Technical Guide

OpenAPI security and authentication guides

October 2021

SAMSUNG SDS

Contents

1. Overview

An Application Programming Interface (API) is provided to enable usage of infrastructure/solution offerings of Samsung Cloud Platform. This document will describe the OpenAPI of Samsung Cloud Platform and how to call the API.

APIs are provided as RESTful APIs and respond in a JSON format. Parameter values can be entered, registered, modified, deleted, or searched according to the API. APIs are used for Post, Get, Put, and Delete method calls in HTTP and they return an error code and message if a call fails.

2. OpenAPI architecture

Samsung Cloud Platform offers OpenAPIs to enable developers to use functions called by users from the web console of major products (e.g. Virtual Server, Storage, or Network).

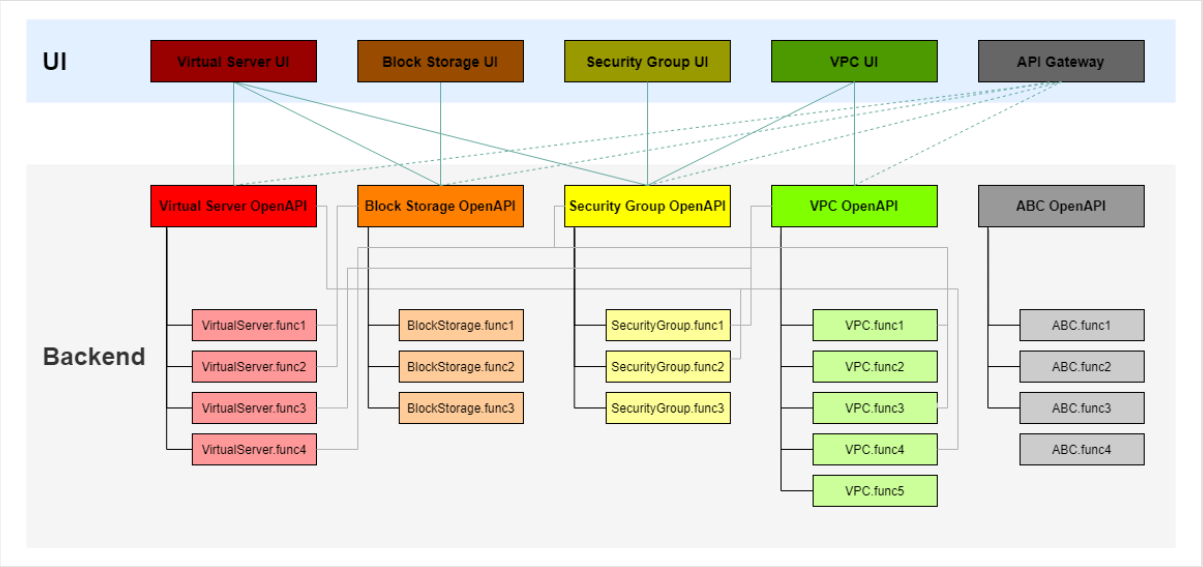


Figure 1. OpenAPI interworking architecture

Samsung Cloud Platform's OpenAPI is provided in a RESTful manner and is designed to organically link the functions of each offering.

- **UI**: The web console is designed to work with each product's OpenAPI.
- **Backend**: The functions provided by each product of the web console are linked with OpenAPI. K8s clusters and S3 among others, which are provisioned through external services other than Samsung Cloud Platform, are can also be provided in conjunction with OpenAPI.

3. OpenAPI security

3.1 Authentication key per group

Samsung Cloud Platform uses two authentication key values and also allows authentication keys in groups (projects). In consideration of users who use OpenAPI, security has been enhanced even further by issuing separate keys for each project.

3.2 MFA

To use OpenAPI, a temporary key is issued upon application of a multi-factor authentication (MFA). The authentication key and temporary key are used together as a pair.

3.3 HMAC algorithm

OpenAPI authentication keys are encoded with Base64 after encrypted with HMAC SHA256 algorithm.

3.4 IP access control

OpenAPI is applied with an IP access control function. If a high security level is required, API calls from unspecified IPs of external networks can be restricted.

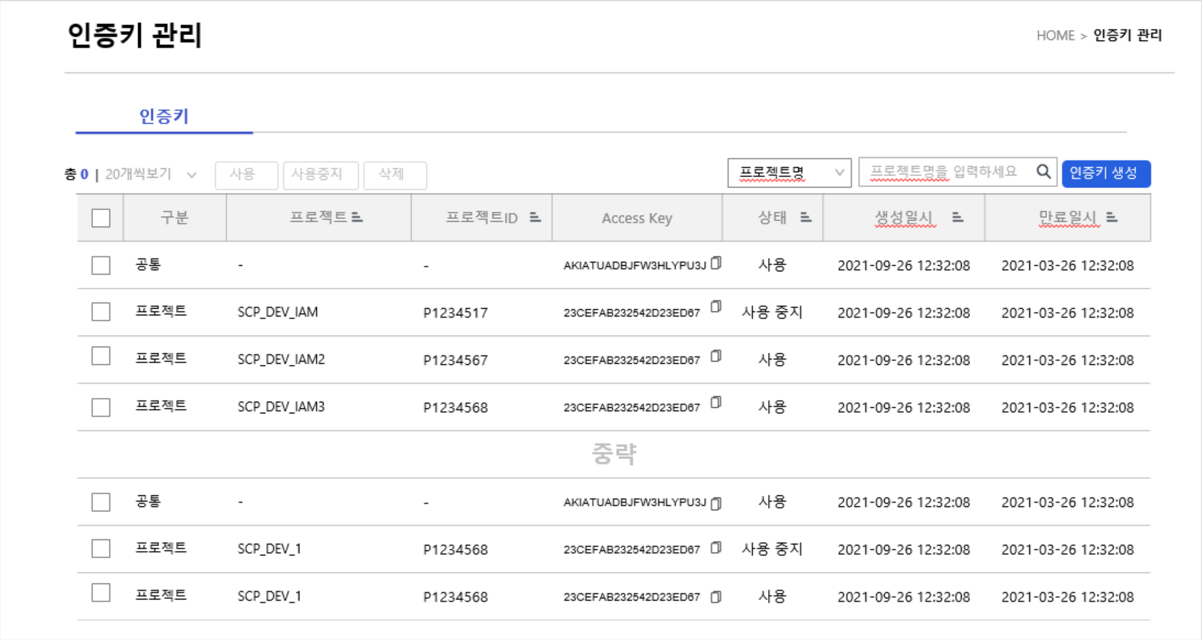
4. OpenAPI call procedure

4.1 Creation and management of authentication keys

To use the OpenAPI function of Samsung Cloud Platform, an authentication key is required. Authentication keys can be issued on [My Profile] > [Authentication Key Management] on the Samsung Cloud Platform console.

The authentication keys include user authentication keys (up to 2) and authentication keys for each project (up to 2). The procedure of creating one is as follows:

1. Log in to Samsung Cloud Platform.
2. Access [My Profile] > [Authentication Key Management] and click the ‘Generate new authentication key’ button.
3. Check issued Access Keys and Access Secret Keys from the authentication key list.



인증키 관리

HOME > 인증키 관리

총 0 | 20개씩보기

□	구분	프로젝트	프로젝트ID	Access Key	상태	생성일시	만료일시
□	공통	-	-	AKIATUADBJFW3HLYPU3J	사용	2021-09-26 12:32:08	2021-03-26 12:32:08
□	프로젝트	SCP_DEV_IAM	P1234517	23CEFAB232542D23ED67	사용 중지	2021-09-26 12:32:08	2021-03-26 12:32:08
□	프로젝트	SCP_DEV_IAM2	P1234567	23CEFAB232542D23ED67	사용	2021-09-26 12:32:08	2021-03-26 12:32:08
□	프로젝트	SCP_DEV_IAM3	P1234568	23CEFAB232542D23ED67	사용	2021-09-26 12:32:08	2021-03-26 12:32:08
				중략			
□	공통	-	-	AKIATUADBJFW3HLYPU3J	사용	2021-09-26 12:32:08	2021-03-26 12:32:08
□	프로젝트	SCP_DEV_1	P1234568	23CEFAB232542D23ED67	사용 중지	2021-09-26 12:32:08	2021-03-26 12:32:08
□	프로젝트	SCP_DEV_1	P1234568	23CEFAB232542D23ED67	사용	2021-09-26 12:32:08	2021-03-26 12:32:08

Figure 2. Authentication key management

4.2 Authentication parameters when calling API

- Authentication parameters

X-Cmp-AccessKey: Access Keys issued by the Samsung Cloud Platform portal
X-Cmp-Signature: A signature of the API request calls encrypted with an Access Secret Key that is mapped to the Access Key. HMAC encryption algorithm uses HMAC SHA256.
X-Cmp-Timestamp: Elapsed time defined in milliseconds since January 1, 1970 00:00:00 Coordinated Universal Time (UTC)

- Example of API calls using authentication parameters

```
curl -i -X GET
-H "X-Cmp-AccessKey:2sd2gg=2agdbSD26svcD"
-H "X-Cmp-Signature:fsfsdf235f9U35sdgf35Xsf/qgsdgsdg326=sfsdr23rsef="
-H "X-Cmp-Timestamp:1605290625682"
"https://cloud.samsungsds.com/iam/v2/access-keys”
```

4.3 Signature

A string to be signed is generated from the request, encrypted with the HMAC SHA256 algorithm using the Access Secret Key, and then encoded with Base64. This value is used as x-Cmp-Signature.

4.4 Sample Java code

```
public sstatic String makeHmacSignature(String method,
                                        String url,
                                        String timestamp,
                                        String accessKey,
                                        String accessSecretKey,
                                        String requestBody,
                                        String headerProjectId,
                                        String headerClientType,
                                        String mediaType) {
        StringBuilder builder = new StringBuilder().append(method)
                                             .append(url)
                                             .append(timestamp)
                                             .append(accessKey)
                                             .append(headerProjectId)
                                             .append(headerClientType);
        if (!mediaType.equals("MULTIPART_FORM_DATA")) {
            builder.append(requestBody);
        }

        String body = builder.toString();
        byte[] message = body.getBytes();
        byte[] secretKey = accessSecretKey.getBytes();

        String encodeBase64Str = null;
        try {
            Mac mac = Mac.getInstance("HmacSHA256");
            SecretKeySpec secretKeySpec = new SecretKeySpec(secretKey, "HmacSHA256");
            mac.init(secretKeySpec);
            byte[] hmacSha256 = mac.doFinal(message);
            encodeBase64Str = Base64.getEncoder().encodeToString(hmacSha256);

        } catch (Exception e) {
            throw new RuntimeException("Failed to calculate hmac-sha256", e);
        }
```

5. List of OpenAPI

Samsung Cloud Platform's OpenAPI offers detailed definitions of OpenAPI provided by the common platform and each offering. The detailed definition documents can be found on HOME > ⚙ of the service portal.

Product group	List of products that provide OpenAPI	Notes
Compute	Bare Metal Server	
	VM Auto-Scaling	

	Virtual Server	
	K8s Engine	
	K8s Cluster	Utilize K8s Native API
Network	LB	
	VPC	
	Security Group	
	VPN	
	DNS	
	VPC Firewall	
	GSLB	
Database	Mysql	
	MariaDB	
	MS SQL Server	
	EPAS	
	PostgreSQL	
	Tibero	
	Vertica	
	Elasticsearch	
	Redis	
Storage	Object Storage	S3 API Compliant
	File Storage	
	Backup	
	Block Storage	
Management	Cloud Monitoring	
	Logging&Audit	
	Job Scheduling	
Security	Certificate Management	
	Security Monitoring	
App Service	Notification	
Container	K8s Apps	
AI Service	Kubeflow	

Table 1. List of products that provide OpenAPI