to display the Access Control screen.

The Access Control screen consists of two screens, the Service Portal Access Control screen, and the Access Code Access Control screen.



4.11.1 Service Portal Access Control Screen

Click the Service Portal tab in the Access Control screen to display the Service Portal Access Control screen.



You can add combinations of users within customer tenants allowed access to the Service Portal and permitted IP addresses on the Service Portal Access Control screen. You can allow ranges of permitted IP addresses, for example, IP addresses from 10.11.22.33-10.11.22.44. Users attempting to access the Service Portal will be denied access if the IP address for the terminal in use differs from the permitted IP address range for the user.

Memo

- Users that are not associated with a single permitted IP address may access the Service Portal from any terminal, regardless of its IP address.

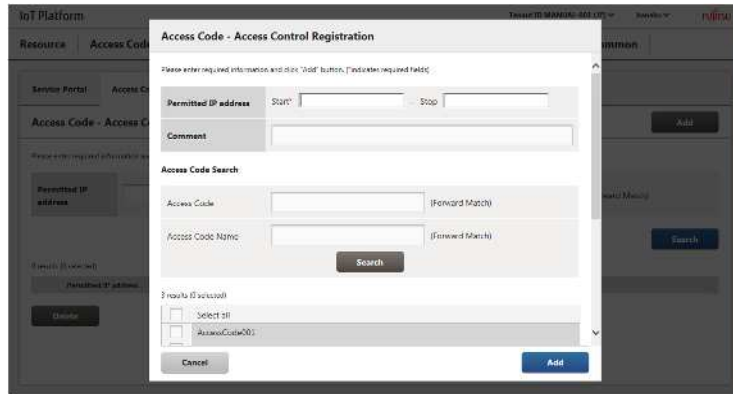
Number	Entry name	Description	Notes
(1)	Add	Adds Service Portal access controls.	Refer to Chapter 4.11.1(1)
(2)	Permitted IP address	- Set when performing Service Portal access control searches.	Refer to Chapter 4.11.1(2)
(3)	User ID	- Set when performing Service Portal access control searches.	Refer to Chapter 4.11.1(2)
(4)	Search	- Search for Service Portal access controls.	Refer to Chapter 4.11.1(2)
(5)	Delete	- Deletes Service Portal access controls.	Refer to Chapter 4.11.1(4)

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Permitted IP address	Text	Single-byte numerals	-	Up to 15	-	Usable characters: Single-byte numerals [.]
User ID	Text	Single-byte alphanumeric characters	-	Up to 254	-	

[1] Adding Service Portal access controls

The following screen will appear when you click Add on the Service Portal Access Control screen described in Chapter 4.11.1.



Number	Entry name	Description	Notes
(1)	Permitted IP address	Set the range of IP addresses permitted access.	Refer to permitted IP address settings
(2)	Comment	Allows users to set user-defined Service Portal access control summaries, etc.	
(3)	User ID	Set when searching for users.	Refer to permitted user settings
(4)	User name	Set when searching for users.	Refer to permitted user settings
(5)	Search	Retrieves users.	Refer to permitted user settings
(6)	Add	Adds the selected user as a permitted user.	Refer to permitted user settings
(7)	Release	Removes the selected user from the permitted user list.	Refer to permitted user settings
(8)	Cancel	Cancels adding Service Portal access controls and closes the screen.	
(9)	Add	Adds Service Portal access controls with the settings applied.	

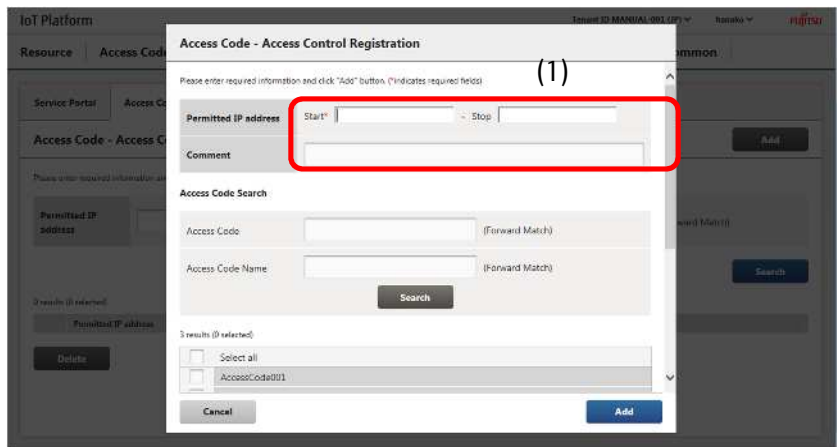
Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Permitted IP address (start)	Text	Single-byte numerals	Yes	Up to 15	-	Usable characters: Single-byte numerals [.]
Permitted IP address (stop)	Text	Single-byte numerals	-	Up to 15	-	Usable characters: Single-byte numerals [.]
Comment	Text	Single-byte numerals		Up to 256	-	Usable characters: Single-byte/double-byte/symbols (Japanese input allowed)
User ID	Text	Single-byte alphanumeric characters	-	Up to 254	-	
User name	Text	Refer to Notes	-	Up to 32	-	Usable characters: Single-byte/double-byte/sy

						mbols (Japanese input allowed)
--	--	--	--	--	--	--------------------------------

- Permitted IP address settings

1. Enter the initial and ending permitted IP addresses in (1). Enter a comment if necessary.



Note

- The permitted IP address (stop) cannot be a smaller value than the permitted IP address (start).

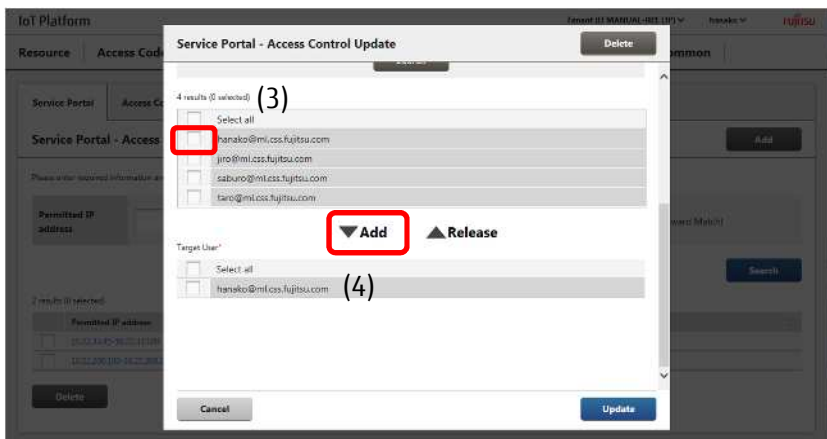
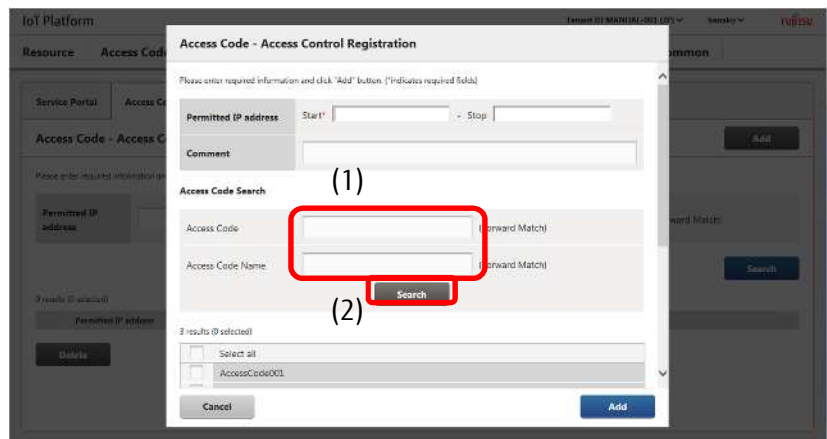
- Permitted user settings

2. Enter the user ID or the user name you prefer to search for in (1).

3. Click Search (2) to display the search results.

4. Select the user from the search results (3), and then click ▼Add (4). This will add the selected user as a permitted user.

*To remove permitted users, select the user and click ▲Release.

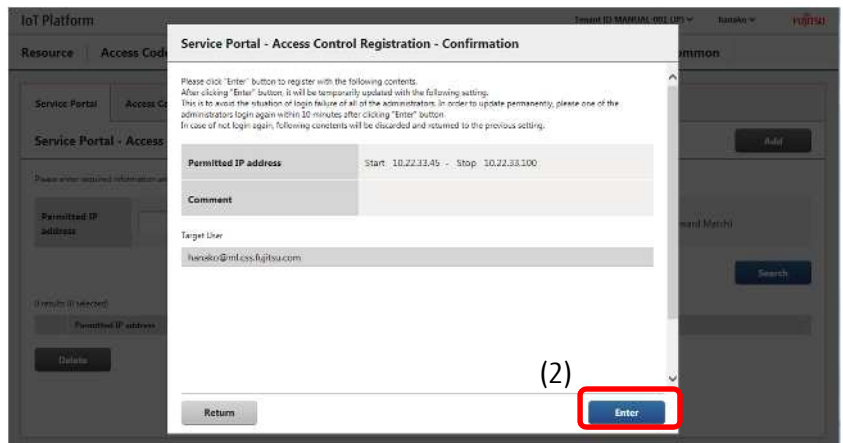
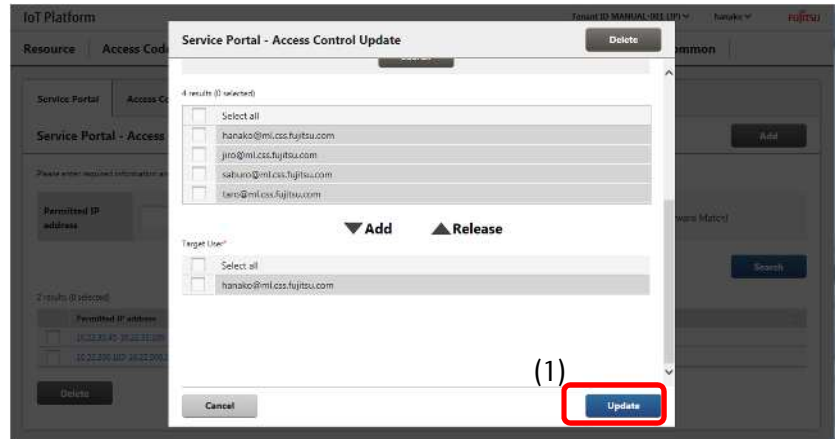


- Add

5. Click Add (1).

6. Confirm the contents of the Confirmation screen when it appears, and then click Enter (2).

7. Login again as a user that has been permitted access within 10 minutes to apply settings.



Memo

- Up to five Service Portal access controls can be added per tenant.

! Note

- Login again as a user that has been permitted access within 10 minutes after adding/changing/deleting Service Portal access controls to apply settings.
- All setting changes will be automatically undone if you do not log in within 10 minutes of adding/changing/deleting Service Portal access controls.
(This is to prevent all users from being unable to log in due to misconfigured settings)

[2] Searching Service Portal access controls

You can search for Service Portal access controls from the Service Portal Access Control screen. This is mainly used to edit Service Portal access controls and to delete unnecessary Service Portal access controls.

1. Enter the permitted IP address or the user name into the fields shown as (1) in the figure.

2. Click Search shown as (2) in the figure to display the search results at the bottom of the screen.

Click (3) to sort the search results. Refer to Chapter 7.2 for more information about the display order for sorting.

The screenshot shows the 'Service Portal - Access Control List' interface. At the top, there are navigation tabs: Resource, Access Code, Event, Log, User, Access Control (selected), Distribution, Certificate, and Common. Below the tabs, there are search fields for 'Permitted IP address' and 'User ID', both labeled '(1)'. A 'Search' button is labeled '(2)'. Below the search fields, there is a table with 2 results. The table has columns for 'Permitted IP address' and 'User ID'. The first row shows '10.22.33.45-10.22.33.100' and 'hanako@ml.sss.fujitsu.com'. The second row shows '10.22.200.100-10.22.200.100' and 'jro@ml.saa.fujitsu.com'. The 'User ID' column header is highlighted with a red box and labeled '(3)'. There is a 'Delete' button at the bottom left.

Memo

- All search keys are compatible with prefix-match searching.

[3] Updating Service Portal access controls

Click the Service Portal access control link after searching the Service Portal access control you prefer to modify to display the Service Portal - Access Control Update screen.

1. You can search for the Service Portal access control you prefer to modify from the Service Portal Access Control screen. Refer to (2) for more information on searching.

2. Click the Service Portal access control you prefer to change settings for, shown as (1) in the figure, to proceed to the Service Portal - Access Control Update screen. The following provides a description of the changes and operation procedures that can be performed in the Service Portal - Access Control Update screen.

The screenshot shows the 'Service Portal - Access Control List' interface. At the top, there are navigation tabs: Resource, Access Code, Event, Log, User, Access Control (selected), Distribution, Certificate, and Common. Below the tabs, there are search fields for 'Permitted IP address' and 'User ID'. A 'Search' button is visible. Below the search fields, there is a table with 2 results. The table has columns for 'Permitted IP address' and 'User ID'. The first row shows '10.22.33.45-10.22.33.100' and 'hanako@ml.sss.fujitsu.com'. The second row shows '10.22.200.100-10.22.200.100' and 'jro@ml.saa.fujitsu.com'. The 'Permitted IP address' column header is highlighted with a red box and labeled '(1)'. There is a 'Delete' button at the bottom left.

Memo

- Entry fields for the Service Portal - Access Control Update screen are the same as that for the Service Portal - Access Control Registration screen.
- Refer to (1) Service Portal - Access Control Registration screen for more details.

- Changing permitted IP addresses

1. Change the permitted IP addresses in (1). You can also change the comment if necessary.

The screenshot shows the 'Service Portal - Access Control Update' dialog box. A red box highlights the 'Permitted IP address' field, which contains 'Start: 10.22.33.45' and 'Stop: 10.22.33.100'. Below this is a 'Comment' field. The 'User Search' section includes 'User ID' and 'User Name' fields, both with '(Forward Match)' labels, and a 'Search' button. Below the search fields is a list of search results with checkboxes and the email address 'hanako@ml.css.fujitsu.com'. At the bottom of the dialog are 'Cancel' and 'Update' buttons.

- Changing permitted users

1. Enter the user ID or the user name you prefer to search for in (1).

2. Click Search (2) to display the search results.

3. Select the user from the search results (3), and then click ▼Add (4). This will add the selected user as a permitted user.

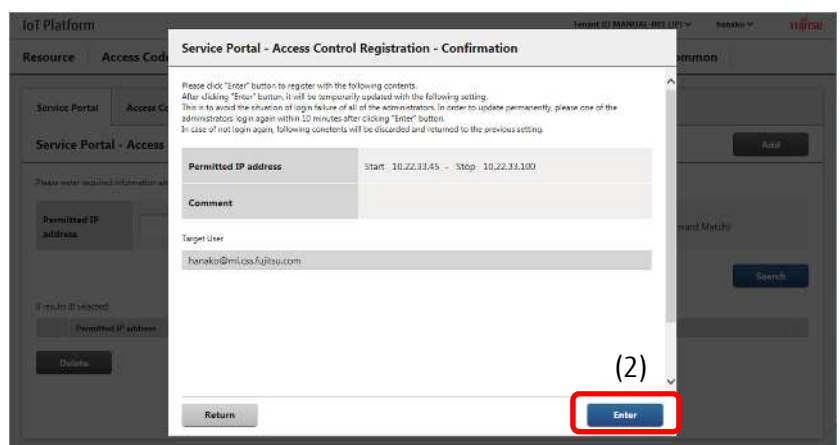
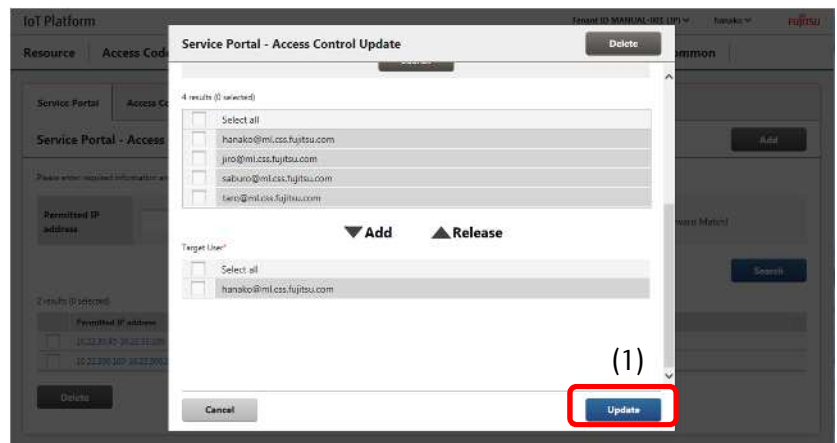
- *To remove permitted users, select the user and click ▲Release.

This screenshot is similar to the previous one, but the 'Search' button is highlighted with a red box and labeled (2). The 'User ID' and 'User Name' input fields are also highlighted with a red box and labeled (1).

This screenshot shows the search results list highlighted with a red box and labeled (3). The 'Add' button is highlighted with a red box and labeled (4). The list contains four entries with checkboxes and email addresses: 'hanako@ml.css.fujitsu.com', 'saburo@ml.css.fujitsu.com', and 'taro@ml.css.fujitsu.com'. The 'Add' and 'Release' buttons are visible at the bottom of the list.

- Updating

1. Click Update (1).
2. Confirm the contents of the Confirmation screen when it appears, and then click Enter (2).
3. Login again as a user that has been permitted access within 10 minutes to apply settings.



[4] Batch deleting Service Portal access controls

Follow the procedure below to delete multiple Service Portal access controls in a batch.

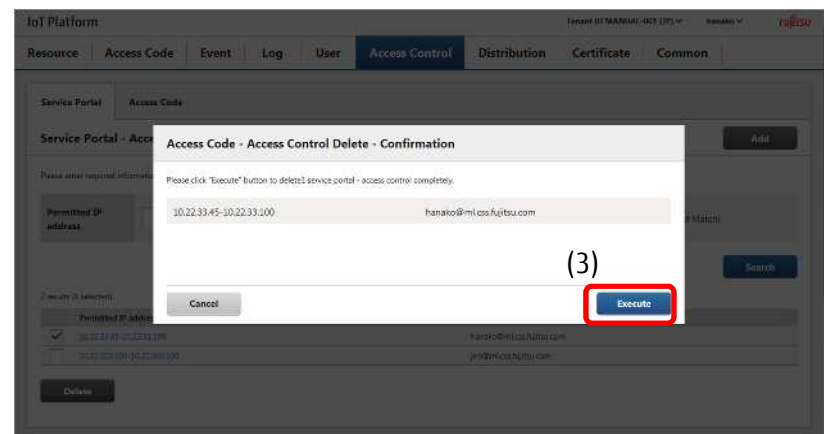
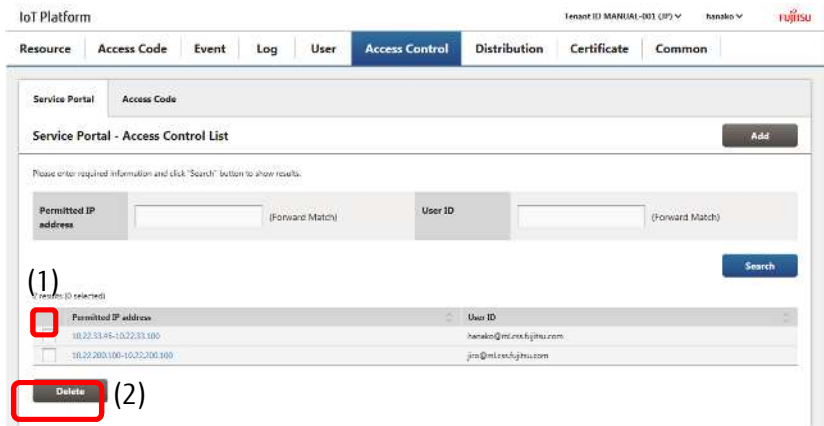
1. You can search for the Service Portal access controls you prefer to delete from the Service Portal Access Control screen. Refer to (2) for more information on searching.

2. Select the check box (1) next to the Service Portal access control you prefer to delete. Select multiple check boxes when you prefer to delete multiple resources.

3. Click (2) Delete.

4. Click (3) Execute after confirming the contents of the Confirmation screen when it appears.

5. Login again as a user that has been permitted access within 10 minutes to apply the deletion changes.

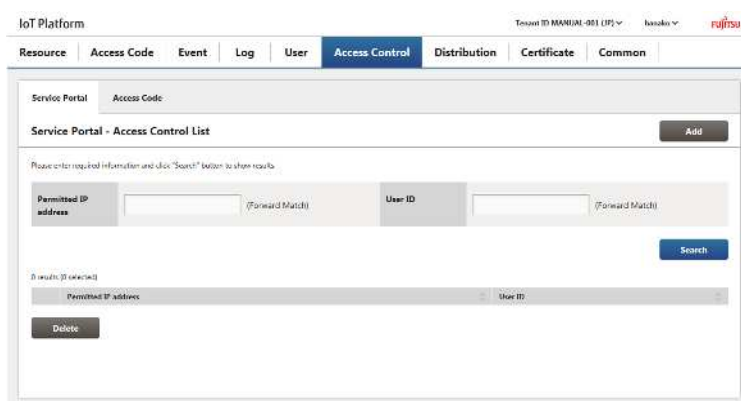


Note

- Login again as a user that has been permitted access within 10 minutes after adding/changing/deleting Service Portal access controls to apply settings. All setting changes will be automatically undone if you do not log in within 10 minutes of adding/changing/deleting Service Portal access controls. (This is to prevent all users from being unable to log in due to misconfigured settings)
- Deleted Service Portal access control information cannot be retrieved after the deletion changes have been applied. Customers are responsible for paying due care in checking which access code to delete before performing deletion actually.

4.11.2 Access Code - Access Control Screen

Click Access Code on the Access Control screen to display the Access Code - Access Control screen.



You can add permitted IP addresses to associate with access codes within customer tenants on the Access Code - Access Control screen.

You can allow ranges of permitted IP addresses, for example, IP addresses from 10.11.22.33-10.11.22.44. Users will be denied access to access codes if the IP address for the terminal they are attempting to access differs from the permitted IP address range.

Memo

- Access codes that are not associated with a single permitted IP address may be used for access from any IP address.

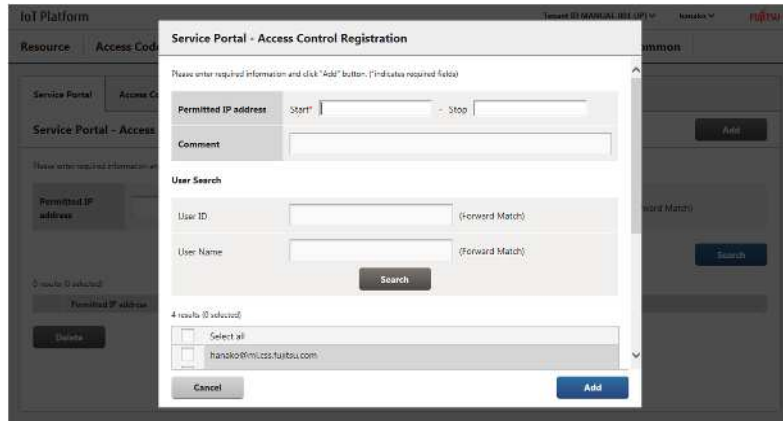
Number	Entry name	Description	Notes
(1)	Add	Adds access code access controls.	Refer to Chapter 4.11.2[1]
(2)	Permitted IP address	Set when searching for access code access controls.	Refer to Chapter 4.11.2[2]
(3)	Access Code	Set when searching for access code access controls.	Refer to Chapter 4.11.2[2]
(4)	Search	Searches for access code access controls.	Refer to Chapter 4.11.2[2]
(5)	Delete	Deletes access code access controls.	Refer to Chapter 4.11.2[4]

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Permitted IP address	Text	Single-byte numerals	-	Up to 15	-	Usable characters: Single-byte numerals [.]
Access Code	Text	Single-byte numerals	-	Up to 48	-	Usable characters: Single-byte numerals [-]

[1] Adding access code access controls

The following screen will appear when you click Add on the Access Code - Access Control screen described in Chapter 4.11.2.



Number	Entry name	Description	Notes
(1)	Permitted IP address	Set the range of IP addresses permitted access.	Refer to permitted IP address settings
(2)	Comment	Allows users to set user-defined access code access control summaries, etc.	
(3)	Access Code	Set when searching for access codes.	Refer to permitted access code settings
(4)	Access Code Name	Set when searching for access codes.	Refer to permitted access code settings
(5)	Search	Retrieves access codes.	Refer to permitted access code settings
(6)	Add	Adds the selected user as an access code permitted access.	Refer to permitted access code settings
(7)	Release	Deletes the selected user from access codes permitted access.	Refer to permitted access code settings
(8)	Cancel	Cancels adding access code access controls and closes the screen.	
(9)	Add	Adds access code access controls with the settings applied.	

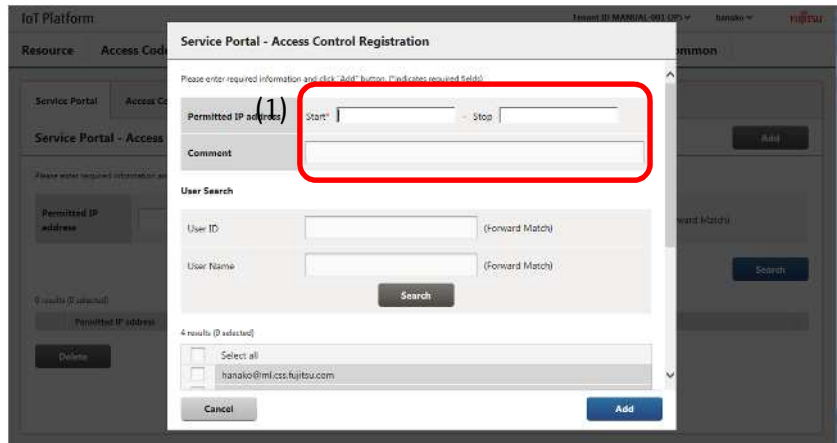
Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Permitted IP address (start)	Text	Single-byte numerals	Yes	Up to 15	-	Usable characters: Single-byte numerals [.]
Permitted IP address (stop)	Text	Single-byte numerals	-	Up to 15	-	Usable characters: Single-byte numerals [.]
Comment	Text	Refer to Notes		Up to 256	-	Usable characters: Single-byte/double-byte/symbols (Japanese input allowed)

Access Code	Text	Single-byte numerals	-	Up to 254	-	Usable characters: Single-byte numerals [-]
Access Code Name	Text	Refer to Notes	-	Up to 32	-	Usable characters: Single-byte/double-byte/symbols (Japanese input allowed)

- Permitted IP address settings

1. Enter the initial and ending permitted IP addresses in (1). Enter a comment if necessary

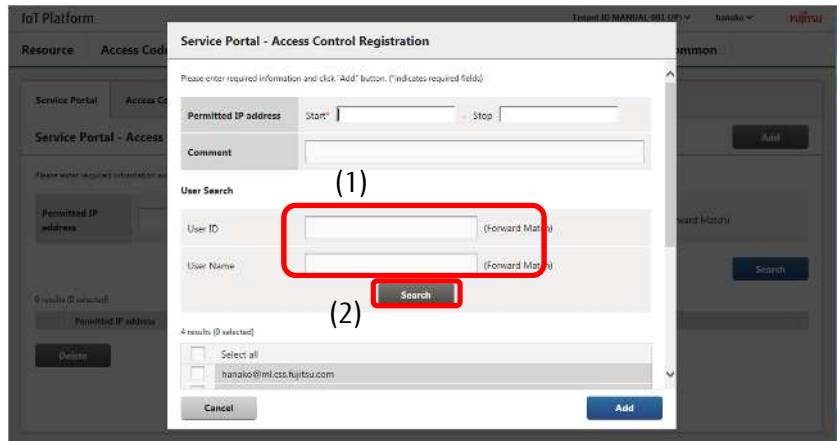


Note

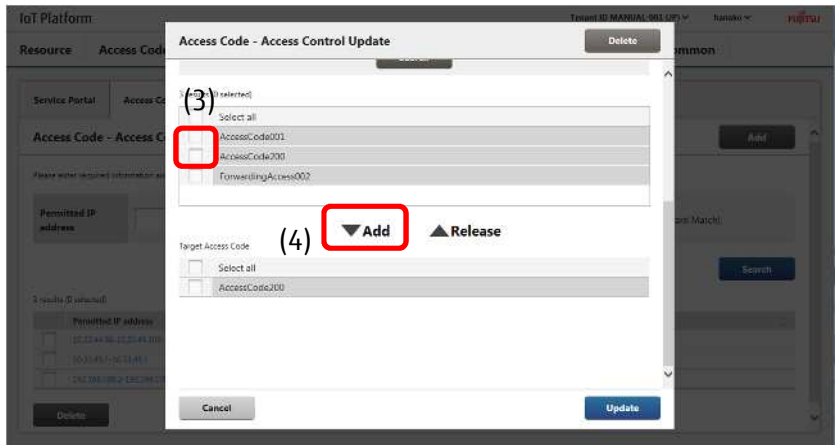
- The permitted IP address (stop) cannot be a smaller value than the permitted IP address (start).

- Permitted access code settings

1. Enter the access code or the access code name you prefer to search for in (1).
2. Click Search (2) to display the search results.
3. Select the access code from the search results (3), and then click Add (4). Adds the selected access code as an access code permitted access.

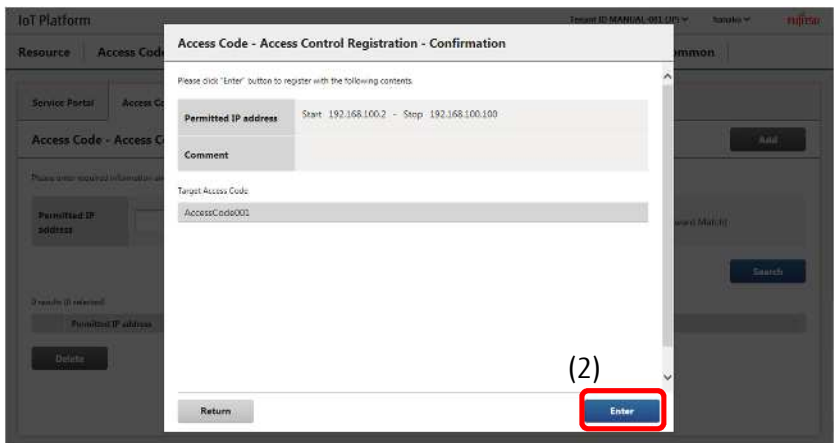
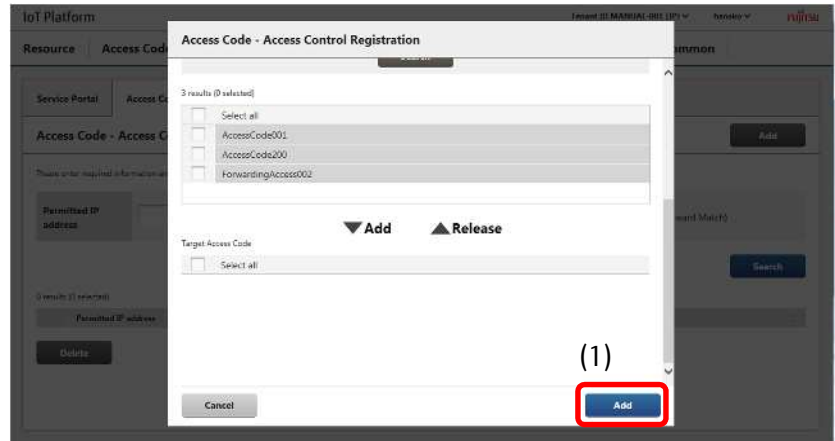


*To remove permitted access codes, select the access code and click



- Add

1. Click Add (1).
2. Confirm the contents of the Confirmation screen when it appears, and then click Enter (2)



Memo

- Up to five access code access controls can be added per tenant.

[2] Searching access code access controls

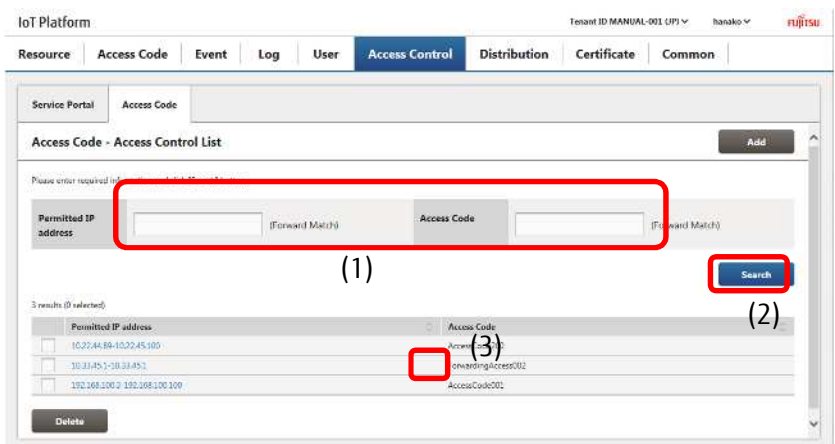
You can search for access code access controls from the Access Code - Access Control screen.

This is mainly used to edit access code access controls, and to delete unnecessary access code access controls.

1. Enter the permitted IP address or the access code into the fields shown as (1) in the figure.

2. Click Search shown as (2) in the figure to display the search results at the bottom of the screen.

Click (3) to sort the search results. Refer to Chapter 7.2 for more information about the display order for sorting.



Memo

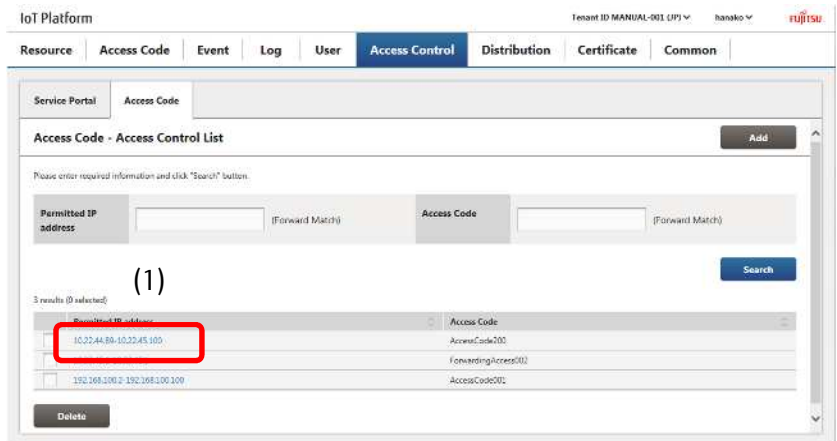
- All search keys are compatible with prefix-match searching.

[3] Updating access code access controls

Click the access code access control link after searching and retrieving the access code access control you prefer to modify to display the Access Code - Access Control Update screen.

1 . Search for access code access controls from the Access Code - Access Control screen. Refer to [2] for more information on searching.

2. Click the access code access control you prefer to change settings for, shown as (1) in the figure, to proceed to the Access Code - Access Control screen. The following provides a description of the changes and operation procedures that can be performed in the Access Code - Access Control screen.

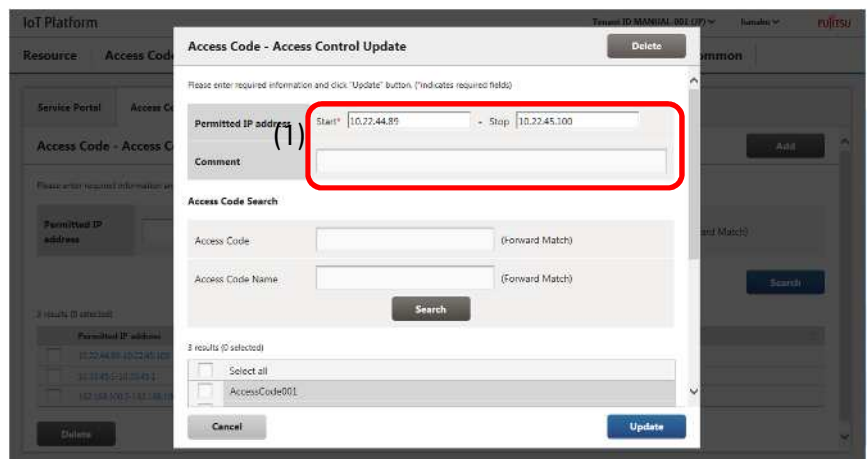


Memo

- Entry fields for the Access Code - Access Control Update screen are the same as that for the Access Code - Access Control Registration screen. Refer to (1) Access Code - Access Control Update screen for more details.

- Changing permitted IP addresses

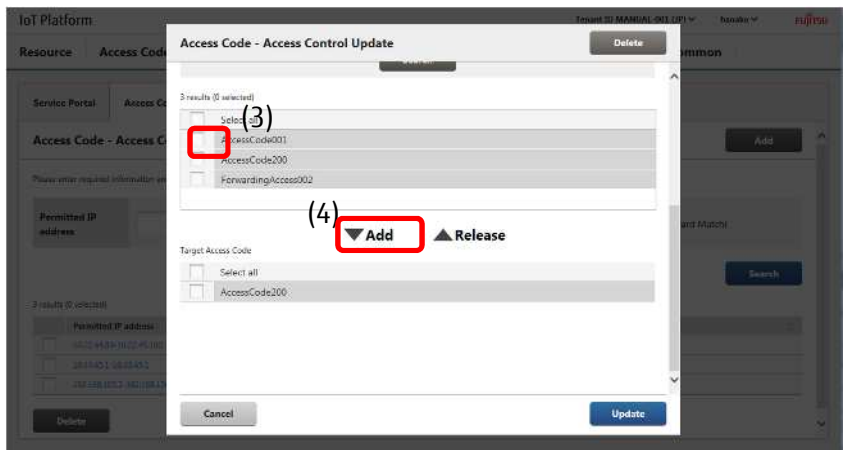
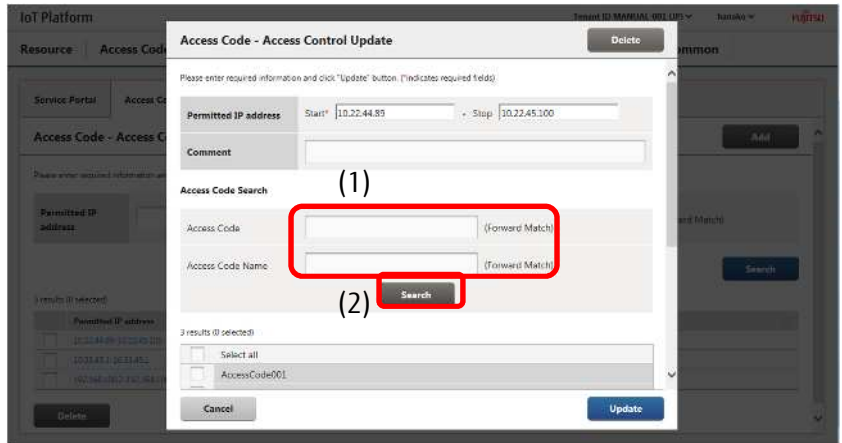
1 . Change the permitted IP addresses in (1). You can also change the comment if necessary.



- Changing permitted access codes

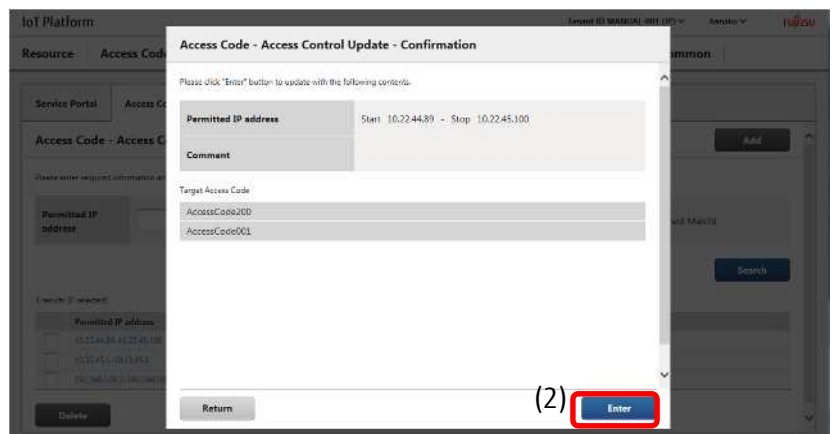
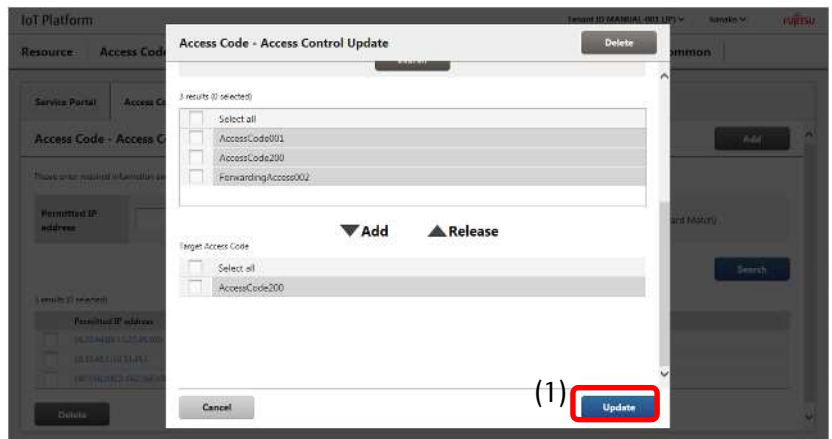
1. Enter the access code or the access code name you prefer to search for in (1).
2. Click Search (2) to display the search results.
3. Select the access code from the search results (3), and then click Add (4). Adds the selected access code as an access code permitted access.

*To remove permitted access codes, select the access code and click Release.



- Updating

1. Click Update (1).
2. Confirm the contents of the Confirmation screen when it appears, and then click Enter (2).



[4] Deleting access code access controls

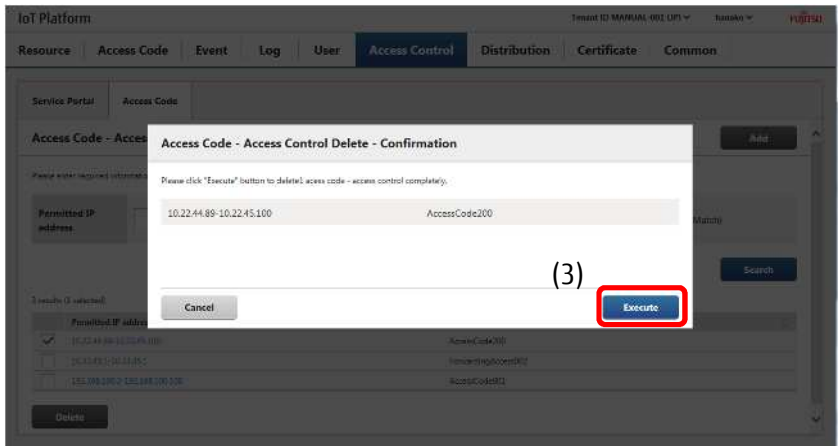
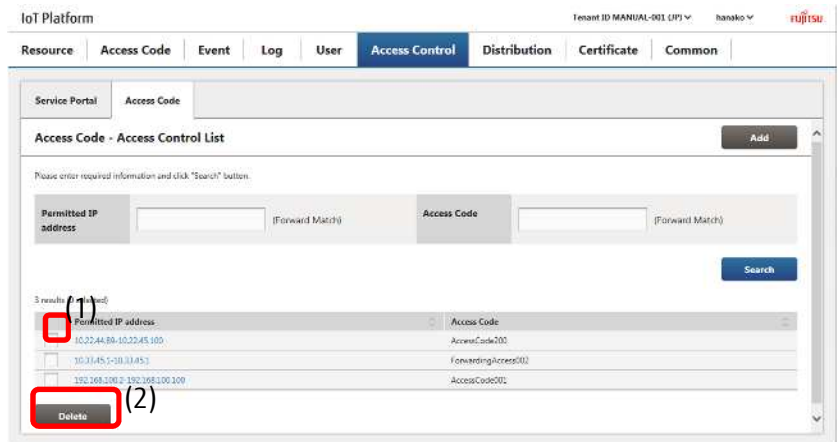
Follow the procedure below to delete multiple access code access controls in a batch.

1. Search for access code access controls you prefer to delete from the Access Code - Access Control screen. Refer to part [2] for more information on searching.

2. Select the check box (1) next to the access code access control you prefer to delete. Select multiple check boxes when you prefer to delete multiple resources.

3. Click (2) Delete.

4. Click (3) Execute after confirming the contents of the Confirmation screen when it appears.



4.12 Distribution Screen

Click Distribution in the Main screen to display the Distribution screen.
The Distribution screen contains the tps/bps distribution settings screen.

4.12.1 tps/bps Distribution Settings Screen

The tps/bps distribution settings screen sets the distribution policy based on the load status measured in tps (transactions per second) or bps (bytes per second).

Number	Entry name	Description	Notes
(1)	Entire Enable/disable	Used to enable/disable all distribution settings.	
(2)	Common distributed policy	Use shared settings.	Refer to Chapter 4.12.1 [1] for more details on each item.
(3)	Load resource	Sets the resource recording the load status.	Refer to Chapter 4.12.1 [1] for more details on each item.
(4)	Search (load resource)	Searches resource paths when setting load resources.	
(5)	Recommend resources 1 to 3	Set the resource used for recommendations.	Refer to Chapter 4.12.1 [1] for more details on each item.
(6)	Search (recommend resource)	Searches resource paths when setting recommend resources.	
(7)	Update	Performs an update with the information entered.	

[1] Updating tps/bps distribution settings
 - Enable/disable all distribution policies

1. Enable/disable all distribution policies in (1).



Note

- Information entered will not be updated when Entire Enable/Disable is set to Disable.

- Common Distributed Policy settings

1. Set the recommendation cycle in (1).
2. Set the calculating period in (2).

Number	Entry name	Description	Notes
(1)	Recommendation Cycle	Set the interval used for recommendations.	
(2)	Calculating Period	Set the interval used for calculating load status.	

Notes on input parameters

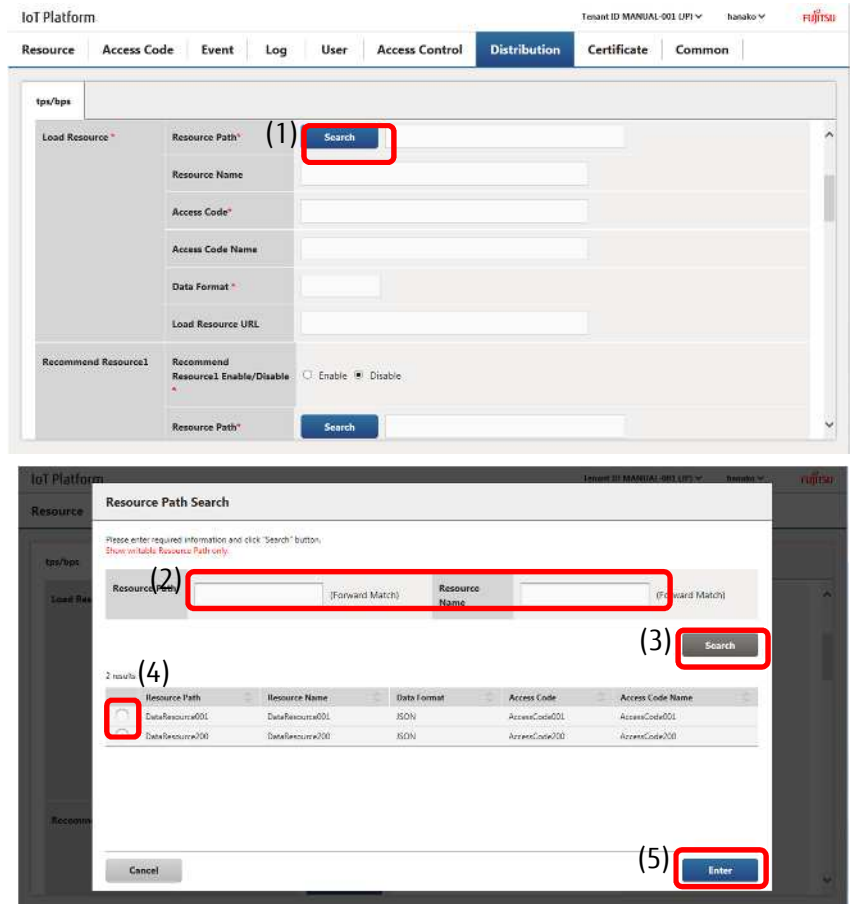
Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Recommendation Cycle	Text	Single-byte numerals	Yes	-	60	Available values: 1 to 1440 (Unit: Minutes)
Calculating Period	Text	Single-byte numerals	Yes	-	120	Available values: 1 to 1440 (Unit: Minutes)

- Load resource settings

1 . Click (1) Search to display the Resource Path Search screen.

2. Enter the resource path or the resource name in the fields shown as (2) in the Resource Path Search screen, and then click Search (3).

3. Select the resource path you prefer to configure from the search results (4), and then click Enter (5).



 Note

- Resource(transfer) type resources and binary-data resources cannot be set to load resources.
- The error collection resource "_error" added by the system when creating a tenant cannot be set to load resources.

* The resource and access code used for the load resource must be configured on the Resource screen and the Access Code screen before they can be retrieved in a search.

Number	Entry name	Description	Notes
(1)	Search	Displays the Resource Path Search screen.	
(2)	Resource path	Sets the resource path.	Select by searching for the resource path. Entered automatically from resource path settings.
(3)	Resource name	Sets the resource name.	
(4)	Access Code	Sets the access code.	
(5)	Access code name	Sets the access code name.	
(6)	Data format	Sets the data format.	

(7)	Load resource URL	Sets the load resource URL.
-----	-------------------	-----------------------------

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Resource path	Text	Single-byte alphanumeric characters	Yes	Up to 128	-	Select by performing a search. The resource path cannot be directly input.
Resource name	-	-	-	-	-	Entered automatically from resource path settings.
Access Code	-	-	-	-	-	
Access code name	-	-	-	-	-	
Data format	-	-	-	-	-	
Load resource URL	-	-	-	-	-	

Memo

- The Resource Path Search screen is the same as the Resource Path Search screen used in Chapter 4.8.1. Refer to Chapter 4.8.1 for more details.

- Configuring recommend resources

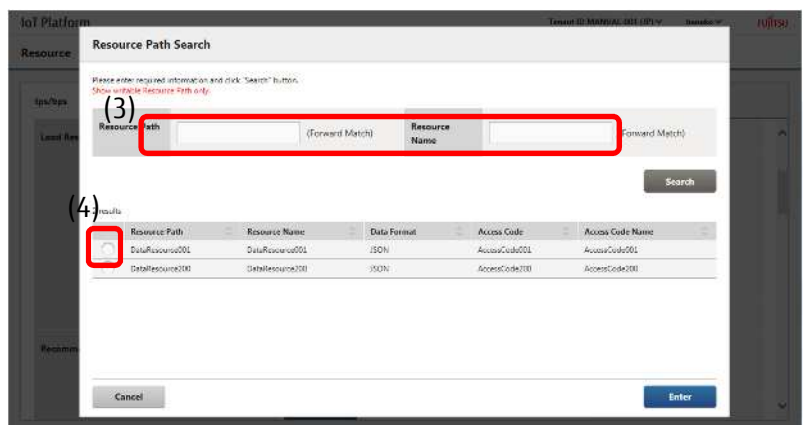
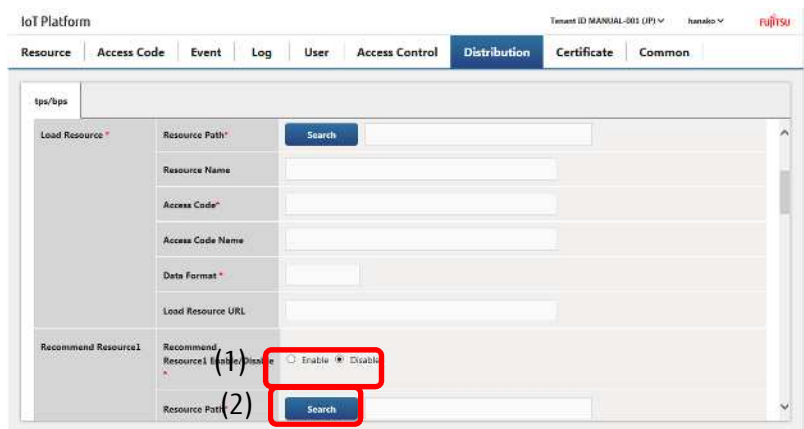
1. Enable/disable recommend resource settings in (1).

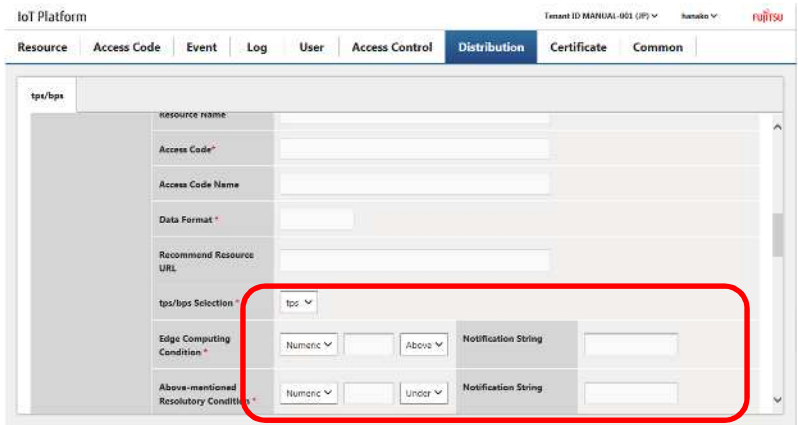
2. Click (2) Search to display the Resource Path Search screen.

3. Enter the resource path or the resource name in the fields shown as (3) in the Resource Path Search screen, and then click Search.

4. Select the resource path you prefer to configure from the search results (4), and then click Enter.

5. Set the measurement type, the edge computing condition, and the above-mentioned resolutory condition in the fields shown as (5) in the figure.





Note

- The error collection resource "_error" added by the system when creating a tenant cannot be used as the recommend resource.
- The resource and access code used for the recommend resource must be configured on the Resource screen and the Access Code screen before they can be retrieved in a search.

Number	Entry name	Description	Notes
(1)	Enable/disable	Enable/disable recommend resource settings.	
(2)	Search	Displays the Resource Path Search screen.	
(3)	Resource path	Sets the resource path.	Select by searching for the resource path.
(4)	Resource name	Sets the resource name.	Entered automatically from resource path settings.
(5)	Access Code	Sets the access code.	
(6)	Access code name	Sets the access code name.	
(7)	Data format	Sets the data format.	
(8)	Recommend resource URL	Set the recommend resource URL.	
(9)	tps/bps selection	Select the load status measurement type.	
(10)	Edge computing condition	Set the edge computing condition.	
(11)	Above-mentioned resolatory condition	Set the edge computing resolatory condition.	



Note

- When recommend resource settings are disabled all other recommend resource entry fields cannot be modified. Additionally, all other recommend resource entry fields will not be updated when updating the distribution policy in this state.

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				

Resource path	Text	Single-byte alphanumeric characters	Yes	Up to 128	-	Select by performing a search. The resource path cannot be directly input.
Resource name	-	-	-	-	-	Entered automatically from resource path settings.
Access Code	-	-	-	-	-	
Access code name	-	-	-	-	-	
Data format	-	-	-	-	-	
Recommend resource URL	-	-	-	-	-	
Edge computing condition	Pull-down	-	Yes		-	Only a value can be selected.
Edge computing condition	Text	Single-byte numerals	Yes	Up to 10	-	
Edge computing condition detection judgment	Pull-down	-	Yes		-	Only or more can be selected.
Edge computing condition notification character string	Text	Optional	Yes	Up to 10	-	
Resolutive condition character type selection	Pull-down	-	-		-	Only a value can be selected.
Resolutive conditions	Text	Single-byte numerals	Yes	Up to 10	-	
Resolutive condition detection judgments	Pull-down		Yes		-	Only less than can be selected.
Resolutive condition notification character string	Text	Optional	Yes	Up to 10	-	

Memo

Up to three recommend resources, 1 to 3, can be set. The settings for each recommend resources are the same.

- Updating distribution settings

1. Click Update (1). This will apply the changed settings.

The screenshot shows the 'Distribution' tab in the IoT Platform interface. The 'tps/bps' resource is selected. The 'Update' button at the bottom right is circled in red and labeled with '(1)'. A red box highlights the 'Update' button. A small red text message at the bottom left reads: 'Change will be generated if updating in flexible mode. Please push "Update" button if it is ok.'

4.13 Generate Certificate Screen

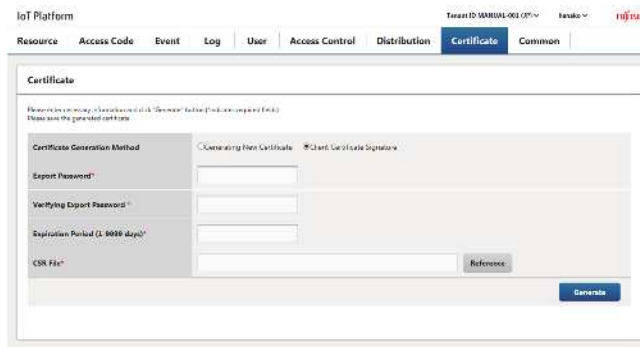
Click Generate certificate on the Main screen to display the Generate Certificate screen.

The options available on the Generate Certificate screen will vary depending on the certificate format selected.

4.13.1 Generate Certificate Screen (Create New Certificate)

An item will appear to create a new certificate when selecting Generate new certificate as the certificate format on the Generate Certificate screen.

Here you can generate and download new client certificates.



Number	Entry name	Description	Notes
(1)	Certificate format	Select the certificate format.	
(2)	Signature hash algorithm	Display the signature hash algorithm.	Refer to Chapter 4.13.1 (1)
(3)	PEM pass phrase	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(4)	Export Password	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(5)	Verifying Export Password	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(6)	Public key length	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(7)	Period of validity	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(8)	Common name (CN)	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(9)	Country (C)	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(10)	Prefecture (ST)	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(11)	Municipality (L)	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(12)	Organization name (O)	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(13)	Organization unit name (OU)	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(14)	E-mail	Set when generating a certificate.	Refer to Chapter 4.13.1 (1)
(15)	Generate button	Generates the certificate.	Refer to Chapter 4.13.1 (1)

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Certificate format	Radio button	-	Yes	-	Create new certificate	Select from Create new certificate and the certificate signature.
PEM pass phrase	Text	Refer to Notes	Yes	8 to 16	-	Usable characters: Upper and lower case alphabetical characters, numbers, # @ - () : . _
Export Password	Text	Refer to Notes	Yes	8 to 16	-	Usable characters: Upper and lower case alphabetical characters, numbers, # @ - () :
Verifying Export Password	Text	Refer to Notes	Yes	8 to 16	-	Usable characters: Upper and lower case alphabetical characters, numbers, # @ - () :
Public key length	Radio button	-	Yes	-	2048bit	Select from 1024bit, 2048bit or 4096bit
Period of validity	Text	Refer to Notes	Yes	4	-	Can set from 1 to 9999 days
Common name (CN)	Text	Refer to Notes	Yes	32	-	Upper and lower case alphabetical characters, numbers, half-width spaces, # @ - () :t
Country (C)	Text	Refer to Notes	Yes	2	-	ISO 3166-1 alpha-2 Country code
Prefecture (ST)	Text	Refer to Notes	-	32	-	Upper and lower case alphabetical characters, numbers, half-width spaces, # @ - () :t
Municipality (L)	Text	Refer to Notes	-	32	-	Upper and lower case alphabetical characters, numbers, half-width spaces, # @ - () :t
Organization name (O)	Text	Refer to Notes	-	32	-	Upper and lower case alphabetical characters, numbers, half-width spaces, # @ - () :t
Organization unit name (OU)	Text	Refer to Notes	-	32	--	Upper and lower case alphabetical characters, numbers, half-width spaces, # @ - () :t
E-mail	Text	Refer to Notes	-	254	-	E-mail address format (RFC5321)

[1] Create new certificate

1. Enter input parameters shown as (1) in the image.

*Enter the same character string for the registration password and the registration password (for confirmation).

2. Click Generate (2) to generate a certificate. The certificate generated will be downloaded. Save the downloaded certificate to a file.



Note

- Certificates will only be downloaded once when first generated. You will not be able to redownload a certificate. If you could not save the certificate due to canceling the download, or for some other reason, you will need to generate a new certificate.

4.13.2 Create Certificate (Certificate Signature)

An item will appear for a certificate signature when selecting Certificate signature as the certificate format on the Generate Certificate screen.

Here you can generate and download new signatures using a CSR (certificate signing request).

Number	Entry name	Description	Notes
	Certificate format	Select the certificate format.	

	Export Password	Set when generating a certificate.	Refer to Chapter 4.13.2 (1).
	Verifying Export Password	Set when generating a certificate.	Refer to Chapter 4.13.2 (1).
	CSR file	Set when generating a certificate.	Refer to Chapter 4.13.2 (1).
	Browse button	Select a file and set the CSR file path.	Refer to Chapter 4.13.2 (1).
	Generate button	Generates the certificate.	Refer to Chapter 4.13.2 (1).

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Certificate format	Radio button	-	Yes	-	Certificate signature	Select from Create new certificate and the certificate signature.
Export Password	Text	Refer to Notes	Yes	8 to 16	-	Usable characters: Upper and lower case alphabetical characters, numbers, # @ - () : . _
Verifying Export Password	Text	Refer to Notes	Yes	8 to 16	-	Usable characters: Upper and lower case alphabetical characters, numbers, # @ - () : . _
CSR file	Text	Refer to Notes	Yes	254	-	Character strings available for use in a file path

[1] Create certificate signature

1. Enter the private key password (1).
2. Enter the registration password and the registration password (for confirmation) (2).
- * Enter the same character string for the registration password and the registration password (for confirmation).
3. Click Browse (3) and select the CSR file.
4. Click Generate (2) to generate a certificate. The certificate generated will be downloaded. Save the downloaded certificate to a file.



Note

- Certificates will only be downloaded once when first generated. You will not be able to redownload a certificate. If you could not download the certificate due to canceling the download, or for some other reason, you will need to generate a new certificate.

4.14 Common Screen

Click Common in the Main screen to display the Common screen.

The Common screen contains the MQTT settings screen, CORS setting screen and Error Correction setting screen.

4.14.1 MQTT Screen

You can change the MQTT password on the MQTT screen.

Number	Entry name	Description	Notes
(1)	User Name	Shows the MQTT user name.	Refer to Chapter 4.14.1 [1]
(2)	Password	Shows the current MQTT password.	Refer to Chapter 4.14.1 [1]
(3)	New Password	Set when updating the MQTT password.	Refer to Chapter 4.14.1 [1]
(4)	Change	Updates the MQTT password.	Refer to Chapter 4.14.1 [1]

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
New Password	Text	Refer to Notes	Yes	8 to 12	-	Usable characters: Upper and lower case alphabetical characters, numbers, # @ - () : . _

[1] Updating MQTT passwords

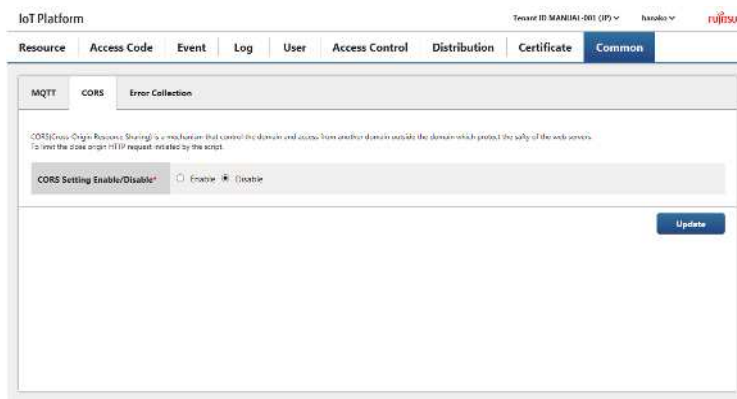
1. Enter the new password in (1) on the MQTT screen.

2. Click Change (2).

*The MQTT user name is the tenant ID and cannot be changed by the customer.

4.14.2 CORS Setting Screen

Configure CORS use settings on the CORS Settings screen.



Number	Entry name	Description	Notes
	Enable/disable CORS settings	Set to enable/disable CORS settings.	Refer to Chapter 4.14.2 [1]
	Update	Update CORS settings.	Refer to Chapter 4.14.2 [1]

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Enable/disable CORS settings	Radio button	-	Yse	-	-	Select from enable or disable. The initial display shows the current setting.

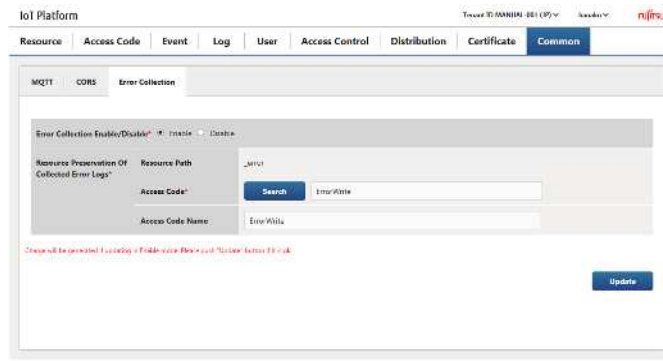
[1] Update CORS settings

1. Select enable/disable (1) CORS settings on the CORS Settings screen.
2. Click Update (2).



4.14.3 Error Correction Setting Screen

Configure error collection use settings on the Error Collection Settings screen.



Number	Entry name	Description	Notes
	Enable/disable error collection	Set to enable/disable CORS settings.	Refer to Chapter 4.14.3 (1)
	Collection storage resource	Set the resource path that collected error information is stored to.	
	Resource path	Displays the resource path that collected error information is stored to.	Fixed to _error.
	Search	Retrieve and set access codes for referencing error information on the Search Access Codes screen.	
	Access code	Displays access codes for referencing error information.	Read-only
	Access code name	Displays access code names for referencing error information.	Read-only
	Update	Update error collection settings.	Refer to Chapter 4.14.3 (1)

Notes on input parameters

Entry name	Entry format		Required	No. of characters	Initial display	Notes
	Input method	Character type				
Enable/disable error collection	Radio button	-	Yse	-	-	Select from enable or disable.
Access code	-	-	*	-	-	Entered by searching.
Access code name	-	-	*	-	-	Entered automatically from access code settings.

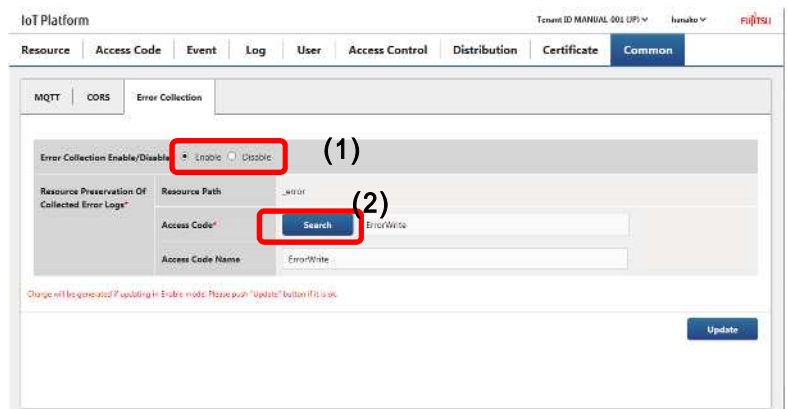
*Only required when error collection is enabled.

(1) Update error collection settings

- If error collection is enabled

1. Set error collection to Enable (1) on the Error Collection Settings screen.

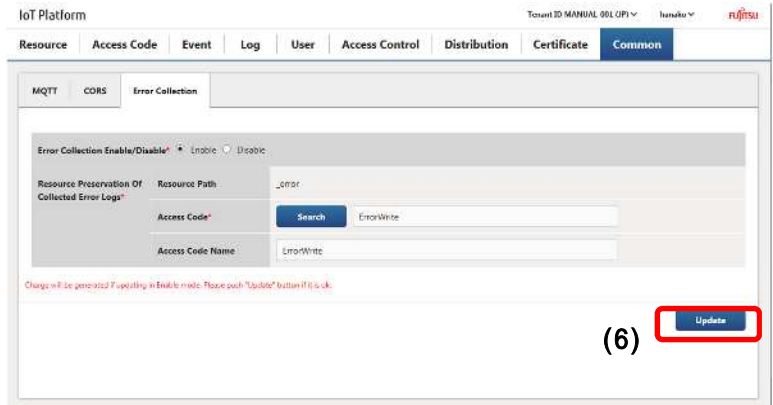
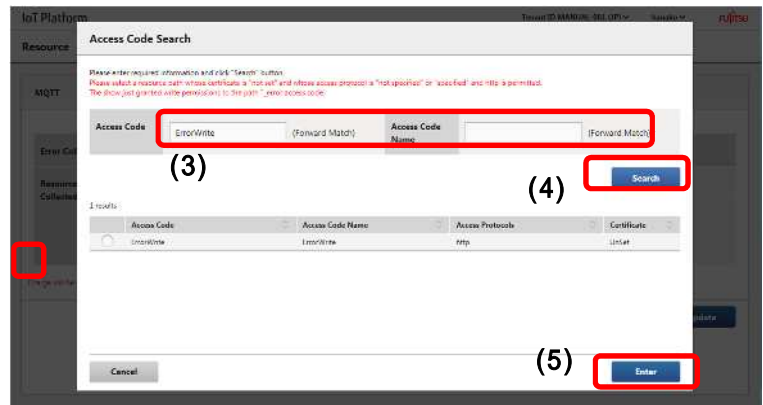
2. Click Search (2) to display the Search Access Codes screen.



3. On the Search Access Codes screen, enter the search conditions (3), and then click Search (4).

4. Select the access code used for error collection from the search results, and then click Enter (5).

5. Click Update (6) on the Error Collection Settings screen.



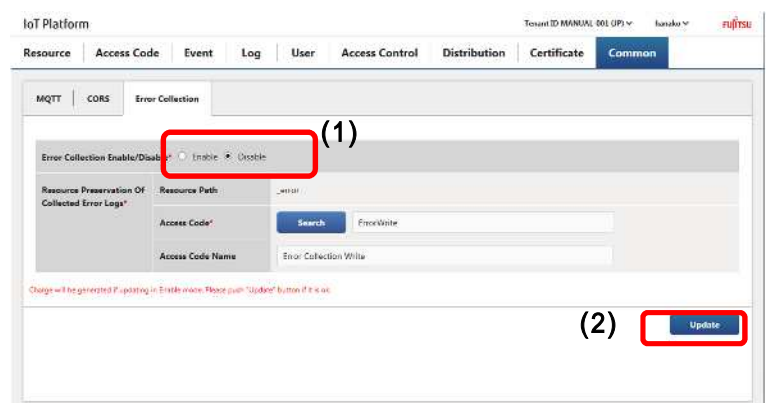
⚠️ Notes

- Only access codes for which U permissions have been granted for the error collection resource “_error”, added by the system when creating a new tenant, will be retrieved on the Search Access Codes screen that appears when clicking the Search button on the Error Collection Settings screen.
- Set the access code used for error collection to one with a specified HTTP protocol when the access protocol is set to “Do not specify” or “Specify”. Error collection cannot be performed if an access code that does not meet the above conditions is set.
- While access codes set as access codes to be used for error collection can be updated on the Update Access Codes screen, do not perform the following updates as doing so will prevent error collection.
 - Deleting U permissions for _error.
 - Deleting _error from the used resource list.

• Disabling error collection.

1. Set error collection to Disable (1) on the Error Collection Settings screen.

2. Click Update (2).



Chapter 5 Example of Settings Using the Service Portal

The following section provides examples of the basic tasks performed when using the Service Portal. Refer to relevant page for more information about screen item contents and operation procedures.

5.1 Sample Data

The examples provided here use an attendance management model as an example where information on employee positions and attendance information is collected from an attendance management app installed in smartphones.

Goals with this setup

- Send attendance and holiday statuses (attendance information) from the attendance management app installed in smartphones to the service
- Permit to write and reference information as to the person's whereabouts with the attendance management app
- Permit all personnels to reference attendance information, and to write personal attendance information exclusively by themselves
- Permit administrative personnel only to reference positional information, and all personnels to write personal positional information exclusively by themselves
- Send an email addressed to administrative personnel when attendance information shows a holiday.
- Call an API when positional information shows the person at a north latitude of 90 degrees.

An employee for which attendance management recorded:

Hanako Fujitsu (administrative personnel)

Taro Fujitsu (regular employee)

Jiro Fujitsu (regular employee)

Item	Sub-item	Setting value
Tenant ID		FJIOT-001
URI immediately before resource path		<Base URL>/v1/FJIOT-001/
Topic name		<Access code/v1/FJIOT-001/Resource path>
Resource 1	Resource Name	Attendance management (Hanako Fujitsu)
	Resource path	diligencs/status/hanako
	Comment	Administrative personnel
	Data format	JSON
	Data	Date(Date) :YYYYMMDD plan (Attendance status) :0: Attending, 1: Holiday JSONData image { "data": { "date": 20150601, "flag": 0 } }
Resource 2	Resource Name	Attendance management (Taro Fujitsu)
	Resource path	diligencs/status/taro
	Comment	Regular employee
	Data format	JSON
	Data	date(Date) , plan (Attendance status)
Resource 3	Resource Name	Attendance management (Jiro Fujitsu)

	Resource path	diligencs/status/jiro
	Comment	Regular employee
	Data format	JSON
	Data	diligencs/status/jiro
Resource 4	Resource Name	Positional management (Hanako Fujitsu)
	Resource path	location/hanako
	Comment	Administrative personnel
	Data format	JSON
	Data	lat(Latitude), lon(Longitude) { "location": { "lat": 30, "lon": 130 } }
Resource 5	Resource Name	Positional management (Taro Fujitsu)
	Resource path	location/taro
	Comment	Regular employee
	Data format	JSON
	Data	lat(Latitude), lon(Longitude)
Resource 6	Resource Name	Positional management (Jiro Fujitsu)
	Resource path	location/jiro
	Comment	Regular employee
	Data	lat(Latitude), lon(Longitude)
Resource 7 (Load resource)	Resource Name	Load resource
	Resource path	drc/load
	Comment	Application load
	Data format	JSON
	Data	Load status
Resource 8 (Recommend resource)	Resource Name	Recommend resource
	Resource path	drc/recommend
	Comment	Recommend
	Data format	JSON
	Data	Notification character string
Resource 9	Resource Name	Line 1
	Resource path	_bin/Line1/Camera
	Comment	Camera image
	Data format	Binary
	Data	Image data
Resource 10	Resource Name	IoT device S1
	Resource path	iot/machine/S1
	Comment	IoT device with certifications
	Data format	text
	Data	Machine data
Access code 1	Access Code	DiligencsManagement11111
	Access Code Name	Reference and update attendance status
	Comment	Anyone can reference and update all users' status
	Target resource	diligencs/status/hanako, diligencs/status/taro, diligencs/status/jiro
Access code 2	Access Code	LocationManagement22222

	Access Code Name	Update positional information (Hanako Fujitsu)
	Comment	Users can only update their own positional information
	Target resource	location/hanako
Access code 3	Access Code	LocationManagement33333
	Access Code Name	Update positional information (Taro Fujitsu)
	Comment	Users can only update their own positional information
	Target resource	location/taro
Access code 4	Access Code	LocationManagement44444
	Access Code Name	Update positional information (Jiro Fujitsu)
	Comment	Users can only update their own positional information
	Target resource	location/jiro
Access code 5	Access Code	LocationManagement55555
	Access Code Name	Reference positional information
	Comment	Only administrative personnel can reference
	Target resource	location/hanako, location/taro, location/jiro
Access code 6	Access Code	DRCLoad
	Access Code Name	Refer/update load information
	Comment	
	Target resource	drc/load
Access code 7	Access Code	DRCRecommend
	Access Code Name	Recommend
	Comment	
	Target resource	drc/recommend
Access code 8	Access Code	Line1Camera
	Access code name	Line 1 image
	Comment	Can update, delete and reference resources from an API
	Target resource	_bin/Line1/Camera
Access code 9	Access Code	SecureIoTMachine
	Access code name	IoT device with certifications
	Comment	Authenticate with certifications
	Target resource	iot/machine/S1
Access code 10	Access Code	ErrorRead
	Access code name	Reference error collection
	Comment	Access code for error collection reference
	Target resource	_error
Access code 11	Access Code	ErrorWrite
	Access code name	Register error collection
	Comment	Access code for registration of error collection
	Target resource	_error
Event 1	Event name	Holiday notification (Hanako Fujitsu)
	Comment	Notify Taro by email if Hanako is on holiday
	Target resource	diligencs/status/hanako
	Settings	Path position: data.flag Detection trigger: Numerical value: Match with 1 Action: Email: Send to taro@ml.css.fujitsu.com

Event 2	Event name	Holiday notification (Taro Fujitsu)
	Comment	If Taro is at a latitude of 90 degrees, call an API
	Target resource	location/taro
	Settings	Path position: location.lat Detection trigger: Numerical value: Match with 90 Action: Call API
Service Portal access control 1	Permitted IP address (start)	10.20.30.1
	Permitted IP address (stop)	10.20.30.200
	User ID	hanako
Access code access control	Permitted IP address (start)	10.10.20.10
	Permitted IP address (stop)	10.10.20.100
	Access Code	LocationManagement22222
Distribution common settings	Recommendation cycle	60
	Calculating period	120
Load resource	Resource path	drc/load
Recommend resource	Resource path	drc/recommend
	tps/bps selection	tps
	Edge computing condition	Character type: Numerical values Condition : 90 Judgment : Or more Notification character string: START
	Above-mentioned resolatory condition	Character type: Numerical values Condition : 50 Judgment : Or less Notification character string: END
Certificate (new)	PEM pass phrase	passphrase
	Export Password	password
	Public key length	2048bit
	Period of validity	365
	Common name (CN)	iotMachine_s1
	Country (C)	JP
	Prefecture (ST)	Tokyo
	Municipality (L)	Kamata
	Organization name (O)	Fujitsu
	Organization unit name (OU)	IoT
	E-mail	mail-iot@iot.com

Actual Use of the Above Model

5.2.1 Login

Service Portal URL will be notified after the service contract. Access this portal from a PC connected to the Internet.

- 1 . Enter the user ID into (1).
2. Enter your password into (2).
3. Click Login.



Log in using the user ID and password provided after the service contract.

5.2.2 Add Resources

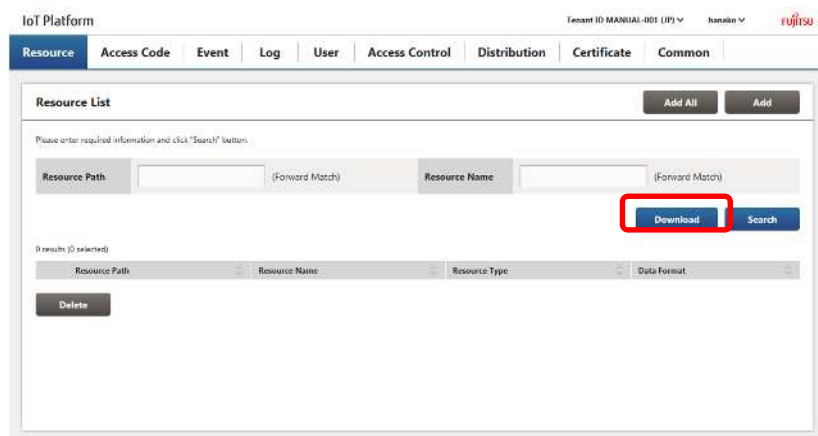
In this section, the process used to add resources using the Add All function is explained. Refer to Chapter 4.6 for more information regarding other functions relating to resources.

- 1 . Click "Resource" in the Main screen.



*Refer to Chapter 4.5.1 for more information about the Main screen.

2. Click Download to download the CSV format template used for batch adding resources and save it to the PC using the Service Portal.

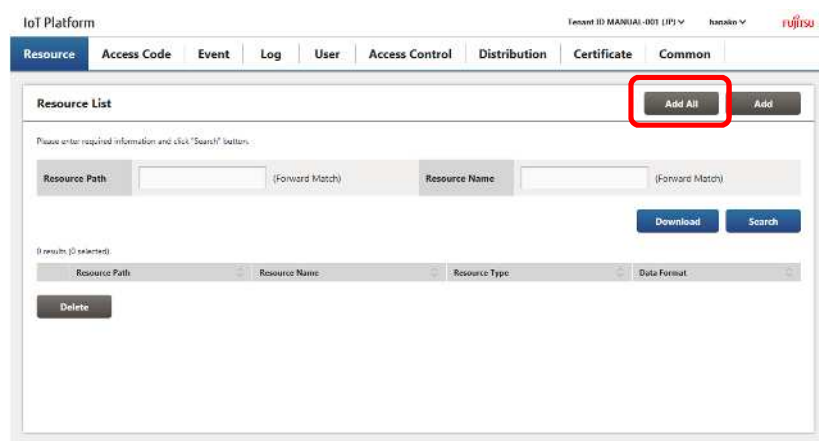


3. Edit and save the downloaded template.

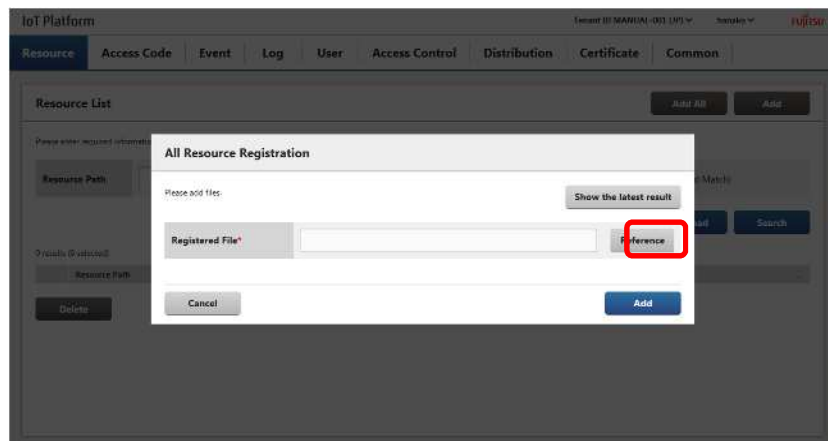
Resource path	Resource Name	Data format	Comment	Retention period	Resource type
diligencs/status/hanako	Attendance management (Hanako Fujitsu)	1	Administrative personnel	1	1
diligencs/status/taro	Attendance management (Taro Fujitsu)	1	Regular employee	1	1
diligencs/status/jiro	Attendance management (Jiro Fujitsu)	1	Regular employee	1	1

location/hanako	Positional management (Hanako Fujitsu)	1	Administrative personnel	1	1
location/taro	Positional management (Taro Fujitsu)	1	Regular employee	1	1
location/jiro	Positional management (Jiro Fujitsu)	1	Regular employee	1	1
drc/load	Load resource	1	Load status	1	1
drc/recommend	Recommend resource	1	Recommend	1	1
_bin/Line1/Camera	Line 1	2	Camera image	1	1
iot/machine/S1	lot device S1	1	Including IoT device certificate	1	1

4. Click Add All.



5. Click Reference and select the CSV file saved in step 3.



6. Click Add.

7. Check the confirmation message, and then click OK.

8. Confirm that there are no problems with the contents of the resource added when this information appears.

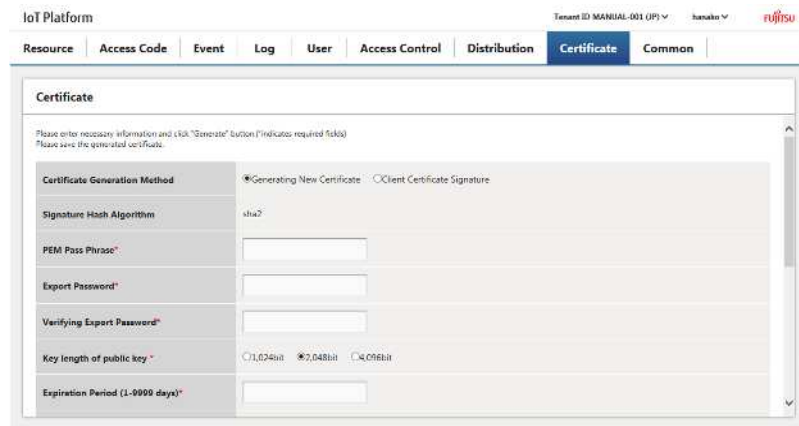
5.2.3. Generate Certificates

In this section, the process used to generate a new certificate using the Generate Certificate function is explained. Refer to Chapter 4.13 for more information regarding other functions relating to resources.

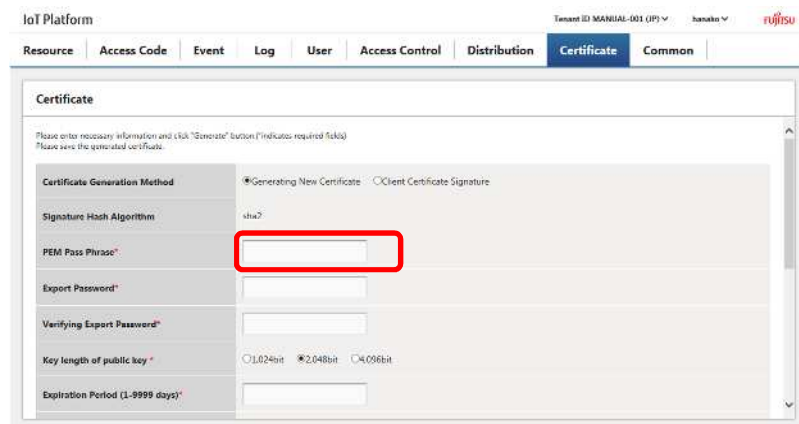
1. Click Generate Certificate in the Main screen.



2. Select Create New Certificate according to the certificate format on the Generate Certificate screen.

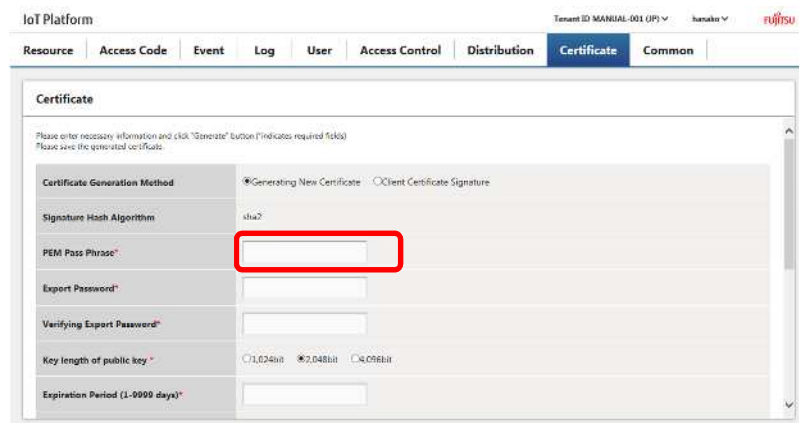


3. Enter PEM pass phrase.



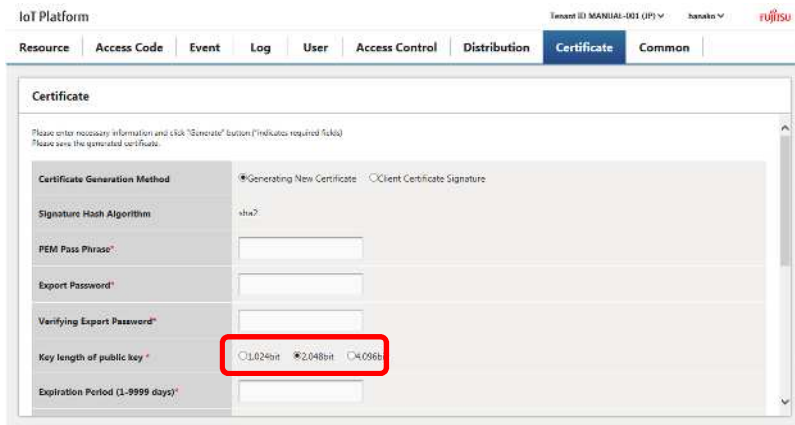
Example: passphrase

4. Enter Export Password. Enter the same password in Verifying Export Password for confirmation.



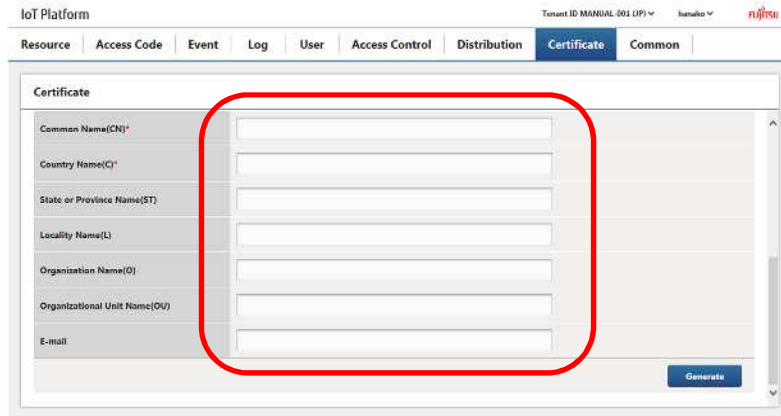
Example: password

5. Select the public key length.



Example: 2,048bit

5. Enter Period of validity, Common name, Country, Prefecture, Municipality, Organization name, Organization unit name, and Email.



Example:

Period of validity: 365

Common name: iotMachine_s1

Country: JP

Prefecture: Tokyo

Municipality: Kamata

Organization name: Fujitsu

Organization unit name: IoT

Email: mail-iot@iot.com

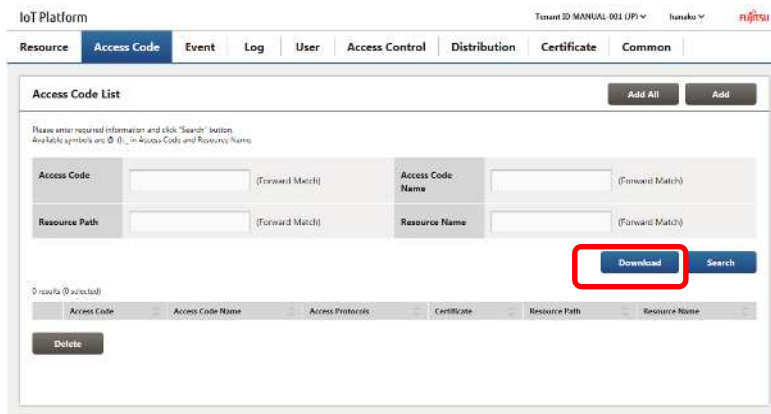
5.2.4. Add Access Codes

In this section, the process used to add access codes using the Add All function is explained. Refer to Chapter 4.7 for more information regarding other functions relating to access codes.

1. Click "Access Code" in the Main screen.



2. Click Download to download the CSV format template used for batch adding resources and save it to the PC using the Service Portal.



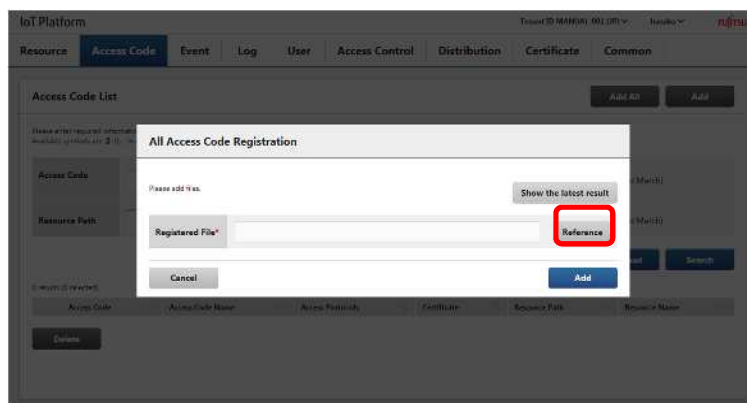
3. Edit and save the downloaded template.

Access Code	Access Code Name	Comment	Access protocol	Resource path 1	Access permission 1	Resource path 2	Access permission 2	...
DiligenceManagement11111	Reference and attendance status update	Anyone can reference and update all users' status		diligence/status/hanako	RU	diligence/status/taro	RU	diligence/status/jiro
LocationManagement22222	Update positional information (Hanako Fujitsu)	Users can only update their own positional information		location/hanako	RU			
LocationManagement33333	Update positional information (Taro Fujitsu)	Users can only update their own positional information		location/taro	RU			
LocationManagement44444	Update positional information (Jiro Fujitsu)	Users can only update their own positional information		location/jiro	RU			
LocationManagement55555	Reference positional information	Only administrative personnel can reference		location/hanako	R	location/jiro	R	
DRCLoad	Refer/update load information			drc/load	RU			
DRCRecommend	Recommend			drc/recommend	RU			
Line1Camera	Line 1 image	Can update, delete and reference resources from an API		_bin/Line1/Camera	CDLRU			
SecureIoTMachine	IoT device including	Authorize by certificate		iot/machine/51	RU			

	certificate				
ErrorRead	Reference error correction	Error correction access code	http	_error	R
ErrorWrite	Register error correction	Error correction access code	http	_error	U

4. Click Add All.

5. Click Reference and select the CSV file saved in step 3.



6. Click Add.

7. Check the confirmation message, and then click OK.

8. Confirm that there are no problems with the contents of the access code added when this information appears.

5.2.5. Integrating APIs into the Application

After resources and access codes have been added, data can be written to resources and referenced by using APIs made available by this service.

Refer to the "IoT Platform User Guide" for more information about API specifications.

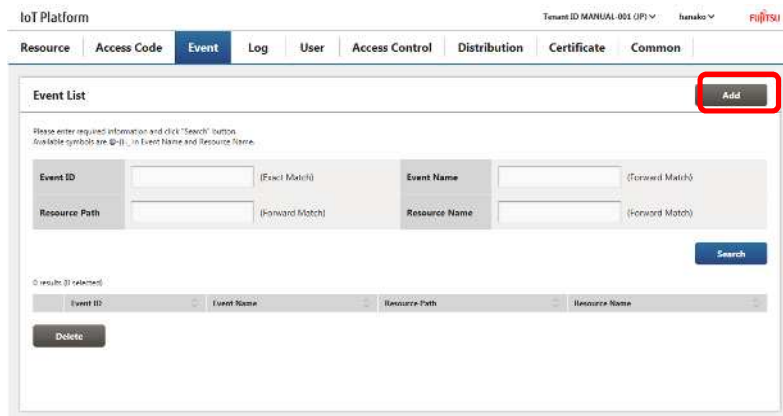
5.2.6. Event Function (Email) Settings

This section describes how to configure "Event 1" settings by adding an event using the model described in 5.1.

1. Click "Event" in the Main screen.



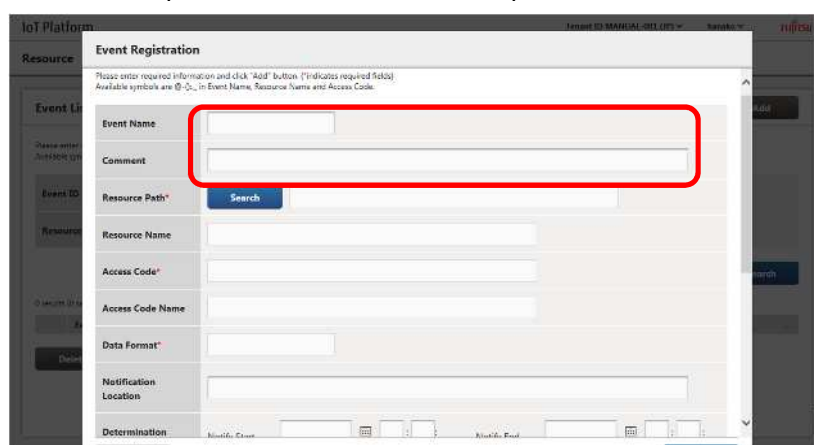
2. Click "Add".



3. Enter the event name and comment.

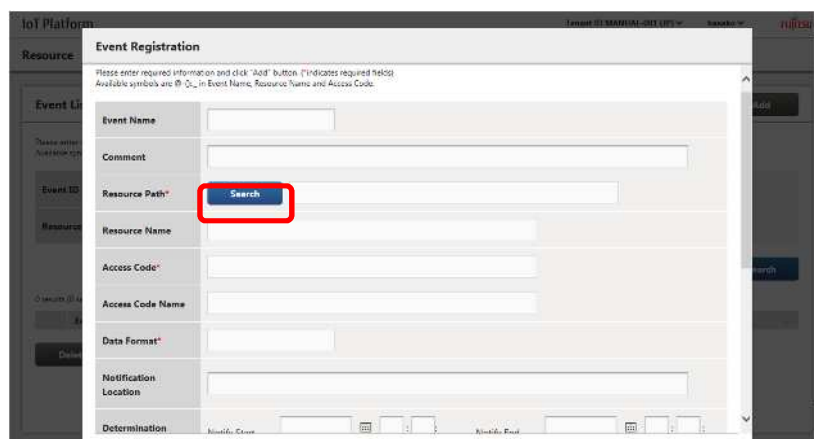
Event name: Holiday notification (Hanako Fujitsu)

Comment: Notifies Taro by email if Hanako is on holiday.

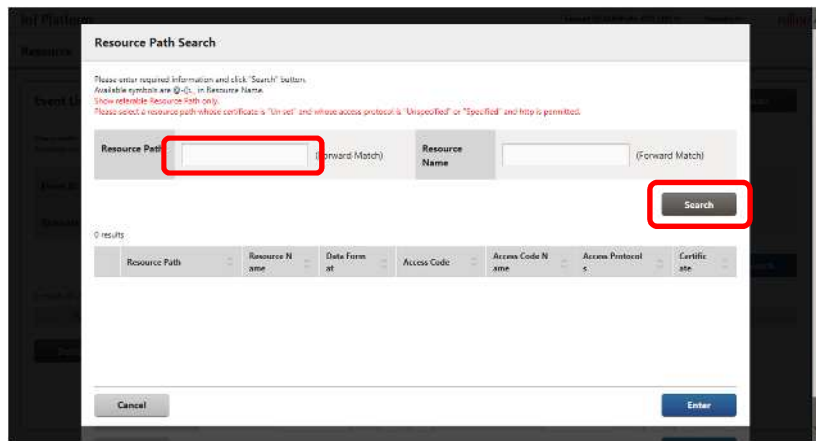


4. Assign a resource as the resource target.

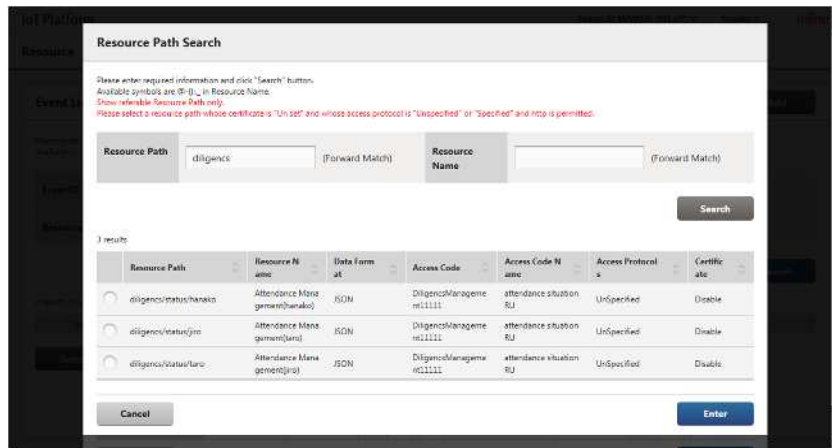
4-1. Click "Search" next to the resource path item.



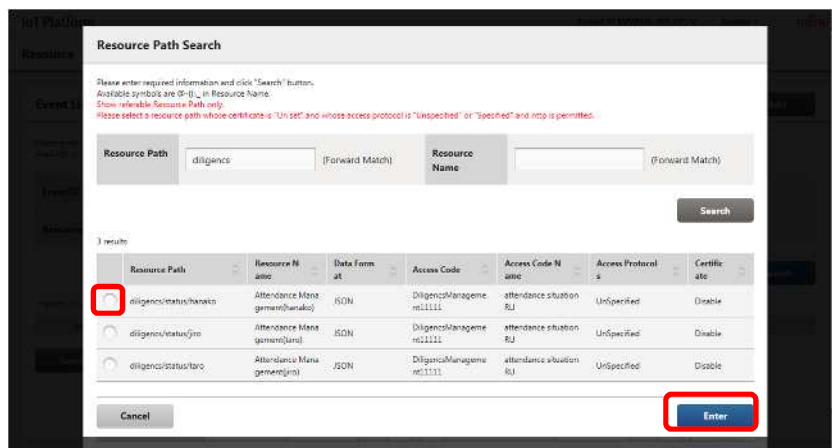
4-2. Enter "diligens" as the resource path and click Search.



4-3. Paths containing "diligens" as the start of the resource path will appear below in the search results.



4-4. Select the resource: diligens/status/hanako with the access code: diligensManagement11111 and click "Enter".



5. After clicking Enter, "Resource name: Attendance management (Hanako Fujitsu)", "Access code: DiligensManagement11111", "Access code name: Reference and update attendance status" will be filled out automatically.

6. Enter the "Data Path". Input the data position in JSONPath format.

Enter data.flag in this example.

The screenshot shows the 'Event Registration' form in the IoT Platform. The 'Notification Location' field is highlighted with a red rectangle and contains the text 'data.flag'. Other fields include 'Resource Path' (diligence/status/hanako), 'Resource Name' (Attendance Management(hanako)), 'Access Code' (DiligenceManagement11111), 'Access Code Name' (attendance situation RU), and 'Data Format' (JSON). The 'Determination' section has 'Notify Start Time' and 'Notify End Time' fields, but they are not yet configured.

7. Enter a time range for detection conditions. This setting is not configured in this case.

This screenshot is similar to the previous one, but the 'Determination' section is highlighted with a red rectangle. It shows the 'Notify Start Time' and 'Notify End Time' fields, which are currently empty, indicating that a time range for detection conditions has not yet been entered.

8. Set detection conditions. In this example, enter "select numerical value, enter 1, and select match".

This screenshot shows the 'Determination' section of the form highlighted with a red rectangle. The dropdown menu is open, showing options for setting detection conditions. The instruction indicates that the user should select 'select numerical value', enter '1', and select 'match'.

9. Set resolutive conditions. This setting is not configured in this case. Refer to Chapter 3.6.3 for more information about resolutive condition specifications.

The screenshot shows the 'Event Registration' form in the IoT Platform. The 'Resource Path' is 'diligence/status/hanako'. The 'Resource Name' is 'Attendance Management(hanako)'. The 'Access Code' is 'DiligenceManagement11111'. The 'Access Code Name' is 'attendance situation RU'. The 'Data Format' is 'JSON'. The 'Notification Location' is 'data.fag'. The 'Determination' section has 'Notify Start Time' and 'Notify End Time' fields. The 'Cancellation' dropdown menu is highlighted with a red box.

10. Configure action settings. Select Email in this example.

The screenshot shows the 'Event Registration' form with the 'Action' dropdown menu set to 'Email'. The 'Email Address', 'Subject', and 'Body' fields are visible below the dropdown. The 'Action' dropdown is highlighted with a red box.

11. Enter the email address, title and text.

The screenshot shows the 'Event Registration' form with the 'Email Address', 'Subject', and 'Body' fields highlighted with a red box. The 'Action' dropdown is still set to 'Email'.

12. Click Add at the bottom of the window.

The image shows a software interface for 'Event Registration'. The form is divided into several sections:

- Notification Location:** A text input field containing 'data Reg'.
- Determination:** Two date/time pickers labeled 'Notify Start Time' and 'Notify End Time'.
- Determination:** Two dropdown menus.
- Cancellation:** Two dropdown menus.
- Action:** A dropdown menu currently set to 'Email'.
- Email Address:** A text input field.
- Subject:** A text input field.
- Body:** A large text area for entering the email content.

At the bottom of the form, there are two buttons: 'Cancel' on the left and 'Add' on the right. The 'Add' button is highlighted with a red rectangular box.

13. Click OK when the Confirmation screen appears to add event settings.

5.2.7. Email Receipt Confirmation When an Event (Email) Occurs

Check that an email is sent after the data writing API is called.
An email like the following will be sent to the address.

Sender: eventinfo@sys.iot.jp.fujitsu.com
Address/title/text: Address/title/text set for the event
Attachment: eventinfo.txt
Attachment contents: JSON format similar to that shown below.

```
{  
  "event ID " : " 123456789abc " ,  
  "operation " : " update " ,  
  "date " : " 20141225T103612.001+0900 " ,  
  "resoucepath " : " diligencs/status/hanako " ,  
  "message " : { "data": { "date": 20150601, "flag": 1 } }  
}
```

- *eventID: A 12 digit event ID automatically assigned by the system.
- operation: Operations occurring with the resource path that the target event is referring to.
- Date: The time of the event.
- Resourcepath: The resource path that the target event is referring to.
- Message: Resource data content at the time of the event.

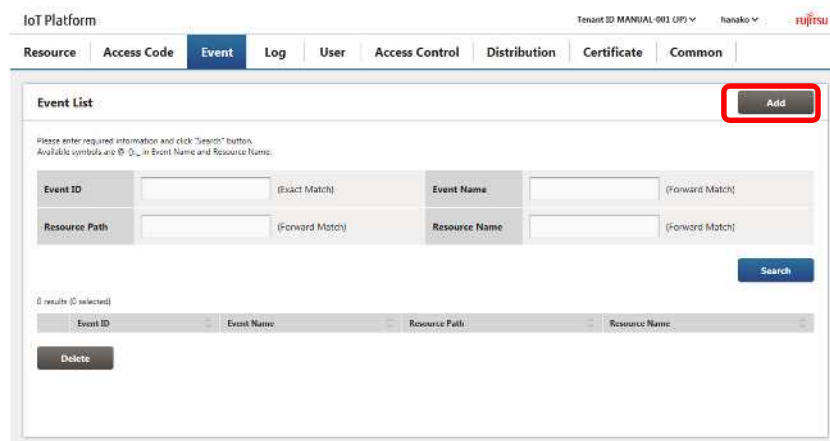
5.2.8. Event Function (Call API) Settings

This section describes how to configure "Event 2" settings by adding an event using the model described in 5.1.

- 1 . Click "Event" in the Main screen.



2. Click "Add".



3. Enter the event name and comment.

Event name: Holiday notification (Taro Fujitsu)

Comment: Call API if Taro is at a latitude of 90 degrees

The screenshot shows the 'Event Registration' form in the IoT Platform console. The form includes fields for 'Event Name', 'Comment', 'Resource Path*', 'Resource Name', 'Access Code*', 'Access Code Name', 'Data Format*', 'Notification Location', and 'Determination'. The 'Event Name' and 'Comment' fields are highlighted with a red box.

4. Assign a resource as the resource target.

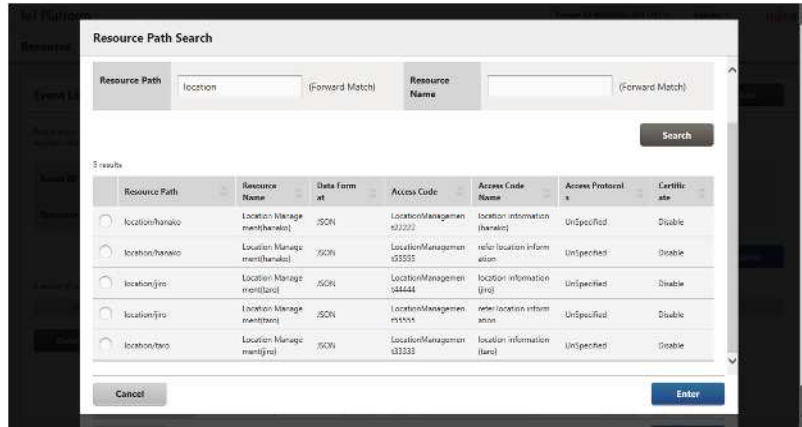
4-1. Click Search next to the resource path item.

The screenshot shows the 'Event Registration' form in the IoT Platform console. The 'Search' button next to the 'Resource Path*' field is highlighted with a red box.

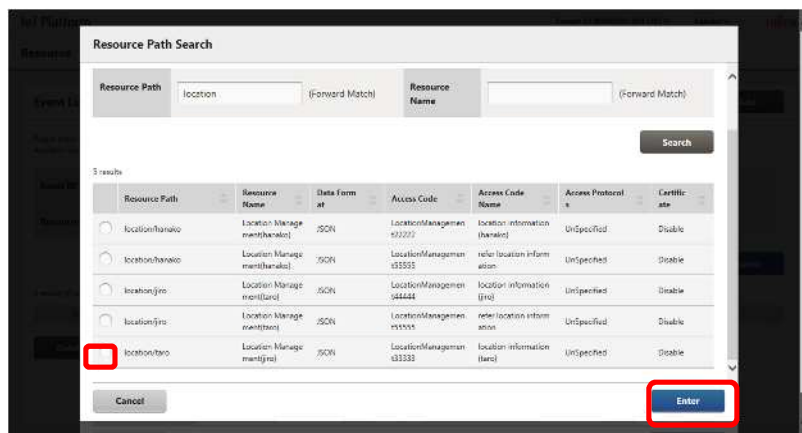
4-2. Enter "location" as the resource path and click Search.

The screenshot shows the 'Resource Path Search' dialog box in the IoT Platform console. The 'Resource Path' field and the 'Search' button are highlighted with red boxes.

5. Paths containing "location" as the start of the resource path will appear below in the search results.



6. Select the resource: location/taro with the access code: LocationManagement33333 and click "Enter".



7. After clicking Enter, "Resource name: Positional management (Taro Fujitsu)", "Access code: LocationManagement33333", "Access code name: "Positional information update (Taro Fujitsu)" will be filled out automatically.

Memo

- Resources without an access code cannot be selected.
- Resources with an access code, but without an R permission, or not under the resource with a G permission, cannot be selected. If permissions not set, modify the access code settings from the access code menu (Chapter 4.7.5 (3)).

8. Enter the "Data Path". Input the data position in JSONPath format. In this example, location.lat is used.

IoT Platform

Event ID MANUAL 001 (01)

Resource

Event List

Event ID

Resource

Event Registration

Resource Path* Search location/taro

Resource Name Location Management(jro)

Access Code* LocationManagement33333

Access Code Name location information(taro)

Data Format* JSON

Notification Location location.lst

Determination Notify Start Time ~ Notify End Time

Determination

Cancellation

9. Enter a time range for detection conditions. This setting is not configured in this case.

IoT Platform

Event ID MANUAL 001 (01)

Resource

Event List

Event ID

Resource

Event Registration

Resource Path* Search location/taro

Resource Name Location Management(jro)

Access Code* LocationManagement33333

Access Code Name location information(taro)

Data Format* JSON

Notification Location location.lst

Determination Notify Start Time ~ Notify End Time

Determination

Cancellation

10. Set detection conditions. In this example, enter "select numerical value, enter 90, and select match".

IoT Platform

Event ID MANUAL 001 (01)

Resource

Event List

Event ID

Resource

Event Registration

Resource Path* Search location/taro

Resource Name Location Management(jro)

Access Code* LocationManagement33333

Access Code Name location information(taro)

Data Format* JSON

Notification Location location.lst

Determination Notify Start Time ~ Notify End Time

Determination

Cancellation

11. Set resolutive conditions. This setting is not configured in this case. Refer to Chapter 3.6.3 for more information about resolutive condition specifications.

Event Registration

Resource Path*

Resource Name

Access Code*

Access Code Name

Data Format*

Notification Location

Determination Notify Start Time Notify End Time

Determination

Cancellation

12. Configure action settings. Select API caller in this example. The following screen will appear when API is selected.

Event Registration

Action*

URI*

Method*

Authentication ID	<input type="text"/>	Authentication Password	<input type="text"/>
Field Name1	<input type="text"/>	Field Value1	<input type="text"/>
Field Name2	<input type="text"/>	Field Value2	<input type="text"/>
Field Name3	<input type="text"/>	Field Value3	<input type="text"/>
Field Name4	<input type="text"/>	Field Value4	<input type="text"/>
Field Name5	<input type="text"/>	Field Value5	<input type="text"/>
Field Name6	<input type="text"/>	Field Value6	<input type="text"/>

13. Configure API settings. Configure API settings based on the API specifications set by the customer.

14. Click Add at the bottom of the window. Click OK on the Confirmation screen to add event settings.

Event Registration

Field Name3	<input type="text"/>	Field Value3	<input type="text"/>
Field Name4	<input type="text"/>	Field Value4	<input type="text"/>
Field Name5	<input type="text"/>	Field Value5	<input type="text"/>
Field Name6	<input type="text"/>	Field Value6	<input type="text"/>
Field Name7	<input type="text"/>	Field Value7	<input type="text"/>
Field Name8	<input type="text"/>	Field Value8	<input type="text"/>
Field Name9	<input type="text"/>	Field Value9	<input type="text"/>
Field Name10	<input type="text"/>	Field Value10	<input type="text"/>

Body

5.2.9. Access Control Settings

- This section includes details on the anticipated methods of use

[1] Service Portal access controls

This section describes how to add settings to restrict PCs able to log into the Service Portal using the user ID used in 5.2.1.

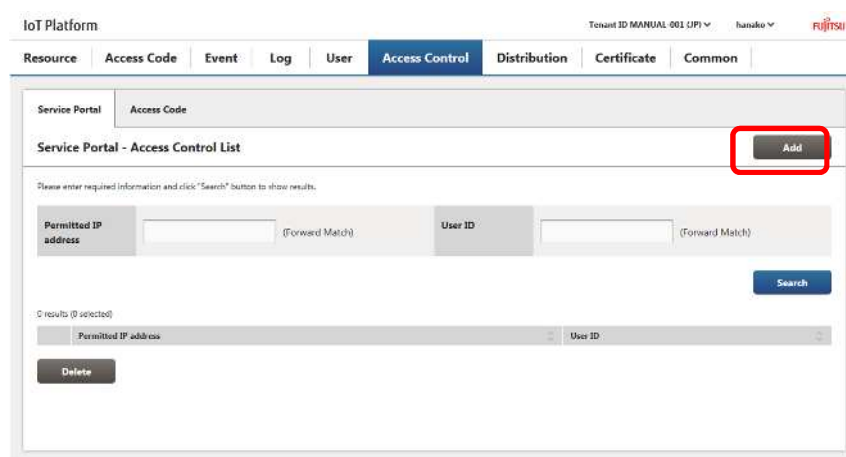
1 . Click "Access Control" on the Main screen.



The Service Portal Access Control screen will appear.

*Refer to Chapter 4.5.1 for more information about the Main screen.

2. Click Add on the Service Portal Access Control screen.



3. Enter the permitted IP address. Enter one of the following.

- a. Enter the first permitted IP address and leave the stop field blank.
- b. Or, enter the permitted IP address range to include the PC being granted access.

Example: If the IP address of the PC being permitted access is 10.20.30.100

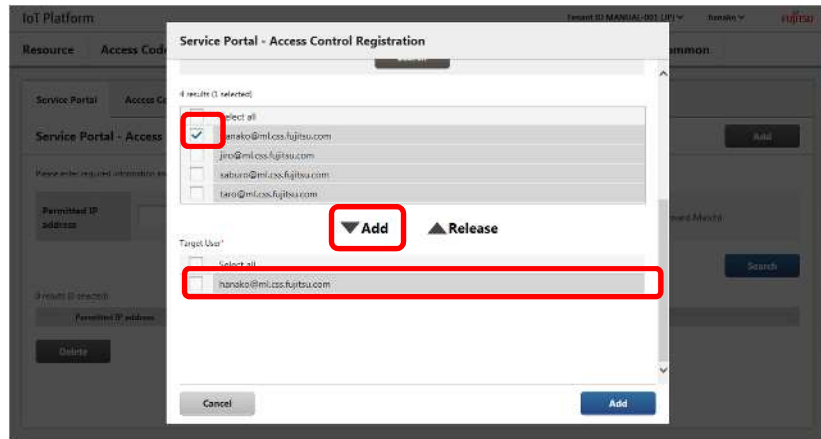
Start: 10.20.30.1

Stop: 10.20.30.200

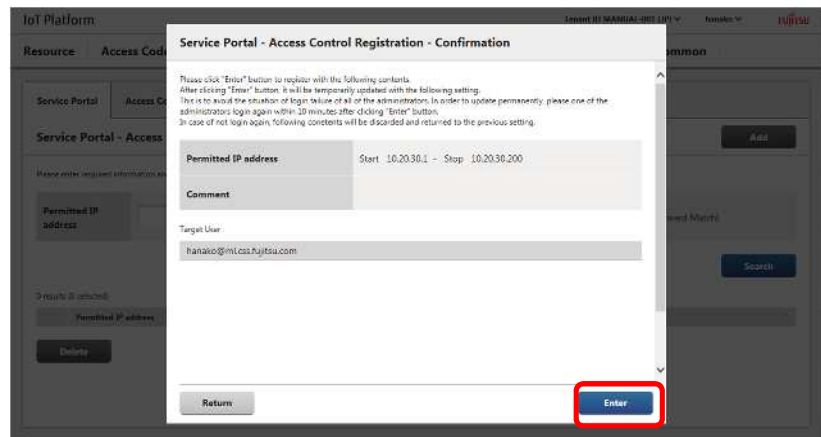
4. Enter the user ID (can also be left blank) and click Search on the Service Portal - Access Control Registration screen.

5. Select the user ID check box for the user (hanako) you prefer to permit access from the search results, and then click Add.

The selected user ID will be moved to the Target User list.



6. Click Add at the bottom of the screen to display the Confirmation screen. Use the Confirmation screen to confirm changes. If this is correct, click Enter.



7. Login again with a user ID that has been permitted access within 10 minutes to enable the Service Portal access controls added.

[2] Access code access controls

This section describes how to add settings to restrict devices permitted access for access codes added in 5.2.4.

1 . Click "Access Control" on the Main screen.



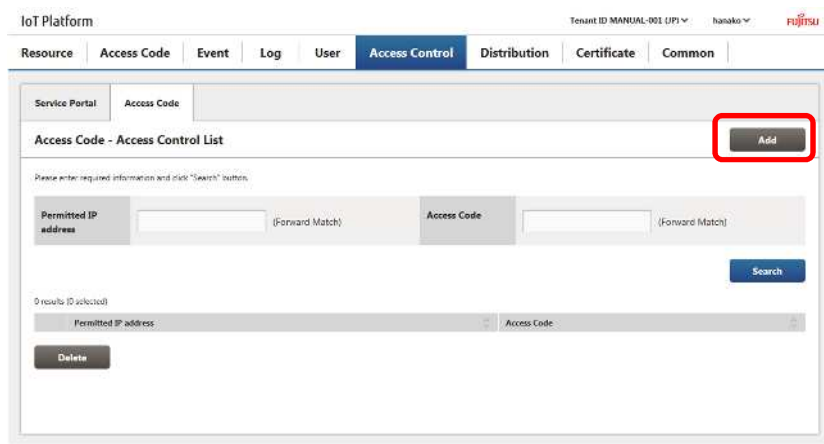
*Refer to Chapter 4.5.1 for more information about the Main screen.

2. Click the Access Code tab.



The Access Code - Access Control screen will appear.

3. Click Add on the Access Code - Access Control screen.



4. Enter the permitted IP address. Enter one of the following.

- a. Enter the first permitted IP address and leave the stop field blank.
- b. Enter the start and stop permitted IP address range to include the device being granted access.

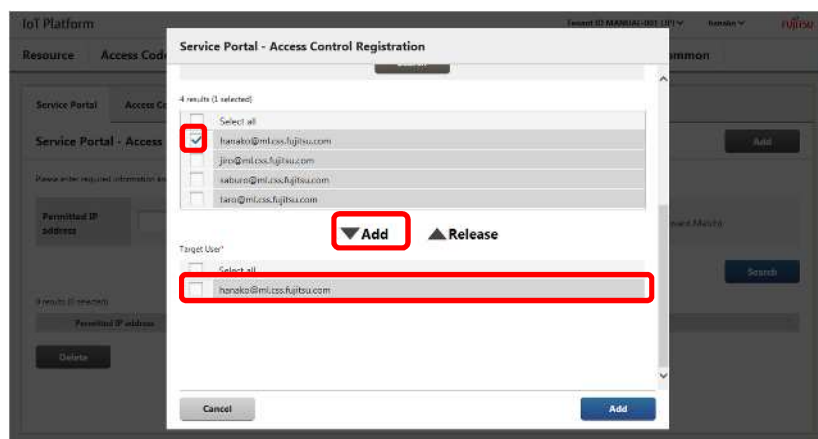
Example: If the IP address of the device being permitted access is 10.10.20.50

Start: 10.10.20.10

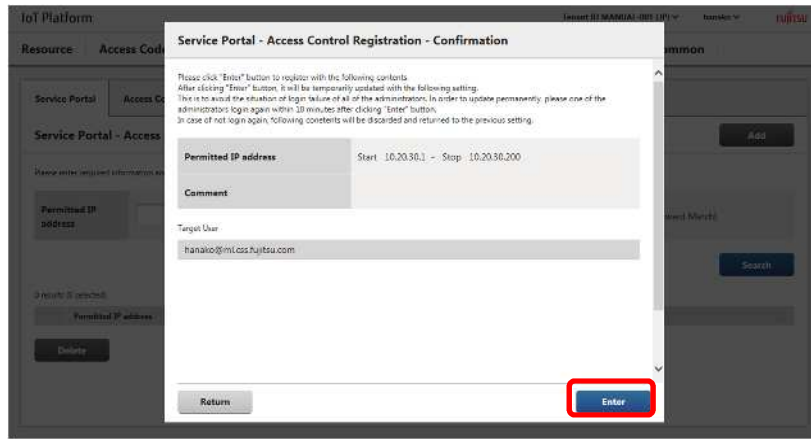
Stop: 10.10.20.100

5. Enter the access code (can also be left blank) and click Search on the Access Code Control Registration screen to display search results at the bottom of the screen.

6. Select the check box for the access code (LocationManagement22222 in this example) you prefer to permit access from the search results, and then click Add. The selected access code will be moved to the Target Access Code list.



7. Click Add at the bottom of the screen to display the Confirmation screen. Use the Confirmation screen to confirm changes. If this is correct, click Enter.



5.2.10. Distribution Settings

This section describes how to add distribution settings.

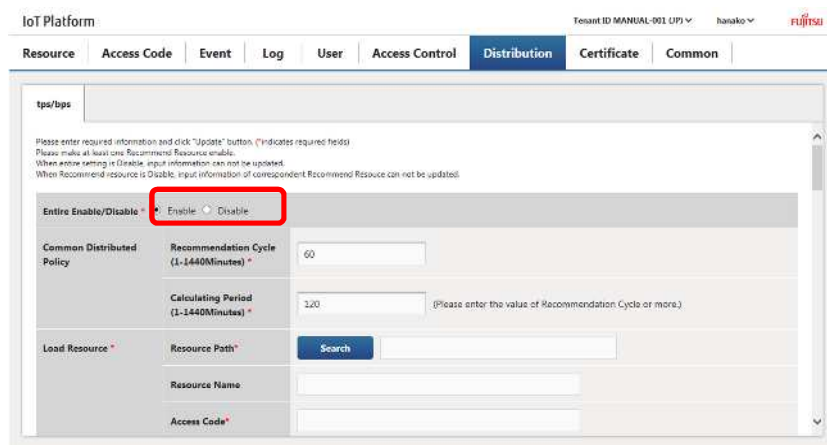
1. Click "Distribution" on the Main screen.



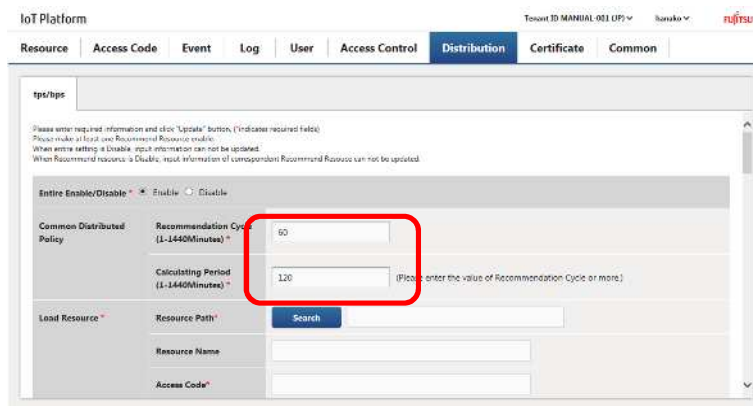
*Refer to Chapter 4.5.1 for more information about the Main screen.

The tps/bps distribution settings screen will appear at the bottom of the screen.

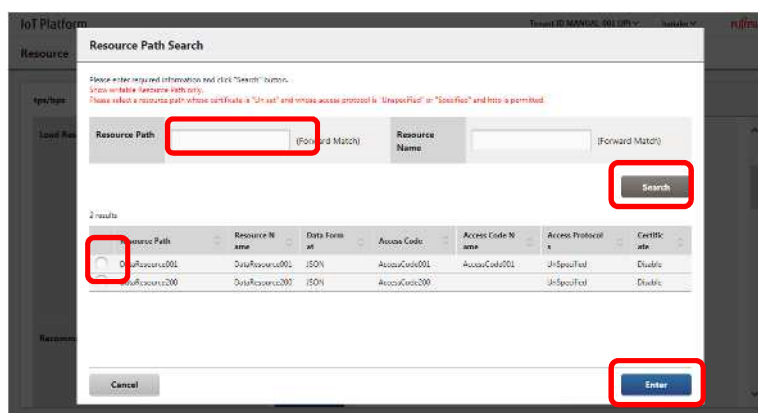
2. Select Enable for the Entire Enable/Disable radio button.



3. Enter a common distributed policy.
 Recommendation cycle: 60
 Calculating period: 120

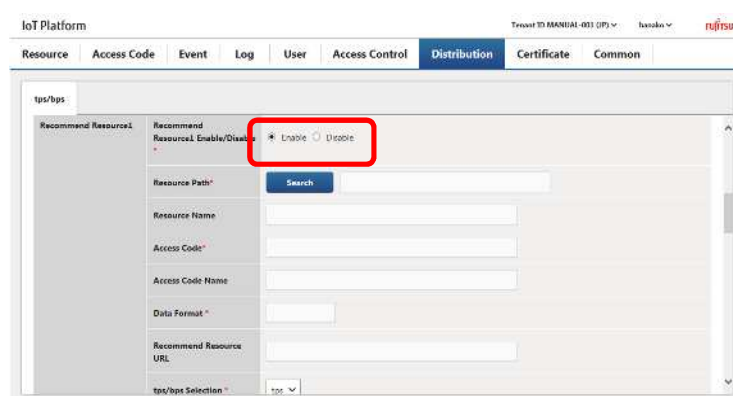


4. Click Search to the right of the load resource to display the Resource Path Search screen. Enter drc for the resource path and perform a search, and then select the resource path assigned as the load resource (drc/load) and click the Enter button.



Information pertaining to the selected resource path will appear in the fields from the resource path for the load resource to the load resource URL. Check this information before proceeding.

5. Select Enable for the recommend resource 1 Enable/Disable radio button.



6. Click Search to the right of recommend resource 1 to display the Resource Path Search screen. Perform a search, and then select the resource path assigned as the recommend resource 1 (drc/recommend) and click the Enter button.

*The Resource Path Search screen is the same as the screen shown in 4.

Information pertaining to the selected resource path will appear in the fields from the resource path for

recommend resource 1 to the recommend resource URL. Check this information before proceeding.

7. Set the edge computing condition for recommend resource 1.

Example: If edge computing is set to start for values 90 and over.

Character type: Numerical values

Condition: 90

Judgment: Or more

Notification character string: START (*)

*: As this character string is used to send notifications to the app performing edge computing, a character string that matches the app must be entered.

8. Set the edge computing resolutory condition for recommend resource 1. Refer to the following as an example setting.

Example: If edge computing is set to be stopped for values 50 and under.

Character type: Numerical values

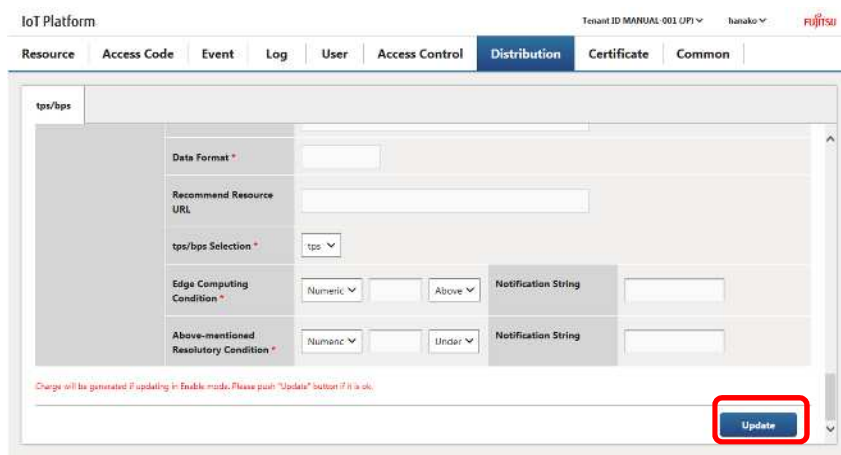
Condition: 50

Judgment: Less than

Notification character string: END (*)

*: As this character string is used to send notifications to the app performing edge computing, a character string that matches the app must be entered.

9. Click Update on the bottom of the screen. This updates the distribution policy with the information entered.



5.2.11. MQTT Settings

In this section, the process used to set MQTT password is explained. Settings are not required when you do not use MQTT, and do not need to change the password.

1. Click "Common" on the Main screen.



*Refer to Chapter 4.5.1 for more information about the Main screen.

2. Enter MQTT password, and click Change. This updates the MQTT password with the information entered.

The screenshot shows the 'MQTT' configuration page in the IoT Platform. The page has a navigation bar with tabs: リソース, アクセスコード, イベント, ログ, ユーザー, アクセス制限, 分散設定, 証明書生成, and 共通設定. The 'MQTT' tab is selected. Below the navigation bar, there are sub-tabs: MQTT, CORS, and エラー-収集. The main content area contains a form with the following fields:

User Name	MANUAL-001
Password	Gp1ZAh0X
新 Password*	<input type="password"/>

A red box highlights the '新 Password*' input field. Another red box highlights the '変更' (Change) button located at the bottom right of the form.

Example: mqttpass

5.2.12. CORS settings

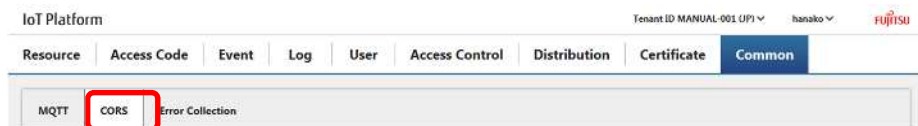
In this section, the process used to set CORS as enabled and disabled is explained.

1. Click "Common" on the Main screen.



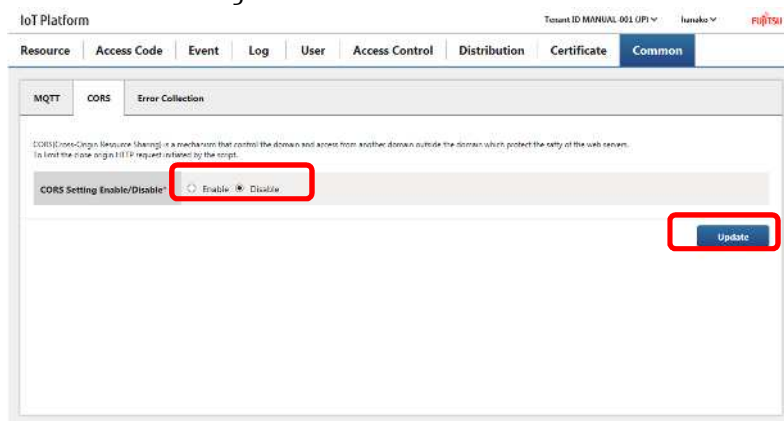
*Refer to Chapter 4.5.1 for more information about the Main screen.

2. Click the CORS tab.



The CORS settings screen will appear.

3. Select Enable when you prefer to use CORS, and Disable when you do not prefer to use CORS, and then click Change. This updates the CORS settings with the information entered.



Example: Disable

5.2.13. Error Collection Settings

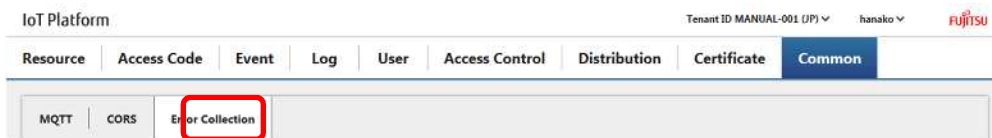
In this section, the process used to set Error Collection Settings is explained.

1. Click "Common" on the Main screen.



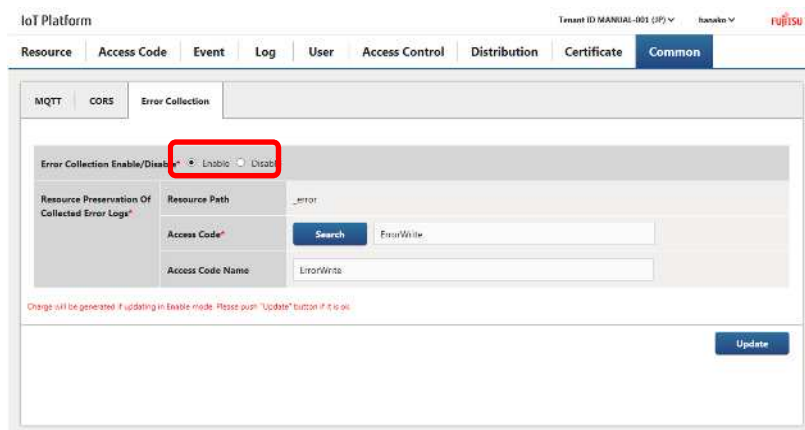
*Refer to Chapter 4.5.1 for more information about the Main screen.

2. Click the Error Collection tab.



The Error Collection settings screen will appear.

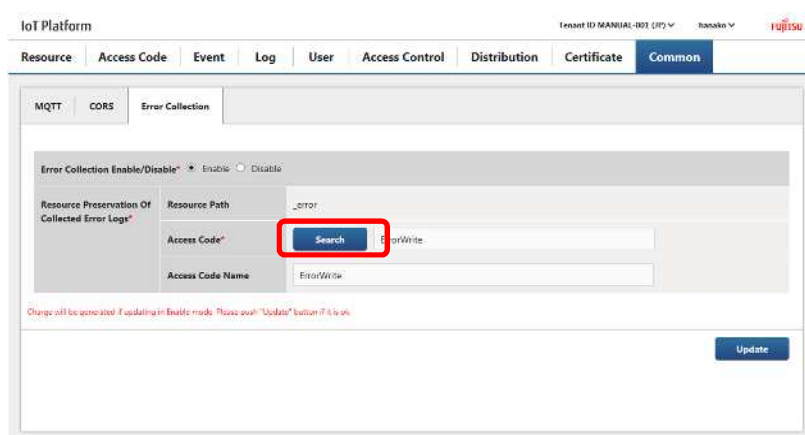
3. Select Error Collection Enable/Disable. Select Enable when you prefer to use Error Collection, and Disable when you do not prefer to use Error Collection.



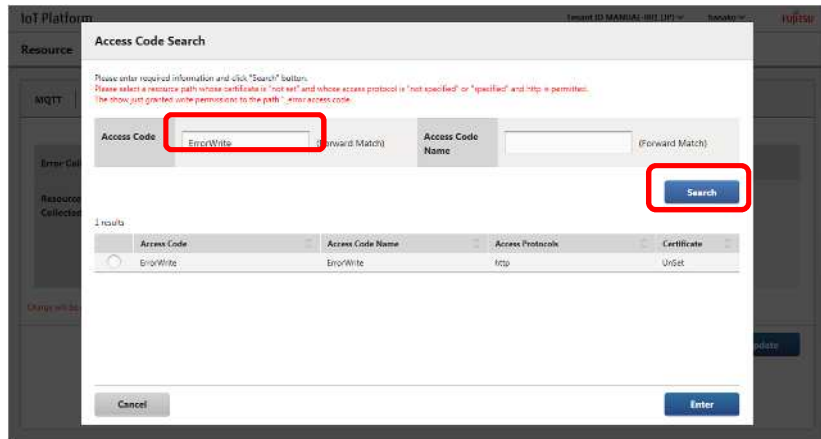
Example: Enable

4. Set the access code to the error collection resource "_error" you prefer to write in.

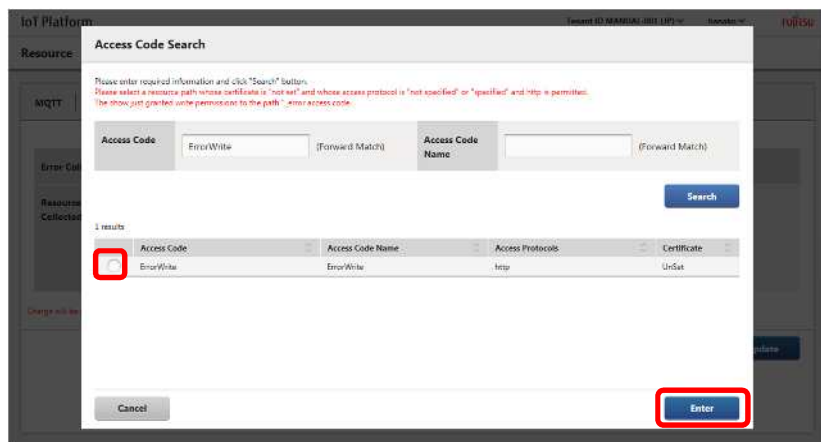
- 4-1. Click Search for the Access Code.



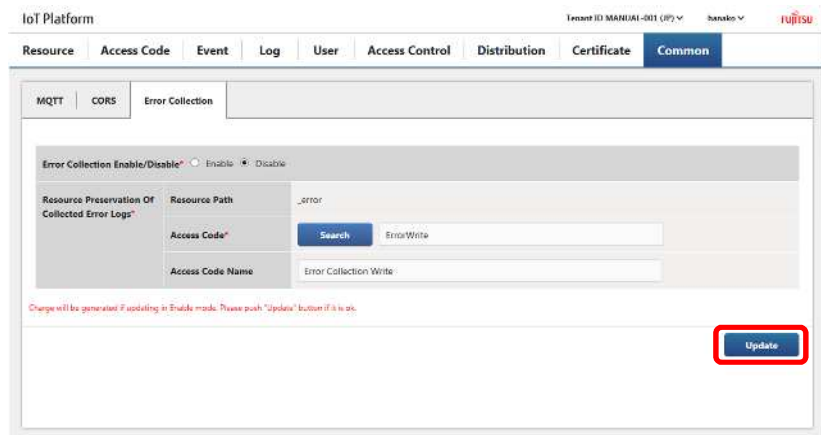
- 4-2. Enter "ErrorWrite" for the Access Code on the Access Code Search screen.



4-3. Select the Access Code "ErrorWrite", and click Execute.



5. Click Update.



Chapter 6 List of Error Messages

MessageID	Message	Countermeasure
00007	User ID and password do not match.	Either the user ID or password entered is wrong. If you have forgotten your password, ask your system administrator to reset it. Additionally, check that the Service Portal access control settings do not contain errors.
00010	Disconnected after a period of inactivity.	Please login again.
00017	User ID and password do not match.	Either the user ID or password entered is wrong. If you have forgotten your password, ask your system administrator to reset it. Additionally, check that the Service Portal access control settings do not contain errors.
06101	The corresponding information has exceeded 100 items. Only displaying the first 100 items.	Narrow down the resource path search conditions set.
06102	Enter a resource path by 128 half-width alphanumeric characters, including -, _ and / symbols, or less. - and / symbols cannot be used at the beginning of a resource path. Additionally, -, _ and / symbols cannot be used after a /.	
06103	Enter a resource name by 32 characters or less.	
06201	Enter a resource path by 2 to 128 half-width alphanumeric characters, including -, _ and / symbols. Symbols cannot be used at the beginning of a resource path and after a /.	
06203	The resource path specified has been registered.	Please specify a non-registered resource path.
06204	Enter a resource name by 32 characters or less.	
06206	The resource name specified has been registered.	Please specify a non-registered resource name.
06207	Select a data format.	
06209	Enter a comment by 256 characters or less.	
06210	Enter an authentication ID by 20 half-width characters or less.	
06211	Enter an authentication password by 20 half-width characters or less.	
06212	Enter header name 1 by 20 half-width characters or less.	The "header name 1" number part shows the corresponding number.
06213	Enter header value 1 by 512 half-width characters or less.	The "header value 1" part shows the corresponding number.
06214	Enter a retention period (days) by 1 to 9999 half-width numerals.	
06215	Enter a URI by 256 half-width characters or less.	

06216	If the resource type is resource (transfer), enter a resource path by 1 to 123 half-width alphanumeric characters, including -, _, and / symbols. Additionally, -, _, and / symbols cannot be used after a /.	
06217	If the resource type is resource and a binary data format is used, enter a resource path by 1 to 123 half-width alphanumeric characters, including -, _, and / symbols. Additionally, -, _, and / symbols cannot be used after a /.	
06301	Specify a file to be used to batch add resources.	Specify a CSV format file when batch adding resources.
06302	An error was found with the CSV format.	Edit the CSV file used when registering the resource again.
06303	The CSV file exceeds 100 rows. Separate the data and register it again.	
06304	The number of items is incorrect.	
06305	Select a resource type.	
06308	Select a method.	
06310	Enter an authentication ID by 20 half-width characters or less.	
06311	Enter an authentication password by 20 half-width characters or less.	
06312	Enter header name 1 by 20 half-width characters or less.	The "header name 1" number part shows the corresponding number.
06313	Enter header value 1 by 512 half-width characters or less.	The "header value 1" part shows the corresponding number.
06314	Enter a retention period (days) by 1 to 9999 half-width numerals.	
06315	Enter a URI by 256 half-width characters or less.	
06316	If resource (transfer) is selected, enter a resource path by 1 to 123 half-width alphanumeric characters (_fwd/ not included in character count), including -, _, and / symbols. Additionally, -, _, and / symbols cannot be used after a /.	
06317	If the resource type is resource and a binary data format is used, enter a resource path by 1 to 123 half-width alphanumeric characters (_bin/ not included in character count), including -, _, and / symbols. Additionally, -, _, and / symbols cannot be used after a /.	
06318	If the resource type is resource (transfer), enter "1" (JSON) for the data format.	
06401	The resource path specified does not exist.	The resource may have been deleted by another user while updating. Check whether another user has deleted the resource.
06402	Enter a resource name by 32 characters or less.	
06404	The resource name specified already exists.	Review the resource name specified at updating the resource name.

06405	The resource path selected has been deleted.	
06410	Enter an authentication ID by 20 half-width characters or less.	
06411	Enter an authentication password by 20 half-width characters or less.	
06412	Enter header name 1 by 20 half-width characters or less.	The "header name 1" number part shows the corresponding number.
06413	Enter header value 1 by 512 half-width characters or less.	The "header value 1" part shows the corresponding number.
06414	Enter a retention period (days) by 1 to 9999 half-width numerals.	
06415	Enter a URI by 256 half-width characters or less.	
06503	Failed to delete.	Delete all events and access codes tied to the resource before attempting to delete the resource.
06504	Delete was failed because Access Code exists under the resource.	
07101	Enter an access code by 48 half-width alphanumeric characters or less.	
07102	Enter an access code by 32 characters or less.	
07103	Enter a resource path by 128 half-width alphanumeric characters, including -, _, and / symbols, or less. - and / symbols cannot be used at the beginning of a resource path. Additionally, -, _, and / symbols cannot be used after a /.	
07104	Enter a resource name by 32 characters or less.	
07105	The corresponding information has exceeded 1,000 items. Only displaying the first 1,000 items.	
07201	Enter an access code by 3 to 48 half-width alphanumeric characters.	
07202	Select a resource path.	Output when the resource you prefer to tie to the access code has not been selected.
07203	Select at least one access permission (UR).	
07204	Enter a comment by 256 characters or less.	
07205	Access permissions CDL and L cannot be selected at the same time.	
07206	Specify one or more access protocol from http, https, mqtt, or mqtts.	
07207	Specify a correct certification file(under 10000 Bytes).	
07208	Specify a text file for certificates.	
07209	Reading the certificate file fails. Please try again.	

07301	Enter an access code by 3 to 48 half-width alphanumeric characters.	
07302	Specify a file to be used to batch add access codes.	
07303	An error was found with the CSV format.	
07304	The CSV file exceeds 100 rows. Separate the data and register it again.	
07305	The number of items is incorrect.	Review the CSV file to be used when batch registering access codes.
07306	Select a combination of CDL, L, R, and U access permissions.	
07401	Select a resource path.	
07402	Select at least one access permission (UR).	
07403	Enter a comment by 256 characters or less.	
07406	Specify one or more access protocol from http, https, mqtt, or mqtts.	
07407	Specify a correct text file (10000 bytes or less) for certificates.	
07408	Specify a text file for certificates.	
07409	Reading the certificate file fails. Please try again.	
07501	Failed to delete.	Check whether or not the event or access code access controls tied to the corresponding access code have been defined.
07601	Enter an access code by 3 to 48 half-width alphanumeric characters.	
07602	Enter an access code by 32 characters or less.	
07603	Enter a comment by 256 characters or less.	
07604	Enter a resource path by 2 to 128 half-width alphanumeric characters, including -, _, and / symbols. Symbols cannot be used at the beginning of a resource path and after a /.	
07605	Enter an access permission by 2-character UR or less.	
07606	The resource path repeats.	
07607	Specify one or more access protocol from http, https, mqtt, or mqtts.	
07702	The access code specified has already been registered.	
07703	The resource path specified does not exist.	
07704	Access code matching search conditions not found.	
07705	Access code matching search conditions not found.	
07706	Information needed for registration not found.	

07707	Event associated with target access code found.	
07708	Insufficient access permissions not associated with a resource.	
07709	Insufficient access code permission information.	
07710	Insufficient resource permission information.	
07711	Insufficient resource permission resource path.	
07712	Insufficient resource access permission.	
07713	IP filters associated with target access code found.	
07714	Enabled distribution policy associated with target access code found.	
07715	Enabled recommend resource associated with target access code found.	
07716	The target access code has a distribution policy with upload permissions.	
07717	The target access code has a recommend resource with upload permissions.	
07718	Event associated with target access code and resource found.	
07719	The number of resource paths that can be added with a single request has been exceeded.	
07720	The access protocol not permitted.	
07721	Certificate file format includes error.	
07722	Access protocol format includes error.	
07723	The certificate file exceeds 10000 bytes.	
07724	Specify a correct text file for certificates.	
07725	Access protocol duplicated.	
08101	Enter an event ID by 12 half-width alphanumeric characters or less.	
08102	Enter an event name by 32 characters or less.	
08103	Enter a resource path by 128 half-width alphanumeric characters, including -, _ and / symbols, or less. - and / symbols cannot be used at the beginning of a resource path. Additionally, -, _ and / symbols cannot be used after a /.	
08104	Enter a resource name by 32 characters or less.	
08105	The corresponding information has exceeded 1,000 items. Only displaying the first 1,000 items.	
08201	Enter an event name by 32 characters or less.	
08202	Enter a comment by 256 characters or less.	
08203	Enter a resource path by 128 half-width alphanumeric characters, including -, _ and / symbols, or less. - and / symbols cannot be used at the beginning of a resource path. Additionally, -, _ and / symbols cannot be used after a /.	
08204	Enter a resource name by 32 characters or less.	

08205	Enter an access code by 3 to 48 half-width alphanumeric characters.	
08206	Enter an access code by 32 characters or less.	
08207	Enter a data position by 1902 half-width characters or less.	
08208	Invalid detection data format.	Check that a character string has not been specified when numerical value is selected.
08209	Invalid released data format.	Check that a character string has not been specified when numerical value is selected.
08210	Enter an email address by 254 characters or less in an email address format.	
08211	Enter a subject line by 256 characters or less.	
08212	Enter the main text by 140 characters or less.	
08213	Enter a URI by 256 half-width characters or less.	
08214	Enter an authentication ID by 20 half-width characters or less.	
08215	Enter an authentication password by 20 half-width characters or less.	
08216	Enter a header name by 20 half-width characters or less.	
08217	Enter a header value by 512 half-width characters or less.	
08218	Enter the body by 1,024 characters or less.	
08219	Enter the event detection condition start time (hour).	
08220	Enter the event detection condition start time (minutes).	
08221	Enter the event detection condition start time (seconds).	
08222	Enter the correct event detection condition start time.	Check whether a value outside the time range (e.g., a value of 25 or higher for hours and 60 or higher for minutes and seconds) has been set.
08223	Enter the event detection condition end time (hour).	
08224	Enter the event detection condition end time (minutes).	
08225	Enter the event detection condition end time (seconds).	
08226	Enter the correct event detection condition end time.	Check whether a value outside the time range (e.g., a value of 25 or higher for hours and 60 or higher for minutes and seconds) has been set.
08227	Set a value lower than the detection condition end time as the detection condition start time.	

08228	Enter the event detection condition start time (date).	
08229	Enter the event detection condition end time (date).	
08230	Select detect event judgment.	
08231	Select cancel event judgment.	
08232	Select event detection condition.	
08233	Select cancel event condition.	
08234	If the detection condition is a numerical value, enter by up to five integer part and five decimal part half-width numbers.	
08235	If the detection condition is a character string, enter by 128 characters or less.	
08236	If the resolatory condition is a numerical value, enter by up to five integer part and five decimal part half-width numbers.	
08237	If the resolatory condition is a character string, enter by 128 characters or less.	
08301	Enter an event name by 32 characters or less.	
08302	Enter a comment by 256 characters or less.	
08303	Enter a resource path by 128 half-width alphanumeric characters, including -, _, and / symbols, or less. Symbols cannot be used at the beginning of a resource path and after a /.	
08304	Enter a resource name by 32 characters or less.	
08305	Enter an access code by 3 to 48 half-width alphanumeric characters.	
08306	Enter an access code by 32 characters or less.	
08307	Enter a data position by 1902 half-width characters or less.	
08308	Invalid detection data format.	Check that a character string has not been specified when numerical value is selected.
08309	Invalid released data format.	Check that a character string has not been specified when numerical value is selected.
08310	Enter an email address by 254 characters or less in an email address format.	
08311	Enter a subject line by 256 characters or less.	
08312	Enter the main text by 140 characters or less.	
08313	Enter a URI by 256 half-width characters or less.	
08314	Enter an authentication ID by 20 half-width characters or less.	
08315	Enter an authentication password by 20 half-width characters or less.	
08316	Enter a header name by 20 half-width characters or less.	

08317	Enter a header value by 512 half-width characters or less.	
08318	Enter the body by 1,024 characters or less.	
08319	Enter the event detection condition start time (hour).	
08320	Enter the event detection condition start time (minutes).	
08321	Enter the event detection condition start time (seconds).	
08322	Enter the correct event detection condition start time.	
08323	Enter the event detection condition end time (hour).	
08324	Enter the event detection condition end time (minutes).	
08325	Enter the event detection condition end time (seconds).	
08326	Enter the correct event detection condition end time.	
08327	Set a value lower than the detection condition end time as the detection condition start time.	
08328	Enter the event detection condition start time (date).	
08329	Enter the event detection condition end time (date).	
08330	Select detect event judgment.	
08331	Select cancel event judgment.	
08332	Select event detection condition.	
08333	Select cancel event condition.	
08334	If the detection condition is a numerical value, enter by up to five integer part and five decimal part half-width numbers.	
08335	If the detection condition is a character string, enter by 128 characters or less.	
08336	If the resolatory condition is a numerical value, enter by up to five integer part and five decimal part half-width numbers.	
08337	If the resolatory condition is a character string, enter by 128 characters or less.	
08502	Failed to delete.	
08704	Failed to send to the event judgment part.	
08705	The response from the event judgment part has timed out.	
08707	Related event information not found.	
08708	Target resource not found.	
08710	Related event information not found.	
08711	Event ID not specified.	
08712	Invalid request URL.	
08713	Invalid event search conditions.	
08714	Invalid filter conditions.	

08715	Invalid top conditions.	
08716	Invalid skip conditions.	
08717	Insufficient event conditions.	
08718	Insufficient event targets.	
08719	Insufficient event target resource path.	
08720	Insufficient target resource data operation.	
08721	Insufficient access code with a target resource path with read permissions.	
08722	Insufficient notification condition path format.	
08723	Insufficient resource path specifying notification condition body elements.	
08724	Insufficient notification condition comparative operators.	
08725	Insufficient notification condition comparative target value.	
08726	Insufficient inhibit condition path format.	
08727	Insufficient resource path specifying inhibit condition body elements.	
08728	Insufficient inhibit condition comparative operators.	
08729	Insufficient inhibit condition comparative target value.	
08730	Insufficient notification content specification.	
08731	Insufficient notification destination email address.	
08732	Insufficient notification email body text.	
08733	Insufficient notification HTTP Method.	
08734	Insufficient notification URI.	
08735	Insufficient notification header field.	
08736	Insufficient notification header field name.	
08737	Insufficient notification header field value.	
08738	Insufficient notification.	
08739	input parameter error. resource_path is duplicated.	
08740	iot-pf Service Unavailable.	
08741	iot-pf Service Unavailable.	
08742	iot-pf Service Unavailable.	
08743	tenant ID not found.	
08744	iot-pf Service Unavailable.	
08745	iot-pf Service Unavailable.	
08746	iot-pf internal error.	
08747	Reload configuration to fail to read config.	
08748	request access code has event.	
08749	request access code can't read event.	
08750	request access code has dispersion policy.	
08751	request access code has recommend resource.	
08752	request access code can't update dispersion policy.	
08753	request access code can't update recommend resource.	
08754	request access code and resource have event.	
09102	Enter the start date in YYYY/MM/DD format.	
09103	Enter the end date in YYYY/MM/DD format.	

09104	Enter the start time in HH:MM format.	
09105	Enter the start time in HH:MM format.	
09106	Enter the end time in HH:MM format.	
09107	Enter the end time in HH:MM format.	
09108	Make sure to enter time later than the start time for an end time.	
09109	The corresponding information was not found.	Please review the detection conditions in the operating log.
09110	Enter a user ID by 254 characters or less in an email address format.	
09111	Enter a user name by 32 characters or less.	
09201	The corresponding condition has exceeded 1,000 items. Only displaying the first 1,000 items.	
09501	Enter the target date in YYYY/MM/DD format.	
09502	A usage amount log for the target date does not exist.	
09700	A usage amount log for the target month does not exist.	
09801	A usage amount log for the target month does not exist.	
09901	Problems were found with the log file which may prevent it from displaying properly.	
09903	The system is busy. Please Try again after a while.	
10101	Enter a user ID by 254 characters or less in an email address format.	
10102	Enter a user name by 32 characters or less.	
10103	The corresponding information has exceeded 1,000 items. Only displaying the first 1,000 items.	
10201	Enter a user ID by 254 characters or less in an email address format.	
10202	A user ID is registered.	Please specify a different user ID to register.
10203	Enter a user name by 32 characters or less.	
10204	Enter a comment by 256 characters or less.	
10301	The user ID selected has been deleted.	The user may have been deleted by another user while user information was being updated. Check whether another user has deleted this user.
10302	Enter a user name by 32 characters or less.	
10303	Enter a comment by 256 characters or less.	
11101	Enter a permitted IP address by 15 characters or less in a IP address format.	
11102	Enter a user ID by 254 characters or less in an email address format.	
11103	The corresponding information was not found.	Please review the search conditions.
11201	Enter a start permitted IP address by 15 characters or less in a IP address format.	The same message may also be output for the stop IP address.
11202	Please enter a higher value for the stop IP address than the start IP address.	

11203	Enter a comment by 256 characters or less.	
11204	Enter a user ID by 254 characters or less in an email address format.	
11205	Enter a user name by 32 characters or less.	
11206	Select user information.	Output when the user you prefer to tie to the permitted IP address has not been selected.
11207	The corresponding information has exceeded 1,000 items. Only displaying the first 1,000 items.	
11208	Cannot add as five entries have already been made.	Up to five Service Portal access controls can be added.
11209	The user ID selected has been deleted.	The user may have been deleted by another user. Check whether another user has deleted this user.
11301	Enter a start permitted IP address by 15 characters or less in a IP address format.	The same message may also be output for the stop IP address.
11302	Please enter a higher value for the stop IP address than the start IP address.	
11303	Enter a comment by 256 characters or less.	
11304	Enter a user ID by 254 characters or less in an email address format.	
11305	Enter a user name by 32 characters or less.	
11306	Select user information.	Output when the user you prefer to tie to the permitted IP address has not been selected.
11307	The corresponding information has exceeded 1,000 items. Only displaying the first 1,000 items.	
11308	The user ID selected has been deleted.	The user may have been deleted by another user. Check whether another user has deleted this user.
11402	Failed to delete.	
11601	Enter a permitted IP address by 15 characters or less in a IP address format.	
11602	Enter an access code by 48 half-width alphanumeric characters or less.	
11603	The corresponding information was not found.	Please review the search conditions.
11701	Enter a start permitted IP address by 15 characters or less in a IP address format.	The same message may also be output for the stop IP address.
11702	Please enter a higher value for the stop IP address than the start IP address.	
11703	Enter a comment by 256 characters or less.	
11704	Enter an access code by 48 half-width alphanumeric characters or less.	
11705	Enter an access code by 32 characters or less.	
11706	Select access code information.	Output when the access code you prefer to tie to the permitted IP address has not been selected.
11707	The corresponding information has exceeded 1,000 items. Only displaying the first 1,000 items.	

11708	Cannot add as five entries have already been made.	Up to five access controls can be added.
11709	The access code selected has been deleted.	The access code may have been deleted by another user. Check whether another user has deleted this access code.
11710	The starting IP address and ending IP address has been registered.	Register a different starting IP address and ending IP address.
11801	Enter a start permitted IP address by 15 characters or less in a IP address format.	The same message may also be output for the stop IP address.
11802	Please enter a higher value for the stop IP address than the start IP address.	
11803	Enter a comment by 256 characters or less.	
11804	Enter an access code by 48 half-width alphanumeric characters or less.	
11805	Enter an access code by 32 characters or less.	
11806	Select access code information.	Output when the access code you prefer to tie to the permitted IP address has not been selected.
11807	The corresponding information has exceeded 1,000 items. Only displaying the first 1,000 items.	
11808	The access code selected has been deleted.	The access code may have been deleted by another user. Check whether another user has deleted this access code.
11902	Failed to delete.	
12101	Enter a recommendation cycle by 1 to 1440 half-width numerals.	
12102	Enter a calculating period (days) by 1 to 1440 half-width numerals.	
12103	Set a greater value for the calculating period than the recommendation cycle.	
12104	Enter the resource path of a load resource by 2 to 128 half-width alphanumeric characters, including -, _, and / symbols. Symbols cannot be used at the beginning of a resource path and after a /.	
12105	Enter a load resource access code by 3 to 48 half-width alphanumeric characters.	
12106	Make sure to enable at least one recommend resource.	Enable recommend resources 1, 2 or 3 to enable distribution settings.
12107	Enter a resource path for recommend resource 1 by 2 to 128 half-width alphanumeric characters, including -, _, and / symbols. Symbols cannot be used at the beginning of a resource path and after a /.	*1
12108	Enter an access code for recommend resource 1 by 3 to 48 half-width alphanumeric characters.	*1
12109	Enter an edge computing condition for recommend resource 1 of up to 10 half-width numerals.	*1

12110	Select the edge computing detection judgment condition for recommend resource 1.	*1
12113	Select the resolutive judgment condition for the above for recommend resource 1.	*1
12115	Failed to send update notification as the planner has not been started.	Please wait a while before trying again.
12116	Failed to send update notification as the planner is still being started, or has been shutdown.	
12117	Failed to send update notification as the data format sent to the planner is incorrect.	
12119	An HTTP request error has been received from the planner.	
12120	The resource path for the load resource does not match the access code permission-controlled resource path.	The access code permissions associated with the resource path may have been changed, or the access code may have been deleted by another user. Check whether another user has changed or deleted this access code.
12121	The resource path for recommend resource 1 does not match the access code permission-controlled resource path.	*1
12122	Please enter Edge Computing Condition is value of Condition Resolutive or more.	
13200	Enter a new password of 8 to 12 characters for the following policy.	

*1: The "recommend resource 1" number part shows the corresponding field number.

Chapter 7 Appendix

7.1 Notes on the CSV Format

7.1.1 Overview of the CSV Format Used for Resources

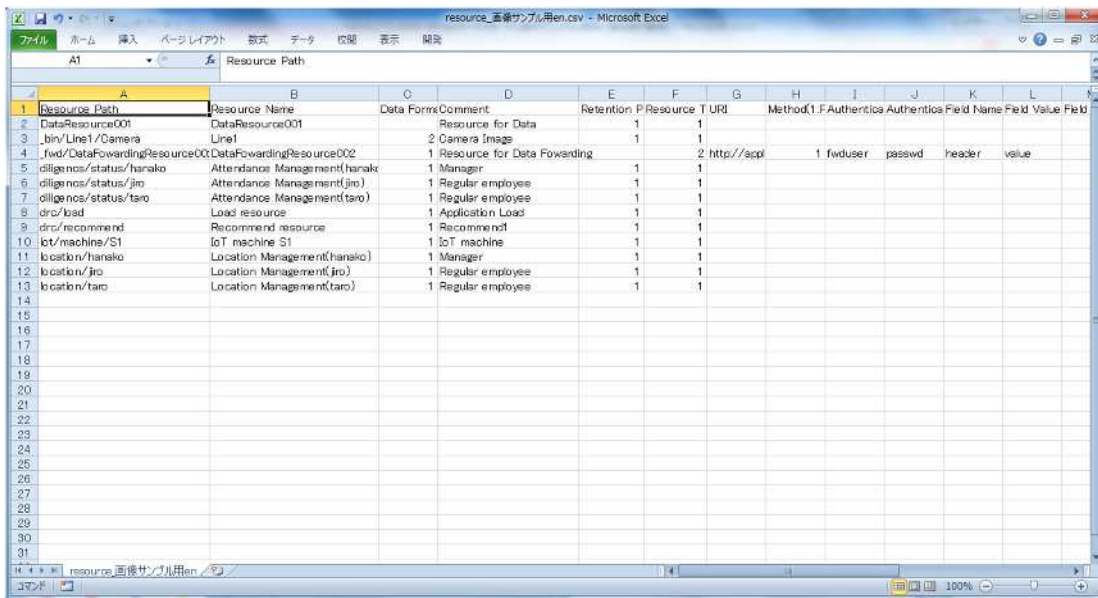
No.	Header name (Japanese)	Header name (English)	Required	Character type	No. of characters	Format	Notes
1	Resource path	Resource Path	Yes	Single-byte alphanumeric characters and symbols	Up to 128	-	Available symbols - (hyphen), _ (underscore), / (slash)
2	Resource Name	Resource Name	-	Single-/double-byte	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters, @ - () : . _
3	Data format (1: JSON 2: Binary)	Data Format (1:JSON 2:BINARY)	Yes	Single-byte numerals	1	Numerical values	
4	Comment	Comment	-	Single-/double-byte	Up to 256	-	Japanese language input available
5	Retention period (1-9999 days)	Retention period	Yes	Single-byte numerals	Up to 4	-	Unit: Days
6	Resource type (1: Resource 2: Resource (transfer))	Resource Kind(1:Accumulation 2:Transfer)	Yes	Single-byte numerals	1	Numerical values	
7	URI	URI	-	Single-byte alphanumeric characters and symbols	Up to 256	-	
8	Method (1:POST 2:PUT 3:GET 4: DELETE 5:HEAD 6:OPTIONS 7:TRACE)	Method(1:POST 2:PUT 3:GET 4: DELETE 5:HEAD 6:OPTIONS 7:TRACE)	-	Single-byte numerals	1	Numerical values	Numbers from 1 to 7
9	Authentication ID	Authentication ID	-	Single-byte alphanumeric characters and	Up to 20	-	

				symbols			
10	Authentication password	Authentication Passwd	-	Single-byte alphanumeric characters and symbols	Up to 20	-	
11	Header name 1	Field Name1	-	Single-byte alphanumeric characters and symbols	Up to 20	-	
12	Header value 1	Field Value1	-	Single-byte alphanumeric characters and symbols	Up to 512	-	
...							
30	Header name 10	Field Name10	-	Single-byte alphanumeric characters and symbols	Up to 20	-	
31	Header value 10	Field Value10	-	Single-byte alphanumeric characters and symbols	Up to 512	-	

 Note

- The character codes that can be used for CSV files with each Add All function are based on the screen display language, as follows.
 - If the display language is Japanese: Shift-JIS, JIS, EUC, and UTF-8 (Automatic discrimination. Character codes cannot be mixed)
 - If the display language is English: UTF-8

CSV image



7.1.2 Overview of the CSV Format Used for Access Codes

No.	Header name (Japanese)	Header name (English)	Required	Character type	No. of characters	Format	Notes
1	Access codes	Access Code	Yes	Single-byte alphanumeric characters	3 to 48	-	
2	Access Code Name	Access Code Name	-	Single-/double-byte	Up to 32	-	Usable characters Numbers, upper and lower case alphabetical characters, Double-byte characters, @ - () : . _
3	Comment	Comment	-	Single-/double-byte	Up to 256	-	Japanese language input available
4	Access protocol	Access Protocol	-	Single-byte alphabetical characters	Up to 21	-	Specify http, https, mqtt, or mqtts by ;
5	Resource path	Resource Path	Yes	Single-byte alphanumeric characters and symbols	Up to 128	-	Available symbols - (hyphen), _ (underscore), / (slash)
6	Access permission	Access Code Permission	Yes	Single-byte alphabetical characters	Up to 5	C, D, L, R, U	A combination of any CDLRU characters (varied order allowed). However, be aware that D and L permissions are required when including C, and C and L permissions are required when including D (setting L permissions without C and D permissions allowed). Possible combinations (varied order allowed). Either R or U permissions are required.

Memo

- Add additional columns to the right as shown in the CSV image below when you prefer to associate multiple resource paths and access permissions.

CSV image

#	A	B	C	D	E	F	G	H
1	Access Code	Access Code Name	Comment	Access P	Resource Path 1	Access Do	Resource Path 2	Access Do
2	DiligenceManagement11111	attendance situation	RU	refer and update for all	diligence/status/hanako	RU	diligence/status/taro	RU
3	LocationManagement22222	location information(hansko)		self location information	location/hanako	RU		
4	LocationManagement33333	location information(taro)		self location information	location/taro	RU		
5	LocationManagement44444	location information(jiro)		self location information	location/jiro	RU		
6	LocationManagement55555	refer location information		refer location information	location/hanako	R		
7	DRCLoad	load information	RU		drc/load	RU	location/jiro	R
8	DRCRecommend	recommend			drc/recommend	RU		
9	Line1Camera	Line1 Image		update,refer/delete	Resource with API	CDLRU		
10	SecureIoTMachine	IoT machine S1		Authentication certificate	_bin/Line1/Camera	RU		
11	ErrorRead	ErrorRead		Error Collection Read	_error	R		
12	ErrorWrite	ErrorWrite		Error Collection Write	_error	U		

7.2 Notes on the Sorting Policy

Search results are sorted in the following order when clicking the Sort button on the Display Search Results screen.

- Single-byte symbols (*1)
- Single-byte numerals
- Single-byte alphabetical characters (upper case)
- Single-byte alphabetical characters (lower case)
- Double-byte hiragana characters
- Double-byte katakana characters
- Double-byte kanji characters
- Double-byte symbols (*2)
- Double-byte numerals
- Double-byte alphabetical characters (upper case)
- Double-byte alphabetical characters (lower case)
- Single-byte katakana characters

Note

- *1: Single-byte symbols are sorted by code order, and may appear behind numbers depending on the symbol type.
- *2: Double-byte characters are sorted by code order, and may not follow the above-mentioned sorting order depending on the character type.

7.3 Event Function Notification Messages

The format for notification messages sent with the event function are as follows.

For email notifications, the following message will be sent as a text file (eventinfo.txt) written in JSON format.

For API calls, this service will automatically store the notification message in the body and send it if settings are configured to not store notification messages to the body in add event settings, and if the resource data format is JSON.

If the binary data format is used, notification messages will be sent without being stored to the body.

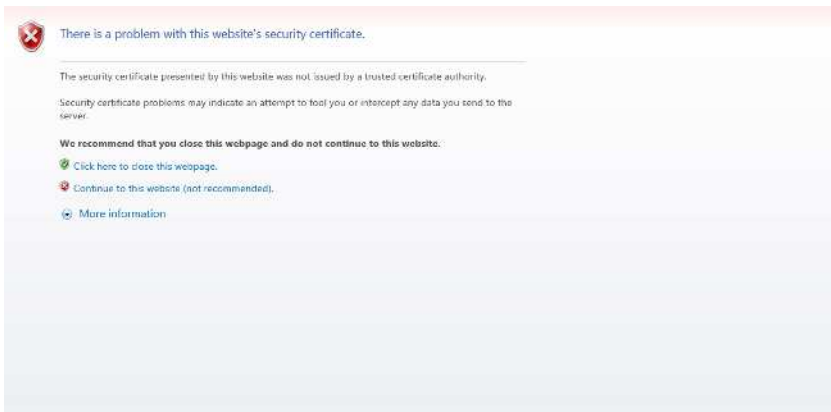
	Entry name	Description	Notes
(1)	Event ID	Stores the event ID detected.	A character string by a combination of 12 alphanumeric characters.
(2)	Operation	Stores resource operation details when the event is detected.	"update": When writing data "delete": When deleting
(3)	Timestamp	Stores the time at which the event judgment was made.	Conforms to ISO8601. (20141225T103612.001+0900, etc.)
(4)	Resource path	The resource path in use when the event was detected.	Refer to 4.6.2
(5)	Message	Data stored to the resource path	Message in JSON format

A formatting example is provided below.

```
{  
  "eventID":"123456789abc",  
  "operation":"update",  
  "date": "20141225T103612.001+0900",  
  "resoucepath": "Kamata/Printers/1F/Printer",  
  "message": {"temp" : 69}  
}
```

7.4 Cautions When Accessing the Login URL

The following screen may appear when accessing the Login URL via Internet Explorer 11.



This issue may be resolved by changing Internet Options settings in Internet Explorer 11.

1. Click the [Advanced] tab in Internet Options.
2. Change the settings for SSL and TLS use under "Security" in the following manner.
 - Deselect the "Use SSL2.0" check box
 - Deselect the "Use SSL3.0" check box
 - Select the "Use TLS1.0"
 - Select the "Use TLS1.1"
 - Select the "Use TLS1.2"

3. Click "Apply" in the bottom right, and then click "OK".

4. Restart Internet Explorer 11.

