



API Gateway

Developer Guide

Date 2025-02-21

Contents

| | |
|--|-----------|
| 1 Application Scenarios..... | 1 |
| 2 Calling APIs Through App Authentication..... | 2 |
| 2.1 Preparation..... | 2 |
| 2.2 App Authentication..... | 3 |
| 2.3 Java..... | 8 |
| 2.4 Go..... | 19 |
| 2.5 Python..... | 22 |
| 2.6 C#..... | 26 |
| 2.7 JavaScript..... | 28 |
| 2.8 PHP..... | 35 |
| 2.9 C++..... | 39 |
| 2.10 C..... | 41 |
| 2.11 Android..... | 44 |
| 2.12 curl..... | 47 |
| 3 Calling APIs Through IAM Authentication..... | 49 |
| 3.1 Token Authentication..... | 49 |
| 3.2 AK/SK Authentication..... | 51 |
| 4 Creating Signatures for Backend Requests..... | 53 |
| 4.1 Pre-signature Preparations..... | 53 |
| 4.2 Java..... | 53 |
| 4.3 Python..... | 60 |
| 4.4 C#..... | 67 |
| 5 Change History..... | 72 |

1 Application Scenarios

APIG involves the following development scenarios:

- **API calling authentication:** For APIs that use app or IAM authentication, API calling authentication should be developed for the service system to add authentication information to API requests.
 - **API calling through app authentication (signature authentication):** API callers provide a key, secret, and SDK through APIG to complete signature authentication for their API requests.
 - **API calling through IAM authentication (token authentication):** API callers obtain a token from the cloud service platform and add the token to their API requests.
 - **API calling through IAM authentication (AK/SK authentication):** API callers sign their API requests using AK (Access Key ID) /SK (Secret Access Key) and SDKs provided by APIG.
- **Signature verification by backend service:** If an API is bound with a signature key on APIG, the request sent by APIG to the backend service of the API carries the corresponding signature information. The backend service of the API must integrate the SDK provided by APIG and verify the signature information in the request.

2 Calling APIs Through App Authentication

2.1 Preparation

Before calling APIs in app authentication mode, complete the following operations:

- Obtain API request information
On the console of a gateway, choose **API Management > APIs**, and click an API name to go to the details page. On the **APIs** tab, view the domain name, request path, and request method.
- Publish APIs in an environment
On the console of a gateway, choose **API Management > APIs**, and click an API name to go to the details page. On the **APIs** tab, navigate to **Frontend Configuration > Frontend Definition**, and view the environment in which the API has been published.
- Obtain API authentication information
To sign an API request cryptographically through app authentication (signature authentication), the key and secret of a credential authorized to call the API are required. On the console of a gateway, choose **API Management > Credentials**. Go to the details page of a credential, and obtain the key and secret.

NOTE

- **AppKey** or **Key**: access key ID of an app. It is the unique ID associated with a secret access key. The access key ID and secret access key are together used to obtain an encrypted signature for a request.
- **AppSecret** or **Secret**: secret access key used together with an access key ID to sign requests. The access key ID and secret access key can be together used to identify a request sender to prevent the request from being modified.
- When sending an API request, add the current time to the **X-Sdk-Date** header and the signature information to the **Authorization** header.

NOTICE

- The local time on the client must be synchronized with the clock server to avoid a large error in the value of the **X-Sdk-Date** request header.
- APIG checks the time format and compares the time with the time when APIG receives the request. If the time difference exceeds 15 minutes, APIG will reject the request.

2.2 App Authentication

1. Construct a standard request.
Assemble the request content according to the rules of APIG (API Management), ensuring that the client signature is consistent with that in the backend request.
2. Create a to-be-signed string using the standard request and other related information.
3. Calculate a signature using the AK/SK and to-be-signed string.
4. Add the generated signature to an HTTP request as a header or query parameter.
5. After receiving the request, APIG performs **1** to **3** to calculate a signature.
6. The new signature is compared with the signature generated in **3**. If they are consistent, the request is processed; otherwise, the request is rejected.

Constraints

The body of a signing request in app authentication mode cannot exceed 12 MB.

Step 1: Constructing a Standard Request

To access an API through app authentication, standardize the request content, and then sign the request. The client must follow the same request specifications as APIG so that each HTTP request can obtain the same signing result from the frontend and backend to complete identity authentication.

The pseudocode of standard HTTP requests is as follows:

```
CanonicalRequest =  
  HTTPRequestMethod + '\n' +  
  CanonicalURI + '\n' +  
  CanonicalQueryString + '\n' +  
  CanonicalHeaders + '\n' +  
  SignedHeaders + '\n' +  
  HexEncode(Hash(RequestPayload))
```

The following example shows how to construct a standard request.

Original request:

```
GET https://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/app1?b=2&a=1 HTTP/1.1  
Host: c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com  
X-Sdk-Date: 20191111T093443Z
```

1. Specify an HTTP request method (**HTTPRequestMethod**) and end with a carriage return line feed (CRLF).

For example:

```
GET
```

2. Add a standard URI (**CanonicalURI**) and end with a CRLF.

Description

Path of the requested resource, which is the URI code of the absolute path.

Format

According to RFC 3986, each part of a standard URI except the redundant and relative paths must be URI-encoded. If a URI does not end with a slash (/), add a slash at its end.

Example

For the URI **/app1**, the standard URI code is as follows:

```
GET  
/app1/
```

A URI must end with a slash (/) for signature calculation. However, the slash is not required when a request is sent.

3. Add a standard query string (**CanonicalQueryString**) and end with a CRLF.

Description

Query parameters. If no query parameters are configured, the query string is an empty string.

Format

Standard query strings must meet the following requirements:

- Perform URI encoding on each parameter and value according to the following rules:
 - Do not perform URI encoding on any non-reserved characters defined in RFC 3986, including A–Z, a–z, 0–9, hyphen (-), underscore (_), period (.), and tilde (~).
 - Use **%XY** to perform percent encoding on all non-reserved characters. **X** and **Y** indicate hexadecimal characters (0–9 and A–F). For example, the space character must be encoded as **%20**, and an extended UTF-8 character must be encoded in the **"%XY%ZA%BC"** format.

- Add **"URI-encoded parameter name = URI-encoded parameter value"** to each parameter. If no value is specified, use a null string instead. The equal sign (=) is required.

For example, in the following string that contains two parameters, the value of parameter **parm2** is null.

```
parm1=value1&parm2=
```

- Sort the parameters in alphabetically ascending order. For example, a parameter starting with uppercase letter **F** precedes another parameter starting with lowercase letter **b**.
- Construct standard query strings from the first parameter after sorting.

Example

The following example contains two optional parameters **a** and **b**.

```
GET  
/app1/  
a=1&b=2
```

4. Add standard headers (**CanonicalHeaders**) and end with a CRLF.

Description

List of standard request headers, including all HTTP message headers in the to-be-signed request. The **X-Sdk-Date** header must be included to verify the signing time, which is in the UTC time format *YYYYMMDDTHHMMSSZ* as specified in ISO 8601. When publishing an API in a non-RELEASE environment, you need to specify an environment name.

NOTICE

- The local time on the client must be synchronized with the clock server to avoid a large error in the value of the **X-Sdk-Date** request header.
- APIG checks the time format and compares the time with the time when APIG receives the request. If the time difference exceeds 15 minutes, APIG will reject the request.

Format

CanonicalHeaders consists of multiple message headers, for example, **CanonicalHeadersEntry0 + CanonicalHeadersEntry1 +** Each message header (**CanonicalHeadersEntry**) is in the format of

Lowercase(HeaderName) + ':' + Trimall(HeaderValue) + '\n'.

- **Lowercase**: a function for converting all letters into lowercase letters.
- **Trimall**: a function for deleting the spaces before and after a value.
- The last message header carries a CRLF. Therefore, an empty line appears because the **CanonicalHeaders** field also contains a CRLF according to the specifications.
- The message header name must be unique. Otherwise, authentication fails.

Example

```
GET
/app1/
a=1&b=2
host:c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com
x-sdk-date:20191111T093443Z
```

NOTICE

Standard message headers must meet the following requirements:

- All letters in a header are converted to lowercase letters, and all spaces before and after the header are deleted.
- All headers are sorted in alphabetically ascending order.

For example, the original headers are as follows:

```
Host: c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com\nContent-Type: application/json;charset=utf8\nMy-header1: a b c \nX-Sdk-Date:20191111T093443Z\nMy-Header2: "a b c" \n
```

A standard header is as follows:

```
content-type:application/json;charset=utf8\nhost:c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com\nmy-header1:a b c\nmy-header2:"a b c"\nx-sdk-date:20191111T093443Z\n
```

5. Add message headers (**SignedHeaders**) for request signing, and end with a CRLF.

Description

List of message headers used for request signing. This step is to determine which headers are used for signing the request and which headers can be ignored during request verification. The **X-Sdk-date** header must be included.

Format

SignedHeaders = Lowercase(HeaderName0) + ';' + Lowercase(HeaderName1) + ";" + ...

Letters in the message headers are converted to lowercase letters. All headers are sorted alphabetically and separated with commas.

Lowercase is a function for converting all letters into lowercase letters.

Example

In the following example, two message headers **host** and **x-sdk-date** are used for signing the request.

```
GET\n/app1/\na=1&b=2\nhost:c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com\nx-sdk-date:20191111T093443Z
```

host;x-sdk-date

6. Use the hash function SHA-256 to create a hash value based on the body (**RequestPayload**) of the HTTP or HTTPS request.

Description

Request message body. The message body needs two layers of conversion (**HexEncode(Hash(RequestPayload))**). **Hash** is a function for generating message digest. Currently, SHA-256 is supported. **HexEncode**: the Base16 encoding function for returning a digest consisting of lowercase letters. For example, **HexEncode ("m")** returns **6d** instead of **6D**. Each byte you enter is expressed as two hexadecimal characters.

If RequestPayload is null, the null value is used for calculating a hash value.

Example

This example uses GET as an example and leaves the request body empty. After hash processing, the request body (empty string) is as follows:

```
GET
/app1/
a=1&b=2
host:c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com
x-sdk-date:20191111T093443Z

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

7. Perform hash processing on the standard request in the same way as that on the **RequestPayload**. After hash processing, the standard request is expressed with lowercase hexadecimal strings.

Algorithm pseudocode:

Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))

Example of standard request after hash processing:

```
af71c5a7ef45310b8dc05ab15f7da50189ffa81a95cc284379ebaa5eb61155c0
```

Step 2: Creating a To-Be-Signed String

After a standard HTTP request is constructed and the request hash value is obtained, create a to-be-signed string by combining them with the signature algorithm and signing time.

```
StringToSign =
  Algorithm + \n +
  RequestDateTime + \n +
  HashedCanonicalRequest
```

Parameters in the pseudocode are described as follows:

- **Algorithm**
Signature algorithm. For SHA256, the value is **SDK-HMAC-SHA256**.
- **RequestDateTime**
Request timestamp, which is the same as **X-Sdk-Date** in the request header. The format is *YYYYMMDDTHHMMSSZ*.
- **HashedCanonicalRequest**
Standard request generated after hash processing.

In this example, the following to-be-signed string is obtained:

```
SDK-HMAC-SHA256
20191111T093443Z
af71c5a7ef45310b8dc05ab15f7da50189ffa81a95cc284379ebaa5eb61155c0
```

Step 3: Calculating the Signature

Use the AppSecret and created character string as the input of the encryption hash function, and convert the calculated binary signature into a hexadecimal expression.

The pseudocode is as follows:

```
signature = HexEncode(HMAC(APP secret, string to sign))
```

HMAC indicates hash calculation, and **HexEncode** indicates hexadecimal conversion. [Table 2-1](#) describes the parameters in the pseudocode.

Table 2-1 Parameter description

| Parameter | Description |
|---------------------|--------------------------------|
| AppSecret | Signature key. |
| To-be-signed string | Character string to be signed. |

If the AppSecret is **FWTh5tqu2Pb9ZGt8NI09XYZti2V1LTa8useKXMD8**, the calculated signature is as follows:

```
01cc37e53d821da93bb7239c5b6e1640b184a748f8c20e61987b491e00b15822
```

Step 4: Adding the Signature to the Request Header

Add the signature to the HTTP Authorization header. The Authorization header is used for identity authentication and not included in the signed headers.

The pseudocode is as follows:

```
Authorization header creation pseudocode:  
Authorization: algorithm Access=APP key, SignedHeaders=SignedHeaders, Signature=signature
```

There is no comma before the algorithm and **Access**. **SignedHeaders** and **Signature** must be separated with commas.

The signed headers are as follows:

```
Authorization: SDK-HMAC-SHA256 Access=FM9RLCN*****NAXISK, SignedHeaders=host;x-sdk-date,  
Signature=01cc37e53d***e00b15822
```

The signed headers are added to the HTTP request for identity authentication. If the identity authentication is successful, the request is sent to the corresponding backend service for processing.

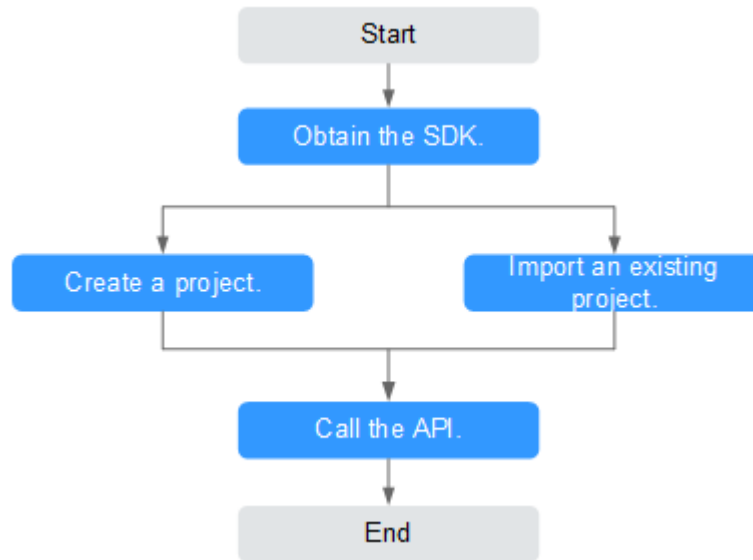
2.3 Java

Scenarios

To use Java to call an API through app authentication, obtain the Java SDK, create a project or import an existing project, and then call the API by referring to the API calling example.

This section uses Eclipse 4.5.2 as an example.

Figure 2-1 API calling process



Prerequisites

- You have obtained API calling information. For details, see [Preparation](#).
- You have installed Eclipse 3.6.0 or a later version. If not, download Eclipse from the [official Eclipse website](#) and install it.
- You have installed Java Development Kit (JDK) 1.8.111 or a later version. If not, download JDK from the [official Oracle website](#) and install it. JDK 17 or later is not supported.

Obtaining the SDK

On the APIG console, choose **Help Center > Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-java-sdk.zip** package. The following table shows the files decompressed from the package.

| Name | Description |
|---|----------------------------------|
| libs\ | SDK dependencies |
| libs\java-sdk-core-x.x.x.jar | SDK package |
| src\com\apig\sdk\demo\Main.java | Sample code for signing requests |
| src\com\apig\sdk\demo\OkHttpDemo.java | |
| src\com\apig\sdk\demo\LargeFileUpload-Demo.java | |
| .classpath | Java project configuration files |
| .project | |

Importing a Project

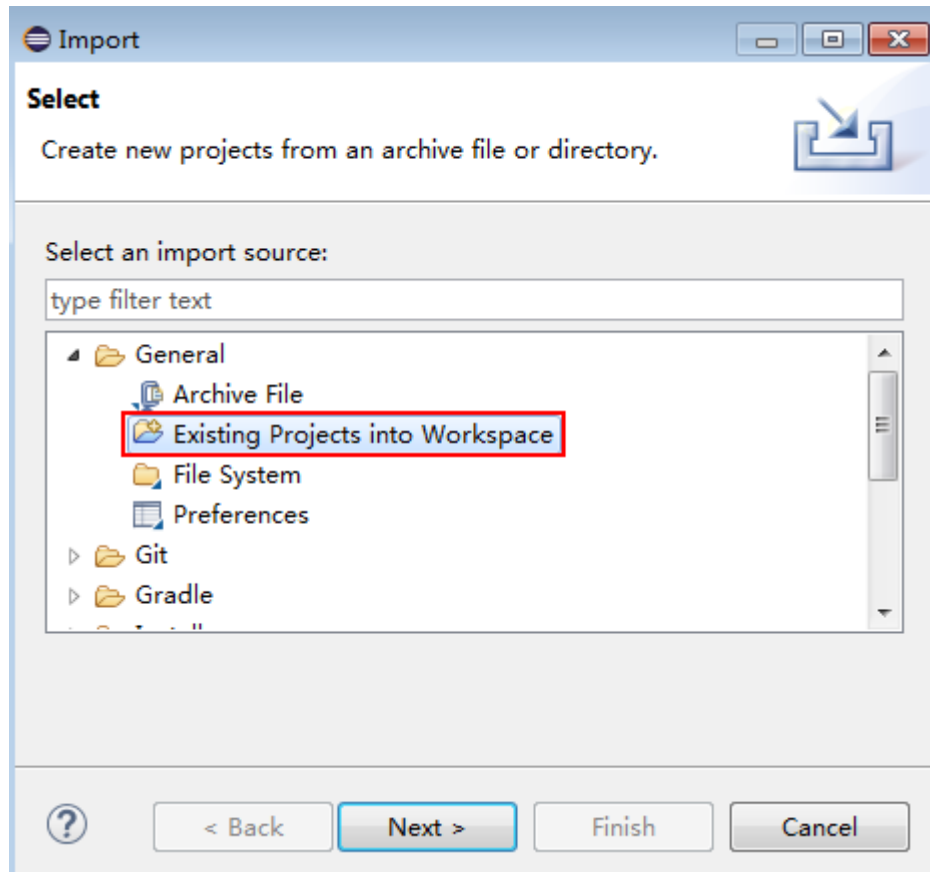
Step 1 Open Eclipse and choose **File > Import**.

The **Import** dialog box is displayed.

Step 2 Choose **General > Existing Projects into Workspace** and click **Next**.

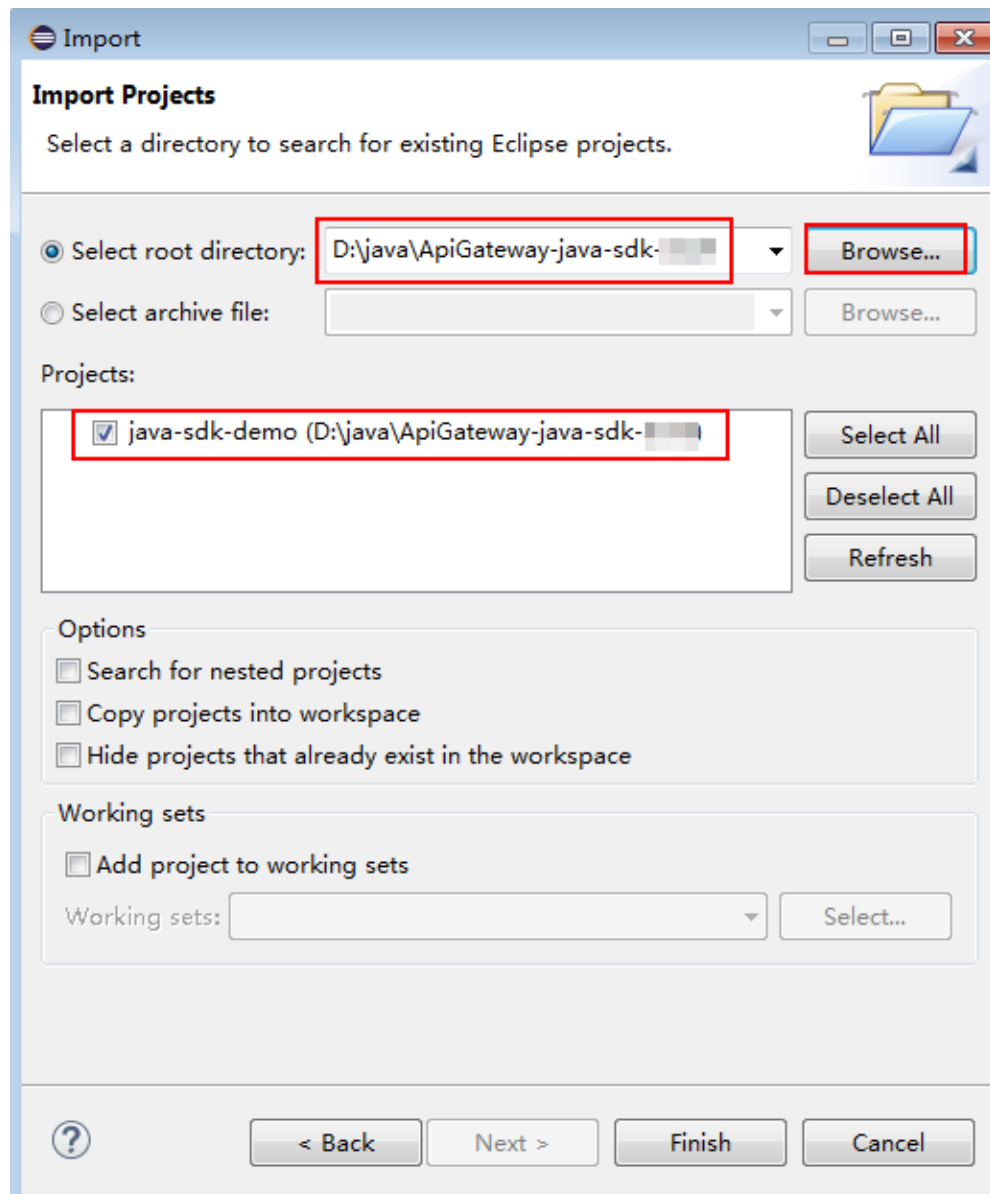
The **Import Projects** dialog box is displayed.

Figure 2-2 Importing a project



Step 3 Click **Browse** and select the directory where the SDK is decompressed.

Figure 2-3 Selecting the demo project



Step 4 Click **Finish**.

Modify the parameters in sample code **Main.java** as required. For details about the sample code, see [API Calling Example](#).

----End

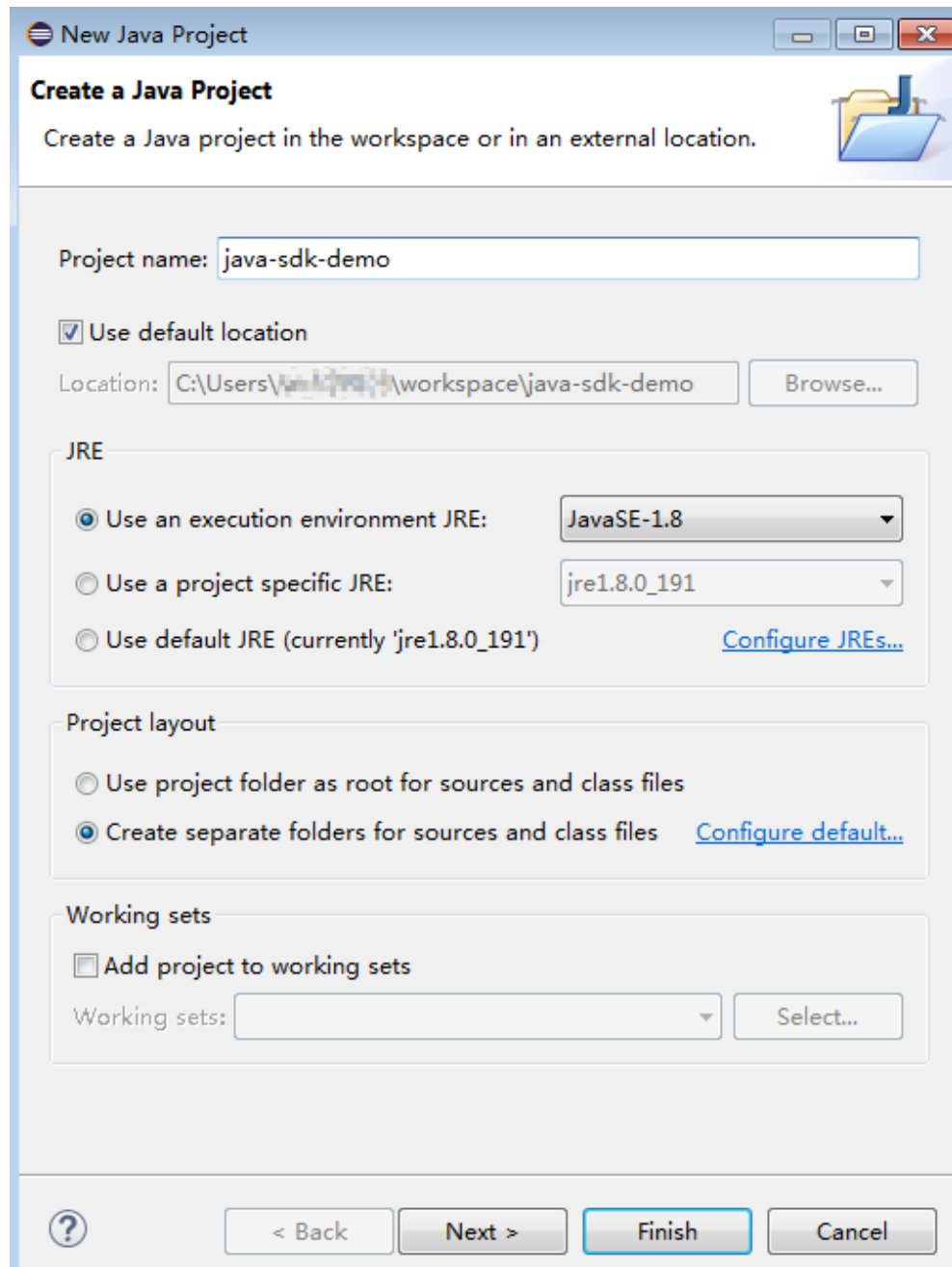
Creating a Project

Step 1 Open Eclipse and choose **File > New > Java Project**.

The **New Java Project** dialog box is displayed.

Step 2 Enter a project name, for example, **java-sdk-demo**, retain the default settings for other parameters, and click **Finish**.

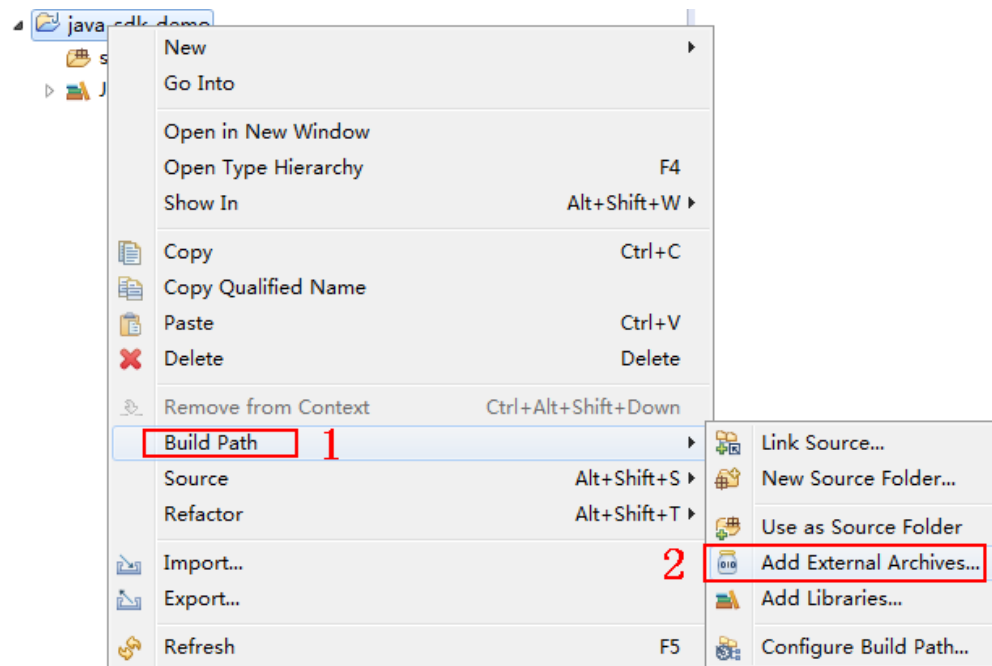
Figure 2-4 Creating a project



Step 3 Import the .jar files in the APIG Java SDK.

1. Choose **java-sdk-demo**, right-click, and choose **Build Path > Add External Archives** from the shortcut menu.

Figure 2-5 Importing the .jar files



2. Select all .jar files in the \libs directory.

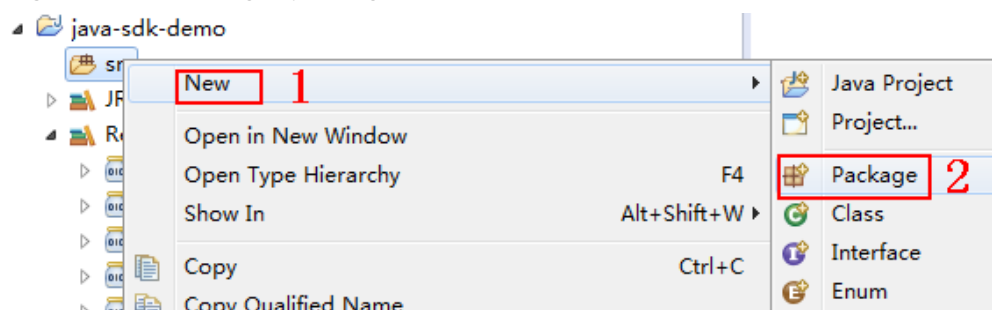
Figure 2-6 Selecting all .jar files

| | | | |
|-------------------------|-----------------|---------------------|--------|
| commons-codec-1.11.jar | 2019/3/15 10:23 | Executable Jar File | 328 KB |
| commons-logging-1.2.jar | 2019/3/15 10:23 | Executable Jar File | 61 KB |
| httpclient-4.5.5.jar | 2019/3/15 10:23 | Executable Jar File | 749 KB |
| httpcore-4.4.9.jar | 2019/3/15 10:23 | Executable Jar File | 318 KB |
| java-sdk-core-3.0.9.jar | 2019/3/15 10:23 | Executable Jar File | 101 KB |
| joda-time-2.9.9.jar | 2019/3/15 10:23 | Executable Jar File | 620 KB |
| okhttp-3.11.0.jar | 2019/3/15 10:23 | Executable Jar File | 404 KB |
| okio-1.15.0.jar | 2019/3/15 10:23 | Executable Jar File | 87 KB |

Step 4 Create a package and **Main** file.

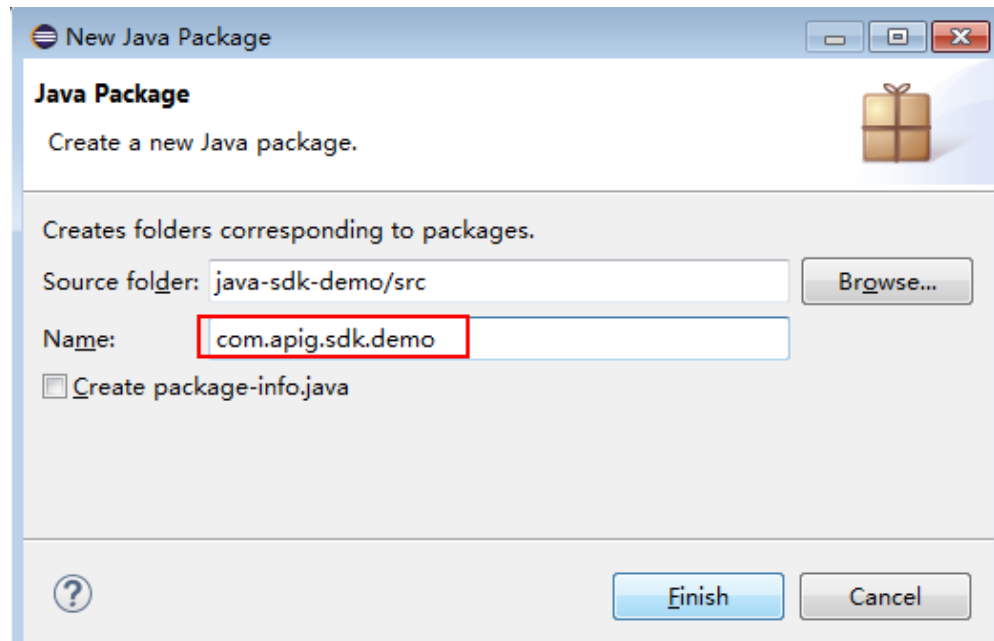
1. Choose **src**, right-click, and choose **New > Package** from the shortcut menu.

Figure 2-7 Creating a package



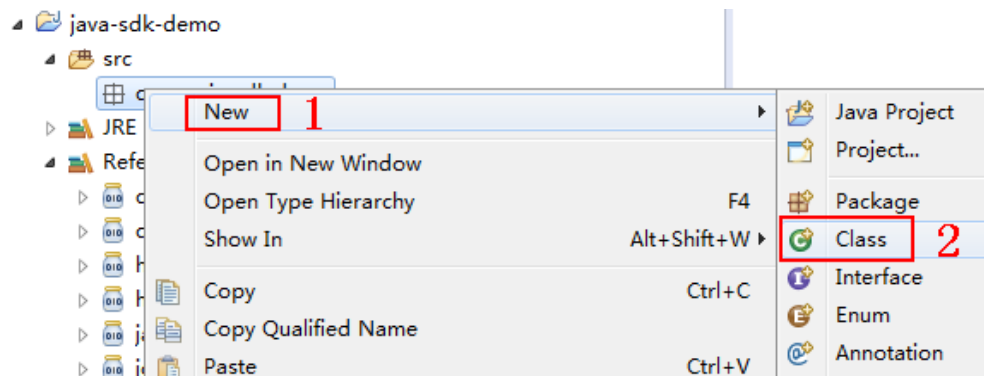
2. Enter **com.apig.sdk.demo** for **Name**.

Figure 2-8 Setting a package name



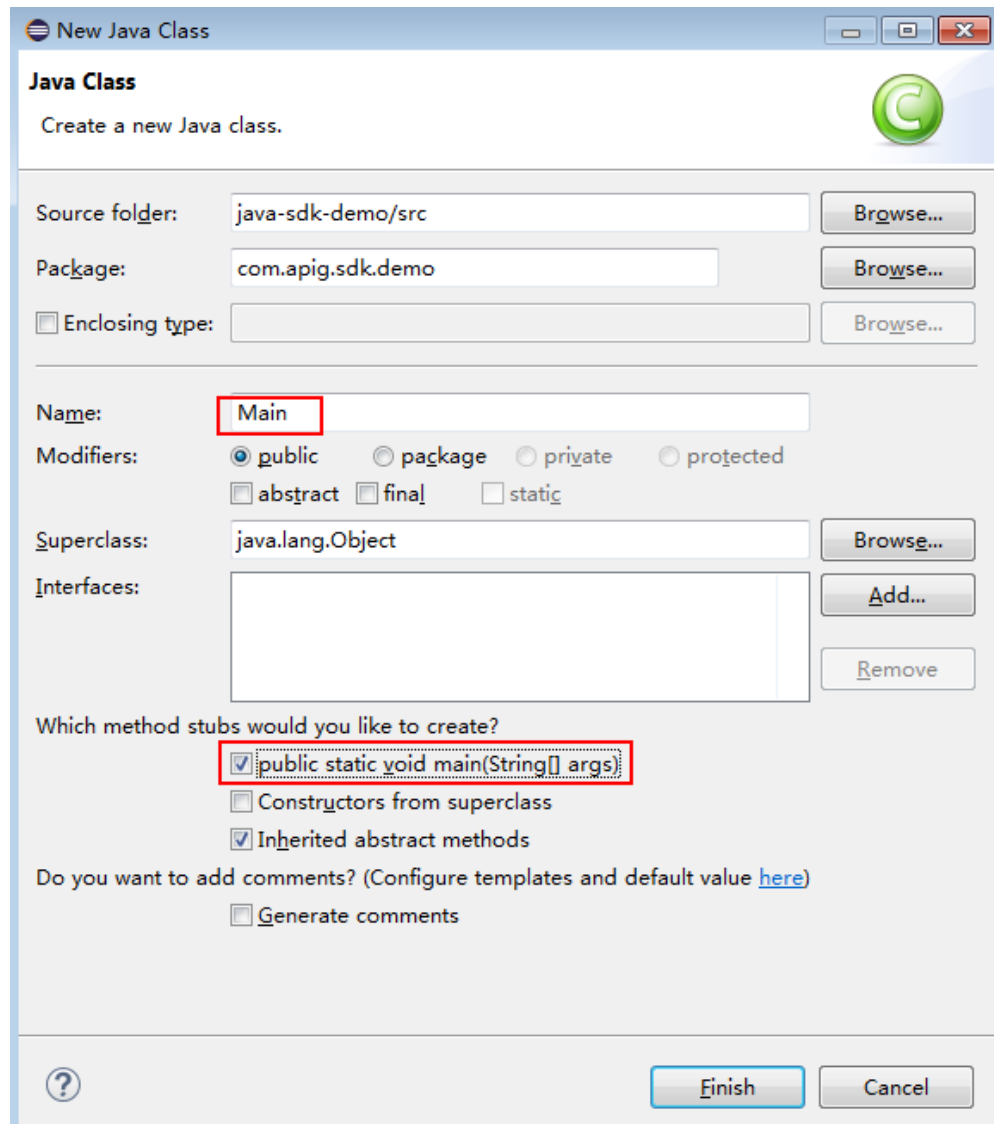
3. Click **Finish**.
The package is created.
4. Choose **com.apig.sdk.demo**, right-click, and choose **New > Class** from the shortcut menu.

Figure 2-9 Creating a class



5. Enter **Main** for **Name** and select **public static void main(String[] args)**.

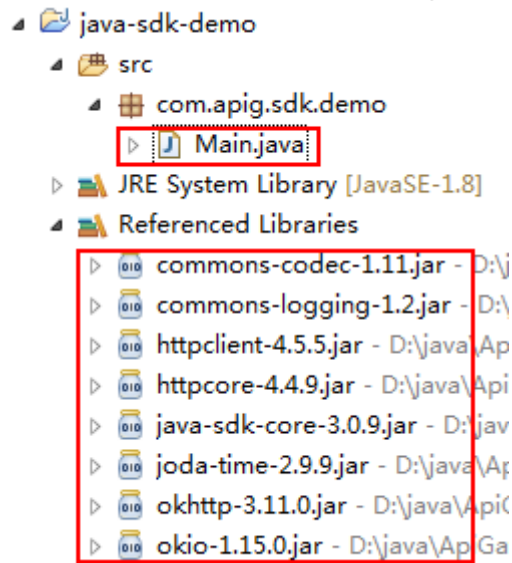
Figure 2-10 Configuring the class



6. Click **Finish**.
The **Main** file is created.

Step 5 View the directory structure of the project.

Figure 2-11 Directory structure of the new project Main



Before using **Main.java**, enter the required code according to the API calling example provided in this section.

----End

API Calling Example

NOTE

- You need to create an API with the Mock backend on the console, and then publish the API. For details about how to create and publish an API, see the *API Gateway User Guide*.
- The backend of this API is a fake HTTP service, which returns response code **200** and message body **Congratulations, sdk demo is running**.

Step 1 Add the following references to **Main.java**:

```
import java.io.IOException;
import javax.net.ssl.SSLContext;

import org.apache.http.Header;
import org.apache.http.HttpEntity;
import org.apache.http.HttpResponse;
import org.apache.http.client.methods.HttpRequestBase;
import org.apache.http.conn.ssl.AllowAllHostnameVerifier;
import org.apache.http.conn.ssl.SSLConnectionSocketFactory;
import org.apache.http.conn.ssl.SSLContexts;
import org.apache.http.conn.ssl.TrustSelfSignedStrategy;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;
import org.apache.http.util.EntityUtils;

import com.cloud.apigateway.sdk.utils.Client;
import com.cloud.apigateway.sdk.utils.Request;
```

Step 2 Construct a request by configuring the following parameters:

- **AppKey** and **AppSecret**: In this example, the AK and SK stored in the environment variables are used. Specify the environment variables **CLOUD_SDK_AK** and **CLOUD_SDK_SK** in the local environment first. The

following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables and fill them in the sample code.

- a. Open the terminal and run the following command to open the environment variable configuration file:

```
vi ~/.bashrc
```

- b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"  
export CLOUD_SDK_SK="Obtained SK"
```

- c. Run the following command to apply the modification:

```
source ~/.bashrc
```

- **Method:** Specify a request method. The sample code uses **POST**.
- **url:** Request URL of the API, excluding the QueryString and fragment parts. Use your own independent domain name. The sample code uses **http://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/java-sdk**.
- **queryString:** Specify query parameters to be carried in the URL. Characters (0-9a-zA-Z./;[]\-=~#%^&_+,:) are allowed. The sample code uses **name=value**.
- **header:** Specify request headers. The sample code uses **Content-Type:text/plain**. If you are going to publish the API in a non-RELEASE environment, specify an environment name. The sample code uses **x-stage:publish_env_name**.
- **body:** Specify the request body. The sample code uses **demo**.

The sample code is as follows:

```
Request request = new Request();  
try  
{  
    request.setKey(System.getenv("CLOUD_SDK_AK"));  
    request.setSecret(System.getenv("CLOUD_SDK_SK"));  
    request.setMethod("POST");  
    request.setUrl("http://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/java-  
sdk");  
    //URL  
    request.addQueryStringParam("name", "value");  
    request.addHeader("Content-Type", "text/plain");  
    //request.addHeader("x-stage", "publish_env_name"); //Specify an environment name before  
publishing the API in a non-RELEASE environment.  
    request.setBody("demo");  
} catch (Exception e)  
{  
    e.printStackTrace();  
    return;  
}
```

Step 3 Sign the request, access the API, and print the result.

The sample code is as follows:

```
CloseableHttpClient client = null;  
try  
{  
    HttpRequestBase signedRequest = Client.sign(request);  
  
    client = HttpClients.custom().build();  
    HttpResponse response = client.execute(signedRequest);  
    System.out.println(response.getStatusLine().toString());  
    Header[] resHeaders = response.getAllHeaders();  
    for (Header h : resHeaders)
```

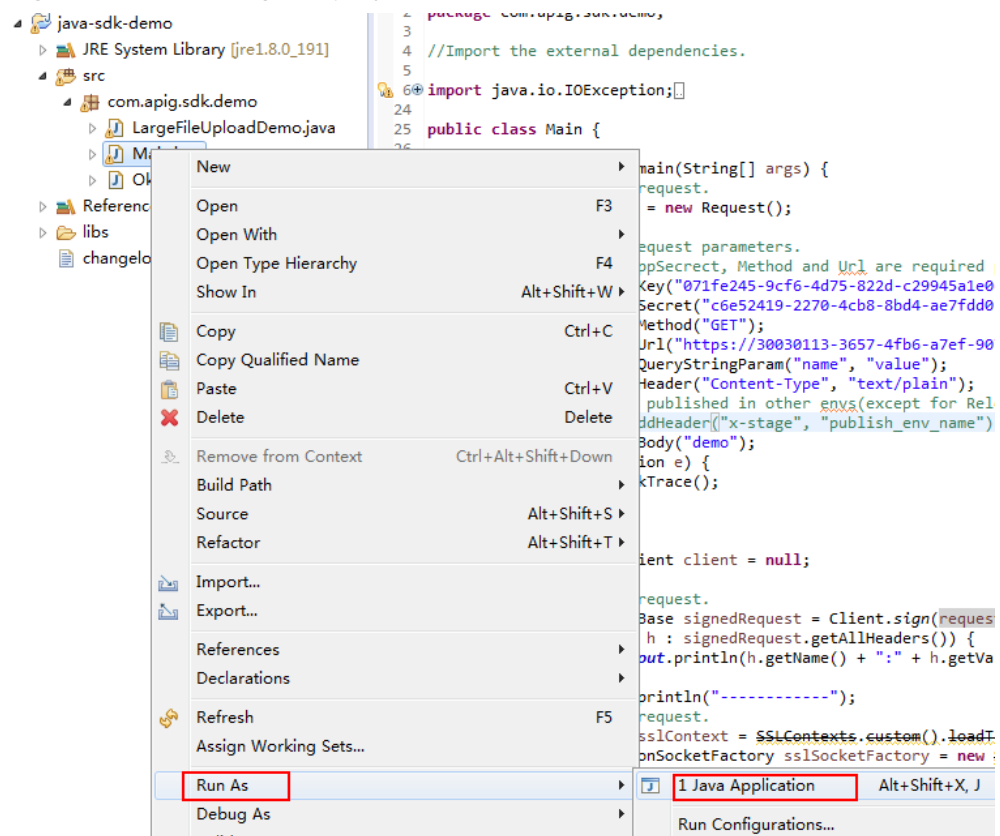
```

    {
        System.out.println(h.getName() + ":" + h.getValue());
    }
    HttpEntity resEntity = response.getEntity();
    if (resEntity != null)
    {
        System.out.println(System.getProperty("line.separator") + EntityUtils.toString(resEntity, "UTF-8"));
    }
} catch (Exception e)
{
    e.printStackTrace();
} finally
{
    try
    {
        if (client != null)
        {
            client.close();
        }
    } catch (IOException e)
    {
        e.printStackTrace();
    }
}
}
}

```

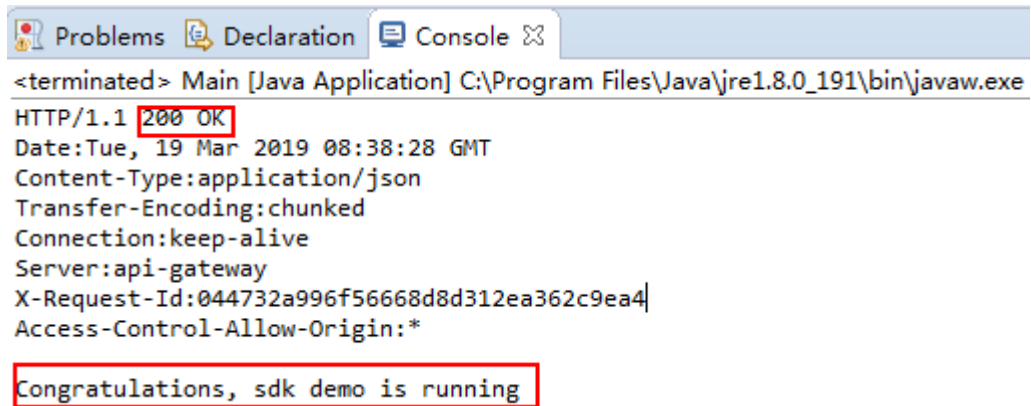
Step 4 Choose **Main.java**, right-click, and choose **Run As > Java Application** to run the project test code.

Figure 2-12 Running the project test code



Step 5 On the **Console** tab page, view the running result.

Figure 2-13 Response displayed if the calling is successful

A screenshot of an IDE console window. The window title bar shows 'Problems', 'Declaration', and 'Console'. The console output shows a terminated Java application with the following HTTP response:

```
<terminated> Main [Java Application] C:\Program Files\Java\jre1.8.0_191\bin\javaw.exe  
HTTP/1.1 200 OK  
Date: Tue, 19 Mar 2019 08:38:28 GMT  
Content-Type: application/json  
Transfer-Encoding: chunked  
Connection: keep-alive  
Server: api-gateway  
X-Request-Id: 044732a996f56668d8d312ea362c9ea4  
Access-Control-Allow-Origin: *  
  
Congratulations, sdk demo is running
```

The status code '200 OK' and the message 'Congratulations, sdk demo is running' are highlighted with red boxes.

----End

2.4 Go

Scenarios

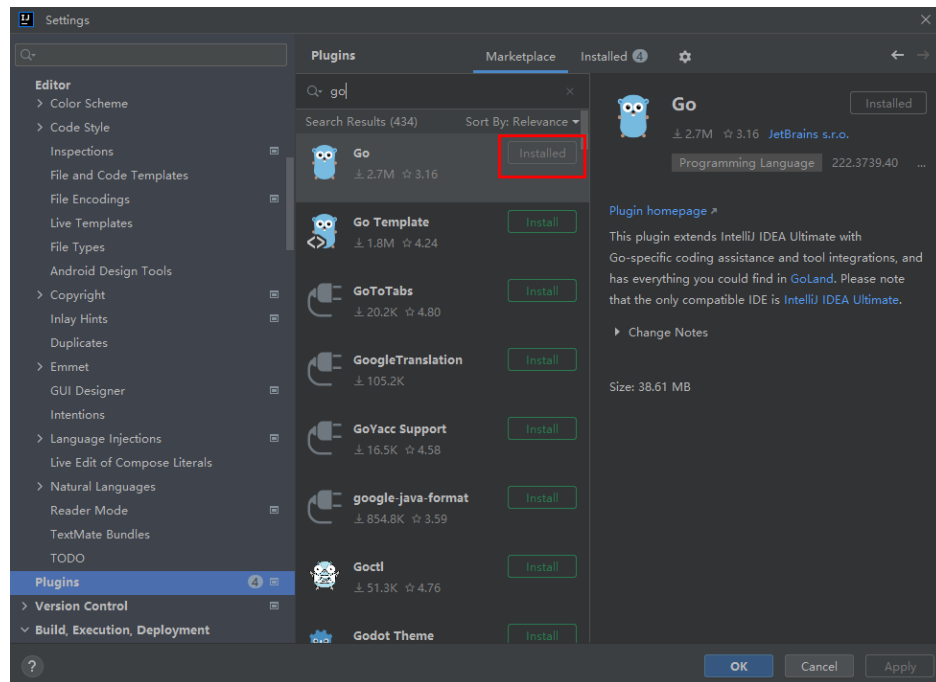
To use Go to call an API through app authentication, obtain the Go SDK, create a new project, and then call the API by referring to the API calling example.

This section uses IntelliJ IDEA 2022.2.1 as an example.

Prerequisites

- You have obtained API calling information. For details, see [Preparation](#).
- You have installed Go 1.14 or a later version. If not, download the Go installation package from the [official Go website](#) and install it.
- You have installed IntelliJ IDEA 2022.2.1 or a later version. If not, download the installation package from the [official IntelliJ IDEA website](#) and install it.
- You have installed the Go plug-in on IntelliJ IDEA. If not, install the Go plug-in according to [Figure 2-14](#).

Figure 2-14 Installing the Go plug-in



Obtaining the SDK

On the APiG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-go-sdk.zip** package. The following table shows the files decompressed from the package.

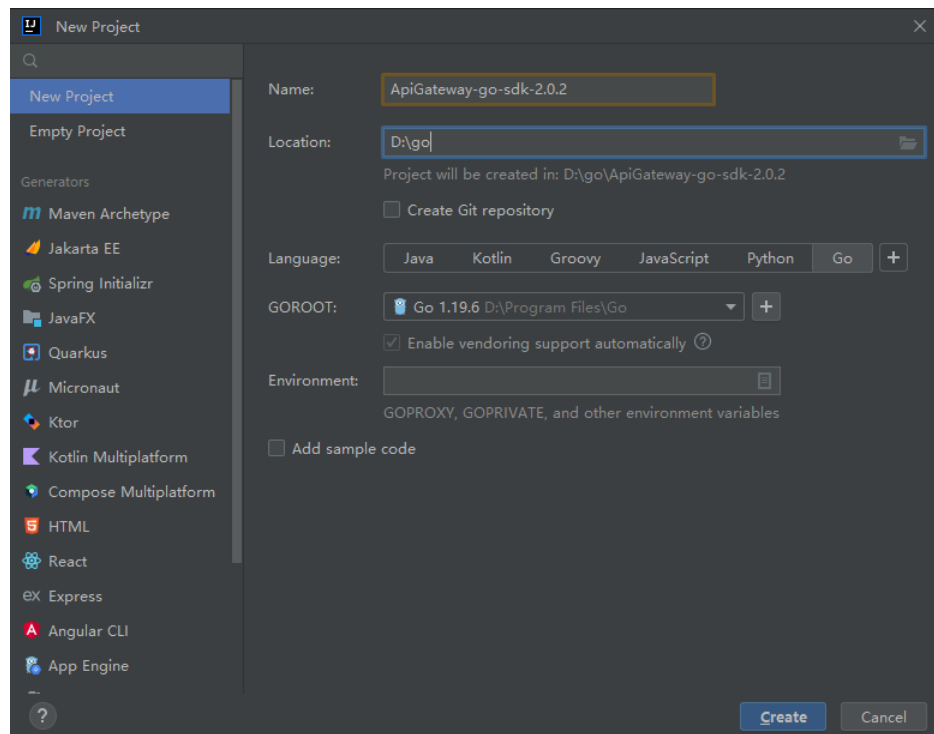
| Name | Description |
|----------------|-------------|
| core\escape.go | SDK code |
| core\signer.go | |
| demo.go | Sample code |

Creating a Project

Step 1 Start IntelliJ IDEA and choose **File** > **New** > **Project**.

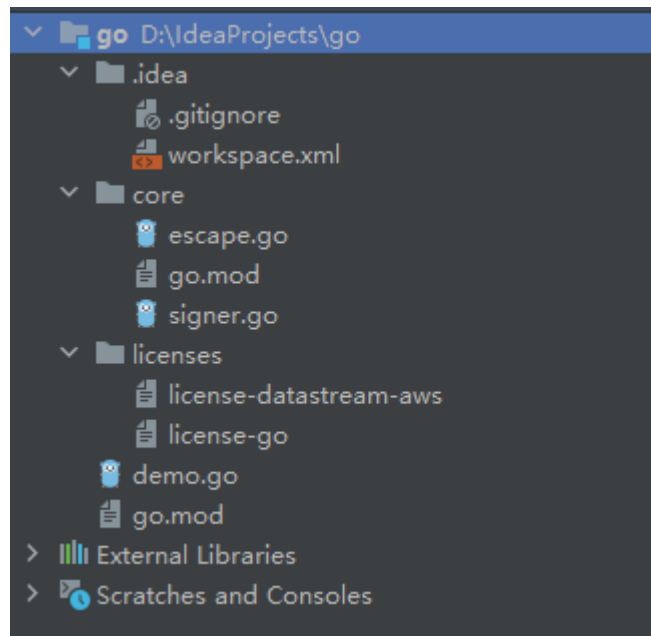
In the displayed **New Project** dialog box, set **Name** to the name of the folder in the SDK package, **Location** to the decompression path of the folder, **Language** to **Go**, and click **Create**.

Figure 2-15 Go



Step 2 View the directory structure shown in the following figure.

Figure 2-16 Directory structure of the new project go



Modify the parameters in sample code **demo.go** as required. For details about the sample code, see [API Calling Example](#).

----End

API Calling Example

Step 1 Import the Go SDK (signer.go) to the project.

```
import "apig-sdk/go/core"
```

Step 2 Generate a new signer and enter the AppKey and AppSecret.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables `CLOUD_SDK_AK` and `CLOUD_SDK_SK` in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.

a. Open the terminal and run the following command to open the environment variable configuration file:

```
vi ~/.bashrc
```

b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"  
export CLOUD_SDK_SK="Obtained SK"
```

c. Run the following command to apply the modification:

```
source ~/.bashrc
```

2. Generate a new signer and enter the configured environment variables.

```
s := core.Signer{  
    Key: os.Getenv("CLOUD_SDK_AK"),  
    Secret: os.Getenv("CLOUD_SDK_SK"),  
}
```

Step 3 Generate a new request, and specify the domain name, method, request URL, query parameters, and body.

```
r, _ := http.NewRequest("POST", "http://c967a237-cd6c-470e-906f-  
a8655461897e.apigw.exampleRegion.com/api?a=1&b=2",  
    ioutil.NopCloser(bytes.NewBuffer([]byte("foo=bar"))))
```

Step 4 Add the x-stage header to the request to specify an environment name. Add other headers to be signed as necessary.

```
r.Header.Add("x-stage", "RELEASE")
```

Step 5 Execute the following function to add the X-Sdk-Date and Authorization headers for signing:

```
s.Sign(r)
```

Step 6 Access the API and view the access result.

```
resp, err := http.DefaultClient.Do(r)  
body, err := ioutil.ReadAll(resp.Body)
```

----End

2.5 Python

Scenarios

To use Python to call an API through app authentication, obtain the Python SDK, create a new project, and then call the API by referring to the API calling example.

This section uses IntelliJ IDEA 2018.3.5 as an example.

Prerequisites

- You have obtained API calling information. For details, see [Preparation](#).
- You have installed Python 2.7.9 or 3.X. If not, download the Python installation package from the [official Python website](#) and install it.

After Python is installed, run the **pip** command to install the **requests** library in the CLI or Shell window.

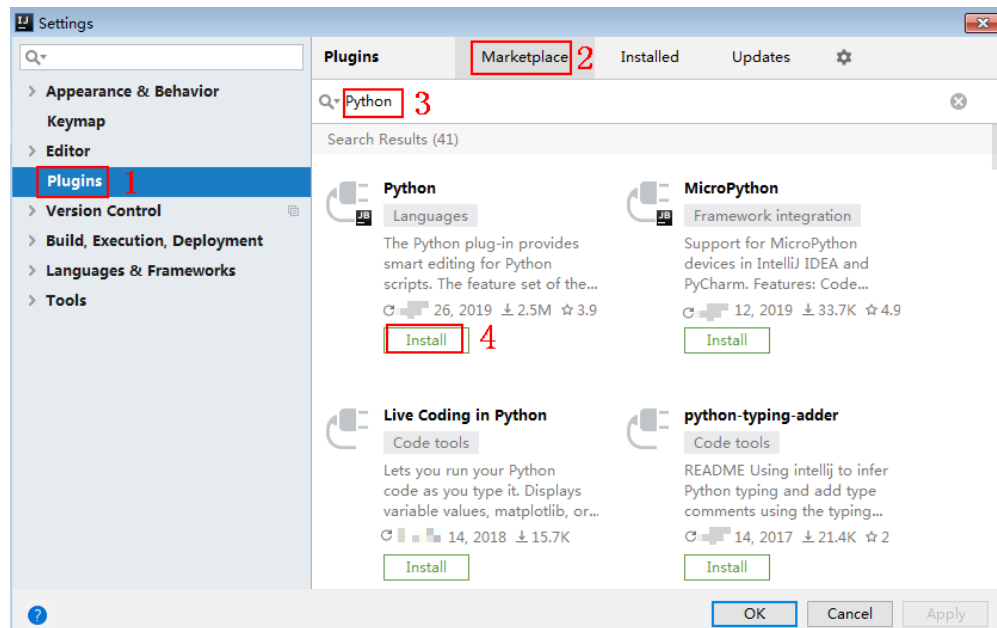
```
pip install requests
```

NOTE

If a certificate error occurs during the installation, download the [get-pip.py](#) file to upgrade the pip environment, and try again.

- You have installed IntelliJ IDEA 2018.3.5 or a later version. If not, download the installation package from the [official IntelliJ IDEA website](#) and install it.
- You have installed the Python plug-in on IntelliJ IDEA. If not, install the Python plug-in according to [Figure 2-17](#).

Figure 2-17 Installing the Python plug-in



Obtaining the SDK

On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-python-sdk.zip** package. The following table shows the files decompressed from the package.

| Name | Description |
|----------------------|-------------|
| apig_sdk__init__.py | SDK code |
| apig_sdk\signer.py | |

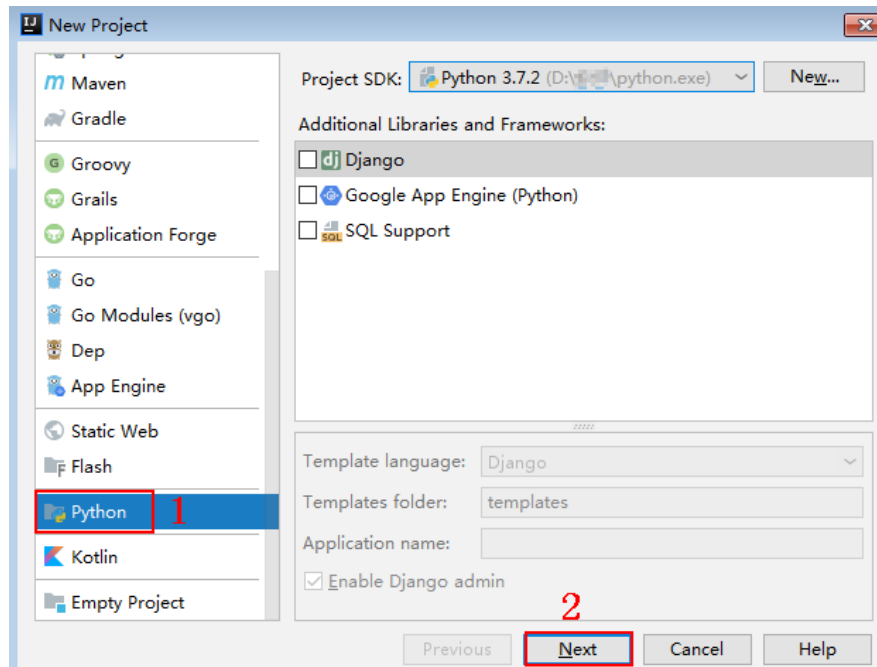
| Name | Description |
|---------------------------|---------------------------------|
| main.py | Sample code |
| backend_signature.py | Sample code for backend signing |
| licenses\license-requests | Third-party license |

Creating a Project

Step 1 Start IDEA and choose **File > New > Project**.

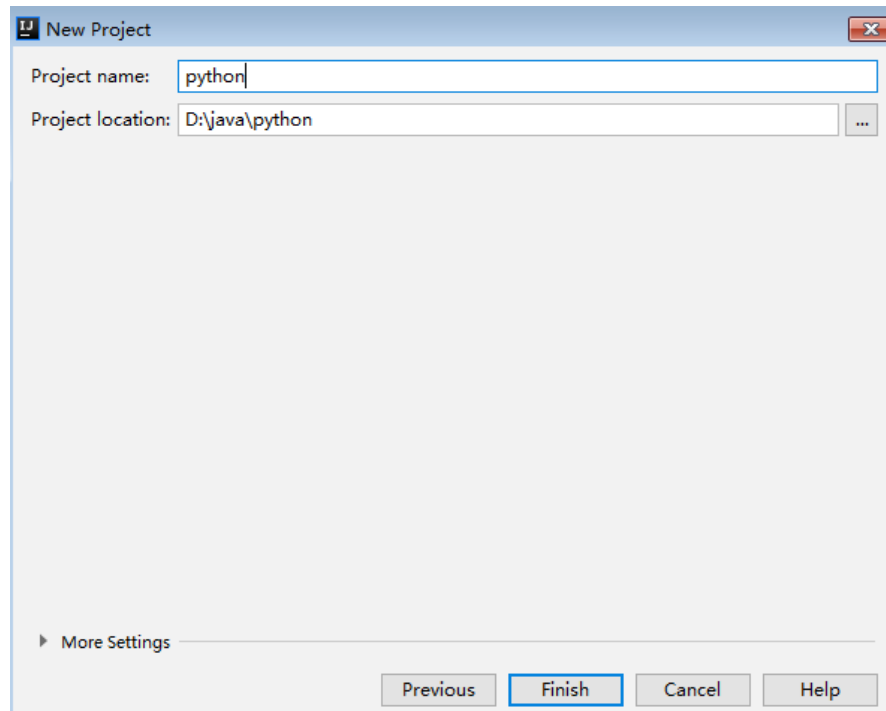
On the displayed **New Project** page, choose **Python** and click **Next**.

Figure 2-18 Python



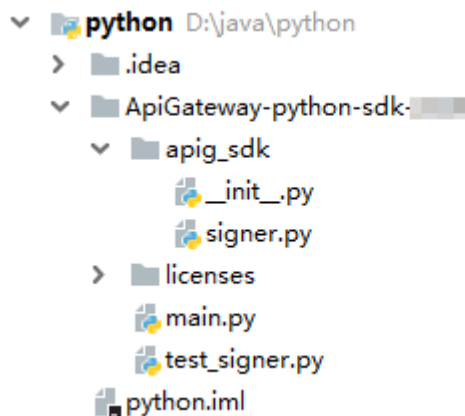
Step 2 Click **Next**. Click ..., select the directory where the SDK is decompressed, and click **Finish**.

Figure 2-19 Selecting the SDK directory after decompression



Step 3 View the directory structure shown in the following figure.

Figure 2-20 Directory structure of the new project python



Modify the parameters in sample code **main.py** as required. For details about the sample code, see [API Calling Example](#).

----End

API Calling Example

Step 1 Import **apig_sdk** to the project.

```
from apig_sdk import signer
import requests
import os
```

Step 2 Generate a new signer and enter the AppKey and AppSecret.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables `CLOUD_SDK_AK` and `CLOUD_SDK_SK` in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.
 - a. Open the terminal and run the following command to open the environment variable configuration file:
vi ~/.bashrc
 - b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"
export CLOUD_SDK_SK="Obtained SK"
```
 - c. Run the following command to apply the modification:
source ~/.bashrc
2. Generate a new signer and enter the configured environment variables.

```
sig = signer.Signer()
sig.Key = os.getenv('CLOUD_SDK_AK')
sig.Secret = os.getenv('CLOUD_SDK_SK')
```

Step 3 Generate a request, and specify the method, request URI, header, and request body.

```
r = signer.HttpRequest("POST",
    "https://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/app1?a=1",
    {"x-stage": "RELEASE"},
    "body")
```

Step 4 Execute the following function to add the X-Sdk-Date and Authorization headers for signing:

X-Sdk-Date is a request header parameter required for signing requests.
`sig.Sign(r)`

Step 5 Access the API and view the access result.

```
resp = requests.request(r.method, r.scheme + "://" + r.host + r.uri, headers=r.headers, data=r.body)
print(resp.status_code, resp.reason)
print(resp.content)
```

----End

2.6 C#

Scenarios

To use C# to call an API through app authentication, obtain the C# SDK, open the project file in the SDK, and then call the API by referring to the API calling example.

Prerequisites

- You have obtained API calling information. For details, see [Preparation](#).
- You have installed Visual Studio 2019 version 16.8.4 or a later version. If not, download it from the [official Visual Studio website](#) and install it.

Obtaining the SDK

On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-csharp-sdk.zip** package. The following table shows the files decompressed from the package.

| Name | Description |
|-------------------------------------|------------------------------------|
| apigateway-signature\Signer.cs | SDK code |
| apigateway-signature\HttpEncoder.cs | |
| sdk-request\Program.cs | Sample code for signing requests |
| backend-signature\ | Sample project for backend signing |
| csharp.sln | Project file |
| licenses\license-referencesource | Third-party license |

Opening a Project

Double-click **csharp.sln** in the SDK package to open the project. The project contains the following:

- **apigateway-signature**: Shared library that implements the signature algorithm. It can be used in the .Net Framework and .Net Core projects.
- **backend-signature**: Example of a backend service signature.
- **sdk-request**: Example of invoking the signature algorithm. Modify the parameters as required. For details about the sample code, see [API Calling Example](#).

API Calling Example

Step 1 Import the C# SDK to your project.

```
using System;
using System.Net;
using System.IO;
using System.Net.Http;
using System.Threading;
using APIGATEWAY_SDK;
```

Step 2 Generate a new signer and enter the AppKey and AppSecret.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables *CLOUD_SDK_AK* and *CLOUD_SDK_SK* in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.
 - a. Open the terminal and run the following command to open the environment variable configuration file:

vi ~/.bashrc
 - b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"
export CLOUD_SDK_SK="Obtained SK"
```
 - c. Run the following command to apply the modification:

source ~/.bashrc

2. Generate a new signer and enter the configured environment variables.

```
Signer signer = new Signer();  
signer.Key = Environment.GetEnvironmentVariable("CLOUD_SDK_AK");  
signer.Secret = Environment.GetEnvironmentVariable("CLOUD_SDK_SK");
```

- Step 3** Generate an `HttpRequest`, and specify the method, request URL, and body.

```
HttpRequest r = new HttpRequest("POST",  
    new Uri("https://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/app1?  
query=value"));  
r.body = "{\"a\":1}";
```

- Step 4** Add the `x-stage` header to the request to specify an environment name. Add other headers to be signed as necessary.

```
r.headers.Add("x-stage", "RELEASE");
```

- Step 5** Execute the following function to generate `HttpWebRequest`, and add the `X-Sdk-Date` and `Authorization` headers for signing the request:

```
HttpWebRequest req = signer.Sign(r);
```

- Step 6** Access the API and view the access result.

```
try  
{  
    var writer = new StreamWriter(req.GetRequestStream());  
    writer.Write(r.body);  
    writer.Flush();  
    HttpWebResponse resp = (HttpWebResponse)req.GetResponse();  
    var reader = new StreamReader(resp.GetResponseStream());  
    Console.WriteLine(reader.ReadToEnd());  
}  
catch (WebException e)  
{  
    HttpWebResponse resp = (HttpWebResponse)e.Response;  
    if (resp != null)  
    {  
        Console.WriteLine((int)resp.StatusCode + " " + resp.StatusDescription);  
        var reader = new StreamReader(resp.GetResponseStream());  
        Console.WriteLine(reader.ReadToEnd());  
    }  
    else  
    {  
        Console.WriteLine(e.Message);  
    }  
}  
Console.WriteLine("-----");
```

----End

2.7 JavaScript

Scenarios

To use JavaScript to call an API through app authentication, obtain the JavaScript SDK, create a project, and then call the API by referring to the API calling example.

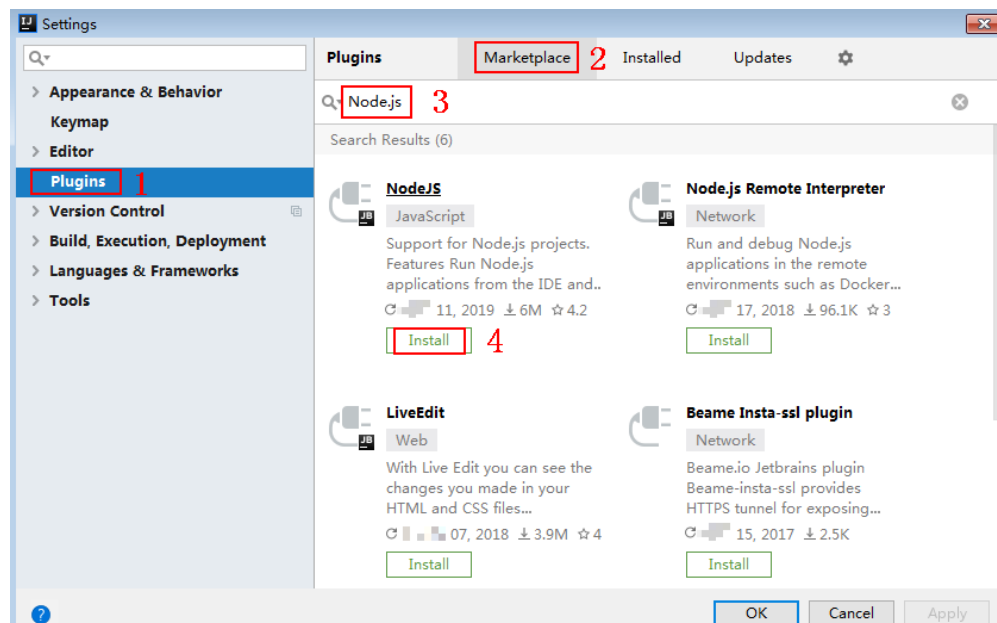
The JavaScript SDK can run in a **Node.js** or **browser** environment.

This section describes the procedure of using IntelliJ IDEA 2018.3.5 to establish a Node.js environment. It also provides examples of calling APIs using a browser.

Preparing the Environment

- You have obtained API calling information. For details, see [Preparation](#).
- You have installed Node.js 15.10.0 or a later version. If not, download it from the [official Node.js website](#) and install it.
- You have installed IntelliJ IDEA 2018.3.5 or a later version. If not, download it from the [official IntelliJ IDEA website](#) and install it.
- You have installed the Node.js plug-in on IntelliJ IDEA. If not, install the Node.js plug-in according to [Figure 2-21](#).

Figure 2-21 Installing the Node.js plug-in



Obtaining the SDK

On the APIG console, choose **Help Center > Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-javascript-sdk.zip** package. The following table shows the files decompressed from the package.

| Name | Description |
|-------------------|--|
| signer.js | SDK code |
| node_demo.js | Node.js sample code |
| demo.html | Browser sample code |
| demo_require.html | Browser sample code (loaded using require) |
| test.js | Test case |
| js\hmac-sha256.js | Dependencies |

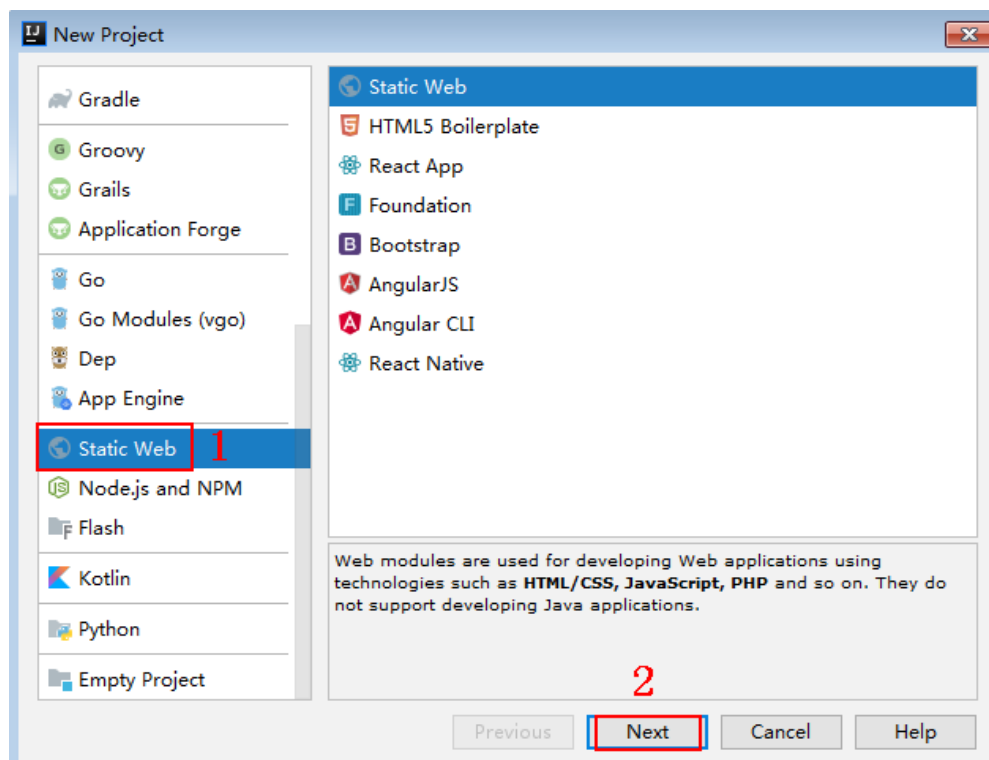
| Name | Description |
|----------------------------|----------------------|
| licenses\license-crypto-js | Third-party licenses |
| licenses\license-node | |

Creating a Project

Step 1 Start IntelliJ IDEA and choose **File > New > Project**.

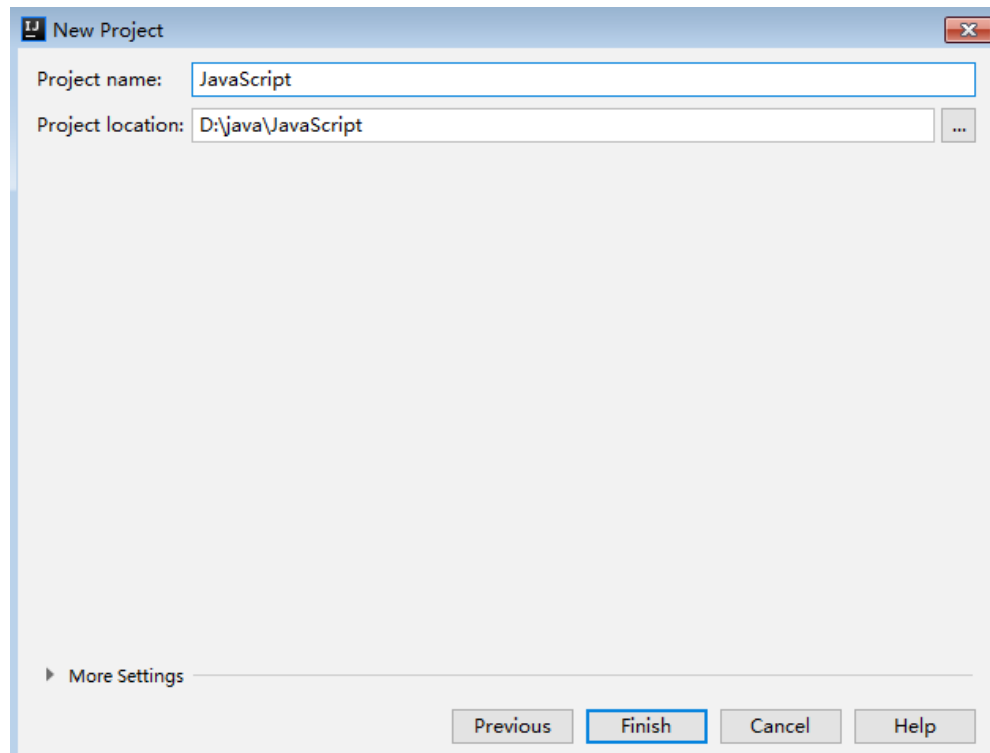
In the **New Project** dialog box, choose **Static Web** and click **Next**.

Figure 2-22 Static Web



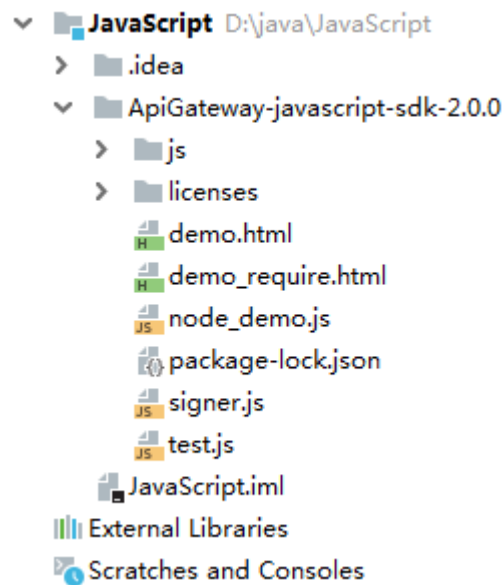
Step 2 Click ..., select the directory where the SDK is decompressed, and click **Finish**.

Figure 2-23 Selecting the SDK directory of JavaScript after decompression



Step 3 View the directory structure shown in the following figure.

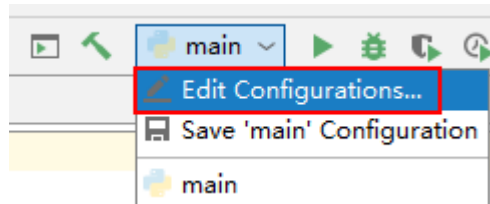
Figure 2-24 Directory structure of the new project JavaScript



- **node_demo.js:** Sample code in Node.js. Modify the parameters in the sample code as required. For details about the sample code, see [API Calling Example \(Node.js\)](#).
- **demo.html:** Browser sample code. Modify the parameters in the sample code as required. For details about the sample code, see [API Calling Example \(Browser\)](#).

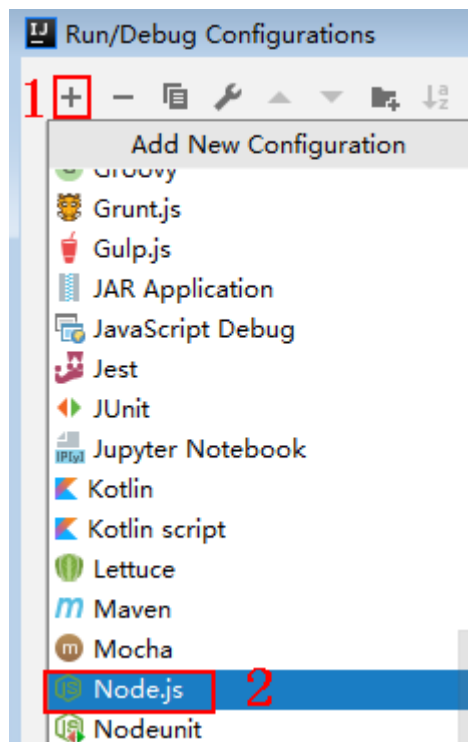
Step 4 Click **Edit Configurations**.

Figure 2-25 Click Edit Configurations



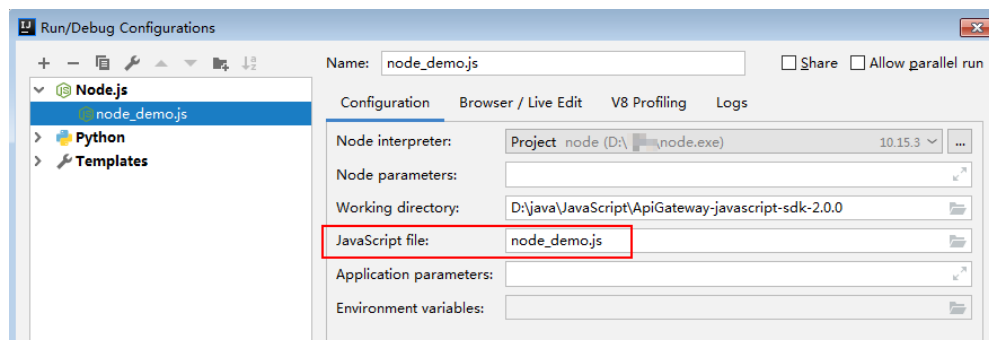
Step 5 Click + and select **Node.js**.

Figure 2-26 Selecting Node.js



Step 6 Set JavaScript file to `node_demo.js` and click **OK**.

Figure 2-27 Selecting node_demo.js



----End

API Calling Example (Node.js)

Step 1 Import `signer.js` to your project.

```
var signer = require('./signer')
var https = require('https')
```

Step 2 Generate a new signer and enter the AppKey and AppSecret.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables `CLOUD_SDK_AK` and `CLOUD_SDK_SK` in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.

a. Open the terminal and run the following command to open the environment variable configuration file:

```
vi ~/.bashrc
```

b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"
export CLOUD_SDK_SK="Obtained SK"
```

c. Run the following command to apply the modification:

```
source ~/.bashrc
```

2. Generate a new signer and enter the configured environment variables.

```
var sig = new signer.Signer()
sig.Key = process.env.CLOUD_SDK_AK
sig.Secret = process.env.CLOUD_SDK_SK
```

Step 3 Generate a request, and specify the method, request URI, and request body.

```
var r = new signer.HttpRequest("POST", "c967a237-cd6c-470e-906f-
a8655461897e.apigw.exampleRegion.com/app1?a=1");
r.body = '{"a":1}'
```

Step 4 Add the `x-stage` header to the request to specify an environment name. Add other headers to be signed as necessary.

```
r.headers = { "x-stage":"RELEASE" }
```

Step 5 Execute the following function to generate HTTP(s) request parameters, and add the `X-Sdk-Date` and `Authorization` headers for signing the request:

```
var opts = sig.Sign(r)
```

Step 6 Access the API and view the access result. If you access the API using HTTPS, change `http.request` to `https.request`.

```
var req=http.request(opts, function(res){
  console.log(res.statusCode)
  res.on("data", function(chunk){
    console.log(chunk.toString())
  })
})
req.on("error",function(err){
  console.log(err.message)
})
req.write(r.body)
req.end()
```

----End

API Calling Example (Browser)

Step 1 The browser restricts the initiation of cross-domain requests from page scripts. Therefore, before accessing an API, you need to create a CORS policy on the APIG

console to allow the browser to send **XMLHttpRequest** requests to the server in a different domain, and bind the policy to the API.

For details about how to create a CORS policy, see "CORS" in the *API Gateway User Guide*.


Figure 2-28 Example for creating a CORS policy

Create Plug-in

* Name

* Type

Description
0/255

Policy Content 

* Allowed Origins

* Allowed Methods

Allowed Headers

Exposed Headers

Maximum Age

Allow Credentials

Step 2 Import **signer.js** and dependencies to the HTML page.

```
<script src="js/hmac-sha256.js"></script>
<script src="js/moment.min.js"></script>
<script src="js/moment-timezone-with-data.min.js"></script>
<script src="signer.js"></script>
```

Step 3 Sign the request and access the API.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables *CLOUD_SDK_AK* and *CLOUD_SDK_SK* in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.
 - a. Open the terminal and run the following command to open the environment variable configuration file:
vi ~/.bashrc
 - b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"
export CLOUD_SDK_SK="Obtained SK"
```
 - c. Run the following command to apply the modification:
source ~/.bashrc

2. Enter the configured environment variables for signature and access.

```
var sig = new signer.Signer()
sig.Key = getenv('CLOUD_SDK_AK')
sig.Secret = getenv('CLOUD_SDK_SK')
var r= new signer.HttpRequest()
r.host = "c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com"
r.method = "POST"
r.uri = "/app1"
r.body = '{"a":1}'
r.query = { "a":"1", "b":"2" }
r.headers = { "Content-Type":"application/json" }
var opts = sig.Sign(r)
var scheme = "https"
$.ajax({
  type: opts.method,
  data: req.body,
  processData: false,
  url: scheme + "://" + opts.hostname + opts.path,
  headers: opts.headers,
  success: function (data) {
    $('#status').html('200')
    $('#recv').html(data)
  },
  error: function (resp) {
    if (resp.readyState === 4) {
      $('#status').html(resp.status)
      $('#recv').html(resp.responseText)
    } else {
      $('#status').html(resp.state())
    }
  },
  timeout: 1000
});
```

----End

2.8 PHP

Scenarios

To use PHP to call an API through app authentication, obtain the PHP SDK, create a new project, and then call the API by referring to the API calling example.

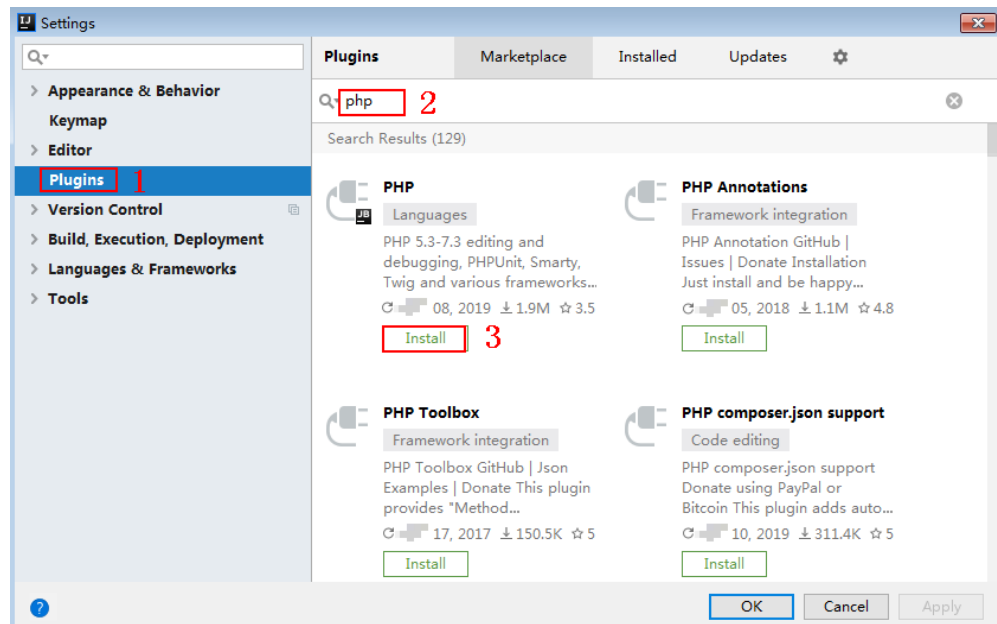
This section uses IntelliJ IDEA 2018.3.5 as an example.

Prerequisites

- You have obtained API calling information. For details, see [Preparation](#).
- You have installed IntelliJ IDEA 2018.3.5 or a later version. If not, download it from the [official IntelliJ IDEA website](#) and install it.
- You have installed PHP 8.0.3 or a later version. If not, download it from the [official PHP website](#) and install it.
- Copy the **php.ini-production** file from the PHP installation directory to the **C:\windows** directory, rename the file as **php.ini**, and then add the following lines to the file:

```
extension_dir = "PHP installation directory/ext"
extension=openssl
extension=curl
```
- You have installed the PHP plug-in on IntelliJ IDEA. If not, install the PHP plug-in according to [Figure 2-29](#).

Figure 2-29 Installing the PHP plug-in



Obtaining the SDK

On the APiG console, choose **Help Center > Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-php-sdk.zip** package. The following table shows the files decompressed from the package.

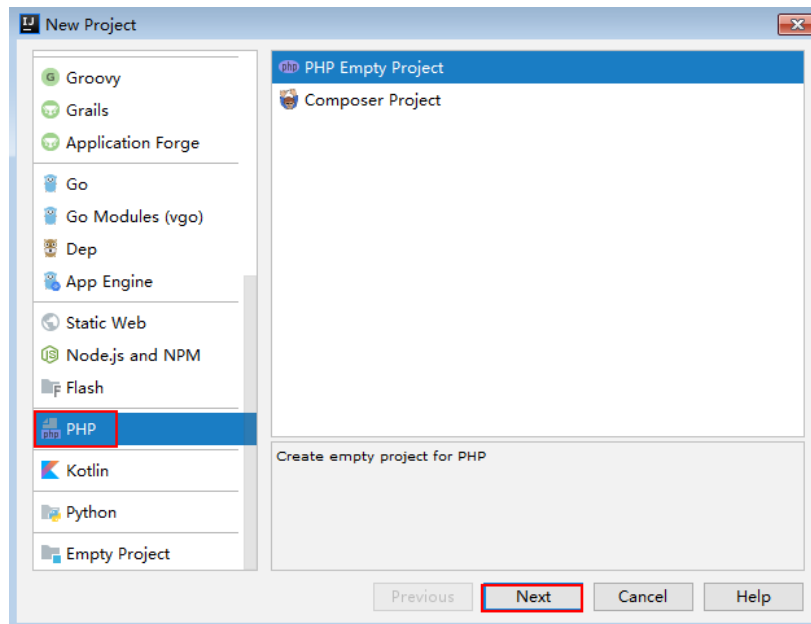
| Name | Description |
|------------|-------------|
| signer.php | SDK code |
| index.php | Sample code |

Creating a Project

Step 1 Start IDEA and choose **File > New > Project**.

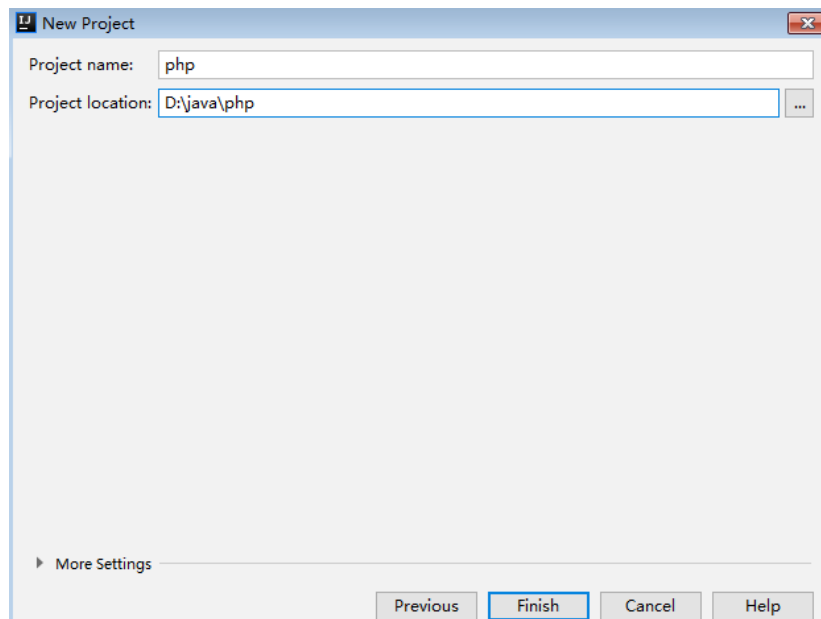
On the displayed **New Project** page, choose **PHP** and click **Next**.

Figure 2-30 PHP

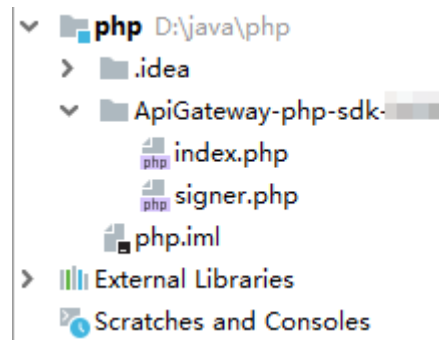


Step 2 Click ..., select the directory where the SDK is decompressed, and click **Finish**.

Figure 2-31 Selecting the SDK directory of PHP after decompression



Step 3 View the directory structure shown in the following figure.

Figure 2-32 Directory structure of the new project php

Modify the parameters in sample code **signer.php** as required. For details about the sample code, see [API Calling Example](#).

----End

API Calling Example

Step 1 Import the PHP SDK to your code.

```
require 'signer.php';
```

Step 2 Generate a new signer and enter the AppKey and AppSecret.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables `CLOUD_SDK_AK` and `CLOUD_SDK_SK` in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.

a. Open the terminal and run the following command to open the environment variable configuration file:

```
vi ~/.bashrc
```

b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"
export CLOUD_SDK_SK="Obtained SK"
```

c. Run the following command to apply the modification:

```
source ~/.bashrc
```

2. Generate a new signer and enter the configured environment variables.

```
$signer = new Signer();
$signer->Key = getenv('CLOUD_SDK_AK');
$signer->Secret = getenv('CLOUD_SDK_SK');
```

Step 3 Generate a new request and specify the method, request URL, and body. (The body should contain the actual request content.)

```
$req = new Request('GET', "https://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/app1?a=1");
$req->body = "";
```

Step 4 Add the x-stage header to the request to specify an environment name. Add other headers to be signed as necessary.

```
$req->headers = array(
    'x-stage' => 'RELEASE',
);
```

Step 5 Execute the following function to generate a **\$curl** context variable.

```
$curl = $signer->Sign($req);
```


Step 6 Access the API and view the access result.

```
$response = curl_exec($curl);
echo curl_getinfo($curl, CURLINFO_HTTP_CODE);
echo $response;
curl_close($curl);
```

----End

2.9 C++

Scenarios

To use C++ to call an API through App authentication, obtain the C++ SDK, and then call the API by referring to the API calling example.

Prerequisites

1. You have obtained API calling information. For details, see [Preparation](#).
2. Install the OpenSSL library.
`apt-get install libssl-dev`
3. Install the curl library.
`apt-get install libcurl4-openssl-dev`

Obtaining the SDK

On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-cpp-sdk.zip** package. The following table shows the files decompressed from the package.

| Name | Description |
|-------------------|----------------------|
| hasher.cpp | SDK code |
| hasher.h | |
| header.h | |
| RequestParams.cpp | |
| RequestParams.h | |
| signer.cpp | |
| signer.h | |
| Makefile | Makefile file |
| main.cpp | Sample code |

API Calling Example

Step 1 Add the following references to **main.cpp**:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <curl/curl.h>
#include "signer.h"
```

Step 2 Generate a new signer and enter the AppKey and AppSecret.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables `CLOUD_SDK_AK` and `CLOUD_SDK_SK` in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.

a. Open the terminal and run the following command to open the environment variable configuration file:

```
vi ~/.bashrc
```

b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"
export CLOUD_SDK_SK="Obtained SK"
```

c. Run the following command to apply the modification:

```
source ~/.bashrc
```

2. Generate a new signer and enter the configured environment variables.

```
Signer signer(getenv("CLOUD_SDK_AK"), getenv("CLOUD_SDK_SK"));
```

Step 3 Generate a new **RequestParams** request, and specify the method, domain name, request URI, query strings, and request body.

```
RequestParams* request = new RequestParams("POST", "c967a237-cd6c-470e-906f-
a8655461897e.apigw.exampleRegion.com", "/app1",
"Action=ListUsers&Version=2010-05-08", "demo");
```

Step 4 Add the x-stage header to the request to specify an environment name. Add other headers to be signed as necessary.

```
request->addHeader("x-stage", "RELEASE");
```

Step 5 Execute the following function to add the generated headers to the request variable.

```
signer.createSignature(request);
```

Step 6 Use the curl library to access the API and view the access result.

```
static size_t
WriteMemoryCallback(void *contents, size_t size, size_t nmemb, void *userp)
{
    size_t realsize = size * nmemb;
    struct MemoryStruct *mem = (struct MemoryStruct *)userp;

    mem->memory = (char*)realloc(mem->memory, mem->size + realsize + 1);
    if (mem->memory == NULL) {
        /* out of memory! */
        printf("not enough memory (realloc returned NULL)\n");
        return 0;
    }

    memcpy(&(mem->memory[mem->size]), contents, realsize);
    mem->size += realsize;
    mem->memory[mem->size] = 0;

    return realsize;
}
```

```
}  
  
//send http request using curl library  
int perform_request(RequestParams* request)  
{  
    CURL *curl;  
    CURLcode res;  
    struct MemoryStruct resp_header;  
    resp_header.memory = (char*)malloc(1);  
    resp_header.size = 0;  
    struct MemoryStruct resp_body;  
    resp_body.memory = (char*)malloc(1);  
    resp_body.size = 0;  
  
    curl_global_init(CURL_GLOBAL_ALL);  
    curl = curl_easy_init();  
  
    curl_easy_setopt(curl, CURLOPT_CUSTOMREQUEST, request->getMethod().c_str());  
    std::string url = "http://" + request->getHost() + request->getUri() + "?" + request->getQueryParams();  
    curl_easy_setopt(curl, CURLOPT_URL, url.c_str());  
    struct curl_slist *chunk = NULL;  
    std::set<Header>::iterator it;  
    for (auto header : *request->getHeaders()) {  
        std::string headerEntry = header.getKey() + ": " + header.getValue();  
        printf("%s\n", headerEntry.c_str());  
        chunk = curl_slist_append(chunk, headerEntry.c_str());  
    }  
    printf("-----\n");  
    curl_easy_setopt(curl, CURLOPT_HTTPHEADER, chunk);  
    curl_easy_setopt(curl, CURLOPT_COPYPOSTFIELDS, request->getPayload().c_str());  
    curl_easy_setopt(curl, CURLOPT_NOBODY, 0L);  
    curl_easy_setopt(curl, CURLOPT_WRITEFUNCTION, WriteMemoryCallback);  
    curl_easy_setopt(curl, CURLOPT_HEADERDATA, (void *)&resp_header);  
    curl_easy_setopt(curl, CURLOPT_WRITEDATA, (void *)&resp_body);  
    //curl_easy_setopt(curl, CURLOPT_VERBOSE, 1L);  
    res = curl_easy_perform(curl);  
    if (res != CURLE_OK) {  
        fprintf(stderr, "curl_easy_perform() failed: %s\n", curl_easy_strerror(res));  
    }  
    else {  
        long status;  
        curl_easy_getinfo(curl, CURLINFO_HTTP_CODE, &status);  
        printf("status %d\n", status);  
        printf(resp_header.memory);  
        printf(resp_body.memory);  
    }  
    free(resp_header.memory);  
    free(resp_body.memory);  
    curl_easy_cleanup(curl);  
  
    curl_global_cleanup();  
  
    return 0;  
}
```

Step 7 Run the **make** command to obtain a **main** executable file, execute the file, and then view the execution result.

----End

2.10 C

Scenarios

To use C to call an API through app authentication, obtain the C SDK, and then call the API by referring to the API calling example.

Prerequisites

1. You have obtained API calling information. For details, see [Preparation](#).
2. Install the OpenSSL library.

```
apt-get install libssl-dev
```
3. Install the curl library.

```
apt-get install libcurl4-openssl-dev
```

Obtaining the SDK

On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-c-sdk.zip** package. The following table shows the files decompressed from the package.

| Name | Description |
|-----------------|---------------|
| signer_common.c | SDK code |
| signer_common.h | |
| signer.c | |
| signer.h | |
| Makefile | Makefile file |
| main.c | Sample code |

API Calling Example

Step 1 Add the following references to **main.c**:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <curl/curl.h>
#include "signer.h"
```

Step 2 Generate a `sig_params_t` variable, and enter the AppKey and AppSecret.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables `CLOUD_SDK_AK` and `CLOUD_SDK_SK` in the local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.
 - a. Open the terminal and run the following command to open the environment variable configuration file:
vi ~/.bashrc
 - b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"
export CLOUD_SDK_SK="Obtained SK"
```
 - c. Run the following command to apply the modification:
source ~/.bashrc

2. Generate a `sig_params_t` variable, and enter the configured environment variables.

```
sig_params_t params;  
sig_params_init(&params);  
sig_str_t app_key = sig_str(getenv("CLOUD_SDK_AK"));  
sig_str_t app_secret = sig_str(getenv("CLOUD_SDK_SK"));  
params.key = app_key;  
params.secret = app_secret;
```

- Step 3** Specify the method, domain name, request URI, query strings, and request body.

```
sig_str_t host = sig_str("c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com");  
sig_str_t method = sig_str("GET");  
sig_str_t uri = sig_str("/app1");  
sig_str_t query_str = sig_str("a=1&b=2");  
sig_str_t payload = sig_str("");  
params.host = host;  
params.method = method;  
params.uri = uri;  
params.query_str = query_str;  
params.payload = payload;
```

- Step 4** Add the `x-stage` header to the request to specify an environment name. Add other headers to be signed as necessary.

```
sig_headers_add(&params.headers, "x-stage", "RELEASE");
```

- Step 5** Execute the following function to add the generated headers to the request variable.

```
sig_sign(&params);
```

- Step 6** Use the `curl` library to access the API and view the access result.

```
static size_t  
WriteMemoryCallback(void *contents, size_t size, size_t nmemb, void *userp)  
{  
    size_t realsize = size * nmemb;  
    struct MemoryStruct *mem = (struct MemoryStruct *)userp;  
  
    mem->memory = (char*)realloc(mem->memory, mem->size + realsize + 1);  
    if (mem->memory == NULL) {  
        /* out of memory! */  
        printf("not enough memory (realloc returned NULL)\n");  
        return 0;  
    }  
  
    memcpy(&(mem->memory[mem->size]), contents, realsize);  
    mem->size += realsize;  
    mem->memory[mem->size] = 0;  
  
    return realsize;  
}  
  
//send http request using curl library  
int perform_request(RequestParams* request)  
{  
    CURL *curl;  
    CURLcode res;  
    struct MemoryStruct resp_header;  
    resp_header.memory = malloc(1);  
    resp_header.size = 0;  
    struct MemoryStruct resp_body;  
    resp_body.memory = malloc(1);  
    resp_body.size = 0;  
  
    curl_global_init(CURL_GLOBAL_ALL);  
    curl = curl_easy_init();  
  
    curl_easy_setopt(curl, CURLOPT_CUSTOMREQUEST, params.method.data);  
    char url[1024];
```

```
sig_sprintf(url, 1024, "http://%V%V?%V", &params.host, &params.uri, &params.query_str);
curl_easy_setopt(curl, CURLOPT_URL, url);
struct curl_slist *chunk = NULL;
for (int i = 0; i < params.headers.len; i++) {
    char header[1024];
    sig_sprintf(header, 1024, "%V: %V", &params.headers.data[i].name, &params.headers.data[i].value);
    printf("%s\n", header);
    chunk = curl_slist_append(chunk, header);
}
printf("-----\n");
curl_easy_setopt(curl, CURLOPT_HTTPHEADER, chunk);
curl_easy_setopt(curl, CURLOPT_POSTFIELDS, params.payload.data);
curl_easy_setopt(curl, CURLOPT_NOBODY, 0L);
curl_easy_setopt(curl, CURLOPT_WRITEFUNCTION, WriteMemoryCallback);
curl_easy_setopt(curl, CURLOPT_HEADERDATA, (void *)&resp_header);
curl_easy_setopt(curl, CURLOPT_WRITEDATA, (void *)&resp_body);
//curl_easy_setopt(curl, CURLOPT_VERBOSE, 1L);
res = curl_easy_perform(curl);
if (res != CURLE_OK) {
    fprintf(stderr, "curl_easy_perform() failed: %s\n", curl_easy_strerror(res));
}
else {
    long status;
    curl_easy_getinfo(curl, CURLINFO_HTTP_CODE, &status);
    printf("status %d\n", status);
    printf(resp_header.memory);
    printf(resp_body.memory);
}
free(resp_header.memory);
free(resp_body.memory);
curl_easy_cleanup(curl);

curl_global_cleanup();

//free signature params
sig_params_free(&params);
return 0;
}
```

Step 7 Run the **make** command to obtain a **main** executable file, execute the file, and then view the execution result.

----End

2.11 Android

Scenarios

To use Android to call an API through app authentication, obtain the Android SDK, create a new project, and then call the API by referring to the API calling example.

Prerequisites

- You have obtained API calling information. For details, see [Preparation](#).
- You have installed Android Studio 4.1.2 or a later version. If not, download it from the [official Android Studio website](#) and install it.

Obtaining the SDK

On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

Then obtain the **ApiGateway-android-sdk.zip** package. The following table shows the files decompressed from the package.

| Name | Description |
|-------------------|----------------------------|
| app\ | Android project code |
| gradle\ | Gradle files |
| build.gradle | Gradle configuration files |
| gradle.properties | |
| settings.gradle | |
| gradlew | Gradle Wrapper scripts |
| gradlew.bat | |

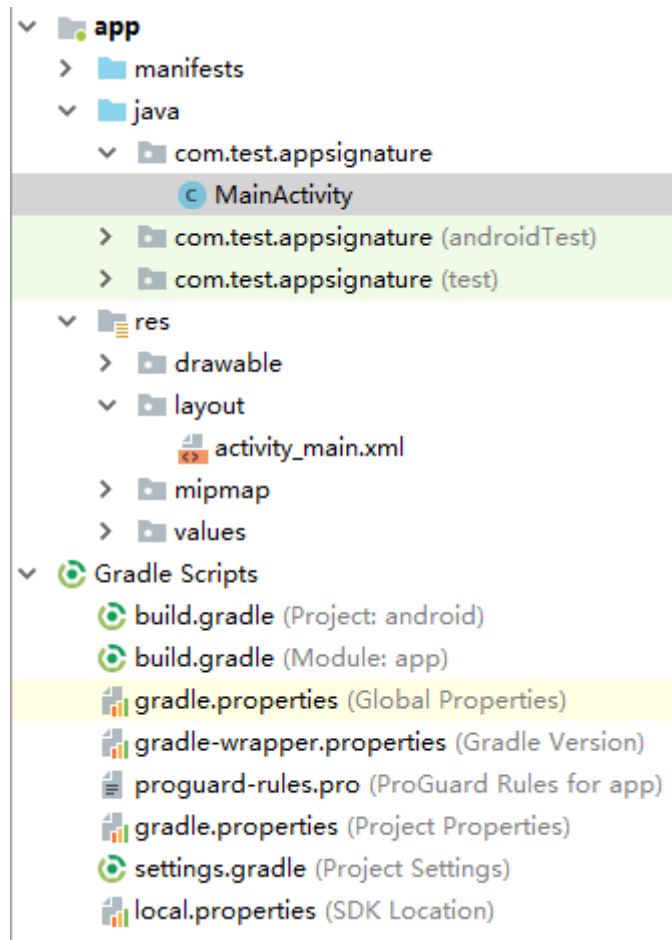
Opening a Project

Step 1 Start the Android Studio and choose **File > Open**.

Select the directory where the SDK is decompressed.

Step 2 View the directory structure of the project shown in the following figure.

Figure 2-33 Project directory structure



----End

API Calling Example

Step 1 Add required JAR files to the **app/libs** directory of the Android project. The following JAR files must be included:

- java-sdk-core-x.x.x.jar
- commons-logging-1.2.jar
- joda-time-2.10.jar

Step 2 Add dependencies of the **okhttp** library to the **build.gradle** file.

Add **implementation 'com.squareup.okhttp3:okhttp:3.14.2'** in the **dependencies** field of the **build.gradle** file.

```
dependencies {
    ...
    ...
    implementation 'com.squareup.okhttp3:okhttp:3.14.3'
}
```

Step 3 Create a request, enter an AppKey and AppSecret, and specify the domain name, method, request URI, and body.

1. In this example, the AK and SK stored in the environment variables are used. Specify the environment variables *CLOUD_SDK_AK* and *CLOUD_SDK_SK* in the

local environment first. The following uses Linux as an example to describe how to set the **obtained AK/SK** as environment variables.

- a. Open the terminal and run the following command to open the environment variable configuration file:

```
vi ~/.bashrc
```

- b. Set environment variables, save the file, and exit the editor.

```
export CLOUD_SDK_AK="Obtained AK"  
export CLOUD_SDK_SK="Obtained SK"
```

- c. Run the following command to apply the modification:

```
source ~/.bashrc
```

2. Create a request, enter the configured environment variables, and specify the domain name, method, request URI, and body.

```
Request request = new Request();  
try {  
    request.setKey(System.getenv("CLOUD_SDK_AK"));  
    request.setSecret(System.getenv("CLOUD_SDK_SK"));  
    request.setMethod("POST");  
    request.setUrl("https://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/app1");  
    request.addQueryStringParam("name", "value");  
    request.addHeader("Content-Type", "text/plain");  
    request.setBody("demo");  
} catch (Exception e) {  
    e.printStackTrace();  
    return;  
}
```

- Step 4** Sign the request to generate an **okhttp3.Request** object for API access.

```
okhttp3.Request signedRequest = Client.signOkhttp(request);  
OkHttpClient client = new OkHttpClient.Builder().build();  
Response response = client.newCall(signedRequest).execute();
```

----End

2.12 curl

Scenarios

To use the curl command to call an API through app authentication, download the JavaScript SDK to generate the curl command, and copy the command to the CLI to call the API.

Prerequisites

You have obtained API calling information. For details, see [Preparation](#).

API Calling Example

- Step 1** Use the JavaScript SDK to generate the curl command.

On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

Open demo.html in a browser. The following figure shows the demo page.

Apigateway Signature Test

Key

Secret

Method Url

Headers

Body


```
curl -X GET "http://30030113-3657-4fb6-a7ef-90764239b038.apigw.exampleRegion.com/" -H "X-Sdk-Date: 20190731T065514Z" -H "host: 30030113-3657-4fb6-a7ef-9076423
```

Note: accessing the API from browser requires [support for CORS](#)

200
Congratulations, sdk demo is running

Step 2 Specify the key, secret, method, protocol, domain name, and URL.

```
Key=4f5f****100c  
Secret=*****  
Method=POST  
Url=https://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com
```

Step 3 Specify query and header parameters in JSON format, and set the request body.

Step 4 Click **Send request** to generate a **curl** command. Copy the **curl** command to the CLI to access the API.

```
$ curl -X POST "https://c967a237-cd6c-470e-906f-a8655461897e.apigw.exampleRegion.com/" -H "X-Sdk-Date: 20180530T115847Z" -H "Authorization: SDK-HMAC-SHA256 Access=071f***e06a, SignedHeaders=host;x-sdk-date, Signature=9e5314bd156d517*****dd3e5765fdde4" -d ""  
Congratulations, sdk demo is running
```

The **curl** command generated using an SDK does not meet the format requirements of Windows. Please run the **curl** command in Git Bash.

----End

3 Calling APIs Through IAM Authentication

3.1 Token Authentication

Scenarios

To call APIs using a token, add the token to the **X-Auth-Token** header in API requests.

 **NOTE**

You can use either of the following authentication methods to call APIs:

- Token authentication: Requests are authenticated using a token.
- AK/SK authentication: Requests are encrypted using an access key ID (AK) and a secret access key (SK).

API Calling Example

1. Obtain a token and set it as an environment variable for authenticating the calling of other APIs.
 - a. Obtain a token. An example request is as follows:

```
curl -X POST https://{iam_endpoint}/v3/auth/tokens -H 'content-type: application/json' -d '{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "{user_name}",
          "domain": {
            "name": "{user_name}"
          }
        },
        "password": "{password}"
      }
    }
  },
  "scope": {
    "project": {
```

```

    "id": "{project_id}"
  }
}
}' -vk

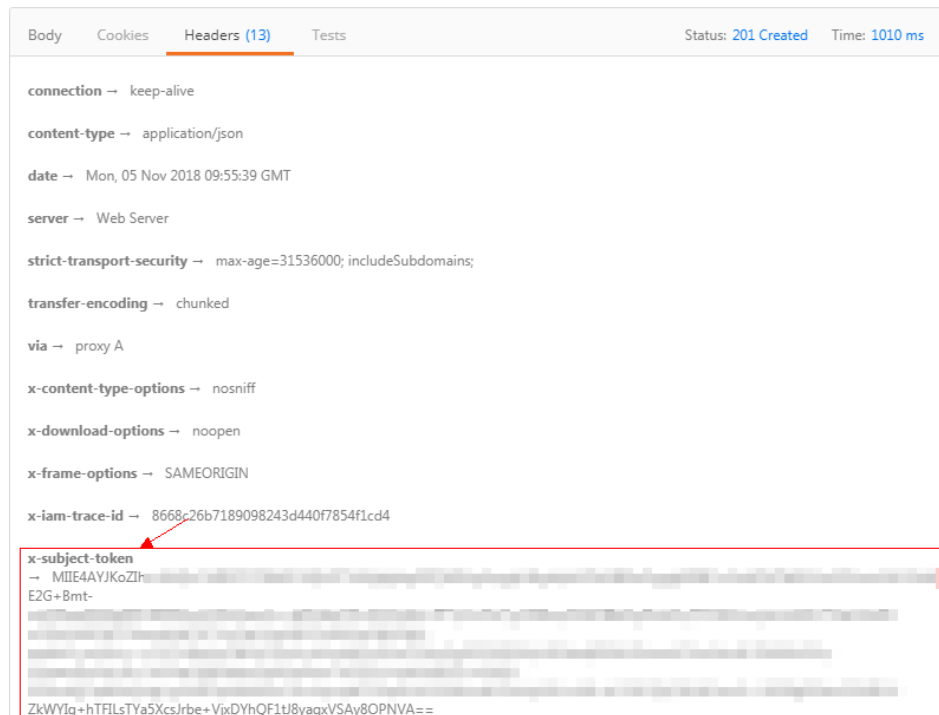
```

Modify the parameters in the preceding command according to the following description. For details, see the API for Obtaining a User Token in the *Identity and Access Management API Reference*.

- Obtain the *{iam_endpoint}* from [Regions and Endpoints](#).
- Replace *{user_name}* and *{password}* respectively with the username and password of the IAM server.
- *{project_id}*: The project ID. On the management console, hover the mouse pointer over the username in the upper right corner, choose **My Credentials** from the drop-down list, and then view the project ID on the displayed page.

The token value is the **X-Subject-Token** value in the response header as shown below:

Figure 3-1 Obtaining the X-Subject-Token response header



- b. Run the following command to set an environment variable for passing the token:

```
export Token={X-Subject-Token}
```

X-Subject-Token is the token obtained in **1.a**. Example:

```
export Token=MIIDkg*****BZQMEAgEwg
```

2. To call an API, obtain the domain name, request method, and URL by referring to [Preparation](#), add **X-Auth-Token** to the request header, and set the value of **X-Auth-Token** to the token obtained in **1**. Set the parameters based on the site requirements.

```
curl -X Request_method Domain name+URL -H "x-auth-token: $Token" -vk
```

3.2 AK/SK Authentication

This section describes how to use AK and SK to sign requests.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

Generating an AK and SK Pair

If an AK/SK pair has already been generated, skip this step. Find the downloaded AK/SK file, which is usually named **credentials.csv**.

As shown in the following figure, the file contains the username, access key ID, and secret access key.

Figure 3-2 Content of the credential.csv file

| | A | B | C |
|---|-----------|-------------------------|--------------------------|
| 1 | User Name | Access Key Id | Secret Access Key |
| 2 | | QWSDSDJWQTFWASDFWQWEDSD | zuIJJhJ...eqXbhSzsdaGwf4 |

Note:

1. You can create a maximum of two access keys with identical permissions and unlimited validity and cannot increase the quota. **Each access key can be downloaded only once when created.** Keep your access keys secure and change them periodically for security purposes. To change an access key, delete it and create a new one.
2. Federated users can only create temporary access credentials (temporary AK/SKs and security tokens).
3. If you are an administrator, you can view the AK of an IAM user on the user details page. The SK is kept by the user.

Perform the following procedure to generate an AK/SK pair:

- Step 1** Log in to the .
 - Step 2** Hover the cursor on the username and choose **My Credentials** from the drop-down list.
 - Step 3** Click the **Access Keys** tab.
 - Step 4** Click **Create Access Key**.
- Each user can create a maximum of two access keys. The quota cannot be increased.**
- To change an access key, delete it and create a new one.
- Step 5** Enter a description, and click **OK**.

Step 6 In the displayed dialog box, click **Download** to save the access key.

You can obtain the AK from the access key list and SK from the downloaded CSV file.

- For details about how to obtain a temporary AK/SK, see the *Identity and Access Management API Reference*.
- Keep the CSV file properly. You can only download the file right after the access key is created. However, if you cannot find the file to obtain the key information, you can create a key.
- Open the CSV file in the lower left corner, or choose **Downloads** in the browser and open the CSV file.
- For security purposes, keep your access keys secure and change them periodically.

----End

Generating a Signature

Generate a signature in the same way as in App authentication mode. Replace AppKey with AK and replace AppSecret with SK to complete the signing and request processing. You can sign requests to access APIs by using [Java](#), [Go](#), [Python](#), [C#](#), [JavaScript](#), [PHP](#), [C++](#), [C](#), and [Android](#).

NOTICE

- The local time on the client must be synchronized with the clock server to avoid a large error in the value of the **X-Sdk-Date** request header.
 - APIG (API Management) checks the time format and compares the time with the time when APIG (API Management) receives the request. If the time difference exceeds 15 minutes, APIG will reject the request.
-

4 Creating Signatures for Backend Requests

4.1 Pre-signature Preparations

Obtaining signature key information:

On the APIG instance console, choose **API Management > API Policies > Policies**, click the *signature key name* to go to the details page, and view the key and secret in the **Policy Content** area.

4.2 Java

Scenarios

To use Java to sign backend requests, obtain the Java SDK, import the project, and verify the backend signature by referring to the example provided in this section.

This section uses IntelliJ IDEA 2018.3.5 as an example.

Constraints

Signature information is added to requests sent to access the backend of an API only after a signature key is bound to the API.

Prerequisites

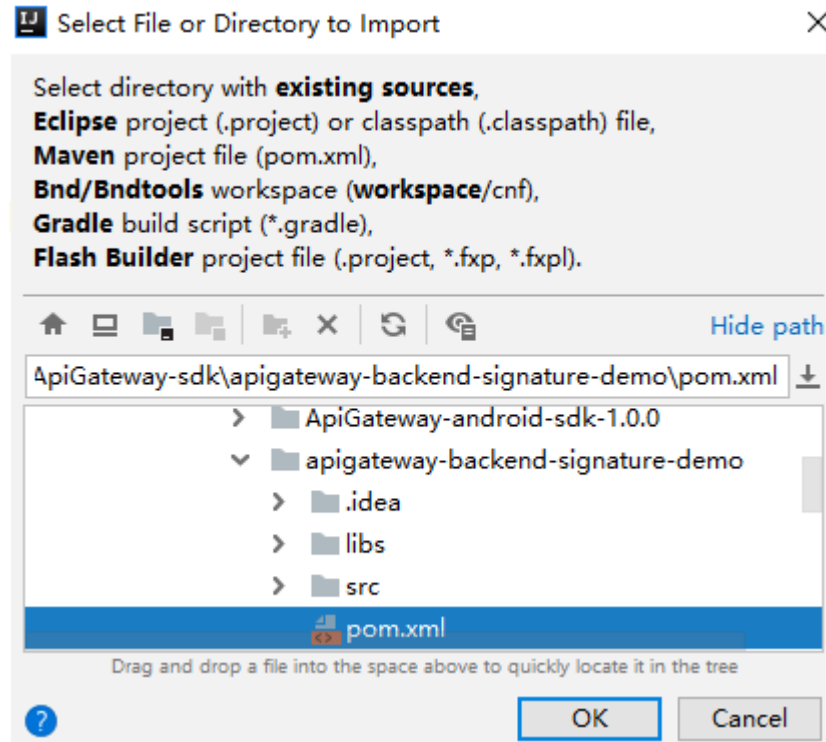
- You have created a signature key on the APIG console and bound it to the API to be called. For more information, see section "Configuring Signature Verification for Backend Services" in the *API Gateway User Guide*.
- You have obtained the signature key and secret. For details, see [Pre-signature Preparations](#).
- On the APIG console, choose **Help Center > Using SDKs**, and download the SDK of the desired language.
- You have installed IntelliJ IDEA 2018.3.5 or a later version. If not, download it from the [official IntelliJ IDEA website](#) and install it.

- You have installed Java Development Kit (JDK) 1.8.111 or a later version. If not, download JDK from the [official Oracle website](#) and install it. JDK 17 or later is not supported.

Importing a Project

- Step 1** Open IntelliJ IDEA, choose **File > New > Project from Existing Sources**, select the **apigateway-backend-signature-demo\pom.xml** file, and click **OK**.

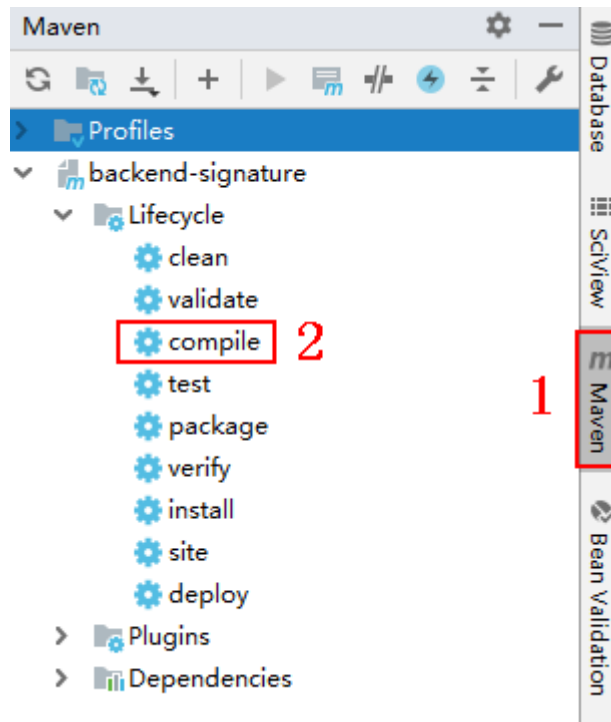
Figure 4-1 Select File or Directory to Import



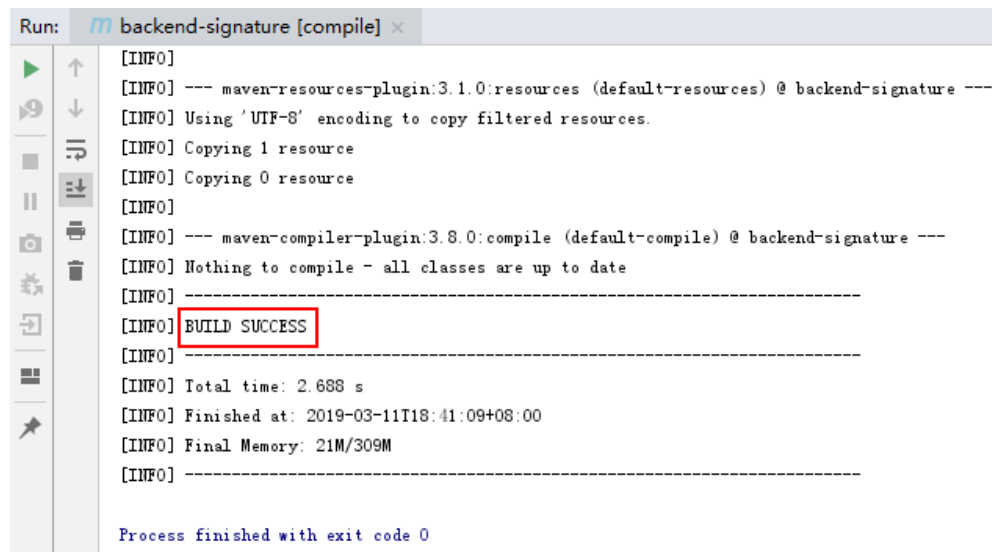
- Step 2** Retain the default settings, click **Next** for the following four steps, and then click **Finish**.

- Step 3** On the **Maven** tab page on the right, double-click **compile** to compile the file.

Figure 4-2 Compiling the project

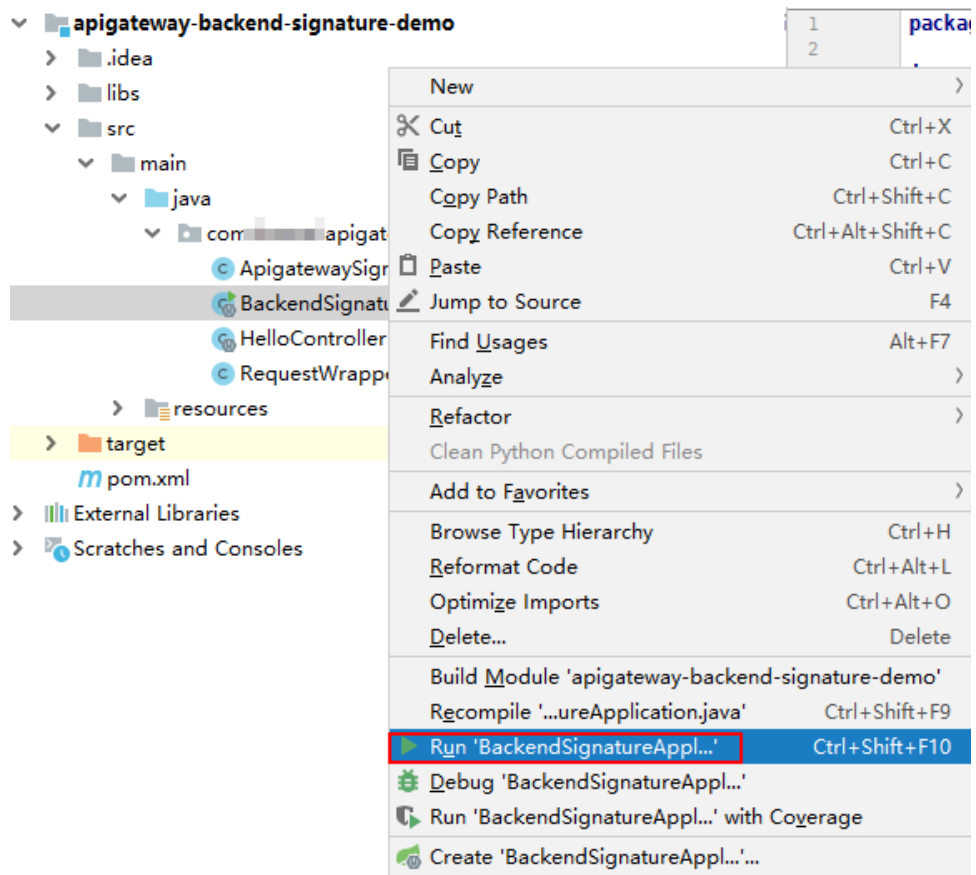


If the message "BUILD SUCCESS" is displayed, the compilation is successful.



Step 4 Right-click **BackendSignatureApplication** and choose **Run**.

Figure 4-3 Running the BackendSignatureApplication service



Modify the parameters in sample code **ApigatewaySignatureFilter.java** as required. For details about the sample code, see [Backend Signature Verification Example](#).

----End

Backend Signature Verification Example

This example demonstrates how to build a Spring boot-based server as the backend of an API and implement a filter to verify the signature of requests sent from APIG (API Management).

- Step 1** Compile a controller that matches all request paths and methods and set the return body to **Hello World!**

```
// HelloController.java
@RestController
@EnableAutoConfiguration
public class HelloController {
    @RequestMapping("/")
    private String index() {
        return "Hello World!";
    }
}
```

- Step 2** Compile a filter that matches all request paths and methods, and put the signature key and secret in a **Map**.

```
// ApigatewaySignatureFilter.java

@Component
@WebFilter(filterName = "ApigatewaySignatureFilter", urlPatterns = "/*")
public class ApigatewaySignatureFilter implements Filter {
    private static Map<String, String> secrets = new HashMap<>();
    static {

        secrets.put(System.getenv("SDK_AK1"), System.getenv("SDK_SK1"));
        secrets.put(System.getenv("SDK_AK2"), System.getenv("SDK_SK2"));
    }

    @Override
    public void init(FilterConfig filterConfig) throws ServletException {
    }

    @Override
    public void doFilter(ServletRequest servletRequest, ServletResponse servletResponse, FilterChain chain) {
        //Signature verification code
        ...
    }
}
```

Step 3 To ensure that the body can be read in the filter and controller, wrap the request and send it to the filter and controller. The `doFilter` function is used for signature verification. For the implementation of wrapper classes, see `RequestWrapper.java`.

```
RequestWrapper request = new RequestWrapper((HttpServletRequest) servletRequest);
```

Step 4 Use a regular expression to parse the **Authorization** header to obtain **signingKey** and **signedHeaders**.

```
private static final Pattern authorizationPattern = Pattern.compile("SDK-HMAC-SHA256\\s+Access=([^,]+),\\s?SignedHeaders=([^,]+),\\s?Signature=(\\w+)");
...

String authorization = request.getHeader("Authorization");
if (authorization == null || authorization.length() == 0) {
    response.sendError(HttpServletResponse.SC_UNAUTHORIZED, "Authorization not found.");
    return;
}

Matcher m = authorizationPattern.matcher(authorization);
if (!m.find()) {
    response.sendError(HttpServletResponse.SC_UNAUTHORIZED, "Authorization format incorrect.");
    return;
}
String signingKey = m.group(1);
String signingSecret = secrets.get(signingKey);
if (signingSecret == null) {
    response.sendError(HttpServletResponse.SC_UNAUTHORIZED, "Signing key not found.");
    return;
}
String[] signedHeaders = m.group(2).split(",");
```

For example, for **Authorization** header:

```
SDK-HMAC-SHA256 Access=signature_key1, SignedHeaders=host;x-sdk-date,
Signature=e11adf65a20d1b82c25419b5*****8d0ba12fed1ceb13ed00
```

The parsing result is as follows:

```
signingKey=signature_key1
signedHeaders=host;x-sdk-date
```

Step 5 Find **signingSecret** based on **signingKey**. If **signingKey** does not exist, the authentication failed.

```
String signingSecret = secrets.get(signingKey);
if (signingSecret == null) {
    response.sendError(ServletResponse.SC_UNAUTHORIZED, "Signing key not found.");
    return;
}
```

- Step 6** Create a request, and add the method, URL, query, and signedHeaders headers to the request. Determine whether the body needs to be set.

The body is read if there is no **x-sdk-content-sha256** header with value **UNSIGNED-PAYLOAD**.

```
Request apiRequest = new DefaultRequest();
apiRequest.setHttpMethod(HttpMethodName.valueOf(request.getMethod()));
String url = request.getRequestURL().toString();
String queryString = request.getQueryString();
try {
    apiRequest.setEndpoint((new URL(url)).toURI());
    Map<String, String> parametersmap = new HashMap<>();
    if (null != queryString && !"".equals(queryString)) {
        String[] parameterarray = queryString.split("&");
        for (String p : parameterarray) {
            String[] p_split = p.split("=", 2);
            String key = p_split[0];
            String value = "";
            if (p_split.length >= 2) {
                value = p_split[1];
            }
            parametersmap.put(URLEncoder.decode(key, "UTF-8"), URLEncoder.decode(value, "UTF-8"));
        }
        apiRequest.setParameters(parametersmap); //set query
    }
} catch (URISyntaxException e) {
    e.printStackTrace();
}

boolean needbody = true;
String dateHeader = null;
for (int i = 0; i < signedHeaders.length; i++) {
    String headerValue = request.getHeader(signedHeaders[i]);
    if (headerValue == null || headerValue.length() == 0) {
        ((ServletResponse) response).sendError(ServletResponse.SC_UNAUTHORIZED, "signed
header" + signedHeaders[i] + " not found.");
    } else {
        apiRequest.addHeader(signedHeaders[i], headerValue); //set header
        if (signedHeaders[i].toLowerCase().equals("x-sdk-content-sha256") &&
headerValue.equals("UNSIGNED-PAYLOAD")) {
            needbody = false;
        }
        if (signedHeaders[i].toLowerCase().equals("x-sdk-date")) {
            dateHeader = headerValue;
        }
    }
}

if (needbody) {
    apiRequest.setContent(new ByteArrayInputStream(request.getBody())); //set body
}
```

- Step 7** Check whether the signature has expired. Obtain the time from the **X-Sdk-Date** header, and check whether the difference between this time and the server time is within 15 minutes. If **signedHeaders** does not contain **X-Sdk-Date**, the authentication failed.

```
private static final DateTimeFormatter timeFormatter =
DateTimeFormat.forPattern("yyyyMMdd'T'HHmmss'Z").withZoneUTC();
...
if (dateHeader == null) {
```

```
response.sendError(HttpServletResponse.SC_UNAUTHORIZED, "Header x-sdk-date not found.");
return;
}
long date = timeFormatter.parseMillis(dateHeader);
long duration = Math.abs(DateTime.now().getMillis() - date);
if (duration > 15 * 60 * 1000) {
    response.sendError(HttpServletResponse.SC_UNAUTHORIZED, "Signature expired.");
    return;
}
```

Step 8 Add the **Authorization** header to the request, and invoke the **verify** method to verify the request signature. If the verification is successful, the next filter is executed. Otherwise, the authentication failed.

```
apiRequest.addHeader("authorization", authorization);
apiRequest.setKey(signingKey);
apiRequest.setSecret(signingSecret);
Signer signer = new Signer();
boolean verify = signer.verify(apiRequest);
if (verify) {
    chain.doFilter(request, response);
} else {
    response.sendError(HttpServletResponse.SC_UNAUTHORIZED, "Verify authorization failed.");
}
```

Step 9 Run the server to verify the code. The following example uses the [HTML signature tool](#) in the JavaScript SDK to generate a signature.

Set the parameters according to the following figure, and click **Send request**. Copy the generated curl command, execute it in the CLI, and check whether the server returns **Hello World!**

If an incorrect key or secret is used, the server returns **401**, which means authentication failure.

Apigateway Signature Test

Key
signature_key1

Secret
signature_secret1

Method: POST | Scheme: http | Host: localhost:8080 | Url: /test

Query
{ "xxx": "yyy" }

Headers
{ "aaa": "bbb" }

Body
dsfasdf=1

Buttons: Debug, Send request

```
curl -X POST "http://localhost:8080/test?xxx=yyy" -H "aaa: bbb" -H "X-Sdk-Date: 20190307T122402Z" -H "host: localhost:8080" -H "Authorization: SDK-HMAC-SHA256 Access=signatur
```

----End

4.3 Python

Scenarios

To use Python to sign backend requests, obtain the Python SDK, import the project, and verify the backend signature by referring to the example provided in this section.

This section uses IntelliJ IDEA 2018.3.5 as an example.

Constraints

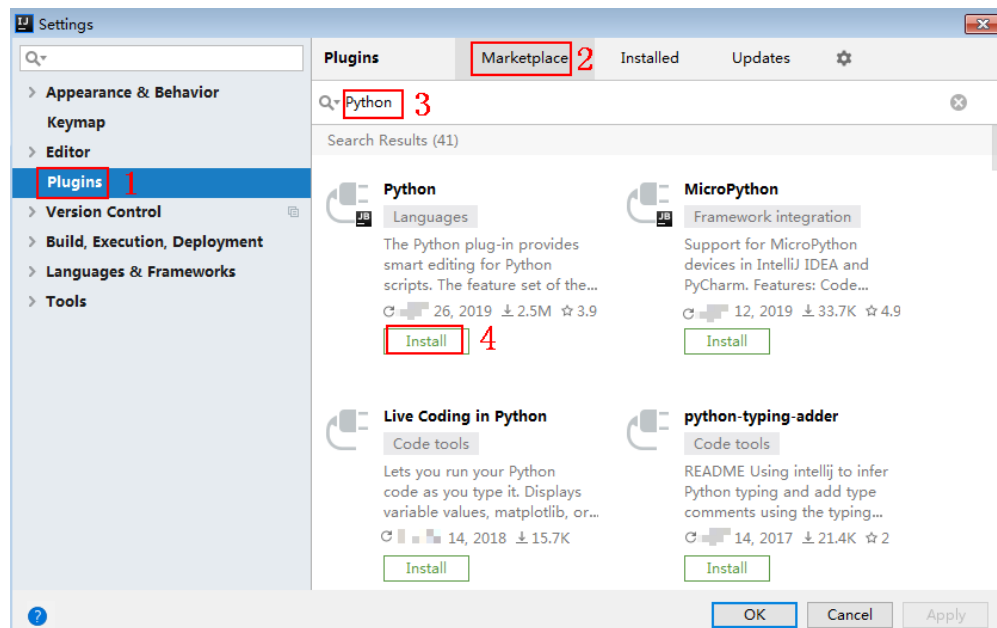
Signature information is added to requests sent to access the backend of an API only after a signature key is bound to the API.

Preparing the Environment

- You have created a signature key on the APIG console and bound it to the API to be called. For more information, see section "Signature Keys" in the *API Gateway User Guide*.
- You have obtained the signature key and secret. For details, see [Pre-signature Preparations](#).
- On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.

- You have installed Python 2.7.9 or 3.X. If not, download the Python installation package from the [official Python website](#) and install it.
- You have installed IntelliJ IDEA 2018.3.5 or a later version. If not, download it from the [official IntelliJ IDEA website](#) and install it.
- You have installed the Python plug-in on IntelliJ IDEA. If not, install the Python plug-in according to [Figure 4-4](#).

Figure 4-4 Installing the Python plug-in

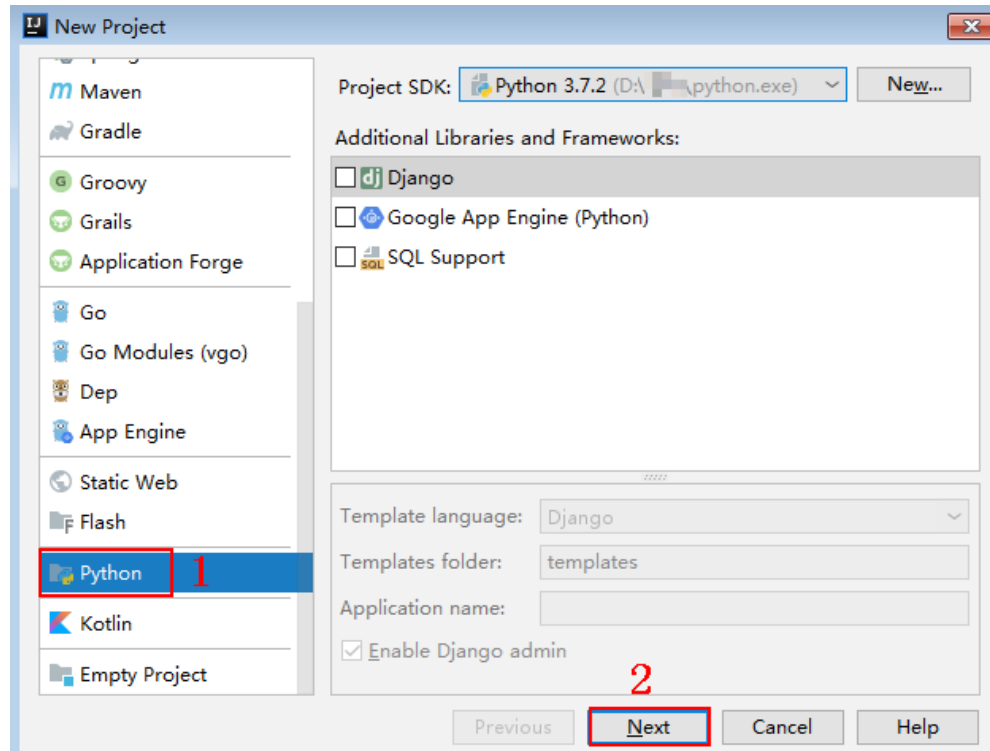


Importing a Project

Step 1 Start IntelliJ IDEA and choose **File > New > Project**.

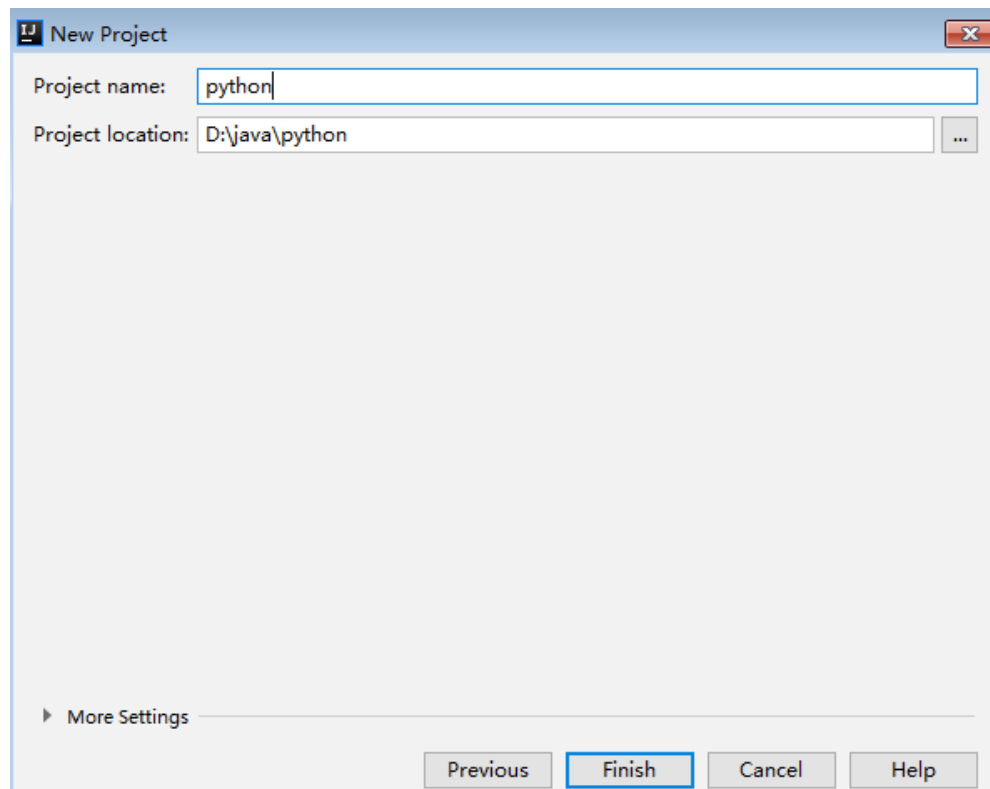
On the displayed **New Project** page, choose **Python** and click **Next**.

Figure 4-5 New Python



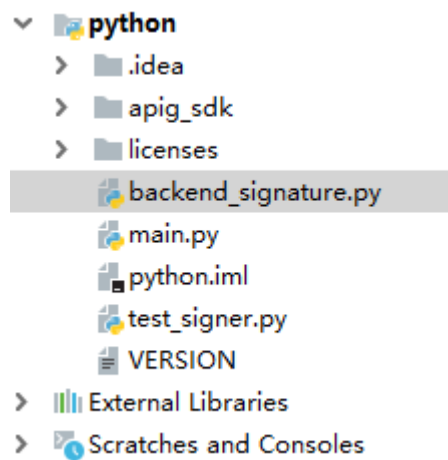
Step 2 Click **Next**. Click ..., select the directory where the SDK is decompressed, and click **Finish**.

Figure 4-6 Selecting the SDK directory of Python after decompression



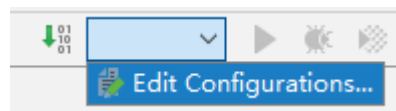
Step 3 View the directory structure shown in the following figure.

Figure 4-7 Directory structure



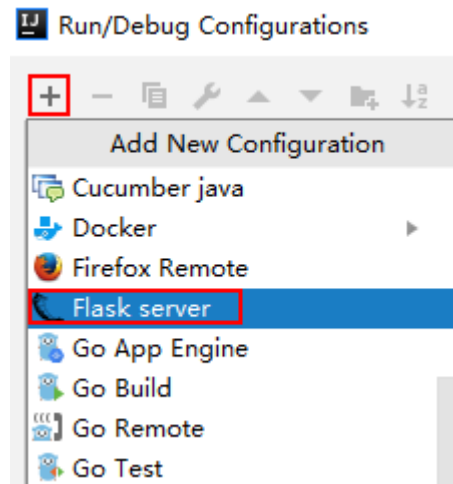
Step 4 Click **Edit Configurations**.

Figure 4-8 Edit Configurations

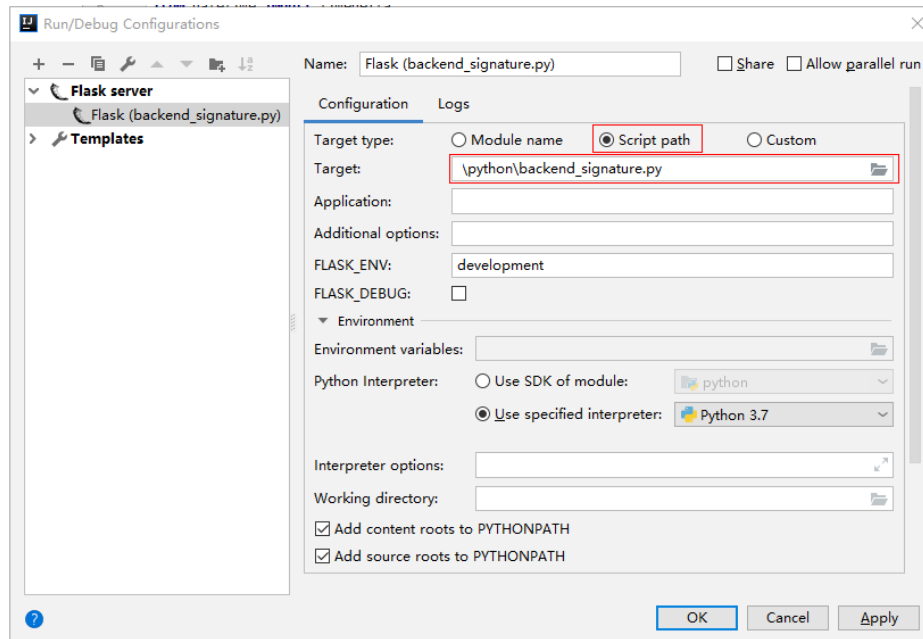


Step 5 Click + and choose **Flask server**.

Figure 4-9 Choosing Flask server



Step 6 Set **Target type** to **Script path**, select **backend_signature.py** from the **Target** drop-down list box, and click **OK**.



----End

Backend Signature Verification Example

This example demonstrates how to build a Flask-based server as the backend of an API and implement a wrapper to verify the signature of requests sent from APIG (API Management).

- Step 1** Compile an interface that returns **Hello World!** Configure the GET, POST, PUT, and DELETE methods and the `requires_apigateway_signature` wrapper.

```
app = Flask(__name__)

@app.route("/<id>", methods=['GET', 'POST', 'PUT', 'DELETE'])
@requires_apigateway_signature()
def hello(id):
    return "Hello World!"
```

- Step 2** Implement `requires_apigateway_signature` by putting the signature key and secret in a **dict**.

```
def requires_apigateway_signature():
    def wrapper(f):

        secrets = {

            os.getenv('SDK_AK1'): os.getenv('SDK_SK1'),
            os.getenv('SDK_AK2'): os.getenv('SDK_SK2'),

        }

        authorizationPattern = re.compile(
            r'SDK-HMAC-SHA256\s+Access=([\,]+),\s?SignedHeaders=([\,]+),\s?Signature=(\w+)')
        BasicDateFormat = "%Y%m%dT%H%M%SZ"

        @wraps(f)
        def wrapped(*args, **kwargs):
            //Signature verification code
            ...

        return f(*args, **kwargs)
```

```

return wrapped
return wrapper

```

- Step 3** Use a regular expression to parse the **Authorization** header. The key and signedHeaders are obtained. The wrapped function is used for signature verification.

```

if "authorization" not in request.headers:
    return 'Authorization not found.', 401
authorization = request.headers["authorization"]
m = authorizationPattern.match(authorization)
if m is None:
    return 'Authorization format incorrect.', 401
signingKey = m.group(1)
signedHeaders = m.group(2).split(";")

```

For example, for **Authorization** header:

```

SDK-HMAC-SHA256 Access=signature_key1, SignedHeaders=host;x-sdk-date,
Signature=e11adf65a20d1b82c25419b5*****8d0ba12fed1ceb13ed00

```

The parsing result is as follows:

```

signingKey=signature_key1
signedHeaders=host;x-sdk-date

```

- Step 4** Find **secret** based on **key**. If **key** does not exist, the authentication failed.

```

if signingKey not in secrets:
    return 'Signing key not found.', 401
signingSecret = secrets[signingKey]

```

- Step 5** Create an `HttpRequest`, and add the method, URL, query, and signedHeaders headers to the request. Determine whether the body needs to be set.

The body is read if there is no **x-sdk-content-sha256** header with value **UNSIGNED-PAYLOAD**.

```

r = signer.HttpRequest()
r.method = request.method
r.uri = request.path
r.query = {}
for k in request.query_string.decode('utf-8').split('&'):
    spl = k.split("=", 1)
    if len(spl) < 2:
        r.query[spl[0]] = ""
    else:
        r.query[spl[0]] = spl[1]
r.headers = {}
needbody = True
dateHeader = None
for k in signedHeaders:
    if k not in request.headers:
        return 'Signed header ' + k + ' not found', 401
    v = request.headers[k]
    if k.lower() == 'x-sdk-content-sha256' and v == 'UNSIGNED-PAYLOAD':
        needbody = False
    if k.lower() == 'x-sdk-date':
        dateHeader = v
    r.headers[k] = v
if needbody:
    r.body = request.get_data()

```

- Step 6** Check whether the signature has expired. Obtain the time from the **X-Sdk-Date** header, and check whether the difference between this time and the server time is within 15 minutes. If **signedHeaders** does not contain **X-Sdk-Date**, the authentication failed.

```

if dateHeader is None:
    return 'Header x-sdk-date not found.', 401

```

```
t = datetime.strptime(dateHeader, BasicDateFormat)
if abs(t - datetime.utcnow()) > timedelta(minutes=15):
    return 'Signature expired.', 401
```

Step 7 Invoke the **verify** method to verify the signature of the request, and check whether the verification is successful.

```
sig = signer.Signer()
sig.Key = signingKey
sig.Secret = signingSecret
if not sig.Verify(r, m.group(3)):
    return 'Verify authorization failed.', 401
```

Step 8 Run the server to verify the code. The following example uses the [HTML signature tool](#) in the JavaScript SDK to generate a signature.

Set the parameters according to the following figure, and click **Send request**. Copy the generated curl command, execute it in the CLI, and check whether the server returns **200**.

If an incorrect key or secret is used, the server returns **401**, which means authentication failure.

Apigateway Signature Test

Key
signature_key1

Secret
signature_secret1

Method: POST | Scheme: http | Host: localhost:8080 | Url: /test

Query
{"xxx": "yyy"}

Headers
{"aaa": "bbb"}

Body
dsfasdf=1

Buttons: Debug, Send request

```
curl -X POST "http://localhost:8080/test?xxx=yyy" -H "aaa: bbb" -H "X-Sdk-Date: 20190307T122402Z" -H "host: localhost:8080" -H "Authorization: SDK-HMAC-SHA256 Access=signatur
```

----End

4.4 C#

Scenarios

To use C# to sign backend requests, obtain the C# SDK, import the project, and verify the backend signature by referring to the example provided in this section.

Constraints

Signature information is added to requests sent to access the backend of an API only after a signature key is bound to the API.

Preparing the Environment

- You have obtained the signature key and secret. For details, see [Pre-signature Preparations](#).
- You have created a signature key on the APIG console and bound it to the API to be called. For more information, see section "Configuring Signature Verification for Backend Services" in the *API Gateway User Guide*.
- On the APIG console, choose **Help Center** > **Using SDKs**, and download the SDK of the desired language.
- You have installed Visual Studio 2019 version 16.8.4 or a later version. If not, download it from the [official Visual Studio website](#) and install it.

Opening a Project

Double-click **csharp.sln** in the SDK package to open the project. The project contains the following:

- **apigateway-signature**: Shared library that implements the signature algorithm. It can be used in the .Net Framework and .Net Core projects.
- **backend-signature**: Example of a backend signature. Modify the parameters as required. For details about the sample code, see [Backend Signature Verification Example](#).
- **sdk-request**: Example of invoking the signature algorithm.

Backend Signature Verification Example

This example demonstrates how to build an ASP.NET Core-based server as the backend of an API and implement an `IAuthorizationFilter` to verify the signature of requests sent from APIG (API Management).

- Step 1** Write a controller that provides the GET, POST, PUT, and DELETE interfaces, and add the **ApigatewaySignatureFilter** attribute.

```
// ValuesController.cs
namespace backend_signature.Controllers
{
    [Route("api/[controller]")]
    [ApiController]
    [ApigatewaySignatureFilter]
    public class ValuesController : ControllerBase
```

```
{
    // GET api/values
    [HttpGet]
    public ActionResult<IEnumerable<string>> Get()
    {
        return new string[] { "value1", "value2" };
    }

    // POST api/values
    [HttpPost]
    public void Post([FromBody] string value)
    {
    }

    // PUT api/values/5
    [HttpPut("{id}")]
    public void Put(int id, [FromBody] string value)
    {
    }

    // DELETE api/values/5
    [HttpDelete("{id}")]
    public void Delete(int id)
    {
    }
}
```

Step 2 Implement **ApigatewaySignatureFilter** by putting the signature key and secret in a **Dictionary**.

```
// ApigatewaySignatureFilter.cs
namespace backend_signature.Filters
{
    public class ApigatewaySignatureFilter : Attribute, IAuthorizationFilter
    {
        private Dictionary<string, string> secrets = new Dictionary<string, string>
        {
            {"signature_key1", "signature_secret1" },
            {"signature_key2", "signature_secret2" },

            {Environment.GetEnvironmentVariable("SDK_AK1"),
            Environment.GetEnvironmentVariable("SDK_SK1" )},
            {Environment.GetEnvironmentVariable("SDK_AK2"),
            Environment.GetEnvironmentVariable("SDK_SK2" )},
        };

        public void OnAuthorization(AuthorizationFilterContext context) {
            //Signature verification code
            ...
        }
    }
}
```

Step 3 Use a regular expression to parse the **Authorization** header. The key and signedHeaders are obtained. The OnAuthorization function is used for signature verification.

```
private Regex authorizationPattern = new Regex("SDK-HMAC-SHA256\\s+Access=([^,]+),\\s?SignedHeaders=([^,]+),\\s?Signature=(\\w+)");
...
string authorization = request.Headers["Authorization"];
if (authorization == null)
{
    context.Result = new UnauthorizedResult();
    return;
}
```

```
}
var matches = authorizationPattern.Matches(authorization);
if (matches.Count == 0)
{
    context.Result = new UnauthorizedResult();
    return;
}
var groups = matches[0].Groups;
string key = groups[1].Value;
string[] signedHeaders = groups[2].Value.Split(';');
```

For example, for **Authorization** header:

```
SDK-HMAC-SHA256 Access=signature_key1, SignedHeaders=host;x-sdk-date,
Signature=e11adf65a20d1b82c25419b5*****8d0ba12fed1ceb13ed00
```

The parsing result is as follows:

```
signingKey=signature_key1
signedHeaders=host;x-sdk-date
```

Step 4 Find **secret** based on **key**. If **key** does not exist, the authentication failed.

```
if (!secrets.ContainsKey(key))
{
    context.Result = new UnauthorizedResult();
    return;
}
string secret = secrets[key];
```

Step 5 Create an `HttpRequest`, and add the method, URL, query, and `signedHeaders` headers to the request. Determine whether the body needs to be set.

The body is read if there is no **x-sdk-content-sha256** header with value **UNSIGNED-PAYLOAD**.

```
HttpRequest sdkRequest = new HttpRequest();
sdkRequest.method = request.Method;
sdkRequest.host = request.Host.Value;
sdkRequest.uri = request.Path;
Dictionary<string, string> query = new Dictionary<string, string>();
foreach (var pair in request.Query)
{
    query[pair.Key] = pair.Value;
}
sdkRequest.query = query;
WebHeaderCollection headers = new WebHeaderCollection();
string dateHeader = null;
bool needBody = true;
foreach (var h in signedHeaders)
{
    var value = request.Headers[h];
    headers[h] = value;
    if (h.ToLower() == "x-sdk-date")
    {
        dateHeader = value;
    }
    if (h.ToLower() == "x-sdk-content-sha256" && value == "UNSIGNED-PAYLOAD")
    {
        needBody = false;
    }
}
sdkRequest.headers = headers;
if (needBody)
{
    request.EnableRewind();
    using (MemoryStream ms = new MemoryStream())
    {
        request.Body.CopyTo(ms);
        sdkRequest.body = Encoding.UTF8.GetString(ms.ToArray());
    }
}
```

```
    }  
    request.Body.Position = 0;  
}
```

- Step 6** Check whether the signature has expired. Obtain the time from the **X-Sdk-Date** header, and check whether the difference between this time and the server time is within 15 minutes. If **signedHeaders** does not contain **X-Sdk-Date**, the authentication failed.

```
private const string BasicDateFormat = "yyyyMMddTHHmssZ";  
  
...  
  
if(dateHeader == null)  
{  
    context.Result = new UnauthorizedResult();  
    return;  
}  
DateTime t = DateTime.ParseExact(dateHeader, BasicDateFormat, CultureInfo.CurrentCulture);  
if (Math.Abs((t - DateTime.Now).Minutes) > 15)  
{  
    context.Result = new UnauthorizedResult();  
    return;  
}
```

- Step 7** Invoke the **verify** method to verify the signature of the request, and check whether the verification is successful.

```
Signer signer = new Signer();  
signer.Key = key;  
signer.Secret = secret;  
if (!signer.Verify(sdkRequest, groups[3].Value))  
{  
    context.Result = new UnauthorizedResult();  
}
```

- Step 8** Run the server to verify the code. The following example uses the **HTML signature tool** in the JavaScript SDK to generate a signature.

Set the parameters according to the following figure, and click **Send request**. Copy the generated curl command, execute it in the CLI, and check whether the server returns **200**.

If an incorrect key or secret is used, the server returns **401**, which means authentication failure.

Apigateway Signature Test

Key

Secret

Method Scheme Host Url

Query

Headers

Body


```
curl -X POST "http://localhost:8080/test?xxx=yyy" -H "aaa: bbb" -H "X-Sdk-Date: 20190307T122402Z" -H "host: localhost:8080" -H "Authorization: SDK-HMAC-SHA256 Access=signatur
```

----End

5 Change History

Table 5-1 Change history

| Date | Description |
|------------|---|
| 2023-12-19 | This issue is the first official release. |