FUJITSU Cloud Service K5 - API Management Service Description

August 8, 2018

1. API Management Service Overview

API Management Service is built on Apigee Edge, an integrated API platform product provided by Apigee Corporation. The Customer may use one APIM organization per Contract Number, where 'an organization' is a unit of management which permits the Customer to use two environments: one for test and one for production. This API Management Service provides the functions described in this section and the Customer can select either 'Pro' or 'Standard' for this API Management Service described in Attachment Table 1. The amounts payable for this API Management Service are calculated based on the number of calls made at the rates prescribed by the Customer Agreement. "Call" for the purposes of that calculation means an action that connects an application to the back-end service via an API Proxy that the Customer has set up using this API Management Service.

(1) Gateway Service

This API Management Service provides functions that enable applications that are accessible on the web to be connected by other applications as follows (An application that can be accessed via the web and is connected via the gateway service is referred to as a back-end service):

1) APIs

This API Management Service provides functions that support configuration management and development of APIs for back-end services.

i. API Proxies

By entering prescribed information, the Customer can create an API Proxy (a unit of service that executes the processing between the back-end service and the application to be connected to the back-end service), and then set up policies and flows. The Customer can then deploy the created API Proxies in the test or production environment and use the trace function to make the status of requests and responses processed by the API Proxies visible and displayed.

- Policy

  The Customer can specify polices for the API Proxies as follows.

Policy type	Details
TRAFFIC MANAGEMENT (Traffic control policy)	Specifies the limits of the numbers of requests and concurrent connections to the back-end service or to store the results of prescribed information or processing results in cache.
SECURITY (Security policy)	Adds access authentication for APIs of the back-end service or the limits of the transfer of messages in XML format or JSON format.
MEDIATION (Mediation type policy)	Specifies the format conversion in transferring messages between the back-end service and the application connecting to the back-end service.
EXTENSION (Extension policy)	Specifies execution of JavaScript or external services and/or collection and storage of data, etc. in accordance with the prescribed conditions.

- Flow

  The Customer can control when to execute policies by specifying the flow for the API Proxies.

ii. Environment Configuration

The Customer can create categories of cache handled by the TRAFFIC MANAGEMENT policies of the API Proxies, such as responses from the back-end service or unprescribed data.

2) Publish

This API Management Service provides a function that enables APIs for the back-end service to be used in the production environment via one or more API Proxy groups (referred to as an “API Product”).

i. Product

This function enables the creation of an API Product. It is possible to specify policies and flows in a batch for the API Product.

ii. Developer

This function allows an End User to be registered as a Developer.

iii. Developer Apps

This function enables a unique API Key to be generated for a combination of applications being connected to the back-end service, one Developer, and one or more API Products. By having the Developer access the back-end service using the API Key so generated, it becomes possible to identify a Developer connecting to the back-end service or to set access limits for respective Developers.

3) Gateway Extension Function

An extension function for gateway services is provided.

i. Publishing APIs in the Customer’s own domain

APIs can be published in the Customer’s own domain.

ii. Setting connection limits to published APIs

Access to published APIs can be limited by specifying the IP addresses of the access sources.

iii. Java function

A function is provided to call and execute Java applications as part of EXTENSION (Extension policy).

(2) Analytics Service

1) Analytics

Usage, performance, and other items related to the API Proxies and developers can be analyzed by a Customer as follows by collecting, analyzing and monitoring the API traffic information (Refer to Attachment Table 1 Service Plan List regarding the functions available under each of the service plans.):

Analysis pattern	Details
Proxy Performance	Creates a chart showing API Proxy traffic volume and average response time.
Target Performance	Creates a chart showing for back-end services the amount of traffic and the number of successful or failed requests, response time, the number of successful or failed responses and payload size.
Cache Performance	Creates a chart showing the hit rate, the number of hits and response time, about cache processed through the TRAFFIC MANAGEMENT policy.
Latency Analytics	Creates a chart showing response time of API Proxy and back-end services.
Error Analytics	Creates a chart showing error information for requests and responses processed by API Proxies (the number of errors, status codes).
Developer Engagement	Creates a chart showing the numbers, access status, amount of traffic and error rate of Developers.
Traffic Composition	Creates a chart showing the top 10 in terms of the volume of traffic about API Proxies, API Products, Developer and application.

Business Transactions	Creates a chart showing amount of traffic for requests, average response times, error rate, amount of data transferred (total data size of request and response) of a back-end service specified by the designated URI.
Devices	Creates a chart showing information on a device accessing an API Proxy (platform, agent, device type, OS type)
Custom Reports	Creates a chart showing information on the selected metrics and dimensions, and a term for analysis.

If the Customer changes from Pro to Standard, detailed data (i.e. log obtained per one request by API) retained for Analytics Service will be deleted upon such change. Also, if the Customer changes from Standard to Pro, such detailed data start being obtained upon such change.

(3) End User Management Function

1) Admin

The Customer can register End Users to use the functions or manage the resources provided under this API Management Service, and configure access privileges for the following functions by specifying a role for each user.

- ➢ API Proxies and Environment Configuration of the APIs
- ➢ Product and Developers Apps of the Publish function
- ➢ Custom Reports of the Analytics function

The following default roles can be specified as the initial settings:

Default role	Details	
User	Available functions	Setting the API Proxy policies and flows, API Proxy trace function, deployment of API Proxies in the test environment.
	Referable functions	Deployment of API Proxies in the production environment, Publish, Analytics.
	Unavailable functions	Environment Configuration, Administration.
Business User	Available functions	API Proxy trace function, deployment of API Proxies in the test environment, Publish, Analytics.
	Referable functions	Setting the API Proxy policies and flows, deployment of API Proxies in the production environment.
	Unavailable functions	Environment Configuration, Administration.
Operations Administrator	Available functions	Deployment of API Proxies, API Proxy trace function.
	Referable functions	Setting the API Proxy policies and flows, Publish, Analytics.
	Unavailable functions	Environment Configuration, Administration.
Organization Administrator	All functions are available	

In addition to the default roles, a new role, to which an arbitrary access privilege is assigned, can be created.

(4) Back-end Secure Connection Function

When the Customer builds back-end services in its own environment, this function enables the back-end services to be connected directly to this service without deploying the back-end services in a DMZ. The back-end secure connection is facilitated by the IPsec VPN function [*1].

With this function, the Customer can publish APIs to the connected network environment. Also, this function provides the DNS function as its option. With this DNS function, the Customer can resolve the name of the FQDN required when APIs are published.

(5) Web APIs

The following features of this Service can be executed by Web APIs.

1) Obtaining, uploading, and exporting of the list of SSL certificates performed as a part of the gateway extension function or the backend secure connection function
2) Obtaining the detailed data and the summary data of Analytics Service

2. Conditions of Use

(1) The Customer agrees that Fujitsu receives, stores, processes, and uses data transferred via API Proxies for the purpose of provision of this API Management Service.

(2) The Customer will be responsible for the access control and management of APIs of the back-end services and API Proxies. Fujitsu will take no responsibility in the event of any damage suffered by the Customer or a third party due to use by any third party.

(3) The Customer agrees that software that is included in this API Management Service may be updated from time to time and that Fujitsu may apply a patch to software without prior notice.

(4) The rights to the software that is included in this API Management Service belong to Apigee Corporation or its licensors, and Fujitsu provides this API Management Service under license from Apigee Corporation. The Customer agrees that, if the Customer breaches the Terms of Use in regard to use of this API Management Service and its licensed software, then Apigee Corporation may exercise its rights under the terms of Use in respect of the Customer, to the extent that the license is applicable.

(5) The Customer may not place any requests or inquiries about use of or access to this API Management Service directly with Apigee Corporation under any circumstance.

3. Availability by Region

This API Management Service is available in the following regions (Refer to Attachment Table 1 Service Plan List regarding the functions available under each of the service plans.):

- Eastern Japan Region 1
- UK Region 1
- Finland Region 1
- Germany Region 1
- Spain Region 1
- US Region 1

4. Restrictions and notes

Provision of this API Management Service and access to its components commences when Fujitsu has completed setting up for the Customer after the Customer has applied for this API Management Service in a way prescribed by Fujitsu. Fees for full one month are charged from the month in which Fujitsu completes setting up. API Proxies are exposed to the Internet once they are deployed in the environment under this API Management Service. The Customer is solely responsible for access control and management of API Proxies and other general security matters. The Customer must register CNAME (a setting to direct the Customer’s domain to Fujitsu’s domain) with the DNS server to publish APIs in the Customer’s own domain. Note that the Customer is required to upload SSL certificates via a Web API if APIs are used over HTTPS.

Footnotes:

*1: A method of connection in which the IPsec VPN function of the FUJITSU Cloud Service for OSS IaaS is used autonomously. Contact the Help Desk prior to using this method as the setting information required for the IPsec VPN function must be requested separately.

Attachment Table 1 Service Plan ListEastern Japan Region 1, UK Region 1

Service Plan Available Function		Basic Configuration			Gateway Extension Configuration			Back-end Secure Connection Configuration		
		Pro	Standard		Pro	Standard		Pro	Standard	
			10M/20M ∗1	3M		10M/20M ∗1	3M		10M/20M ∗1	3M
(1) Gateway Service	1) APIs	A	A	A	A	A	A	A	A	A
	2) Publish	A	A	A	A	A	A	A	A	A
	3) Gateway Extension Function	N/A	N/A	N/A	A	A	A	A	A	A
(2) Analytics Service ∗2	Proxy Performance	A	A	A	A	A	A	A	A	A
	Target Performance	A	A	A	A	A	A	A	A	A
	Cache Performance	A	E	N/A	A	E	N/A	A	E	N/A
	Latency Analysis	A	A	A	A	A	A	A	A	A
	Error Analysis	A	A	A	A	A	A	A	A	A
	Developer Engagement	A	E	N/A	A	E	N/A	A	E	N/A
	Traffic Composition	A	A	A	A	A	A	A	A	A
	Business Transactions	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Devices	A	A	A	A	A	A	A	A	A
	Custom Reports	A	A	A	A	A	A	A	A	A
(3) End User Management Function		A	A	A	A	A	A	A	A	A
(4) Back-end Secure Connection Function ∗3		N/A	N/A	N/A	N/A	N/A	N/A	A	A	A
(5)WebAPI ∗4		A	A	A	A	A	A	A	A	A

Finland Region 1, Germany Region 1, Spain Region 1, US Region 1

Service Plan Available Function		Basic Configuration	
		Pro	Standard
(1) Gateway Service	1) APIs	A	A
	2) Publish	A	A
	3) Gateway Extension Function	N/A	N/A
(2) Analytics Service ∗2	Proxy Performance	A	A
	Target Performance	A	N/A
	Cache Performance	A	N/A
	Latency Analysis	A	A
	Error Analysis	A	N/A
	Developer Engagement	A	N/A
	Traffic Composition	A	A
	Business Transactions	A	A
	Devices	A	A
	Custom Reports	A	A
(3) End User Management Function		A	A
(4) Back-end Secure Connection Function ∗3		N/A	N/A
(5)WebAPI ∗4		A	A

A: Available

E: Available under the Full Analytics Plan (*5)

N/A: Not available

*1 The Full Analytics Plan can be selected.

*2 Different Analytics Patterns are available between the Pro and the Standard plans. For details, refer to 1. Service Specifications > (2) Analytics Services > Analytics.

*3 The DNS option is available only in Eastern Japan Region 1.

*4 In the Basic Configuration, only the data acquisition API in the Analytics Service can be executed.

*5 The Full Analytics Plan is available only in Eastern Japan Region 1.

*6 The change between the plans is available as shown in the following table.

Change to: Change from:	Basic Configuration Pro	Basic Configuration Standard 3M	Basic Configuration Standard 10M	Basic Configuration Standard 20M	Gateway Extension Configuration Pro	Gateway Extension Configuration Standard 3M	Gateway Extension Configuration Standard 10M	Gateway Extension Configuration Standard 20M	Back-end Secure Connection Configuration Pro	Back-end Secure Connection Configuration	Back-end Secure Connection Configuration	Back-end Secure Connection Configuration
Basic Configuration Pro		HD	HD	HD	-	-	-	-	-	-	-	-
Basic Configuration 3M	HD		SP	SP	-	-	-	-	-	-	-	-
Basic Configuration 10M	HD	SP		SP	-	-	-	-	-	-	-	-
Basic Configuration 20M	HD	SP	SP		-	-	-	-	-	-	-	-
Gateway Extension Configuration Pro	-	-	-	-		HD	HD	HD	-	-	-	-
Gateway Extension Configuration Standard 3M	-	-	-	-	HD		SP	SP	-	-	-	-
Gateway Extension Configuration Standard 10M	-	-	-	-	HD	SP		SP	-	-	-	-
Gateway Extension Configuration Standard 20M	-	-	-	-	HD	SP	SP		-	-	-	-
Back-end Secure Connection Configuration Pro	-	-	-	-	-	-	-	-		HD	HD	HD
Back-end Secure Connection Configuration Standard 3M	-	-	-	-	-	-	-	-	HD		SP	SP
Back-end Secure Connection Configuration Standard 10M	-	-	-	-	-	-	-	-	HD	SP		SP
Back-end Secure Connection Configuration Standard 20M	-	-	-	-	-	-	-	-	HD	SP	SP	

SP: Possible to change (apply via the Service Portal)

HD: Possible to change (request via the Help Desk)

-: Not possible to change

Supplementary Provision (July 31, 2016)

The present Service Description is effective from July 31, 2016.

Supplementary Provision (August 19, 2016)

The present Service Description is effective from August 19, 2016.

Supplementary Provision (January 27, 2017)

The present Service Description is effective from January 27, 2017.

Supplementary Provision (March 23, 2017)

The present Service Description is effective from March 23, 2017.

Supplementary Provision (May 8, 2017)

The present Service Description is effective from May 8, 2017.

Supplementary Provision (August 9, 2017)

The present Service Description is effective from August 9, 2017.

Supplementary Provision (March 22, 2018)

The present Service Description is effective from March 22, 2018.

Supplementary Provision (August 8, 2018)

The present Service Description is effective from August 8, 2018.