

FUJITSU Cloud Service K5
API Reference Manual

Version 1.4

FUJITSU LIMITED

Preface

Purpose of This Document

This guide describes the specification of the API (Application Programming Interface) provided by the FUJITSU Cloud Service K5.

You are recommended to also refer to the following related manuals:

- K5 API User Guide
- K5 Portal User Guide

Compliance with Export Control Regulations

When exporting this document or providing it to a third party, check the export control laws and regulations of your country and the U.S. and take necessary procedures.

Notices

- The contents of this manual are subject to change without notice.
- The contents of this manual shall not be reproduced without express written permission from FUJITSU LIMITED.
- FUJITSU LIMITED shall bear no responsibility for any claims of violation of a third party's patent or other rights arising from the use of the data described in this document.

Document history

Version	Date	Edited places	Description
1.1	Oct 7, 2016	2.2 API Execution Errors 3.2 API Execution Errors	Update error messages.
1.2	Dec 22, 2016	1.2 Access Rights by Role	Add the section
		1.1 List of API 2.3.1 Get Access Token 3.3.5 Update user authentication information	Modifications corresponding to the new function
1.3	May 15, 2017	2.3.1 Get Access Token	Add explanation
1.4	Sept 4, 2017	2.3.1 Get Access Token	Add explanation

Table of Contents

1	Chapter 1 – API Outline.....	1
1.1	List of API.....	2
1.2	Access Rights by Role.....	3
1.3	Glossary.....	4
2	Chapter 2 – Authentication API.....	5
2.1	Request Headers.....	6
2.2	API Execution Errors.....	6
2.3	API Specification.....	8
2.3.1	Get access token.....	8
3	Chapter 3 – User management API.....	10
3.1	Request Headers.....	11
3.2	API Execution Errors.....	11
3.3	API Specification.....	13
3.3.1	Create new user.....	13
3.3.2	Change user information.....	15
3.3.3	Change user password.....	17
3.3.4	Delete user.....	18
3.3.5	Update user authentication information.....	19

Chapter 1 – API Outline

1.1 List of API

No.	API Group	API	Method	URL	Description
1	Authentication	Get access token	POST	https://auth-api.jp-east-1.paas.cloud.global.fujitsu.com/API/paas/auth/token	Get token for API authentication.
2	User management	Create user	POST	https://k5-apiportal.paas.cloud.global.fujitsu.com/API/v1/api/users	Create a new user.
3		Change user information	PUT	https://k5-apiportal.paas.cloud.global.fujitsu.com/API/v1/api/users	Change information of the contractor or the specified user.
4		Change user password	PUT	https://k5-apiportal.paas.cloud.global.fujitsu.com/API/v1/api/userspassword	Change password of the specified user.
5		Delete user	DELETE	https://k5-apiportal.paas.cloud.global.fujitsu.com/API/v1/api/users/?login_id={UserName}	Delete the specified user.
6		Update user authentication information	PUT	https://k5-apiportal.paas.cloud.global.fujitsu.com/API/v1/api/usersauthenticationmethod	Update user authentication method of the contractor or a user.

API character encoding is UTF-8.

1.2 Access Rights by Role

Each user of the K5 Portal is assigned a 'Role' that controls the operations the user is authorized to perform on the K5 Portal. (Refer to the 'K5 Portal User Guide' for detail.)

Also for the use of APIs, access rights are assigned by role as shown below.

API group	API name	K5 common service Roles								
		Contractor	USER						Developer	
			Administrator			Developer				
Authentication	Get Access Token	✓		✓						
User Management	Get Access Token	Operation object		Operation object						
		Oneself	USER	Oneself	Contractor	USER	Oneself	Contractor	USER	
		Create New User	X	✓	X	X	✓	X	X	X
		Change User Information	*1	✓	✓	*1	✓	✓	X	X
		Change User Password	✓	X	✓	X	X	✓	X	X
		Delete User	X	✓	X	X	✓	X	X	X
		Update user authentication information	✓	X	✓	X	X	✓	X	X

✓: Permitted X: Not Permitted *1: Permitted with restrictions (See [Change user information] below.)

By API name, the roles to which the executions are permitted are shown below.

[Create New User]

- The Contractor and Administrator can create a user except with the role of Contractor.

[Change user information]

- The Administrator and Developer can change the information of one's own, including password.
- The information of the Contractor which can be changed by an Administrator is only its password.
- The Contractor can change his/her own information, except its user status.
- The Contractor and Administrator can change the information of USERS (Administrator / Developer).

[Change user password]

- Regardless of role, a user can change one's own password.

[Delete user]

- The Contractor and Administrator can delete a user with a role except Contractor.

[Update user authentication information]

- All users can update his/her own user authentication method.

1.3 Glossary

Term	Explanation
User	Person (or system, service) who uses or manages a function
User name	Unique ID of a user
Role	Authorization granted to a person or a group. Role of a user determines which API that user can execute.
Role code	Unique ID of a role

Chapter 2 – Authentication API

2.1 Request Headers

Request headers for authentication API

No.	Header Name	Required	Header value
1	Content-Type	Yes	application/json
2	X-FCX-Client-Cert	*See note	Client certificate mapped to the user

*Note: Required, in cases where 'Certificate and Password' authentication is used.

2.2 API Execution Errors

API execution error information is returned in HTTP response body under json format.

No.	Format	Item	Type	Cardinality	Description
1	JSON [Body]	errorLevel	string	1..1	Error level
2		framework	object	1..1	Framework object
3		└systemErrorCode	string	1..1	System error code
4		business	object	1..1	Business object
5		└businessErrorInfo	string	1..1	Error message
6		└responseErrorCode	string	1..1	Response error code
7		└embeddedString	string array	1..1	Additional information

Example :

```
{
  "errorLevel": "888",
  "framework": {
    "systemErrorCode": ""
  },
  "business": {
    "businessErrorInfo": "Cannot create token from the specified user information.",
    "responseErrorCode": "RCM301802",
    "embeddedString": []
  }
}
```

List of response errors

No.	HTTP status	Error Information	Error message	Error reason
1	400	Request parameter error	Parameter is invalid. Specified parameter: XXX * XXX is the parameter name.	Request parameter error (empty parameter, invalid length, invalid format...)
2	401	Cannot create token	Cannot create token from the specified user information.	User information specified in the request is invalid
3	500	Server error	Failed to create token (Internal Error).	Internal server error

2.3 API Specification

2.3.1 Get access token

1. Request

Parameter definition

No.	Format	Item	Required	Cardinality	Min. length	Max. length	Restrictions	Description
1	JSON [Body]	auth	Yes	1..1	-	-	Object	Authentication object
2		└identity	Yes	1..1	-	-	Object	Identity object
3		└└password	Yes	1..1	-	-	Object	Password object
4		└└user	Yes	1..1	-	-	Object	User object
5		└└└contract_number	Yes	1..1	8	8	See Note(*)	Contract number of authentication user
6		└└└name	Yes	1..1	4	246	See Note(*)	User name of authentication user
7		└└└password	Yes	1..1	16	64	See Note(*)	Password of authentication user
8		timezone	No		-	-	See Note(*)	Timezone *case-insensitive If no timezone, a timezone other than 'UTC', or an invalid timezone is specified, 'JST' is automatically set.

(*): Upper/Lower case alphanumeric characters. For more details please refer to K5 Portal User Guide (1.1.2 Essential Information for the use of the K5 Portal) input restrictions.

Example:

```
{
  "auth":{
    "identity":{
      "password":{
        "user":{
          "contract_number":"xxxxxxx",
          "name":"user-name",
          "password":"user-password"
        }
      }
    }
  },
  "timezone":"UTC"
}
```

2. Response

HTTP STATUS : 200

Response body:

No.	Format	Item	Cardinality	Description
1	JSON [Body]	token	1..1	Token object
2		└expires_at	1..1	Expiration of an access token. The expiration from the time of an initial issuance is 30 minutes later. Timezone : 'UTC' if 'UTC' is specified in 'timezone' of 1. Request. 'JST' if other than 'UTC'. Format : YYYY-mm-ddTHH:MM:SS.SSSZ (if 'UTC') YYYY-mm-ddTHH:MM:SS (if 'JST')
3		└scope	1..1	Token scope
4		└user	1..1	User object
5		└contract_number	1..1	Contract number of authentication user
6		└name	1..1	User name of authentication user

Example:

```
{
  "token":{
    "expires_at":"2016-05-16T03:20:42",
    "scope":"paas",
    "user":{
      "contract_number":"xxxxxxx",
      "name":"user-name"
    }
  }
}
```

Chapter 3 – User management API

3.1 Request Headers

API execution error information is returned in HTTP response body under json format.

No.	Header Name	Required	Header value
1	Token	Yes	Access token acquired by executing "Get access token API"
2	Content-Type	Yes	application/json

3.2 API Execution Errors

API execution error information is returned in HTTP response body under json format.

No.	Format	Item	Type	Cardinality	Description
1	JSON [Body]	errorLevel	string	1..1	Error level
2		framework	object	1..1	Framework object
3		└systemErrorCode	string	1..1	System error code
4		business	object	1..1	Business object
5		└businessErrorInfo	string	1..1	Business error information
6		└responseErrorCode	string	1..1	Response error code
7		└embeddedString	string array	1..1	Error message

Example:

```
{
  "errorLevel": "888",
  "framework": {
    "systemErrorCode": ""
  },
  "business": {
    "businessErrorInfo": "BECSA000113",
    "responseErrorCode": "RCS100001",
    "embeddedString": [
      "Internal Server Error"
    ]
  }
}
```

List of response errors

No.	HTTP status	Error Information	Error message	Error reason
1	400	Request parameter error * XXX is the parameter name.	- Parameter is insufficient. Required parameter: XXX - Parameter is required.	Insufficient parameters
			Character count of parameter is invalid. Specified parameter: XXX	Input parameter check error (digit number fault)
			The format of parameter is invalid. Specified parameter: XXX	Input parameter format error (other than digit number)
2	400	Delete contractor error	Could not delete user because the target user is a contractor.	Try to delete a contractor
3	400	Password check error	Password is of invalid format or does not satisfy password policy. Please try again.	Violate password policy
			Password cannot be changed again within 24 hours since the last change. Please try again after 24 hours.	Try to change password again within 24 hours
			Failed to change password. The old password was invalid.	Previous password error
4	400	Invalid user status	Cannot change user information because user status of the target user is invalid.	Try to change information of user whose status is invalid
5	401	Invalid token	The specified access token is not valid.	Access token is not valid
6	403	Authorization error	Authorization Error.	Action not authorized
7	403	Change contractor status error	Unauthorized to change information of the specified user.	Try to change user status of a contractor
8	404	Not found	The target information does not exist.	Target information not found
9	409	Exclusive error	Operation conflicts with another one.	Target information has already been changed by another process
10	500	Internal Server Error	Internal Server Error.	Consistency error, or other server errors

3.3 API Specification

3.3.1 Create new user

1. Request

Parameter definition

No.	Format	Item	Required	Cardinality	Min. length	Max. length	Restrictions	Description
1	JSON [Body]	login_id	Yes	1..1	4	246	See Note (**)	User name of the user to be created
2		user_description	No	0..1	1	255	See Note (**)	User description of the user to be created
3		mailaddress	Yes	1..1	1	256	Proper email address format (*)	Email address of the user to be created
4		user_status	Yes	1..1	1	1	Invalid (0) / Valid (1)	User status of the user to be created
5		password	Yes	1..1	16	64	See Note (**)	Password of the user to be created
6		language_code	Yes	1..1	2	2	Japanese (ja) / English (en)	Language code of the user to be created
7		role_code	Yes	1..1	2	2	Administrator (00), Developer (01)	Role code of the user to be created
8		user_last_name	Yes	1..1	1	64	See Note (**)	Last name of the user to be created
9		user_first_name	Yes	1..1	1	64	See Note (**)	First name of the user to be created

(*): For the detail of email address format, please refer to K5 Portal User Guide (1.1.2 Essential Information for the use of the K5 Portal) input restrictions.

(**): Upper/Lower case alphanumeric characters. For more details, please refer to K5 Portal User Guide (1.1.2 Essential Information for the use of the K5 Portal) input restrictions.

Example:

```
{
  "login_id": "fujitsu123",
  "user_description": "User description",
  "mailaddress": "abc@xyz.com",
  "user_status": "1",
  "password": "Abcdefgh12345678",
  "language_code": "ja",
  "role_code": "00",
  "user_last_name": "Smith",
  "user_first_name": "John"
}
```

3. Response

HTTP STATUS : 200

Response body:

No.	Format	Item	Cardinality	Description
1	JSON [Body]	login_id	1..1	User name of the newly created user
2		user_description	1..1	User description of the newly created user
3		mailaddress	1..1	Email address of the newly created user
4		user_status	1..1	User status of the newly created user Invalid (0) / Valid (1)
5		language_code	1..1	Language code of the newly created user Japanese (ja) / English (en)
6		authentication_method	1..1	Authentication method * This API returns fixed value: Password authentication (0)
7		user_last_name	1..1	Last name of the newly created user
8		user_first_name	1..1	First name of the newly created user

Example:

```
{  
  "login_id": "fujitsu123",  
  "user_description": "User description.",  
  "mailaddress": "abc@xyz.com",  
  "user_status": "1",  
  "language_code": "ja",  
  "authentication_method": "0",  
  "user_last_name": "Smith",  
  "user_first_name": "John"  
}
```

3.3.2 Change user information

1. Request

Parameter definition

No.	Format	Item	Required	Cardinality	Min. length	Max. length	Restrictions	Description
1	JSON [Body]	login_id	Yes	1..1	4	246	See Note (**)	User name of the target user
2		mailaddress	No (*)	0..1	1	256	Proper email address format (***)	New email address
3		user_description	No (*)	0..1	1	255	See Note (**)	New user description
4		language_code	No (*)	0..1	2	2	Japanese (ja) / English (en)	New language code
5		user_status	No (*)	0..1	1	1	Invalid (0) / Valid (1) * Trying to change user status of a contractor will result in error	New user status
6		password	No (*)	0..1	16	64	See Note(**)	New password
7		user_last_name	No (*)	0..1	1	64	See Note(**)	New user Last name
8		user_first_name	No (*)	0..1	1	64	See Note (**)	New user First name

(*): At least one parameter must be set. Upper / Lower case alphanumeric characters.

(**): Upper / Lower case alphanumeric characters. For more details, please refer to K5 Portal User Guide (1.1.2 Essential Information for the use of the K5 Portal) input restrictions.

(***): For the detail of email address format, please refer to K5 Portal User Guide (1.1.2 Essential Information for the use of the K5 Portal) input restrictions.

Example:

```
{
  "login_id": "fujitsu123",
  "mailaddress": "abc@xyz.com",
  "user_description": "User description.",
  "language_code": "ja",
  "user_status": "1",
  "password": "Abcdefgh12345678",
  "user_last_name": "Smith",
  "user_first_name": "John"
}
```

2. Response

HTTP STATUS: 200

Response body:

No.	Format	Item	Cardinality	Description
1	JSON [Body]	login_id	1..1	User name of the target user
2		language_code	1..1	New language code
3		user_status	1..1	New user status
4		mailaddress	1..1	New email address
5		user_description	1..1	New user description
6		user_last_name	1..1	New user Last name
7		user_first_name	1..1	New user First name
8		accesstoken_destruction_information_list	1..1	User information whose token was cancelled.
9		customer_group_id	1..1	Group ID to which the user belongs to.
10		login_id	1..1	Login ID of the user.

Example:

```
{
  "login_id": "fujitsu123",
  "language_code": "ja",
  "user_status": "1",
  "mailaddress": "abc@xyz.com",
  "user_description": "User description.",
  "user_last_name": "Smith",
  "user_first_name": "John"

  "accesstoken_destruction_information_list":[
    {
      "customer_group_id": "HvlgXxym",
      login_id:" fujitsu123"}
  ]
}
```

3.3.3 Change user password

1. Request

Parameter definition

No.	Format	Item	Required	Cardinality	Min. length	Max. length	Restrictions	Description
1	JSON [Body]	login_id	Yes	1..1	4	246	See Note (*)	User name of the target user
2		after_password	Yes	1..1	16	64	See Note (*)	New password
3		before_password	Yes	1..1	16	64	See Note (*)	Old password

(*): Upper / Lower case alphanumeric characters. For more details, please refer to K5 Portal User Guide (1.1.2 Essential Information for the use of the K5 Portal) input restrictions.

Example:

```
{
  "login_id": "fujitsu123",
  "after_password": "Newpassword12345678",
  "before_password": "Abcdefgh12345678"
}
```

2. Response

HTTP STATUS: 200

Response body:

No.	Format	Item	Cardinality	Description
1	JSON [BODY]	accesstoken_destruction_information_list	1..1	User information whose token was cancelled.
2		customer_group_id	1..1	Group ID to which the user belongs to.
3		login_id	1..1	Login ID of the user.

Example:

```
{
  "accesstoken_destruction_information_list": [
    {
      "customer_group_id": "HvlgXxym",
      "login_id": " fujitsu123"
    }
  ]
}
```

3.3.4 Delete user

1. Request

Parameter definition

No.	Format	Item	Required	Cardinality	Min. length	Max. length	Restrictions	Description
1	URL query parameter	login_id	Yes	1..1	4	246	See Note (*)	User name of the user to be deleted

(*): Upper / Lower case alphanumeric characters. For more details, please refer to K5 Portal User Guide (1.1.2 Essential Information for the use of the K5 Portal) input restrictions.

Example:

```
/API/v1/api/users/?login_id= fujitsu123
```

2. Response

HTTP STATUS: 200

Response body:

No.	Format	Item	Cardinality	Description
1	JSON [BODY]	accesstoken_destruction_information_list	1..1	User information whose token was cancelled.
2		customer_group_id	1..1	Group ID to which the user belongs to.
3		login_id	1..1	Login ID of the user.

Example:

```
{
  "accesstoken_destruction_information_list": [
    {
      "customer_group_id": "HvlgXxym",
      "login_id": " fujitsu123"
    }
  ]
}
```

3.3.5 Update user authentication information

1. Request

Parameter definition

No.	Format	Item	Required	Cardinality	Min. length	Max. length	Restrictions	Description
1		login_id	Yes	1..1	4	246	See Note (*)	User name of the target user
2	JSON [Body]	authentication_method	Yes	1..1	1	1	See Note (*)	Authentication method for the user 0: Authentication by a password 1: Authentication by a certificate & password

(*): Upper / Lower case alphanumeric characters. For more details, please refer to K5 Portal User Guide

Example:

```
{
  "login_id": "fujitsu123",
  "authentication_method": "1",
}
```

2. Response

HTTP STATUS: 200

Response body:

No.	Format	Item	Cardinality	Description
1	JSON [Body]	authentication_method	1..1	Authentication method for the user. 0: Authentication by a password 1: Authentication by a certificate & password
2		accesstoken_destruction_information_list	1..1	User information whose token is to be canceled.
3		customer_group_id	1..1	Contract number of the user whose token is to be canceled.
4		login_id	1..1	Login ID of the user whose token is to be canceled.

Example:

```
{
  "authentication_method": "1",
  "accesstoken_destruction_information_list": [
    {
      "customer_group_id": "HvlgXxym",
      "login_id": "fujitsu123"}
  ]
}
```


FUJITSU Cloud Service K5

API Reference Manual Version 1.4

Issued August 2017

All Rights Reserved, Copyright FUJITSU LIMITED