

Alibaba Cloud Smart Access Gateway

SAG-1000 Configuration Guide

Issue: 20190228

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

| Style | Description | Example |
|---|--|--|
|  | This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. |  Danger: Resetting will result in the loss of user configuration data. |
|  | This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. |  Warning: Restarting will cause business interruption. About 10 minutes are required to restore business. |
|  | This indicates warning information, supplementary instructions, and other content that the user must understand. |  Notice: Take the necessary precautions to save exported data containing sensitive information. |
| | This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user. |  Note: You can use Ctrl + A to select all files. |
| > | Multi-level menu cascade. | Settings > Network > Set network type |
| Bold | It is used for buttons, menus, page names, and other UI elements. | Click OK. |
| <code>Courier font</code> | It is used for commands. | Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder. |
| <i>Italics</i> | It is used for parameters and variables. | <code>bae log list --instanceid Instance_ID</code> |
| [] or [a b] | It indicates that it is an optional value, and only one item can be selected. | <code>ipconfig [-all -t]</code> |

| Style | Description | Example |
|--|--|------------------------------------|
| <code>{}</code> or <code>{a b}</code> | It indicates that it is a required value, and only one item can be selected. | <code>swich {stand slave}</code> |

Contents

| | |
|--|----|
| Legal disclaimer..... | I |
| Generic conventions..... | I |
| 1 SAG-1000 overview..... | 1 |
| 2 Configuration guide..... | 6 |
| 3 Web configuration..... | 7 |
| 3.1 Step 1: Configure the local client..... | 7 |
| 3.2 Step 2: Set the password when you log on for the first time..... | 8 |
| 3.3 Step 3: Configure the service IP and the administration IP..... | 9 |
| 3.4 Step 4: Configure the ports and routes..... | 10 |
| 3.5 Step 5: Configure ACL (optional)..... | 11 |
| 4 Activate the device..... | 12 |
| 5 Configure the network connection..... | 13 |
| 6 View routes..... | 15 |

1 SAG-1000 overview

The SAG-1000 Smart Access Gateway is suitable for connecting large branches and headquarters to Alibaba Cloud through one-arm mode.

Specifications

| Property | SAG-1000 |
|-----------------------|---|
| Casing | Metal, matte black, mountable |
| Size | 1 U, halfwidth |
| Operating environment | Indoors |
| Operating temperature | 0°C–45°C |
| Storage temperature | -40°C–70°C |
| Power supply | 12 V DC (Power adapter and power cable included) |
| Power consumption | <60 W |
| Interface | Two SFP optical ports |
| | The number of electric ports varies by manufacturer. Generally, four or six GE/FE RJ45 electric ports are provided. |

Accessories

After receiving the Smart Access Gateway device, check that the following items are provided:

- A Smart Access Gateway device
- A power cable

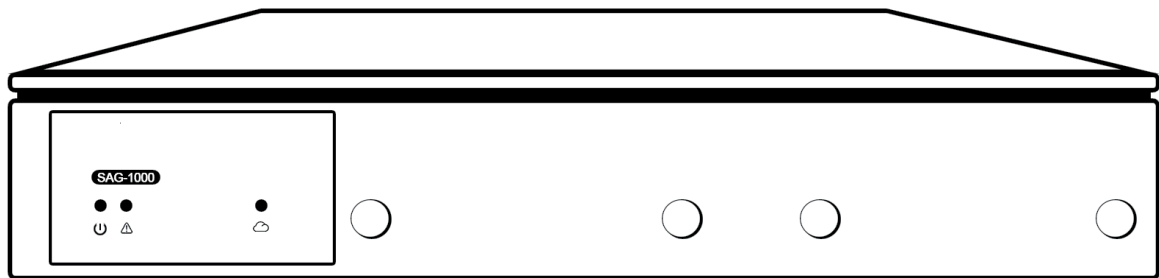


Note:

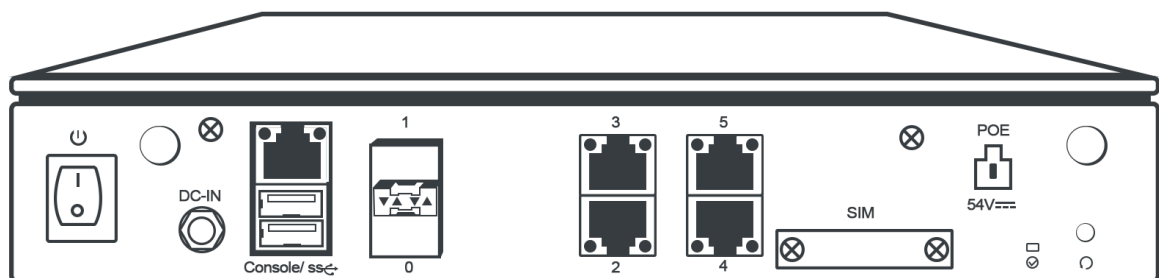
If any item is missing or damaged, contact Alibaba Cloud after-sales personnel. SAG-1000 are delivered from three manufacturers randomly.

Type 1

- Front panel

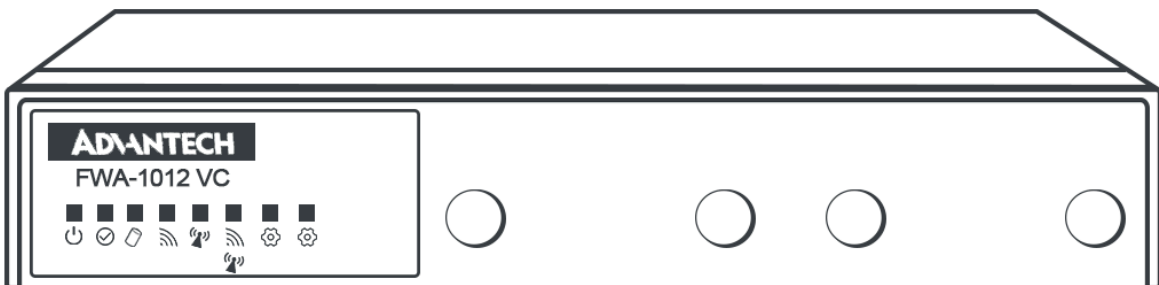


- Rear panel

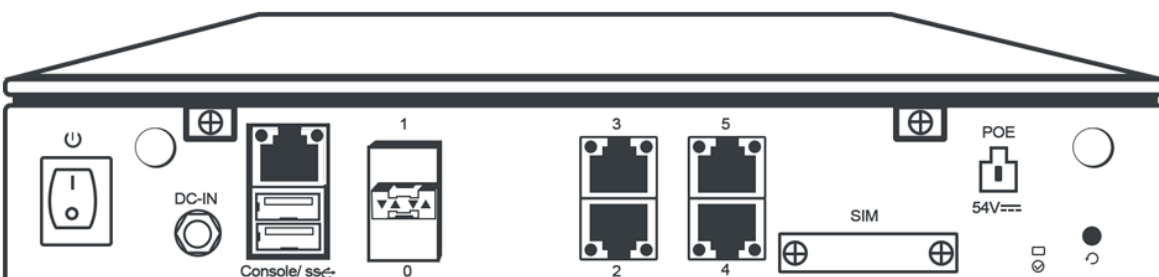


Type 2

- Front panel

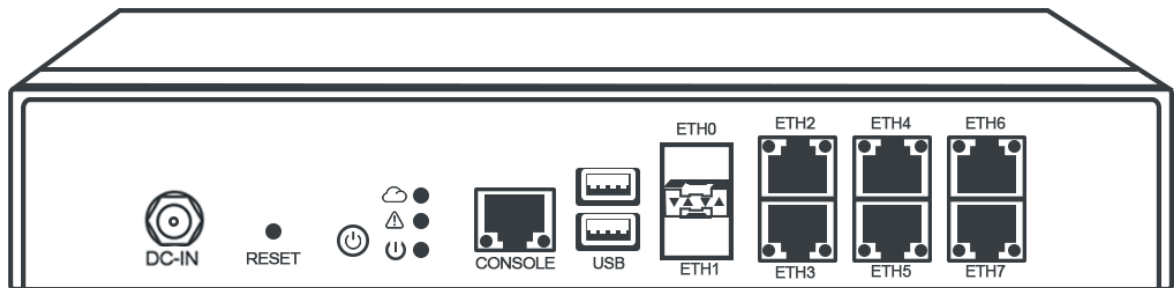


- Rear panel

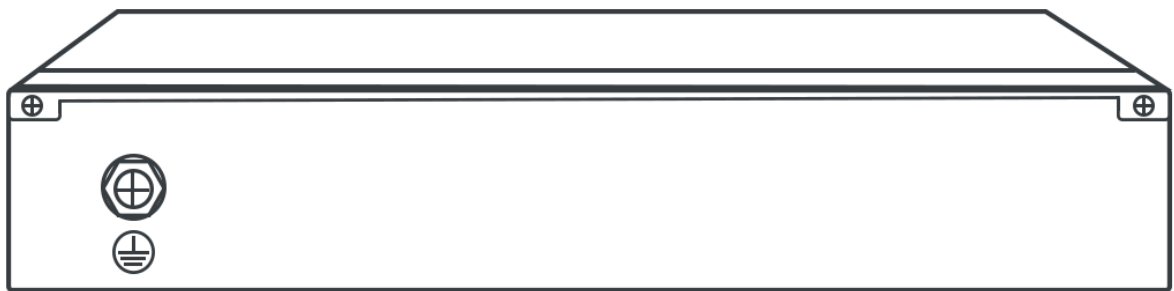


Type 3

- Front panel



- Rear panel



The following is an overview about a Smart Access Gateway device of the Type 1 category. (Types 2 and 3 devices, although different in appearance, possess the same functions as Type 1 devices.)

- Front panel

- LED indicators

Three LED indicators designated for power, alarms, and the cloud connection status.

- Rear panel

- Ports

Two SFP optical ports and four electric ports. Port 2 is the default administration port. Port 2 is the default administration port.



Note:

The default administration IP address of the Smart Access Gateway device is 192.168.0.1.

- **Reset button**

You can reset the Smart Access Gateway to its default configurations by pressing the reset button three times within 10 seconds while the device is powered on.

- **USB port**

You can use a 4G USB drive to access the Internet.

- **Power socket**

Located on the left-hand side of the front panel. The power supply must be 12 V DC.

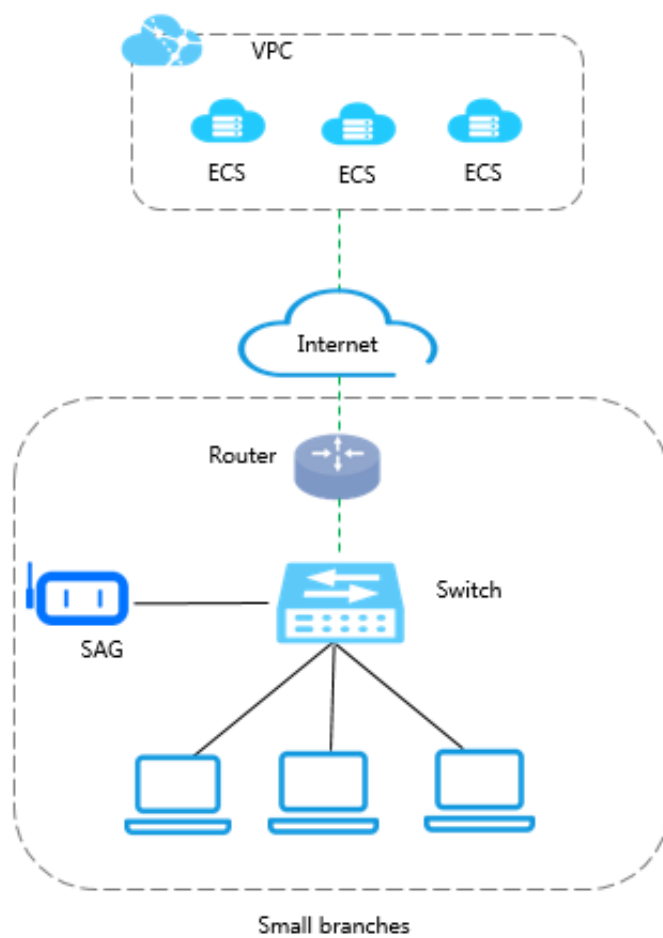


Note:

We recommend that you use the original power cable.

Networking mode

The SAG-1000 Smart Access Gateway device is connected to the switch through one-arm mode. This means it can connect local clients to Alibaba Cloud without changing the current network topology.



2 Configuration guide

After you receive your new gateway device, power on the gateway device to complete the web configurations so that you can start using it.

If you use the SAG-100 device to access Alibaba Cloud, the process is as follows:



When you receive the device after you [Buy a Smart Access Gateway device](#), follow these steps to access Alibaba Cloud through the SAG-100.

- [Step 1: Configure the local client](#)
- [Step 2: Set the password when you log on for the first time](#)
- [Step 3: Configure the service IP and the administration IP](#)
- [Step 4: Configure the ports and routes](#)

3 Web configuration

3.1 Step 1: Configure the local client

Before performing web configurations on the SAG-100, you must configure the static IP address of the local client to access the web configurations.

Windows client configuration

To configure a static IP for a Windows client, follow these steps:

1. Right-click the network connection icon in the lower right corner, then click **Open the Network and Sharing Center**.
2. In the left-side panel, click **Change Adapter Configurations**.
3. Right-click the connected network and then click **Properties**.
4. Double-click the **Internet Protocol Version 4 (TCP/IPv4)** option.
5. Select the **Use the following IP addresses** option and enter the static IP address and subnet mask to use.



Notice:

Ensure that the IP address is in the administration CIDR block of the gateway device (the default administration CIDR block is 192.168.0.0/24) and does not conflict with other IP addresses. For example, 192.168.0.99. You do not need to configure the gateway and DNS.

6. Click **OK**.

Mac client configuration

To configure a static IP for a Mac client, follow these steps:

1. On the desktop, click the **System Preferences** icon, and then click **Network** in the **Internet and Wi-Fi** option. Open **Network and Sharing Center**.
2. Click the connected network and then click **Advanced**.
3. On the **Ethernet configuration** page, click the **TCP/IP** tab page.
4. In the **Configure IPv4** option, select **Manual**, and enter the static IP and subnet mask to use.



Notice:

Ensure that the IP address is in the administrator CIDR block of the gateway device (the default administrator CIDR block is 192.168.0.0/24) and does not conflict with other IP addresses. For example, 192.168.0.99. You do not need to configure the router and DNS.

3.2 Step 2: Set the password when you log on for the first time

When you log on to the Web console for the first time after powering on the Smart Access Gateway, you must set the logon password of the Web console.

Prerequisites

Before logging on to the web configuration page, make sure that:

- The Smart Access Gateway has been started.
- The local client is already configured with a static IP. For more information, see [Step 1: Configure the local client](#).
- The local PC is connected to Port 2 of the Smart Access Gateway through a network cable.

Procedure

1. Enter `192 . 168 . 0 . 1` in your browser.

`192 . 168 . 0 . 1` is the default web configuration address of the gateway device.

2. Enter a logon password.

Keep your logon password securely. If you forget the password, press the reset button once within 10 seconds to reset the password.



Notice:

If you press the reset button at least three times within 10 seconds, all configurations will be cleared.


3. Log on to the web configuration page.

3.3 Step 3: Configure the service IP and the administration IP

After you configure the user name and password and log on to the web configuration page, you can configure the service IP and administration IP of the gateway device. Port 2 is the administration port by default.

Procedure

1. On the web configuration page, click Service IP Configuration.
2. Configure the service IP and administration IP according to the following information, and then click OK.


| Configuration | Description |
|---------------------|---|
| Service IP | <p>The service IP is used to establish the VPN tunnel.</p> <div> Notice: Make sure that the specified service IP can access the Internet. For one-arm mode, you must enable NAT mapping at the Internet egress.</div> |
| Administration port | The administration port is used for local web access. Port 2 is the administration port by default. |
| Administration IP | The administration IP is used for web access of the local client. |
| Whether to isolate | <p>Select whether to isolate the service port from the administration port:</p> <ul style="list-style-type: none">· Yes: This port can only be used as a local web administration port and cannot be used as a service port. <p>In the isolation mode, the service traffic and the administration traffic do not affect each other, so higher security is achieved.</p> <ul style="list-style-type: none">· No: This port is used as both the local web administration port and the service port. |
| Next hop | If you choose to isolate the service port from the administration port, specify the next hop of the administration port. |

3.4 Step 4: Configure the ports and routes

There are six ports on the SAG-1000 device. Port 0 and Port 1 are SFP optical ports, and Ports 2-5 are RJ45 electrical ports. You can configure a static route or OSPF routes for port connection.

Procedure

1. On the Web configuration page, click Port Settings.
2. Configure the ports of the gateway device according to the following information, and then click OK.

| Configuration | Description |
|----------------------------|---|
| Connection method | <p>Choose to access the switch using static or dynamic routing.</p> <div> Notice: When dual-device one-arm mode is used, only dynamic routing is supported.</div> |
| Port | <p>Click the Edit option in the Configuration Information area, enter the IP of the port used for communication and select whether to enable OSPF.</p> <p>Port 2 is the default administrator port.</p> |
| OSPF routing configuration | |
| Area ID | <p>The ID of the area.</p> <p>Make sure that area IDs of Smart Access Gateway 1 and Smart Access Gateway 2 are different.</p> |
| Hello_time | <p>The interval at which hello packets are sent, in seconds.</p> <p>Default value: 3 seconds.</p> |
| dead_time | <p>The dead interval of OSPF neighbor, in seconds. The neighbor relation stops if no hello packet is received during the dead time.</p> <p>Default value: 10 seconds.</p> |
| Authentication method | <p>Select an authentication method.</p> <ul style="list-style-type: none">· Do not authenticate: Do not perform authentication.· Clear Text Authentication: Enter a clear text password.· MD5 Authentication: Use the MD5 method to perform authentication. Enter the MD5 key ID and the MD5 key. |
| Routerid | <p>The ID of the OSPF router. We recommend that you directly use the service IP.</p> |

| Configuration | Description |
|---------------|-----------------------------------|
| Area Type | The area type is NSSA by default. |

3.5 Step 5: Configure ACL (optional)

You can add security group rules to manage the intranet traffic of local branches.

Procedure

1. Log on to the web configuration page of the Smart Access Gateway device.
2. After the WAN port is configured, click Next to configure ACL.
3. Select a rule direction, and then click Add Rule to configure security rules.

| Configuration | Description |
|----------------------|--|
| Rule direction | <ul style="list-style-type: none">· Outbound: Traffic sent from the local branch connected to Smart Access Gateway.· Inbound: Traffic sent to the local branch connected to Smart Access Gateway. |
| Source address | <ul style="list-style-type: none">· Outbound: The private CIDR block of the local branch that initiates the access.· Inbound: The private CIDR block that accesses the local branch. |
| Destination address | <ul style="list-style-type: none">· Outbound: The external destination CIDR block to be accessed.· Inbound: The destination CIDR block of the local branch to access. |
| Source port | The source port range of the transport layer. 0/65535 represents all ports. |
| Protocol type | The transport layer protocol. |
| Destination port | The destination port range of the transport layer. 0/65535 represents all ports. |
| Authorization policy | Select Allow or Deny. |
| Priority | Valid range: 1 ~ 100. The smaller the number, the higher the priority. If the priority of two rules is the same, the rule added earlier takes effect. |

4 Activate the device

After receiving the gateway device, you must activate it.

Procedure



1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, find the target gateway instance.
3. Click Activate in the Actions column.


5 Configure the network connection

After activating the Smart Access Gateway device, you must attach it to a CCN instance and then attach the CCN instance to a CEN instance, so that local branches can be connected to Alibaba Cloud.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, find the target gateway instance.
3. Click Configure Network in the Actions column.
4. Complete network configurations according to the following information.

| Configuration | Description |
|----------------------|--|
| Name/ID | Displays the name and ID of the Smart Access Gateway instance. |
| Private CIDR Block | <p>Configure the private CIDR blocks used by the local gateway device to access Alibaba Cloud. Make sure all private CIDR blocks do not conflict with one another. Click Add Private CIDR Block to add more CIDR blocks. Up to five private CIDR blocks can be added.</p> <div> Note: Configuring a CIDR block with a 32-bit mask is not supported.</div> |
| CCN Instance ID/Name | <p>Select the CCN instance to attach. You can use the default CCN instance or a created CCN instance.</p> <p>CCN is a device access matrix composed of Alibaba Cloud distributed access gateways. After a Smart Access Gateway device is attached to a CCN instance, the gateway device can communicate with other gateway devices attached to the CCN instance.</p> <div> Note: Make sure that the CCN instance and the Smart Access Gateway instance are in the same area.</div> |

| Configuration | Description |
|-------------------|---|
| Bind CEN Instance | <p>Select the CEN instance to attach.</p> <p>After the CCN instance is attached to the CEN instance, all networks (VPCs and VBRs) attached to the CEN instance can communicate with the CCN instance.</p> <div> Note: Make sure that the CCN instance and the CEN instance are in the same area. For more information, see Cloud Connect Network.</div> |

When you no longer need the Smart Access Gateway instance to be attached to a CCN instance, you can detach it from the CCN instance. On the SAG page, click **Unbind** in the actions column of the target gateway instance. After the gateway instance is detached from the CCN instance, local branches connected to the gateway instance cannot access Alibaba Cloud.

6 View routes

After you complete the web configurations and network configurations, you can log on to the web console to view routes.

Procedure

1. Log on to the web configuration page of the Smart Access Gateway device.
2. After you complete the web configurations, the connection status of the device is directly displayed after you log on. You can also click Query Status to view the device status.