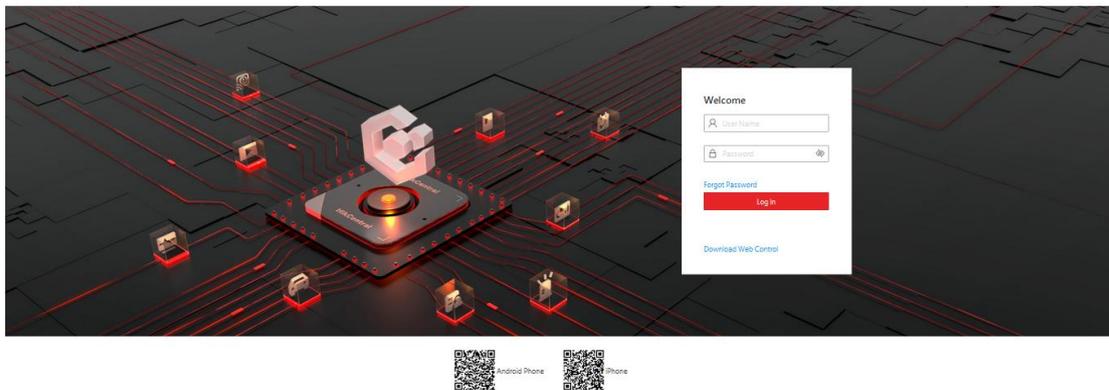
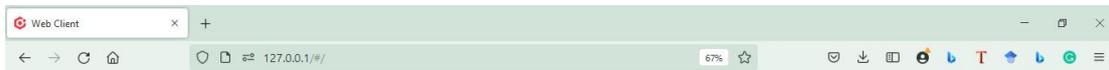


How to install and Configure Open API

OpenAPI Installation

1. The prerequisite for using OpenAPI is to install HCP, and the HCP version must be at least 1.5.
2. OpenAPI is only available for HCP 1.5 and above, and it is called OpenSDK below 1.5 , with different architectures and different protocols.

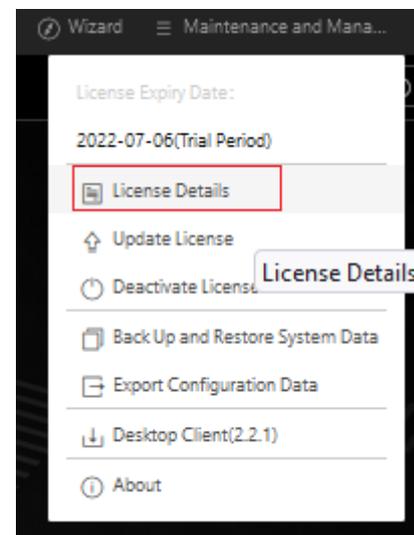
Name	Date modified	Type	Size
HikCentral-Professional_V2.2.1.202205121837_Win_x64_Installer.exe	6/5/2022 10:09 PM	Application	1,200,652 KB
HikCentral Professional_OpenAPI_V2.2.1.202204140135_Win_x64_Installer.exe	5/31/2022 12:16 PM	Application	569,458 KB



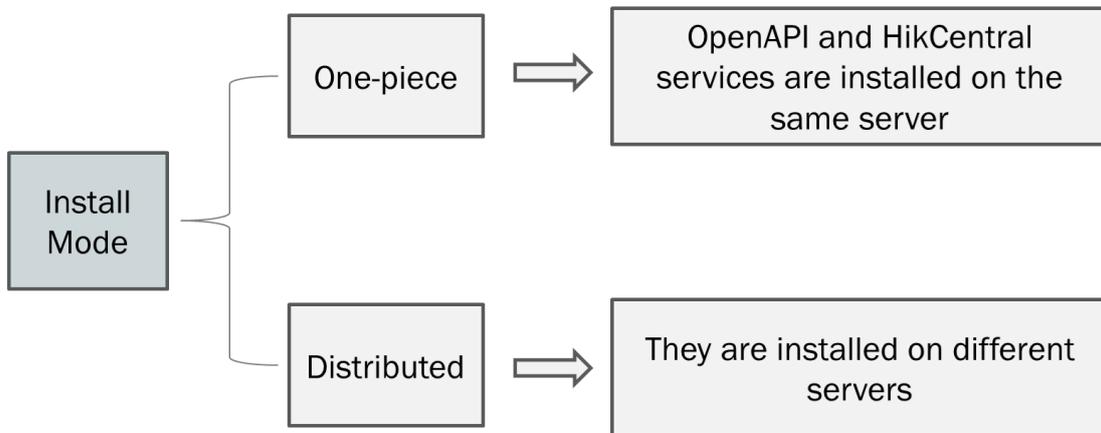
3. Before installing OpenAPI, make sure that "Third-Party Integration" in the license item of HCP has been enabled. That is, the applied license must include the three-party integration function.

License Details

License Details		License List	License Expiry Date : 2022-07-06(Tr...
Authorization Details		Details	
Person Feature Analysis	Enabled		
Pathway Analysis Group	Enabled		
Third-Party Integration	Enabled		
Archive Search	Enabled		
Visual Tracking	Enabled		



4. OpenAPI has two installation methods: One-piece installation and distributed installation.
5. If you install to a different computer, you need to configure it on the watchdog



6. In the case of distributed installation, the HCP watchdog software (Service Manager) requires system information authentication.

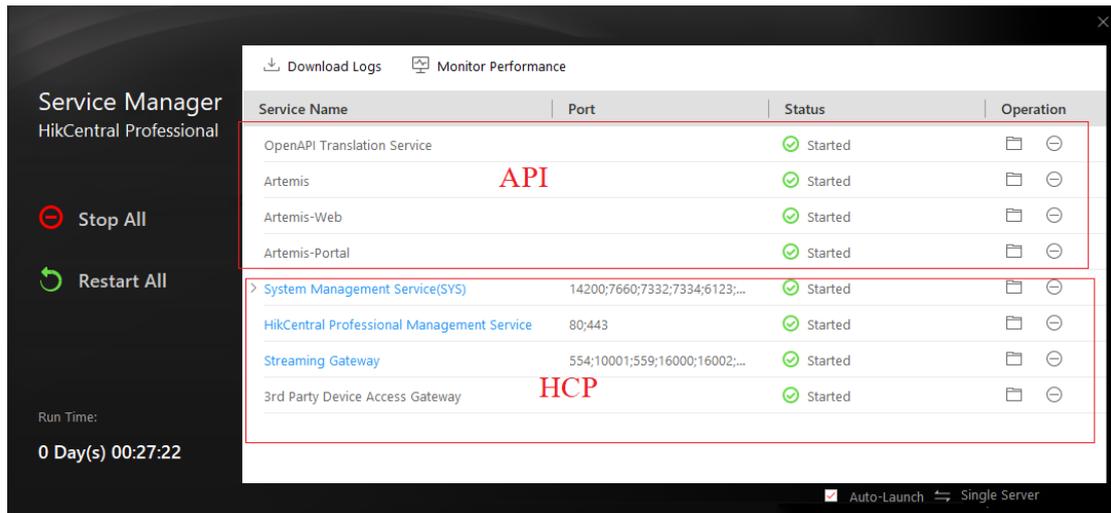
Note; If it is installed on the same computer, this step is not required.

1. Log in to the HikCentral Professional via the Web Client, refer to *HikCentral Professional Web Client User Manual* for details.
2. Click **System** → **Security** → **Service Component Certificate**
3. View and get the service **Certificate** information in the **Certificate between Services in System** field.
4. Run the Service Manager as an administrator.
5. Click **Security Certificate** to open Enter **Certificate** information dialog.
6. Enter the obtained service **Certificate** information in the dialog.
7. Click **OK**

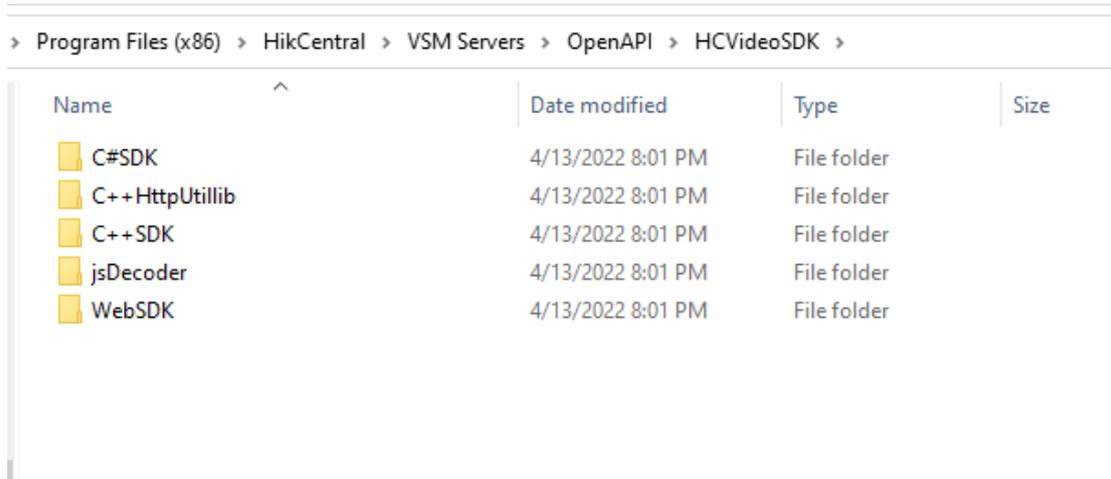
The screenshot shows the 'Service Component Certificate' configuration page. A sidebar on the left lists various system settings, with 'Service Component C...' selected. The main area contains instructions to select a certificate and two sections for certificate generation. The first section, 'Certificate between Services in Sy...', has a dropdown menu set to 'admin Account's Password' and a 'Generate Again' button. Below this, a red box highlights the generated certificate ID 'BB78T48U76i9'. The second section, 'Certificate between System and R...', has an 'Export' button. Below the export button, several fields are displayed: 'Digest Algorithm Name: sha256', 'Secret Key Component: 5E03697F4B194DF6', 'Secret Key Salt Value: 5E03697F4B194DF6', and 'Security Level: 2'.

The screenshot shows the 'Service Manager HikCentral Professional' interface. A yellow warning banner at the top reads: 'Perform security certificate authentication to the server first, or the server cannot work normally'. Below the banner is a 'Download Logs' button. A table lists several services, with an 'Enter Certificate Information' dialog box overlaid on top. The dialog box has a 'Certificate Information' input field and 'OK' and 'Cancel' buttons. The table has columns for 'Service Name', 'Port', and 'Status'. The 'Security Certificate' option in the left sidebar is highlighted with a red box. At the bottom left, there are buttons for 'Stop All' and 'Restart All', and a 'Run Time' display showing '0 Day(s) 00:00:21'.

Service Name	Port	Status
OpenAPI Translat		Started
Artemis		Started
Artemis-Web		Started
Artemis-Portal		Started
HikCentral Profes		Started
BeeAgent	8208	Started
PostgreSQL	5432	Started

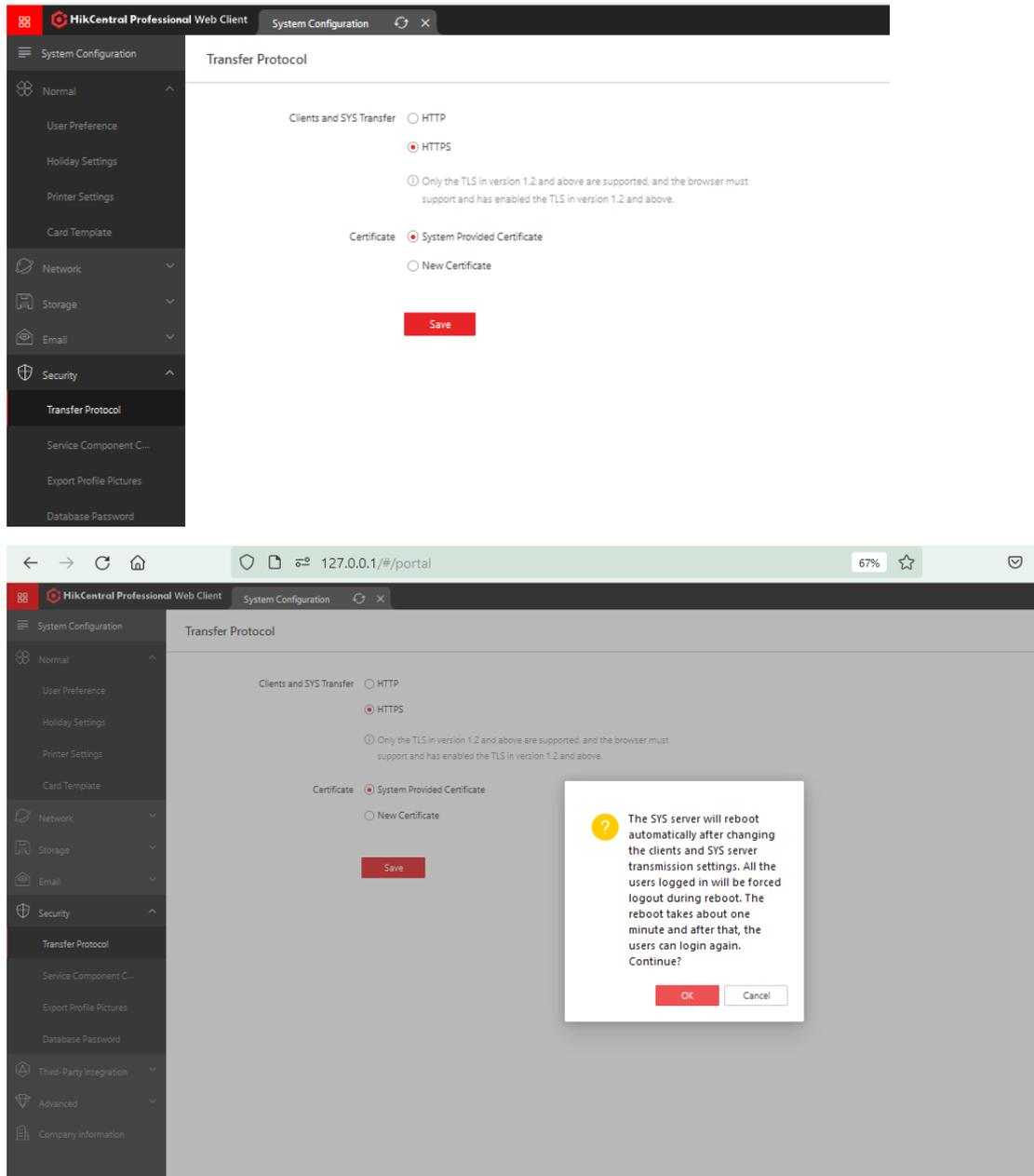


After OpenAPI is installed, you can see the demo of HCVideoSDK in the installation directory. There are 5 versions of the demo in total, and customers can choose reference according to their different development languages

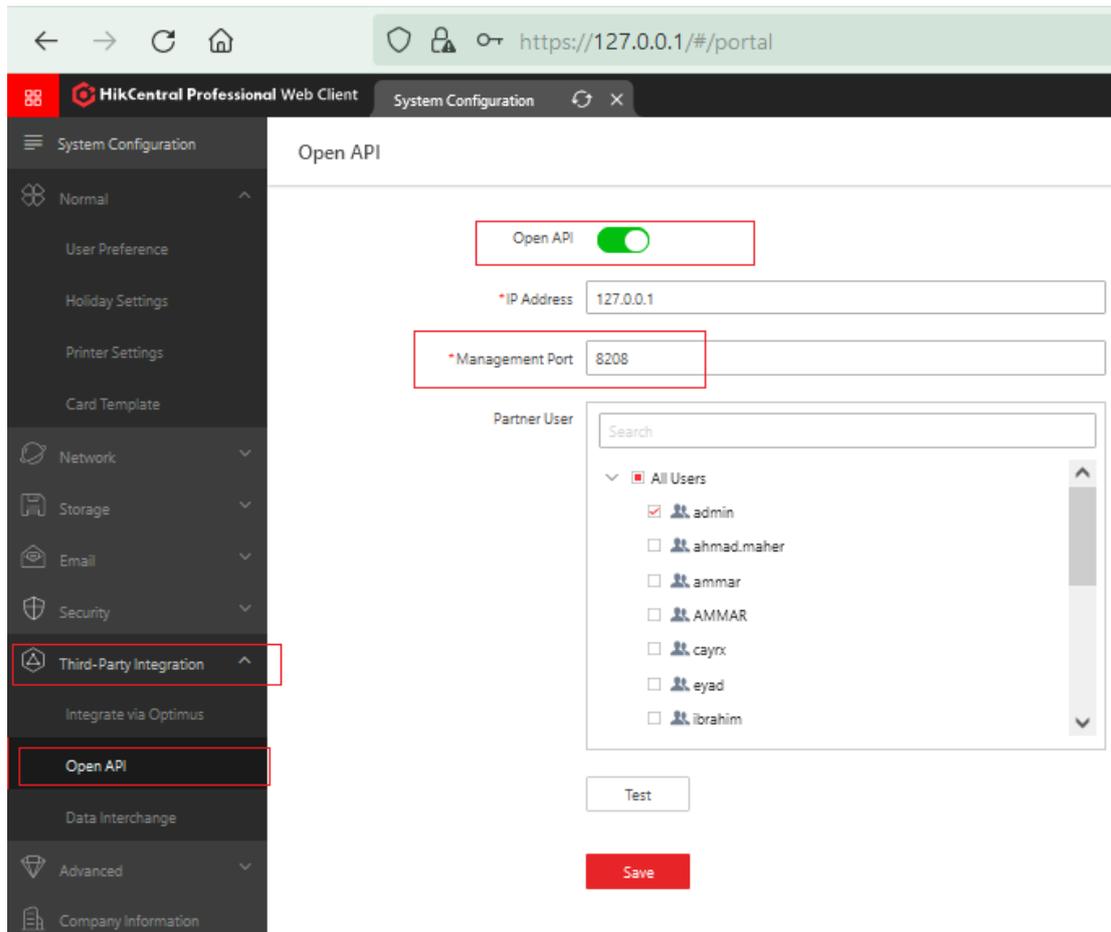


OpenAPI Configuration

1. OpenAPI protocol supports http protocol and https protocol, you can switch the protocol in HCP configuration page, System->Security->Transfer Protocol



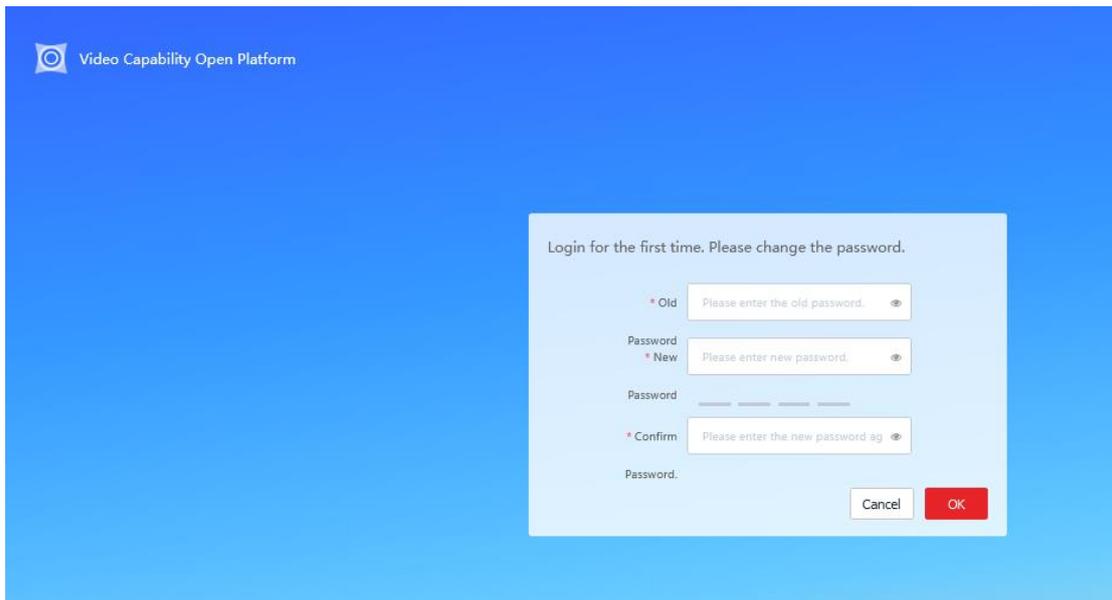
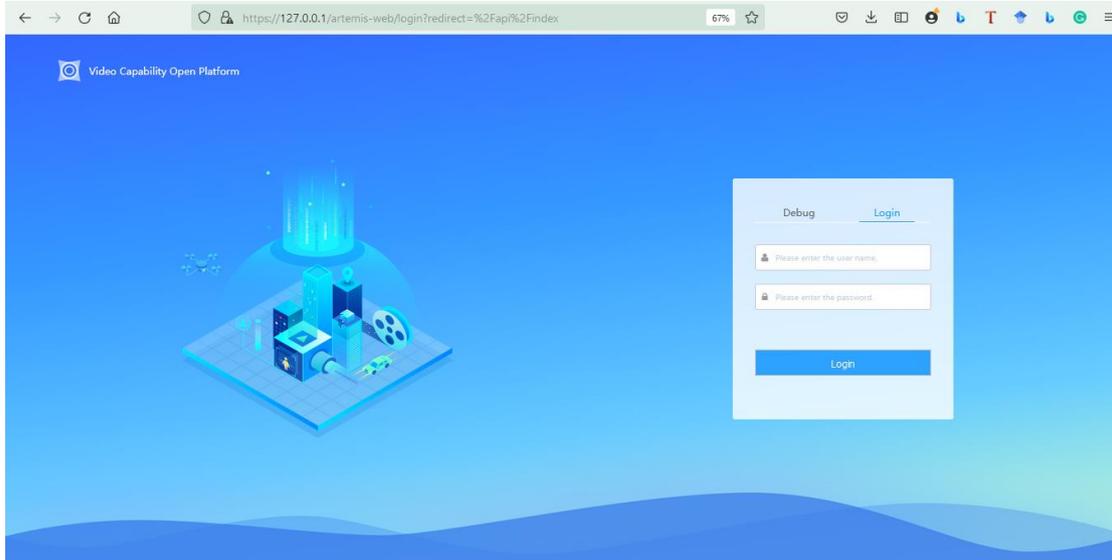
- By default, OpenAPI is closed, we need to open it on HCP. On the HCP configuration page, System->Third Party Integration, turn on the Open API option, and configure the IP and port of OpenAPI. If HCP and OpenAPI are installed on the same computer, the IP is 127.0.0.1. If it is distributed installation, you need to fill in the actual service IP address. The default port is 8208. And you need to configure a user for OpenAPI



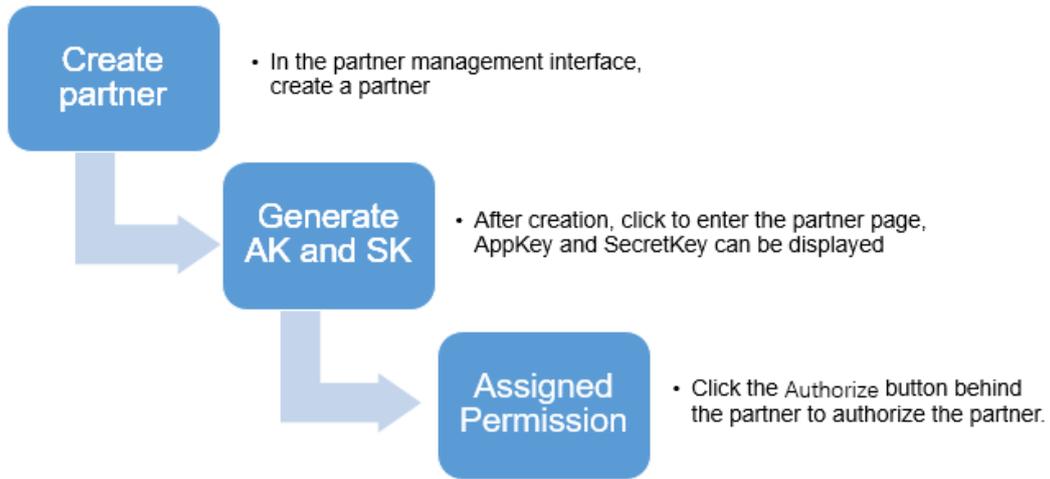
3. After installing HCP and OpenAPI, and after the above series of configurations, you can log in to the OpenAPI service through the web. The default password for the first login is admin@123, the first time you need to change the password. The IP is 127.0.0.1 if on the same computer, and the is the service IP address if you log in on the other computer.

IP: <https://127.0.0.1/artemis-web>

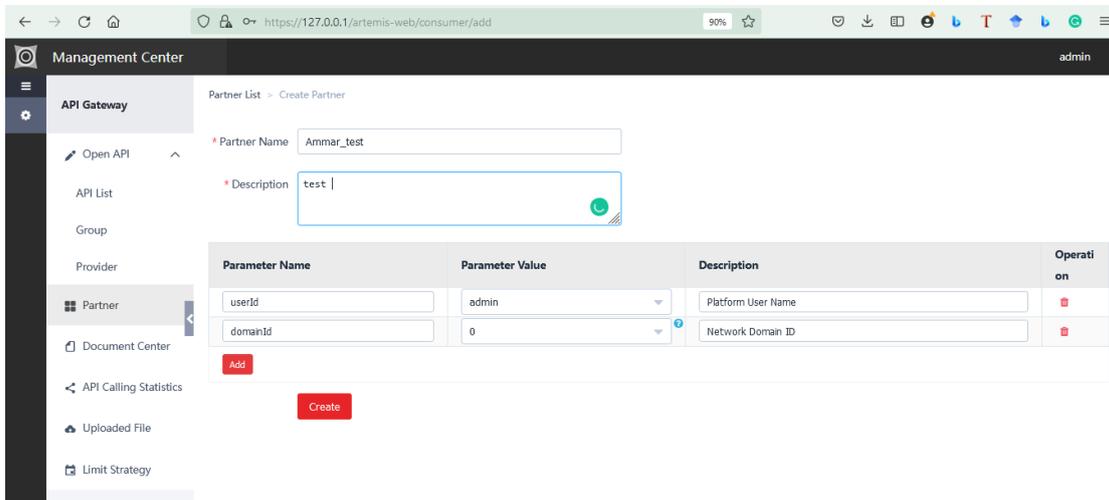
Default password: admin@123



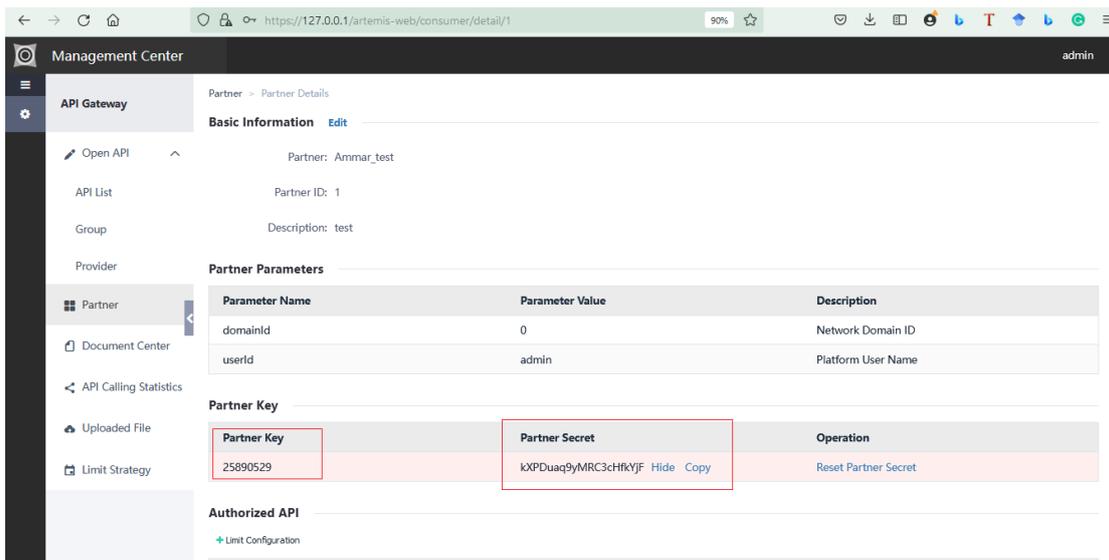
4. Before the user can integrate, the final step is required to configure and create a partner



Create Partner



Get AppKey and AppSecret



Authorize the partner

The screenshot shows the Management Center interface for API Gateway. At the top, there are buttons for '+ Create Partner', 'Delete', 'Batch Import', 'Batch Export', and 'Export All'. Below these are input fields for 'Partner:' and 'AppKey:', each with a 'Please enter the content' placeholder, and 'Reset' and 'Filter' buttons. A table lists partners with columns for 'Partner Name', 'Description', 'Created On', and 'Operation'. One partner, 'Ammar_test', is listed with a description of 'test' and a creation date of '2022-06-19 22:48:02'. The 'Operation' column for this partner has an 'Authorize' button highlighted with a red box, along with 'Call Limit' and 'Delete' options. A pagination bar at the bottom shows 'Total 1', '20 /page', and 'Go to 1'.

The screenshot shows the 'Authorize' dialog for the partner 'Ammar_test'. The title bar reads 'Partner List > Authorize' and 'Authorized Partners: Ammar_test' with 'OK' and 'Cancel' buttons. The dialog is split into two panes. The left pane, titled 'Group-API (87)', contains a list of API categories with checkboxes: Common API, Physical Resources API, Logical Resources API, Video API, Alarm and Event API, ANPR API, Access Control API, Vehicle API, and Mobile Monitoring. The right pane, titled 'Selected (106)', shows a list of selected APIs: Common API, Physical Resources API, Logical Resources API, and Access Control API. A red '>>' button is located between the two panes.