Contents

- About Web API
- Major Web API Usage Scenarios
- Service Overview
- API Management Features
- Functions for Publishing APIs
- API Development Flow
- API Proxy Functions
  - Policy
  - Flow
- Development Functions
  - Deploy Function
  - API Tracer Function
  - Publish Function
- Analytics & Monitoring Functions
  - Analytics
  - Custom Report
  - Dashboard
  - Gateway Extension Function (Publishing APIs in Own Domain)
  - Gateway Extension Function (Limit Connections to Published APIs)
  - Gateway Extension Function (Java Function)
  - Back-end Secure Connection Function (IPsec VPN Connection)
  - Web APIs
- Service Account and Environment
- Service Menu
- Billing Model
  - Pro Plan
  - Standard Plan
- Changing Plans
- Using the Back-end Secure Connection
- Restrictions and Notes
- References
About Web API

- Web API enables IT engineers to access various kinds of services through programming code
  - API users can access various functionality by aggregating many kinds of APIs. Engineers are starting to customize applications themselves or create new applications using APIs.

- Differences from existing web-based systems
  - Existing web-based systems provide data and functions via a screen (HTML-based).
  - The Web API only exchanges data. The client side is not necessarily a browser. (Any HTTP compatible format can be used)
Major Web API Usage Scenarios

Service mash-up
- Cloud service
- Open data
- Own system
- Private API
- Shop guide/ Navi
- Area service

Community-wide usage
- SNS link/ advertisement
- Data analytics
- Buzzword Search
- Marketing

Mobile back-end (MBaaS)
- Mobile app
- Data storage
- Membership mgmt
- Location data
- SNS link

Cloud platform/ development environment
- Developer
- Source code mgmt service
- Commit, push.....
- Set, activate, deploy.....

Public API

Copyright 2016-2018 FUJITSU LIMITED
Service Overview

K5 API Management provides valuable functionality such as API development, publishing, enhancement and operation. K5 API Management will continuously contribute to your business.

API PROXY

Safe access
- Authorization
- Security checking
- Traffic control

Improved convenience
- Request/response editor
- Service mashup
- Cache
- API programmability
- API version management

Monitoring & reporting
- Monitoring of API traffic
- Dashboard display
- Customized reporting

Offered by FUJITSU Cloud Service K5
# API Management Features

- **Functions provided by the API Management service**
  - Shared functions/ Private API functions
  - Public API functions

<table>
<thead>
<tr>
<th>Compatibility/ connection</th>
<th>Optimization</th>
<th>Security</th>
<th>API development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract data from messages</td>
<td>Response cache</td>
<td>OAuth 2.0</td>
<td>Add-on programs</td>
</tr>
<tr>
<td>Convert XSL</td>
<td>Key value store</td>
<td>Basic authentication</td>
<td>Development/ operation environment</td>
</tr>
<tr>
<td>Convert SOAP to REST</td>
<td>Limit the number of concurrent connections</td>
<td>SAML support</td>
<td>Non-stop deployment</td>
</tr>
<tr>
<td>Edit requests</td>
<td>Prevent traffic spikes</td>
<td>LDAP link</td>
<td>Multi-version management</td>
</tr>
<tr>
<td>Edit responses</td>
<td>Limit traffic volume</td>
<td></td>
<td>Policy/ flow editor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Publishing</th>
<th>Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package APIs</td>
<td>Statistics for the operations administrator</td>
</tr>
<tr>
<td>Set ACL (update/reference)</td>
<td>API developer usage statistics</td>
</tr>
<tr>
<td>Limit traffic volume</td>
<td>Application statistics</td>
</tr>
<tr>
<td>Assign key (API keys)</td>
<td>Business statistics</td>
</tr>
</tbody>
</table>

- **Shared functions**
- **Functions for Public API**
- **Functions for Private API**

- **Compatibility/ connection**
  - Extract data from messages
  - Convert XSL
  - Convert SOAP to REST
  - Edit requests
  - Edit responses

- **Optimization**
  - Response cache
  - Key value store
  - Limit the number of concurrent connections
  - Prevent traffic spikes
  - Limit traffic volume

- **Security**
  - OAuth 2.0
  - Basic authentication
  - SAML support
  - LDAP link

- **API development**
  - Add-on programs
  - Development/ operation environment
  - Non-stop deployment
  - Multi-version management
  - Policy/ flow editor
  - Monitoring (API performance, errors)
Functions for Publishing APIs

- Functions are offered to simplify the publishing of APIs

### Convert protocol/data format

<table>
<thead>
<tr>
<th>Published API</th>
<th>Existing applications</th>
<th>Add authentication functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTful API</td>
<td>SOAP interface</td>
<td>OAuth authentication</td>
</tr>
<tr>
<td>RESTful API</td>
<td>XML data</td>
<td>API key authentication</td>
</tr>
</tbody>
</table>

### Add authentication functions

<table>
<thead>
<tr>
<th>Published API</th>
<th>Non-authenticated API</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>API in system</td>
</tr>
<tr>
<td></td>
<td>API in system</td>
</tr>
</tbody>
</table>

### Publish APIs without an AP server/mash-up of existing APIs

<table>
<thead>
<tr>
<th>Published API</th>
<th>DB server</th>
<th>Add-on programs (Java, JavaScript, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTful API</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Published API</th>
<th>Existing API</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XX function API</td>
</tr>
<tr>
<td></td>
<td>YY function API</td>
</tr>
</tbody>
</table>

Add-on programs
The following chart shows the process flow for developing an API using the API Management service.

**API proxy functions**
- Create/correct an API proxy
  - Configure an API proxy
  - Configure policies
  - Configure the flow

**Development functions**
- Deploy
  - Development environment
  - Production environment
- Debug
  - Trace function

**Publishing function**
- Publish API
  - Create an API product
  - Register application developers
  - Register applications
  - Generate API keys

**Analysis & monitoring functions**
- Analyze & monitor
  - Various analytics screens
  - Custom reporting
  - Dashboard

Enhance
- API developer
The API Proxy is a core component of API Management and acts as a gateway. The API provider can flexibly edit the API request and response without writing any code.

- Policy (add various kinds of features to the back-end service)
- Flow (control the processing sequence of the attached policy)
API Proxy Function – Policy

The Policy is easily attached to your API. This significantly reduces the amount of coding required.

More than 30 functions can be added through configuration only, without any coding

- Authentication/security
- Modification of request/response information
- Caching
- Restriction of traffic volume
- Data format conversion
- Logging

*For all functions, please refer to: 'APIM: Reference: Policy’

Custom functions can be added using scripts

- JavaScript
- Java
- Python
- Node.js

Back-end services can be implemented on API Proxy

Administrators can place a policy icon on the API proxy screen and end users can use the added functions

Reduce Time to market
Policies are run at the appropriate time. The flow defines the policy order and scope for each API.

- **PreFlow**: Specify policies to be run prior to Conditional Flows.
- **Conditional Flows**: Specify policies to be run only in response to certain requests (specify conditions).
- **Post Flow**: Specify policies to be run after Conditional Flows.
- **PostClientFlow**: Specify policies to be run after sending a response to the application.

A Policy is easily attached Using a GUI-based flow editor.
Realize effective API development using the Deploy, Version Management, and Environment functions.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Item</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy</td>
<td>Seamless</td>
<td>Deploy API Proxy with minimal change to back-end applications</td>
</tr>
<tr>
<td></td>
<td>Multi version Deployment</td>
<td>Support multiple version deployment in the same environment</td>
</tr>
<tr>
<td>Version Management</td>
<td>Version</td>
<td>API Proxy manages the lifecycle changes of API policy configurations</td>
</tr>
<tr>
<td></td>
<td>Revision</td>
<td>Revision (smaller unit of a version) support</td>
</tr>
<tr>
<td>Environment</td>
<td>Test/ prod environment</td>
<td>Prepare both test and production environments</td>
</tr>
<tr>
<td></td>
<td>HTTP／HTTPS</td>
<td>HTTP/HTTPS are available</td>
</tr>
</tbody>
</table>
Development Function – API Tracer

API Tracer enables developers to debug APIs effectively by displaying API proxy transactions and clarifying each policy's result.

**Transaction Map**
- Displays each step of a transaction using icons.
- Details are displayed by clicking an icon.
- The masking function hides confidential information when icon details are displayed.
- End users can trace transactions using tools such as a browser, curl, etc.

**Filter**
- Transactions can be filtered in the trace with the following conditions.
  - HTTP header
  - Query parameter

**Offline Trace**
- Results of a trace can be exported and imported via the online trace screen.
Publish Function

This function is used to publish the created APIs (API Proxy) to the application developers. It can publish packaged API Proxy as a product based on usage by configuring access rights and traffic restrictions.

Supports flexible product offerings which meet business demands

The API keys required to run an API are provided when application developers, applications and the products to be used are registered.

Example of Products
- Free version (refer to data with restrictions on traffic)
- Lite version (update of data with restrictions on traffic)
- Full version (update of data without restrictions on traffic)

(* )Scope of management by the Publish function is shown in Red
The Analytics service enables effective operation and boosts business using various kinds of real time reports.

Example of Collection of API Traffic

Analytics Screen

End users can monitor the information collected via the following 9 screens:

- Proxy Performance
- Target Performance
- Cache Performance
- Latency Analytics
- Error Analytics
- Developer Engagement
- Traffic Composition
- Business Transactions
- Devices

* For details of each screen, please refer to: ‘APIM: Reference: Analytics List’
Custom Report enables users to create tailored reports by choosing the horizontal (Dimensions) and vertical (Metrics) axes.

**Custom Report Example**

**Dimensions**
- Users can specify the type of information they want included in traffic reports, such as the IP addresses of clients, OS types, etc.
- End users can select multiple dimensions and then drill down to further analyze the statistical data.

**Drill down example**
The “OS” and “IP address” dimensions are selected to help analyze the usage of Windows by each IP address.

**Metrics**
- Users can select information related to API usage such as the number of requests, number of errors, response times, etc.
- The selected items are displayed using charts in the report.

**Filter**
- Statistical data can be filtered when Dimensions and Metrics are selected.
Dashboards provide end-to-end visibility using various metrics.

### Description

The following two dashboard options are available:

- **Predefined dashboards**
  Display all API Proxy traffic information on a single screen.
  E.g. API Proxy traffic, developer usage, app error rates

- **Custom Report dashboard**
  Four custom reports can be displayed on a single screen.
  Further details are shown by clicking on the chart name.
Analytics & Monitoring Function – Gateway Extension Function (Publishing APIs in Own Domain)

The Customer can use their own domain name rather than the ".paas.cloud.global.fujitsu.com" domain name provided by Fujitsu (so there is no need to change the URL to use the APIs). APIs can be published in the Customer’s domain (CNAME must be registered with the DNS server).

Publishing APIs in the Customer’s domain and example of use

API published as below:
- Domain name: api.mycompany.com
- Port number: 443

API User

```{  
  "catalog": [
    ...
  ]
}
```

API Proxy

Specify URL

K5 PaaS

API Management

Back-end service
IP addresses that are permitted to access the published APIs can be limited.

Setting connection limits for published APIs and an example of use

At the firewall, permit communication only with the access source of the following IP addresses: 203.0.113.0/24

```
$ curl -X GET -H "Content-Type: application/json" -H "Accept: application/json"
https://api.mycompany.com:443/v1/catalog
```

```
{
  "catalog": [
    ...
  ]
}
```

```
$ curl -X GET -H "Content-Type: application/json" -H "Accept: application/json"
https://api.mycompany.com:443/v1/catalog
```

Request

Response

Request

Response
The Java programs make links to business systems and DB servers possible. This enables API functions to be extended.

**Using Java programs**

**Create standard APIs**

- App server
- Business logic
- DB server
- Internal APIs/External APIs
- Mashup program

**Create APIs using the Java Callout Policy**

- Java program
- DB server
- Business system
- Virtual server function
- JavaCallout

New APIs
Analytics & Monitoring Function – Back-end Secure Connection Function (IPsec VPN Connection)

A secure connection to back-end services built in the cloud or on-premise environment is made possible using the IPsec VPN function* of FUJITSU Cloud Service K5 IaaS. Data sources of the back-end services that cannot be deployed in a DMZ can now be accessed. Functions for gateway expansion can also be used.

* Refer to the following link for details on the IPsec VPN function.
Analytics & Monitoring Function – Web APIs

- **Web APIs**

- A REST API that enables HTTPS access to the API services using the HTTP client

- Web APIs are published so that the following operations can be performed on the APIs
  - Procuring, uploading, and exporting of the SSL Certificate list (gateway extension function and back-end secure connection function)
    - The list can also be procured via the GUI.
  - Procuring analytics service data (procure statistical data on APIs, developers, and developer applications)
    - The data can be referenced via the GUI but Web APIs enable efficient analysis.

- Follow the web page reference trail below for details on the Web APIs that can be used:
  K5 Portal> Documents> Manuals> API Management> “Web API Reference”
Service Account and Environment

- **ID / Password API**
  - Notify the system administrator of the userID / password with administrative rights. This userID is permitted to add new user accounts.
  - Four roles are available: Organization Administrator, Operations Administrator, Business User and User.

- **Organization, Environment**
  - One organization is activated per contract.
  - Organization is a management unit of API Management.
  - Test and production environments are available for each organization.
## Service Menu

<table>
<thead>
<tr>
<th>Menu</th>
<th>Billing unit</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APIM Pro</td>
<td>Month</td>
<td>[Pro] No. of API calls (* aggregated every 3 months)</td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APIM Standard (3M)</td>
<td>Month</td>
<td>Pro (Fixed Menu) + Pay-per-use (Overage Option)</td>
</tr>
<tr>
<td>APIM Standard (10M)</td>
<td></td>
<td>• Fixed: 25 million calls/ 3 months</td>
</tr>
<tr>
<td>APIM Standard (20M)</td>
<td></td>
<td>• Overage Option: Per 2.5 million calls</td>
</tr>
<tr>
<td><strong>Advanced Gateway</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Gateway Pro</td>
<td>Month</td>
<td>[Standard] No. of API calls (* aggregated monthly)</td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Gateway Standard (3M)</td>
<td>Month</td>
<td>Standard (Fixed Menu) + Pay-per-use (Overage Option)</td>
</tr>
<tr>
<td>Advanced Gateway Standard (10M)</td>
<td></td>
<td>• Standard (3M): 3 million calls per month</td>
</tr>
<tr>
<td>Advanced Gateway Standard (20M)</td>
<td></td>
<td>• Standard (10M): 10 million calls per month</td>
</tr>
<tr>
<td><strong>Backend Secure Connection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backend Secure Connection Pro</td>
<td>Month</td>
<td></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backend Secure Connection Standard</td>
<td>Month</td>
<td></td>
</tr>
<tr>
<td>Standard (3M)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard (10M)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard (20M)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APIM Pro Overage</td>
<td>Per 2.5 million calls</td>
<td></td>
</tr>
<tr>
<td>APIM Standard Overage</td>
<td>Per 1 million calls</td>
<td></td>
</tr>
</tbody>
</table>
### Available Function for Pro/Standard

<table>
<thead>
<tr>
<th>Available Function</th>
<th>Service plan</th>
<th>Basic Configuration</th>
<th>Gateway Extension Configuration</th>
<th>Back-end Secure Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Pro</td>
<td>Standard</td>
<td>Pro</td>
</tr>
<tr>
<td><strong>(1) Gateway Service</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) APIs</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>2) Publish</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>3) Gateway Extension Function</td>
<td></td>
<td>–</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td><strong>(2) Analytics Service</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy Performance</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Target Performance</td>
<td></td>
<td>○</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td>Cache Performance</td>
<td></td>
<td>○</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td>Latency Analysis</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Error Analysis</td>
<td></td>
<td>○</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td>Developer Engagement</td>
<td></td>
<td>○</td>
<td>–</td>
<td>○</td>
</tr>
<tr>
<td>Traffic Composition</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Business Transactions</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Devices</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Custom Reports</td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td><strong>(3) Other functions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(4) Back-end Secure Connection Function</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(5) WebAPI</strong></td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

○ : Available  – : Not available
Billing Model (Pro Plan)

- Billing
  - Fixed monthly fee + pay-per-use (Extra Call Option) are billed based on the number of API calls subscribed to for this service.
  - Fixed monthly fee: Fixed fee per month
    Note: No. of API calls that can be made: 25 million/ 3 months
  - Pay-per-use (Extra Call Option): Per 2.5 million calls
    Note 1: Starts once the total number of API calls in a 3-month period exceeds 25 million
    Note 2: Billed/ invoiced at 3-monthly intervals
    However, if use of the service is canceled, billing/ invoicing takes place in the month that usage ends.

- Service start and end dates
  - The service start date is 3 business days after the date an application is lodged for using the service (i.e. the date an application is lodged via the K5 Portal).
  - Fees are charged from the month in which the service start date occurs to the month in which the service end date occurs.
  - The service end date is the date on which an application is lodged to turn off the service.

Refer to the next slide for billing example.
Billing Example

Billing Cycle A: Usage starts during month/ with pay-per-use
Aggregated quarterly, including usage start month. In the above example, the 25 million calls allowed under the fixed monthly fee plan is exceeded during the second month (month n+1), but is billed in the third month (month n+2) because of pay-per-use. Because 27.5 million < No. of calls ≤ 30 million, month n+2 is billed at \((x+y)\).

Billing Cycle B: Continuous usage/ without pay-per-use
Pay-per-use billing does not apply because the total number of API calls for the quarter is less than 25 million. Month n+5 is billed at \(x\).

Billing Cycle C: Contract canceled without the billing cycle reaching the full 3 months
Usage ends during the second month (month n+7) of the billing cycle. Pay-per-use is billed at the end of the month in which usage ends. Month n+7 is billed at \((x+y)\).
Billing Model (Standard Plan)

- **Fixed monthly fee + Pay-per-use**
  - Fixed monthly fee + pay-per-use (Extra Call Option) are billed based on the number of API calls subscribed to for this service
  - Fixed monthly fee: Fixed fee per month
    - Note: No. of API calls that can be made: subscribed Plan per month
  - Pay-per-use (Extra Call Option): Per million calls
    - Note 1: Starts once the number of API calls in a month period exceeds the number of calls allocated by the Plan.
    - Note 2: Billed/ invoiced at monthly intervals
  - Service start date and service end date
    - Same as the Pro Plan.

Example:

<table>
<thead>
<tr>
<th>No. of API calls</th>
<th>Application date</th>
<th>Service start date</th>
<th>End of month n</th>
<th>End of month n+1</th>
<th>Service end date</th>
<th>End of month n+2</th>
</tr>
</thead>
<tbody>
<tr>
<td>3M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Monthly invoice + Pay-per-use invoice (Extra Call Option x 2)
- Monthly invoice
- Monthly invoice + Pay-per-use invoice (Extra Call Option x 1)

Note: Usage starts 3 business days after the application date.

The number of API calls is reset when the billing cycle ticks over.
Changing Plans

- The Customer may change their Plan to better suit their situation, such as the number of API calls and function usage.
  - The Customer can continue to use the same Organization, Environment, and registered API Proxies after changing the Plan.
  - There is no service down time (unable to log on to the service) while changing Plan.

- Changing of plans to and from the Basic Configuration, Gateway Extension Configuration, or Back-end Secure Connection Configuration is not permitted.
Changing Plans (between Standard Plans)

How to Change Plans

- Plans can be changed via the “Service In Use” of the K5 Portal.
- The Customer will be billed for the Plan current at midnight (00:00) on the first day of each month (UTC).

![Diagram]

Operation to make changes in Plan can be performed before midnight on the first day of each month.

- Change to Standard-5M
- Change to Standard-10M

Month n (Standard-3M in use) → Midnight on the 1st day of Month n+1 (UTC) → Month n+1 (changed to Standard-10M)
How to Change Plans

- Contact the Help Desk to change Plans from Pro to Standard or Standard to Pro. The Help Desk will advise the Customer on how to change plans. For details, refer to the FAQ published on the K5 website.
- The timing of the notification of Plan change will impact when the change takes effect.
  - If notified on or before the 20th: Effective from the following month
  - If notified between the 21st and the end of the month: Effective from the month after the next month

Notes on Changing Plans

Analytics Service

- When changing from the Pro to Standard Plan, data collected exclusively via the Pro Plan will be deleted. Therefore, the Customer will no longer be able to use the Analytics patterns provided exclusively via the Pro Plan.
- When changing from the Standard to Pro Plan, data collected exclusively by the Pro Plan will start accumulating. Therefore, from the month in which the Pro Plan begins, the Customer can start using the Analytics patterns provided exclusively via the Pro Plan.
Notes on Changing Plans

Billing

- The aggregation cycle of API calls (normally quarterly) is reset when the Plan is changed to Standard during the Pro billing cycle.

Example: The following sample shows the Plan changed to Standard during the second month of the Pro billing cycle (B) (effective from the next month).
Using the Back-end Secure Connection

- To connect to this service, the connection with the counterpart IPsec VPN gateway must be registered. Please contact the Help Desk for details. For details, refer to the following FAQs: https://apimng.uk-1.paas.cloud.global.fujitsu.com/docs/faq.pdf

- A flow of the stages leading up to service usage is as follows:

1) Contact the Help Desk
2) Instructions on how to apply, check environment information
3) Apply to use the back-end secure connection (via the K5 portal)
4) Notified of procedure completion
5) Final check, start using

Customer → Help Desk → Customer → Help Desk → Customer
Restrictions and Notes

- Refer to the Service Description on the FUJITSU Cloud Service K5 website to confirm the regions in which this service is offered.

- The time required from application submission to start of service is as follows:
  - Basic Configuration Plan (Pro and Standard): Within three business days from completing the application via the service settings application screen on the K5 Portal.
  - Gateway Extension Configuration Plan (Pro and Standard): Deployment in the environment will be completed approximately 10 business days after the application has been submitted via the service settings application screen on the K5 portal.
  - Back-end Secure Connection Configuration Plan (Pro and Standard): Before lodging the application form, contact the Help Desk to confirm the information regarding the line connecting to the back-end services. The service can be used approximately 10 business days after confirmation of the line information.
# APIM: Reference: Policy - Traffic Management

## API traffic processing (flow control, caching, etc.)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota</td>
<td>Uses the Quota policy to configure the number of request messages that an API proxy allows over a period of time; such as a minute, hour, day, week, or month.</td>
</tr>
<tr>
<td>Spike Arrest</td>
<td>Throttles the number of requests generated per second e.g. If set to allow 30 requests every minute (30pm) then 1 request will be allowed in 2 seconds. If it receives 2 requests within 2 seconds, then the 2nd request will be denied.</td>
</tr>
<tr>
<td>Concurrent Rate Limit</td>
<td>Throttles inbound concurrent connections from your API proxies running on Apigee Edge to your back-end services.</td>
</tr>
<tr>
<td>Response Cache</td>
<td>Caches the response from a back-end resource.</td>
</tr>
<tr>
<td>Lookup Cache</td>
<td>Retrieves the data cached by Populate Cache.</td>
</tr>
<tr>
<td>Populate Cache</td>
<td>Caches data such as session IDs, authorization values, etc.</td>
</tr>
<tr>
<td>Invalidate Cache</td>
<td>Deletes cached data specified in the conditions.</td>
</tr>
<tr>
<td>Reset Quota</td>
<td>Allows resetting of the no. of requests counted by the Quota policy based on specific variables.</td>
</tr>
</tbody>
</table>
## APIM: Reference: Policy - Data Processing

API data processing (format change, message modification, etc.)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON to XML</td>
<td>Converts messages from JSON format to XML format</td>
</tr>
<tr>
<td>XML to JSON</td>
<td>Converts messages from XML format to JSON format</td>
</tr>
<tr>
<td>Raise Fault</td>
<td>Generates a custom message in response to a status code (error condition)</td>
</tr>
<tr>
<td>XSL Transform</td>
<td>Transforms XML to another format, such as HTML, plain text or other format</td>
</tr>
<tr>
<td>SOAP Message Validation</td>
<td>Validates a message against an XSD schema or WSDL definition and rejects the message if it does not conform</td>
</tr>
<tr>
<td>Assign Message</td>
<td>Creates or modifies an HTTP request or response messages (during an API proxy flow)</td>
</tr>
<tr>
<td>Extract Variables</td>
<td>Extracts information from a request or response and sets a variable (with the specified message content)</td>
</tr>
<tr>
<td>Access Entity</td>
<td>Retrieves the entity profiles of developers, apps, API products, etc. and places these in a variable</td>
</tr>
<tr>
<td>Key Value Map Operations</td>
<td>Key / Value pairs can be stored, retrieved and deleted using PUT, GET, DELETE</td>
</tr>
</tbody>
</table>
# API security restrictions (Authorization, Vulnerability Management, etc.)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authentication</td>
<td>Sets Basic Authentication (Base64 encoding and decoding)</td>
</tr>
<tr>
<td>XML Threat Protection</td>
<td>Addresses XML vulnerabilities and minimizes attacks on your API</td>
</tr>
<tr>
<td>JSON Threat Protection</td>
<td>Addresses JSON vulnerabilities and minimizes attacks on your API</td>
</tr>
<tr>
<td>Regular Expression Protection</td>
<td>Rejects requests that include regular expressions</td>
</tr>
<tr>
<td>OAuth v2.0</td>
<td>Allows you to configure (generate and verify access tokens, etc.) OAuth v2.0 endpoints</td>
</tr>
<tr>
<td>Get OAuth v2.0 Info</td>
<td>Retrieves the attributes of OAuth v2.0’s access tokens and authorization codes, etc.</td>
</tr>
<tr>
<td>Set OAuth v2.0 Info</td>
<td>Adds or updates custom attributes associated with OAuth v2.0 access tokens</td>
</tr>
</tbody>
</table>
### API security restrictions (Authorization, Vulnerability Management, etc.)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth v1.0a</td>
<td>Allows you to configure (generate and verify access tokens, etc.) OAuth v1.0a endpoints</td>
</tr>
<tr>
<td>Get OAuth v1.0a Info</td>
<td>Retrieves the attributes of OAuth v1.0a’s access tokens, authorization codes, etc.</td>
</tr>
<tr>
<td>Verify API Key</td>
<td>Allows you to configure the API Key that allows access</td>
</tr>
<tr>
<td>Access Control</td>
<td>Allows or denies access to your APIs based on IP address</td>
</tr>
<tr>
<td>LDAP</td>
<td>Allows you to configure LDAP</td>
</tr>
<tr>
<td>Generate SAML Assertion</td>
<td>Attaches SAML assertions to outbound XML requests</td>
</tr>
<tr>
<td>Validate SAML Assertion</td>
<td>Validates SAML assertions that are attached to inbound SOAP requests and rejects them if they are invalid</td>
</tr>
</tbody>
</table>
APIM: Reference: Policy - Extension

Execute scripts and collect data in a message.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JS JavaScript</td>
<td>Implements custom behaviors using JavaScript</td>
</tr>
<tr>
<td>Service Callout</td>
<td>Allows calls to an external service (from your API proxy flow)</td>
</tr>
<tr>
<td>Statistics Collector</td>
<td>Collects statistics for data in a message, such as product ID, price, target URL, etc.</td>
</tr>
<tr>
<td>Message Logging</td>
<td>Logs custom messages to a local disk or to syslog</td>
</tr>
</tbody>
</table>
## Display traffic volumes, response times, no. of errors, etc.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Performance</td>
<td>Shows API traffic volumes and average processing times</td>
</tr>
<tr>
<td>Target Performance</td>
<td>Shows traffic volume patterns, success and failure of requests, response times, success and failure of responses, and payload size of back-end services</td>
</tr>
<tr>
<td>Cache Performance</td>
<td>Shows cache hits, cache hit rates and response times</td>
</tr>
<tr>
<td>Latency Analytics</td>
<td>Shows the response times for API and back-end services</td>
</tr>
<tr>
<td>Error Analytics</td>
<td>Shows error data (no. of errors, status codes, etc.) for API proxies and targets</td>
</tr>
<tr>
<td>Developer Engagement</td>
<td>Shows the no. of your registered app developers and their access status, traffic generated by them and errors</td>
</tr>
<tr>
<td>Traffic Composition</td>
<td>Gives a quick glance at the top 10 traffic patterns of APIs, products, developers, and applications</td>
</tr>
<tr>
<td>Business Transactions</td>
<td>Shows traffic volumes, response times, error rates, and amount of data exchanged (aggregate of requests and responses) based on a request generated by a specific URI</td>
</tr>
<tr>
<td>Devices</td>
<td>Provides information on the devices (platforms, agents, device types, OS, etc.) being used to access your APIs</td>
</tr>
<tr>
<td>Reports</td>
<td>Allows free selection of the matrix and dimensions (time) and generates charts</td>
</tr>
</tbody>
</table>
Fujitsu
shaping tomorrow with you