Alibaba Cloud
Smart Access Gateway

sag-100wm Configuration Guide

Issue: 20190510

MORE THAN JUST CLOUD | Alibaba Cloud

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**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

1 SAG-100WM overview

The SAG-100WM device is suitable for connecting small branches and outlets to Alibaba Cloud. This device does not require a pre-existing web configuration.

Specifications

Property	SAG-100WM
Operating environment	Indoor environment (no fan provided)
Operating temperature	0℃–45℃
Storage temperature	-40℃–70℃
Power	12 V DC
Power consumption	12 W
Network interface	Two GE/FE RJ45 WAN ports
	Three GE/FE RJ45 LAN ports
Wi-Fi	IEEE 802.11 b/g/n, 2.4 G 150 Mbps, 20 terminals, 100m2 coverage
4G LTE (Mainland China)	LTE FDD: B1, B3, B5, B8
	LTE TDD: B38, B39, B40, B41
	WCDMA: B1, B5, B8
	TD SCDMA: B34, B39
	GSM: B3, B8
	CDMA EVDO/1X: 800M
4G LTE (Outside China)	LTE FDD: B1, B3, B5, B8
	WCDMA: B1, B5, B8
	GSM: B3, B8
USB	USB 2.0, 500ma

Accessories

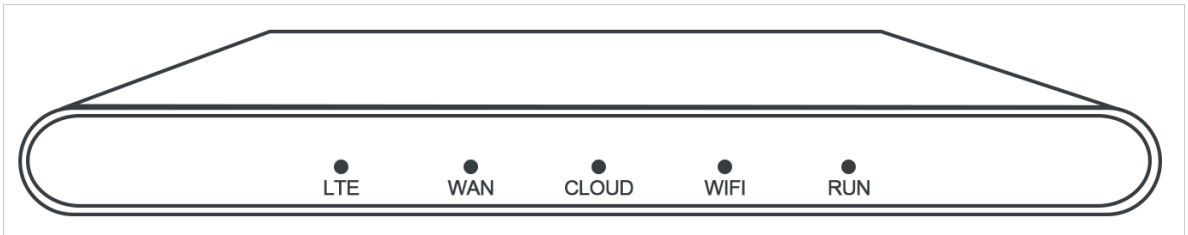
After receiving the Smart Access Gateway device, check that the following items are provided:

- A Smart Access Gateway device
- A power cable

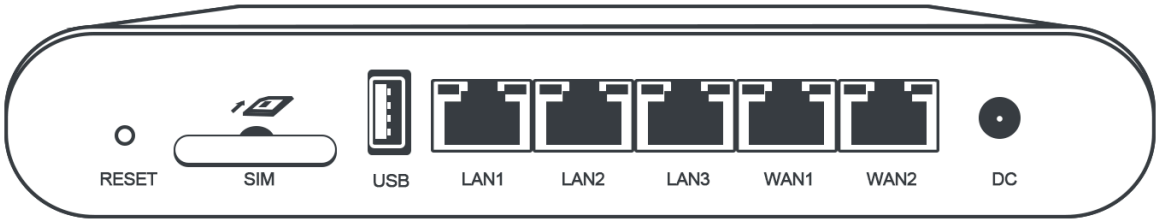
Note:
If any item is missing or damaged, contact Alibaba Cloud after-sales personnel.

Type 1 (size: 180×110×30mm)

- Front panel

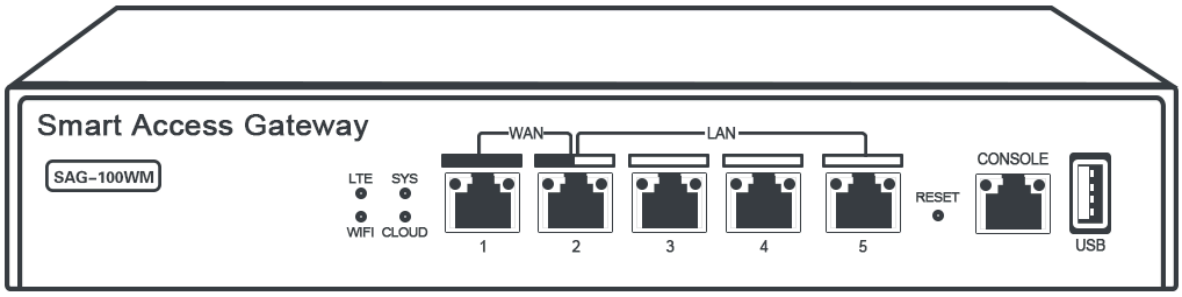


- Real panel



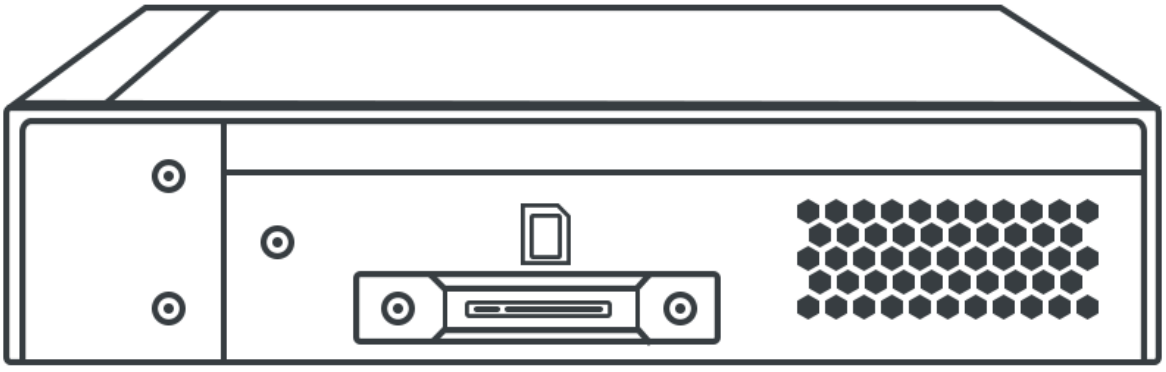
Type 2 (size: 275×175×44.4mm)

- Front panel



./images/39754_en-US.png

- Side panel



- Real panel

Front panel

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

- Front panel: There are five LED indicators on the front panel.

LED indicator	Description
LTE	Indicates whether the device communication is normal: - Flickering: Data transmission is normal. - Off: No card is inserted.
WAN	Indicates the Ethernet status of the device: - On: The device is connected to the Ethernet. - Flickering: Data transmission is normal. - Off: The device is not connected to the Ethernet.
WIFI	Indicates the WIFI connection status of the device: - On: The WLAN is enabled. - Flickering: Data transmission is normal. - Off: The WLAN is not enabled.
RUN	Indicates the status of the Smart Access Gateway device: - On: The device is powered on. - Flickering: Data transmission is normal. - Off: The device is not powered on.
CLOUD	Indicates whether the device is connected to Alibaba Cloud: - On: The device is connected to the CEN. - Off: The device is not connected to the CEN.

- Rear panel: There is one reset button, one SIM slot, one USB port, two WAN ports, three LAN ports, and a power interface on the rear panel of Smart Access Gateway:
  - RESET button

    To restore the Smart Access Gateway to its default configurations, press and hold the reset button for five seconds while the device is powered on.

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

    Insert a SIM card into the slot.
  - USB interface

    Currently, you cannot use a 4G USB to access the Internet.
  - WAN port

    The WAN port is used for accessing the Internet. It supports SNAT forwarding, dynamic IP, static IP, and PPoE.
  - LAN port

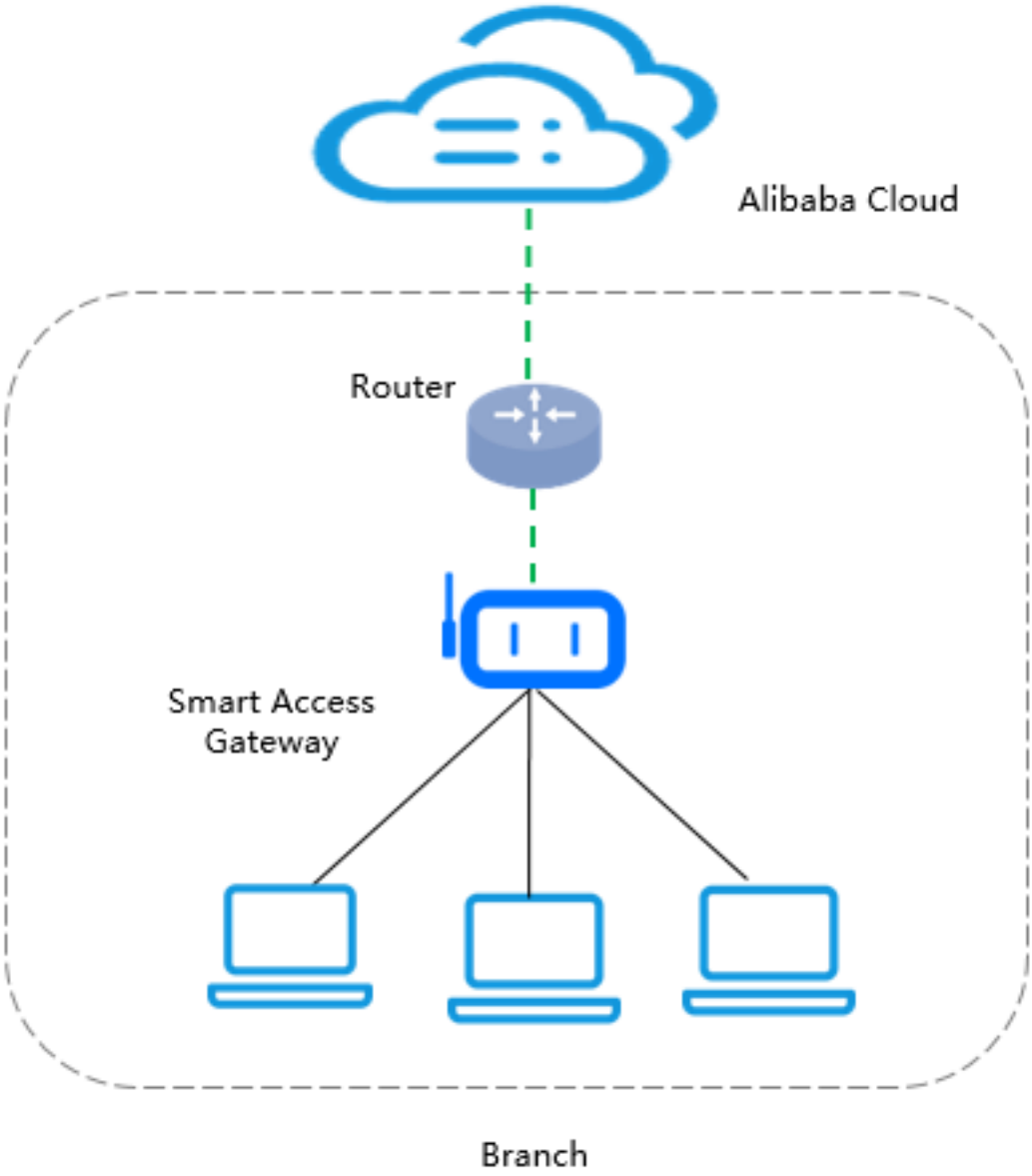
    LAN ports are used for connecting local clients and can be connected to the switch through configured routes.
  - DC power socket

    The power interface is on the far right side of the panel. The power supply must be 12-V DC power supply.

    Note:
    We recommend that you use the original power cable.

Networking mode

The SAG-100WM device connects local clients to Alibaba Cloud through inline mode. The network topology is unchanged for this device.


Alibaba Cloud
Router
Smart Access Gateway
Branch

2 Configuration guide

Before you can use your gateway device, you need to power it on and complete the Web and network configurations.

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

When you receive the device after you *Buy a Smart Access Gateway Hardware*, follow these steps to access Alibaba Cloud through the SAG-100WM device:

1. *Configure the local client*
2. *Activate the device*
3. *Configure the network connection*
4. *Configure access control (optional)*
5. *View the connection status of the device*

3 Web configuration

3.1 Step 1: Configure the local client

Before performing the Web configuration for the SAG-100WM gateway device, you must enable DHCP on local clients so that the clients can connect to the device.

Windows client configuration

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

1. In the lower right corner, right-click the network connection icon, and 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 Automatically Obtain the IP Address and Automatically Obtain the DNS Server Address.
6. Click OK.

Mac client configuration

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

1. On the desktop, click the System Preferences icon, then click Network in the Internet and Wi-Fi option.
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 Use DHCP.

3.2 Step 2: Set the password upon your first logon

After you power on the Smart Access Gateway device for the first time, you need to go to the Web configuration page and set the logon password before you can continue using the device.

Prerequisites

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

- The Smart Access Gateway is powered on.

- The LAN port of the Smart Access Gateway is connected to the local client.
- The local client has DHCP enabled to automatically obtain an IP address.

Procedure

1. Enter the default Web configuration address `192 . 168 . 0 . 1` of the gateway device in your browser.

   Note:

   - If the LAN port uses a static IP address that you configured, log on by using that IP address.
   - If the LAN port uses a dynamic IP address (that is, you have configured CIDR blocks on the console, the WAN port has DHCP enabled, and the cloud status LED turns on when the network cable is connected), log on by using the first IP address in the first CIDR block configured on the console.

     For example, if the first CIDR block specified by you is 192.168.0.0/16, the Web configuration address is 192.168.0.1.
   - If neither the LAN port nor the console is configured, the default address is `192 . 168 . 0 . 1` .
2. Set the logon password.
3. Click OK.

   Keep your logon password confidential. If you forget your password, press and hold the reset button on your device for two seconds and then log on to the Web console to reset the password.

   - To clear all configurations of the gateway device, power the device on and press and hold the reset button for five seconds or until the cloud status LED starts to flicker.
   - To restore the gateway device to its default configurations, first power off the device, and then press and hold the reset key while powering the device back on until the cloud status LED is on, which means the device is restoring.

     The default configurations are fully restored when the cloud LED status goes off.

3.3 Step 3: Configure the WAN port

The WAN port of Smart Access Gateway is used for configuring Internet access and supports dynamic IP addresses, static IP addresses, and PPPoE connections.

Procedure

1. Log on to the web configuration page of the Smart Access Gateway device.
2. Enter the logon password and click OK.
3. Click WAN Port Management. On the WAN Configuration page, configure the WAN port.
4. Select whether to enable SNAT forwarding. If SNAT forwarding is enabled, packets sent to the WAN from the LAN are forwarded by using NAT by default.

   Select a connection mode:

   - Dynamic IP address:

     Select this mode to allow access to the Internet by using an IP address allocated by a DHCP server from a router.
   - Static IP address:

     Select this mode to allow access to the Internet by using a specified IP address . If this mode is selected, you must configure the subnet mask and gateway in addition to the Static IP address.

     Note:
     The specified static IP address and the uplink router device must be in the same CIDR block.
   - PPPoE connection: Select this mode if you want to access the Internet by using dial-up. Afterwards, enter the PPPoE account and password given by the service provider.
5. Click OK.

3.4 Step 4: Configure the LAN ports

This topic describes how to configure the LAN ports. The LAN ports are used for connecting the local clients.

Procedure

1. Log on to the web configuration page of the Smart Access Gateway device.
2. After the WAN port is configured, click LAN Port Management.
3. On the LAN Port Management page, configure the LAN ports.
   - Wi-Fi function

     The LAN ports are used for connecting local clients. If you enable the Wi-Fi function, configure the LAN ports according to the following information.

Configuration	Description
SSID	The name of the LAN. It is used for differentiating networks and can be customized.
SSID broadcast	Wi-Fi devices can search out the Wi-Fi signal of the SSID only after SSID broadcast is enabled.
Wi-Fi Security	If you enable Wi-Fi security, you can set a password. If you disable Wi-Fi security, no password is set and the Wi-Fi can be accessed by any one.
Authentication type	WPA-PSK and WPA2-PSK authentication are supported. Of the two, WPA2-PSK authentication features a higher level of security.
Encryption algorithm	- TKIP is a temporal key integrity protocol and is insecure. We do not recommend using it. - AES is an efficient encryption standard for Wi-Fi authorization.

Configuration	Description
Password	Set the Wi-Fi password.

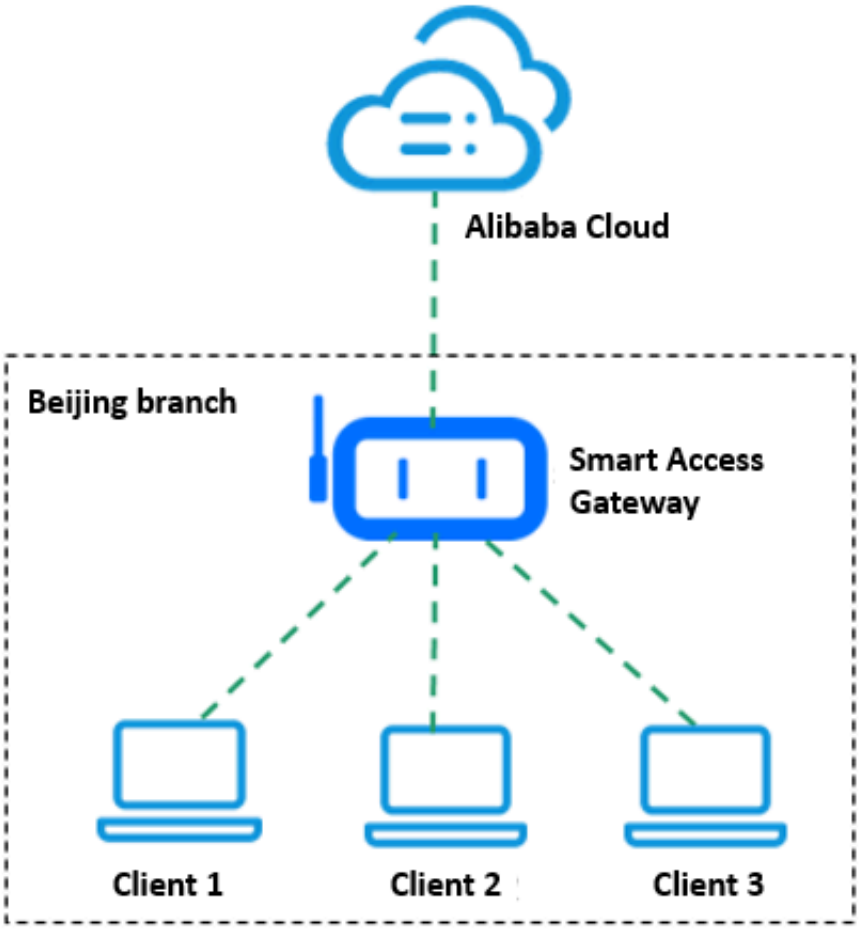
- Wired mode

  The LAN ports are used for connecting local clients. If you use network cables to connect the LAN ports, select a connection mode:

  - Dynamic IP address:

    The IP addresses used by the LAN ports are allocated from the first CIDR block in the network configuration of the console.

    If your local clients directly access Alibaba Cloud by using Smart Access Gateway as shown in the following figure, use the default configuration.



  - Static IP address:

    If the IP address of the local client has been configured by using the switch as shown in the following figure, use a static IP address.

To use a static IP address, you must configure the static IP address and the route:

- Static IP address: The IP address of the gateway device.

  Note:
  Make sure the static IP address does not conflict with any network connected to the gateway device.

- If the LAN ports are connected through static IP, you need to add a route to the Smart Access Gateway and the switch separately.
  - Route configuration of Smart Access Gateway

    On the LAN configuration page, click Route configuration. Add a route. The destination CIDR block of the route is the IP address of the client and the next hop of the route is the IP address of the switch.

    If you have multiple clients, you must configure a route for each client.
  - Route configuration of the switch
    - To connect the switch to VPC, you must add a route in the switch. The destination CIDR block of the route is the CIDR block of the VPC and the next hop is the static IP address of the LAN port.
    - If local branches want to connect with each other by using Smart Access Gateway, add routes to the switch. The destination CIDR block of each route is the IP address of each local branch and the next hop of each route is the static IP address of each LAN port.

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 you activate the Smart Access Gateway device, you must attach it to a Cloud Connect Network (CCN) instance and then attach the CCN instance to a Cloud Enterprise Network (CEN) instance, so that local branches can be connected to Alibaba Cloud.

Procedure

1. Log on to the *Smart Access Gateway console*.
2. In the left-side navigation pane, click Smart Access Gateway Hardware.
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.
CCN Instance ID/ Name	Select the CCN instance to attach. You can use the default CCN instance or a created CCN instance. 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.  Note: Make sure that the CCN instance and the Smart Access Gateway instance are in the same area.

Configuration	Description
Private CIDR Block	Configure the CIDR blocks used by the local gateway device to access Alibaba Cloud. Make sure all CIDR blocks do not conflict with one another. Click Add Private CIDR Block to add more CIDR blocks. You can add up to five CIDR blocks. The LAN port configuration of the local gateway device determines which private IP address is used: · If the LAN port of the Smart Access Gateway device uses a dynamic IP and DHCP is enabled on the client, the IP address used by the local client is allocated from the first CIDR block specified by you. · If the LAN port of the Smart Access Gateway device uses a static IP, the static IP must be in the specified CIDR block.  Note: · The priviate CIDR block of the Smart Access Gateway instance must belong to the CIDR block of the connected CCN instance. · Configuring a CIDR block with a 32-bit mask is not supported.
Enable SNAT	· Disable SNAT: Networks attached to the CCN instance can directly communicate with each other. Make sure that the CIDR blocks of the networks do not conflict with one another. · Enable SNAT: The SNAT function is enabled to hide internal addresses and resolve private address conflict. Local sites can only initiate access and cannot be accessed. - Public IP Address: An IP address in the SNAT CIDR block of the CCN instance. If you leave this option blank, the system automatically allocates an available IP address from the SNAT CIDR block of the CCN instance. - Internal CIDR Block: The private CIDR blocks used by local terminals to access Alibaba Cloud. Make sure that the private CIDR blocks do not conflict with one another.

When you no longer require 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 Configure ACL (optional)

You can choose to add security group rules that allow or deny IP addresses in a security group access to the Internet.

Procedure

1. Log on to the *Smart Access Gateway console*.
2. In the left-side navigation pane, click ACL.
3. On the ACL page, click Create ACL.
4. Configure the name of the ACL, and then return to the ACL page.
5. Click the ID of the ACL instance or Configure Rule in the Actions column.
6. In the left-side navigation pane, click ACL Rule and then click Add ACL Rule to add an ACL rule to the ACL instance.

Configuration	Description
Rule direction	· Outbound: Traffic from the local branch connected to Smart Access Gateway to the external environment. · Inbound: Traffic from the external environment to the local branch connected to Smart Access Gateway.
Authorization policy	Select Allow or Refuse.
Protocol type	The transport layer protocol.
Source address	· Outbound: The CIDR block of the local branch that initiates access. · Inbound: The CIDR block that accesses the local branch.
Source port	The source port range of the transport layer. 0/65535 represents all ports.
Destination address	· Outbound: The external destination CIDR block to be accessed. · Inbound: The destination CIDR block of the local branch to access.
Destination port	The destination port range of the transport layer. 0/65535 represents all ports.

Configuration	Description
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.

7. Click OK.
8. After the ACL rule is configured, click Add Instance in the Actions column to add Smart Access Gateway instances that use the ACL rule.

7 View the connection status of the device

After you complete the Web configurations and network configurations, you can also click back to the Homepage to view the connection status of the device.

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 Homepage to view the device status.**