

Alibaba Cloud Smart Access Gateway

User Guide

Issue: 20190517

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 a 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 Smart Access Gateway Hardware.....	1
1.1 What is a Smart Access Gateway Hardware instance?.....	1
1.2 Activate the SAG device.....	1
1.3 Configure the network.....	2
1.4 Lock an offline device.....	4
1.5 Modify the bandwidth.....	5
1.6 Renew an instance.....	6
1.7 Device-level high availability configurations.....	6
1.8 Link-level high availability configurations.....	7
1.9 Reboot through the console.....	8
1.10 Upgrade the software version.....	8
2 Smart Access Gateway Software.....	10
2.1 What is Smart Access Gateway Software?.....	10
2.2 Configure the network.....	10
2.3 Manage accounts.....	11
2.4 Renew an instance.....	14
3 CCN.....	15
3.1 Cloud Connect Network.....	15
3.2 Create a CCN instance.....	16
3.3 Attach a CCN instance to a CEN instance.....	18
3.4 Cross-account CEN instance authorization.....	18
3.5 Detach a CEN instance.....	19
3.6 Delete a CCN instance.....	20
4 Access control list (ACL).....	21
4.1 What is an access control list?.....	21
4.2 Configure an access control list.....	22
5 Configure a Smart Access Gateway Hardware device.....	24
5.1 Log on to the Web configuration page.....	24
5.2 Web configurations for SAG-100WM devices.....	25
5.3 Web configurations for SAG-1000 devices.....	29

1 Smart Access Gateway Hardware

1.1 What is a Smart Access Gateway Hardware instance?

A Smart Access Gateway instance is the logical mapping of a Smart Access Gateway Hardware (the physical gateway device). You can manage the gateway instance in the console, which is equivalent to operating the Smart Access Gateway device.

After you buy an SAG device on the console, you can view the condition of the SAG device through the instance status. An SAG device can be in any of the following statuses:

Instance status	Instructions
Ordered	The SAG device has been ordered but has not been shipped.
Shipped	The SAG device has been shipped and is awaiting confirmation of receipt.
Ready	The SAG device is in a normal state and can be used.
Not bound	The SAG device is not associated to a CCN instance.
Offline	The SAG device is not connected to the controller.
Locked	The SAG has overdue payments associated with it.

After establishing the network architecture, you can view the network topology on the details page of the instance, as shown in the following figure.

1.2 Activate the SAG device

After receiving the Smart Access Gateway device (SAG device), you must activate it in the console. You can only use the SAG device after activating it.

Context

Billing starts right after the SAG device is activated. For more information, see [Billing](#).



Note:

If the device is not manually activated, by default the system automatically activates the SAG device and billing starts 15 days after the device is received.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Hardware and find the ID of the target gateway instance.
3. Click Activate in the Actions column.



1.3 Configure the network

After you activate the Smart Access Gateway device (SAG device), you must configure the private IP addresses of the local branches and the CCN instance to attach in the console so that local clients can connect 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 and find the ID of 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.

Configuration	Description
Private CIDR Block	<p>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. Up to five CIDR blocks can be added.</p> <p>The LAN port configuration of the local gateway device determines which private IP address is used:</p> <ul style="list-style-type: none">· 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. <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
Enable SNAT	<ul style="list-style-type: none">· 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.<ul style="list-style-type: none">- 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 do not 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.

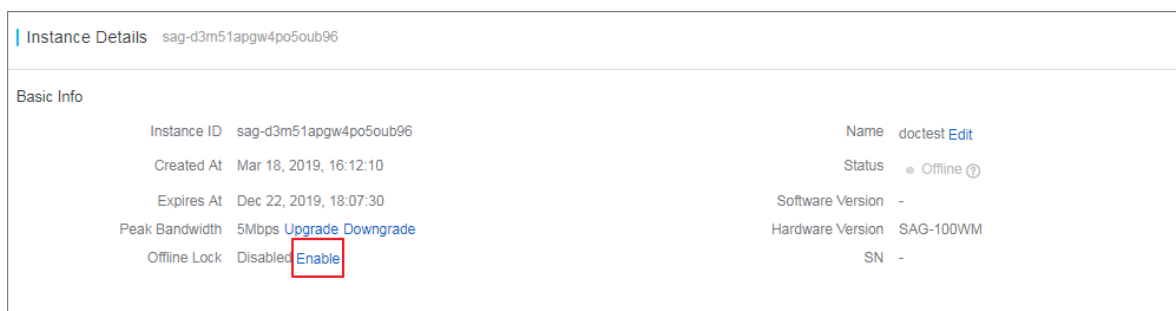
1.4 Lock an offline device

When a Smart Access Gateway device (SAG device) is offline, you can lock the SAG device and then the device cannot be used any more.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click **Smart Access Gateway Hardware** and then click the ID of the target gateway instance.

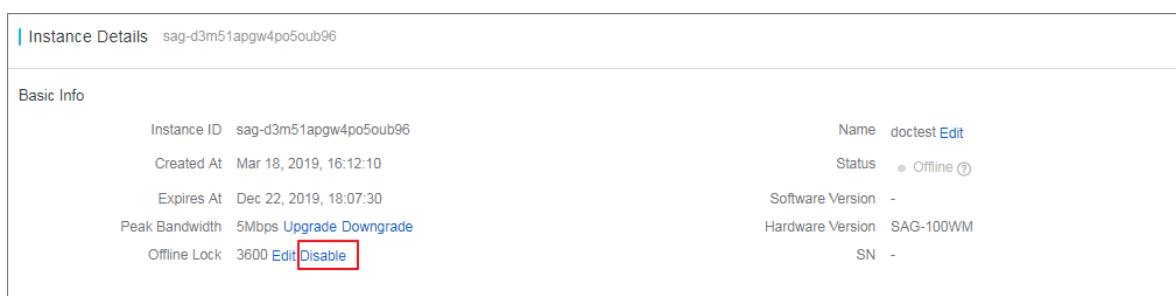
3. On the Instance Details page, click **Enable** next to the Offline Lock configuration .



4. Enter a threshold (in seconds) for the locked status to take effect and click OK.

For example, if 3600 is entered, the SAG device becomes locked after 60 minutes.

When you need to enable the SAG device, click **Disable** next to the Offline Lock configuration. After you click **Disable**, the button changes to **Enable**, indicating that you can use the SAG device as normal.



1.5 Modify the bandwidth

You can modify the bandwidth of the Smart Access Gateway device according to your needs.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Hardware and then click the ID of the target gateway instance.
3. On the Instance Details page, click the Upgrade or Downgrade option configured for Peak Bandwidth.
4. On the Upgrade or Downgrade page, adjust the bandwidth and complete the payment.

1.6 Renew an instance

We recommend that you renew an instance before it expires to avoid interruptions to your services.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Hardware and find the target gateway instance.
3. Click Renew in the Actions column.
4. Select the renewal duration and complete the payment.

1.7 Device-level high availability configurations

If you choose the active/standby mode when you purchase devices, the device can quickly switch to the standby device when the active device fails.

Prerequisites

- Make sure that you select the Active/Standby mode when purchasing the device.

The screenshot displays the 'Basic Configuration' section of the Smart Access Gateway console. The 'Area' is set to 'China Mainland'. The 'Name' field is empty, with a note stating: 'Instance name is optional. An instance name must include 2 to 128 characters starting with an English or Chinese character. Numbers, '.', '_' or '-' can be used as part of an instance name.' The 'Device Spec' is set to 'SAG-100WM', with 'SAG-1000' also visible. Below this, 'sag-100wm' is listed. The 'Peak Bandwidth' is set to '2 Mbps', with a slider showing options from 12Mbps to 50Mbps. The 'Usage' is set to 'Standby', which is highlighted with a red box, and 'Stand-alone' is also visible. Below this, 'Two devices per branch site' is noted. The '购买数量' (Purchase Quantity) is set to '1'. The 'Purchase Plan' section shows 'Sub Period' with options for '9 mont', '1 yr', '2 yr', and '3 yr'.

- Make sure the device configurations are the same for both devices.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Hardware and then click the ID of the target gateway instance.
3. In the High-Availability Configurations area, click Switch to switch to the other device.

Instance Details

sag-ke3kq4evpi8p75ba4w

Basic Info

Instance ID

sag-ke3kq4evpi8p75ba4w

Name

connectNorthAmerica [Edit](#)

Status

Ordered

Software Version

-

Hardware Version

sag-100b(Free Trial)

SN

-

Private CIDR Block

-

Created At

Jun 12, 2018, 00:00:20

Expires At

-

Peak Bandwidth

1Mbps Upgrade Downgrade

Offline Lock

Disabled [Enable](#)

High-Availability Configurations

Device Level

Disabled ?

Active SN

-

Standby SN

-

Channel

Disabled

Main Channel

Backup Channel

Cloud Connect Network Instance

Instance ID

-

Name

-

CEN Instance

-

Created At

-

Description

-



Note:

For SAG-100WM devices, after you switch to the standby device in the console, you must connect the WAN port of the standby SAG device to the Internet.

SAG-100WM devices support manual switching between active and standby devices. SAG-1000 devices support automatic switching between active and standby devices and do not support manual switching between them.

1.8 Link-level high availability configurations

By default, active/standby links are enabled on the SAG-100WM device. The broadband link operates as the active link and the wireless 4G-LTE operates as the standby link. If the active link fails, traffic is automatically distributed to the standby link.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Hardware and then click the ID of the target gateway instance.
3. In the High-Availability Configurations area, view the active/standby links.

Instance Details

sag-ke3kq4evpi8p75ba4w

Basic Info

Instance ID

sag-ke3kq4evpi8p75ba4w

Name

connectNorthAmerica [Edit](#)

Status

Ordered

Software Version

-

Hardware Version

sag-100b(Free Trial)

SN

-

Private CIDR Block

-

Created At

Jun 12, 2018, 00:00:20

Expires At

-

Peak Bandwidth

1Mbps Upgrade Downgrade

Offline Lock

Disabled [Enable](#)

High-Availability Configurations

Device Level

Disabled [?](#)

Active SN

-

Standby SN

-

Channel

Disabled

Main Channel

Backup Channel

Cloud Connect Network Instance

Instance ID

-

Name

-

CEN Instance

-

Created At

-

Description

-

1.9 Reboot through the console

You can reboot a Smart Access Gateway through the Smart Access Gateway console.

Procedure

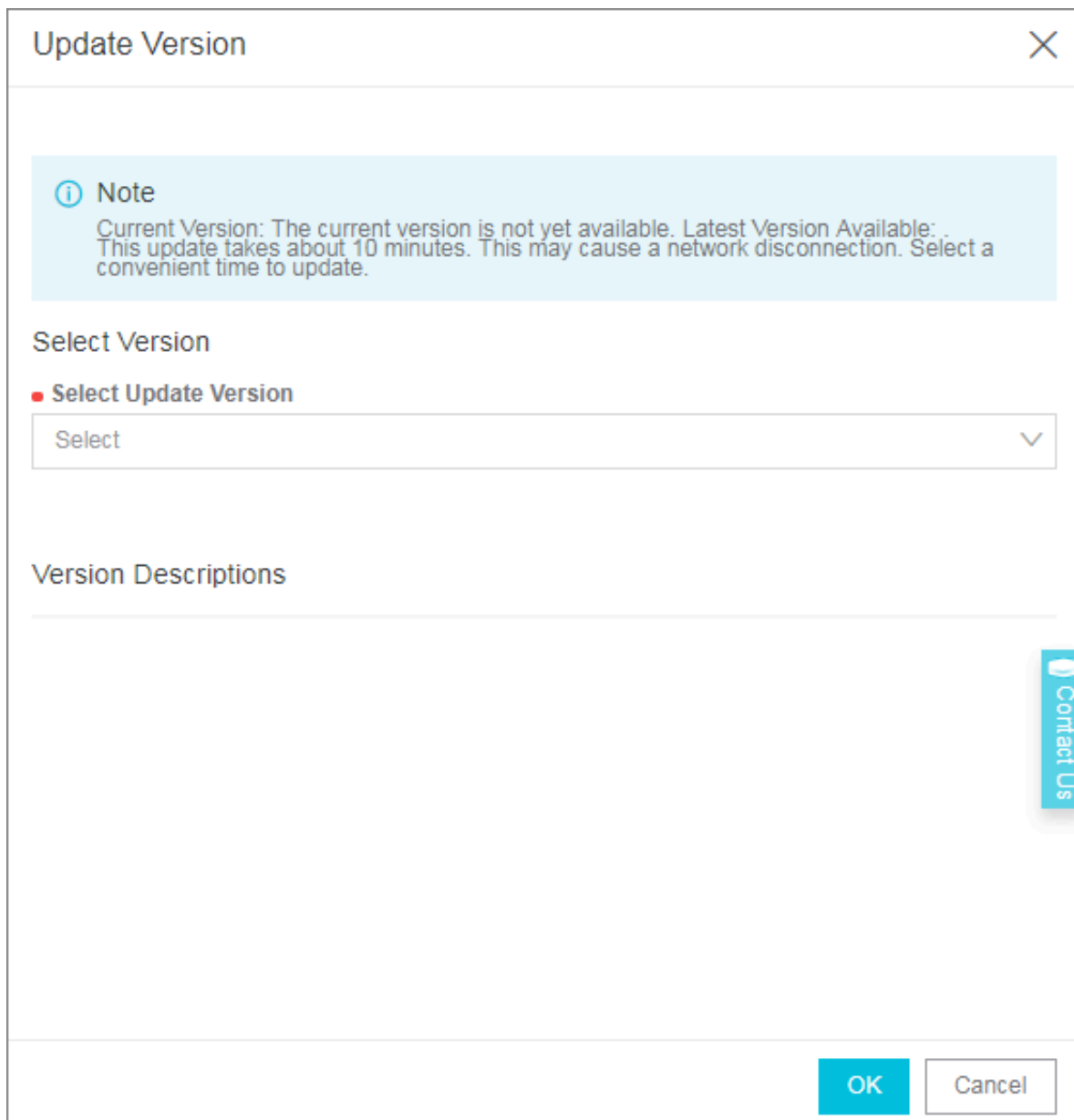
1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Hardware, and then click Reboot in the Actions column of the target gateway instance.
3. In the displayed dialog box, click OK.

1.10 Upgrade the software version

You can upgrade the software version of the Smart Access Gateway device (SAG device) on the Smart Access Gateway console. The upgrade may cause network interruptions. We recommend that you upgrade the software version when the traffic volume is low.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Hardware, and then click the ID of the Smart Access Gateway instance to be upgraded.
3. On the Instance Details page, click Update Version.
4. Select the target version and enter a description of the version.



The screenshot shows a modal dialog titled "Update Version" with a close button (X) in the top right corner. Inside the dialog, there is a light blue informational box with an "i" icon and the text: "Note: Current Version: The current version is not yet available. Latest Version Available: . This update takes about 10 minutes. This may cause a network disconnection. Select a convenient time to update." Below this, the section "Select Version" contains a red bullet point followed by the text "Select Update Version" and a dropdown menu with the word "Select" and a downward arrow. Underneath is a section titled "Version Descriptions" with a horizontal line below it. On the right side of the dialog, there is a vertical blue button labeled "Contact Us". At the bottom right, there are two buttons: "OK" (in a blue box) and "Cancel" (in a white box with a gray border).

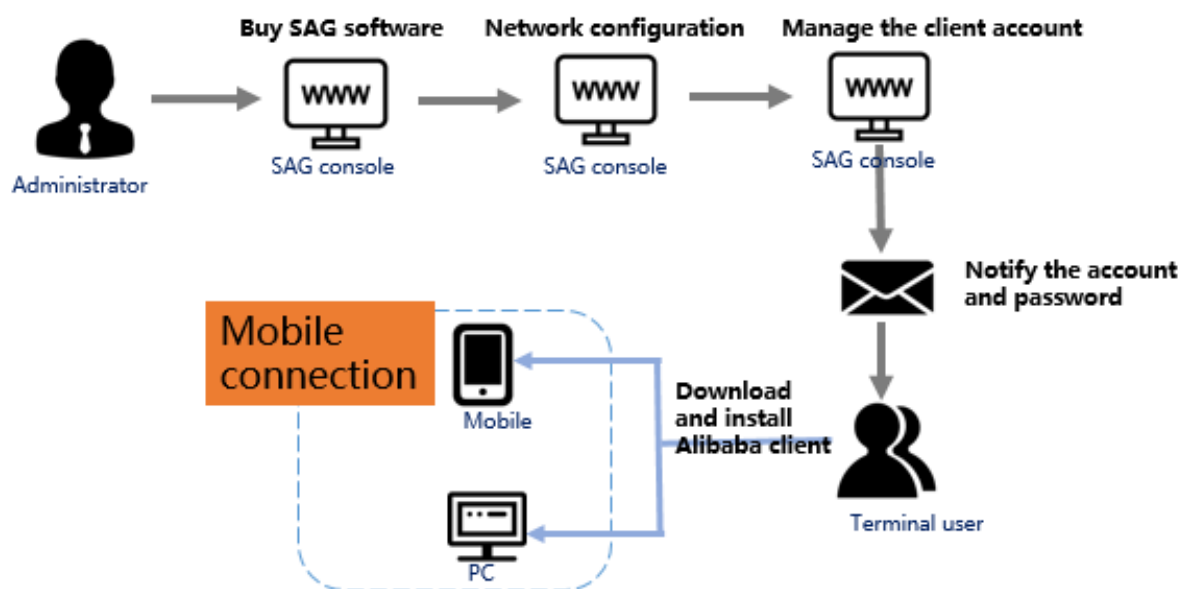
5. Click OK.

2 Smart Access Gateway Software

2.1 What is Smart Access Gateway Software?

Smart Access Gateway (SAG) is an all-in-one solution for connecting local branches to the Alibaba Cloud. By using Smart Access Gateway Software (SAG Software), you can directly connect a terminal (such as PC or mobile phone) to Alibaba Cloud over an encrypted channel through dial-up. SAG Software is suitable for mobile working scenarios and remote O&M.

The following figure shows the implementation process of SAG Software:




2.2 Configure the network

Before you can run the Smart Access Gateway Software (SAG Software) in your environment, you need to configure the network of the target instance.

Procedure

1. Log on to the [SAG console](#).
2. On the Smart Access Gateway Software page, find the target software and click **Configure Network** in the Actions column.

3. Configure the network according to the configuration items described in the following table.

Configuration	Description
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>After a Smart Access Gateway device (SAG device) is attached to a CCN instance, the SAG device can communicate with other SAG 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>
Private CIDR Block	<p>Configure the private CIDR blocks used by the mobile client. Then, the client uses IP addresses allocated from the private CIDR blocks to access Alibaba Cloud. The private CIDR blocks must belong to the private CIDR block of the CCN instance. Make sure all private CIDR blocks do not conflict with one another.</p> <p>Click Add Private CIDR Block to add more CIDR blocks. Up to five private CIDR blocks can be added.</p>

4. Click OK.

2.3 Manage accounts

This topic describes how to create and manage accounts as an administrator.

After completing the network configuration, you can create multiple accounts and distribute them to end users so that clients can access Alibaba Cloud.

Procedure

1. Log on to the [SAG console](#).
2. Click the instance ID of the target Smart Access Gateway Software (SAG Software).
3. In the Client Accounts area of the Smart Access Gateway Software Details page, click Create Client Account.

4. On the Create Client Account page, set the configurations for the accounts to be used by end users to log on to SAG software clients.

- **Username:** Optional. By default, it is an email account. The username must be 2 to 32 characters in length, and can contain letters, numbers, underscores (_), at signs (@), periods (.), and hyphens (-).
- **Email Address:** Required. The email address of the end user used by the administrator to send the newly created account information.

The email address must contain the at sign (@) and must be 2 to 32 characters in length. It can contain letters, numbers, underscores (_), at signs (@), periods (.), and hyphens (-).

- **Whether to use a specified IP address:**
 - If you enable this option, you must specify an IP address for the client. The account will always use the specified IP address to access Alibaba Cloud.



Note:

The IP address specified for the client must be within the private CIDR block of the SAG software.

- If you disable this option, the system automatically allocates an IP address from the private CIDR block of the SAG software to the client each time a connection is established.
- Peak Bandwidth

The available bandwidth range is 1 kbps to 2 Mbps, and the default value is 2 Mbps.

Create Client Account

Username ?

Email Address ?

?

Peak Bandwidth ?

2000 Kbps

After the client account is created, the system automatically sends the SAG instance ID, username, password, and App download method to your email address. Check your email for this information.

Contact Us

OK Cancel

5. Click OK.

After the preceding configurations are set, the end user receives the account information and instructions about how to download the client.

2.4 Renew an instance

We recommend that you renew a Smart Access Gateway instance before its expiration date to avoid interruptions to your services.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway Software and then click the ID of the target gateway instance.
3. Click Renew in the Actions column.
4. Select the renewal duration and complete the payment.

3 CCN

3.1 Cloud Connect Network

Cloud Connect Network (CCN) is another important component of the Smart Access Gateway. It is a device access matrix composed of Alibaba Cloud distributed access gateways. You can add multiple Smart Access Gateway devices to a CCN instance and then bind the CCN instance to a Cloud Enterprise Network (CEN) instance to connect the local branches to the Alibaba Cloud.

You must specify an area when buying a Smart Access Gateway device or creating a CCN instance. Each Smart Access Gateway area corresponds to a country, while a CEN area contains one or more Alibaba Cloud regions. The relationships between CCN areas and CEN areas are shown in the following table.

A CCN instance and a CEN instance can directly communicate with each other and no cross-area bandwidth is required if the CCN instance and the CEN instance are in the same area. For example, to connect a local branch in Hangzhou to a VPC in Shanghai, you just need to bind the CCN instance to which the Smart Access Gateway is bound to the CEN instance where the VPC is located.



Note:

- Currently, Smart Access Gateway is available only in Mainland China.
- Cross-area connection through Smart Access Gateway is not supported.

CCN area	CEN area	Regions in the CEN area
Mainland China	Mainland China	China (Qingdao) China (Beijing) China (Zhangjiakou) China (Shenzhen) China (Hangzhou) China (Shanghai) China (Hohhot)

CCN area	CEN area	Regions in the CEN area
Hong Kong	Asia Pacific	Hong Kong
Singapore		Singapore
Malaysia (Kuala Lumpur)		Malaysia (Kuala Lumpur)
Japan (Tokyo)		Japan (Tokyo)
India (Mumbai)		India (Mumbai)
North America	North America	US (Silicon Valley)
		US (Virginia)
Europe	Europe	Germany (Frankfurt)
Australia	Australia	Sydney


3.2 Create a CCN instance


To connect local branches attached to a Smart Access Gateway device to Alibaba Cloud, you must first create a CCN instance, attach the gateway instance to the CCN instance, and then attach the CCN instance to the CEN instance.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click CCN.
3. Click Create CCN Instance.
4. On the Create CCN Instance page, configure the CCN instance according to the configuration items described in the following table.

Parameter	Description
Name	The name of the CCN instance. It must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). It must begin with a letter.

Parameter	Description
Description	<p>The description of the CCN instance.</p> <p>It must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). It must begin with a letter.</p>
Private CIDR Block	<p>The private CIDR blocks used by the CCN instance to access Alibaba Cloud. Click Add Private CIDR Block to add more. You can click Add Private CIDR Block to add up to CIDR blocks as needed.</p> <div> Note:<ul style="list-style-type: none">• The private CIDR blocks of the CCN instance are the collections of the IP address ranges of attached Smart Access Gateway instances. Make sure that the specified private CIDR blocks do not conflict with the CIDR block of the VPC to connect.• We recommend that you use RFC private CIDR blocks 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. By default, the CIDR block 192.168.0.0/16 is used if you leave the option blank.<p>By default, the mask is /8 to /24 in length. To use other masks, open a ticket.</p></div>

Parameter	Description
SNAT CIDR Block	<p>A CIDR block that belongs to the private CIDR blocks of the CCN instance. The mask is /8 to /30 in length.</p> <div>  Note: You can use the SNAT function to resolve IP address conflicts or hide intranet IP addresses. The SNAT CIDR block is a subset of the private CIDR blocks of the CCN instance. When you configure the SNAT rule, you can use an IP address in the SNAT CIDR block as the public IP address. </div>

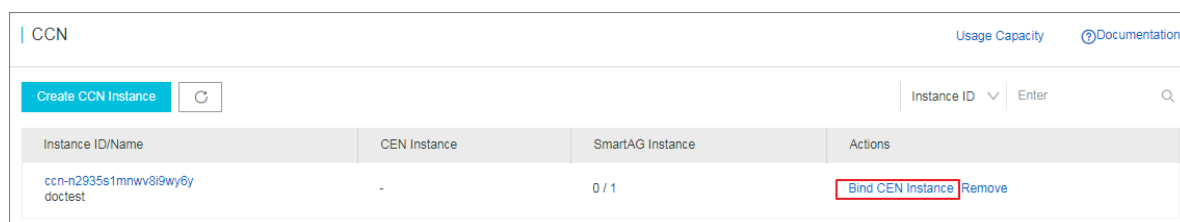
5. Click OK.

3.3 Attach a CCN instance to a CEN instance

After you attach a CCN instance to a CEN instance, local branches connected to the CCN instance can communicate with networks (VPCs and VBRs) in the CEN instance.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click CCN.
3. Select the area of the CCN instance, and click Bind CEN Instance in the Actions column of the target CCN instance.



4. Select the CEN instance to attach and click OK.


3.4 Cross-account CEN instance authorization

If the CEN instance to be attached belongs to another account, authorization by the CEN instance is required.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click CCN.
3. Click the ID of the target CCN instance. On the CEN cross account authorization information tab page, click CEN Cross Account Authorization.
4. On the Attach to CEN page, enter the peer account UID and the peer CEN ID to authorize the peer account to access the CEN instance under this account.

Attach to CEN

 The account that you have authorized can attach your network to their CEN instances and communicate with your network. Use caution when performing this operation.

Peer Account UID

Peer Account CEN ID

OK

Cancel

3.5 Detach a CEN instance

When you do not need gateway devices added to a CCN instance to communicate with networks (VPCs or VBRs) in the CEN instance, you can detach the CEN instance.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click CCN.
3. Select the area where the target CCN instance belongs, and click Unbind CEN Instance in the Actions column.
4. In the displayed dialog box, click OK. After you detach the CEN instance, the CCN instance cannot communicate with resources (VPCs and VBRs) in the CEN.

3.6 Delete a CCN instance

After a CCN instance is deleted, local branches connected to the CCN instance cannot access Alibaba Cloud.

Prerequisites

- If the CCN instance to be deleted is attached to a CEN instance, detach the CCN instance from the CEN instance first. For more information, see [Detach a CEN instance](#).
- If the CCN instance to be deleted is attached to any Smart Access Gateway devices, detach the devices first.

Procedure

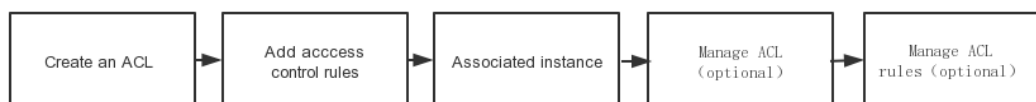
1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click CCN.
3. Select the area where the target CCN instance belongs, and click Remove in the Actions column of the target CCN instance.
4. In the displayed dialog box, click OK.

4 Access control list (ACL)

4.1 What is an access control list?

Smart Access Gateway (SmartAG) provides the access control list (ACL) function in the form of whitelists and blacklists for different SmartAG instances that are applicable to different access requirements.

Access Control List usage process



The process is described as follows:

1. Create an ACL, and set the ACL name.
2. Set access control rule for ACL.
3. Add an SmartAG instance to ACL.
4. You can configure multiple access control rules for an ACL. Add or remove a SmartAG instance.



Note:

A SmartAG instance can only be associated with one ACL, unable to adjust.

5. You can modify or delete existing ACL rules.

Access Control List Configuration Recommendations

The ACL configuration recommendations are as follows:

- ACL is used as a whitelist.
- Open application access rules follow the minimum authorization principle. For example, you can choose to open a specific port (such as port 80).
- All application should not be managed with one ACL, and different layers have different access control requirements.

- Add instances with the same security protection requirements to the same ACL, there is not necessary to set up a separate security group for each instance.

4.2 Configure an access control list

This topic describes how to configure an access control list (ACL) rule for a target Smart Access Gateway instance (SmartAG) to permit or deny access to or from the specified public or private network IP address entered in the ACL rule.

Procedure

1. Log on to the [Smart Access Gateway management console](#).
2. In the left-side navigation pane, click ACL.
3. Click Create Access Control List, and then set a name for the ACL (in this example, the name is test).
4. Then, return to the ACL page.
5. Click the target ACL instance ID or click Configure Rule in the Actions column on the right.
6. In the left-side navigation pane, select the target ACL and click Add ACL Rule to add an ACL rule to the ACL instance. Then, configure the rule according to the following information:

Item	Description
Rule Direction	Select a rule direction. <ul style="list-style-type: none">· Out direction: Refers to external traffic accessed internally from the local branch (where the SmartAG instance is located).· In direction: Refers to internal traffic of the local branch (where the SmartAG instance is located) that is accessed from an external network.
Authorization Policy	Select Allow or Deny.
Potocol Type	The specified protocol. Select TCP or UDP.

Item	Description
Source Network Segment	The address segment by which access is initiated. Supported parameters include: <ul style="list-style-type: none">· Out direction: The private network address segment where the local branch initiates access to an external network.· In direction: The private network address segment that accepts access from an external network.
Source Port Range	The transport layer source port range. Supported values include: <ul style="list-style-type: none">· TCP/UDP protocol value range: 1 to 65535· ICMP protocol value: -1/-1· All value: -1/-1
Destination Network Segment	The address segment that is involved with receiving network communications. Supported parameters include: <ul style="list-style-type: none">· Out direction: The external destination network segment to be accessed.· In direction: The target network segment of the local branch to be accessed.
Destination Port Range	The destination port range of the transport layer. <ul style="list-style-type: none">· TCP/UDP protocol value range: 1 to 65535· ICMP protocol value: -1/-1· All value: -1/-1
Priority	Value range: 1 to 100. A smaller value indicates a higher the priority. If the priority levels of two rules are the same, the rule created first takes effect.

7. Click OK.
8. Click Add Instance in the Actions column, and then add the target SmartAG instance that needs to comply with the created ACL rule.
9. Click Save.

You can also click Manage Instance in the Actions column to add or remove SmartAG instances as needed.

5 Configure a Smart Access Gateway Hardware device

5.1 Log on to the Web configuration page

After you power on the Smart Access Gateway device, you need to log on to the Web configuration page.

Prerequisites

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

- The Smart Access Gateway is powered on.
- For a SAG-100WM device, its LAN port is connected to the local client. For a SAG-1000 device, the administration port 2 is connected to the network cable.
- 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 SAG device in your browser.

For an SAG-100WM device, note the following:

- If you have configured the LAN port, the Web configuration address of the SAG device is the static IP address of the LAN port.
- If you have not configured a static IP address for the LAN port, but have configured a private CIDR block for the SAG instance in the console, the Web configuration address is the first address in the first private CIDR block configured by you. 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.

2. Set the logon password.

Keep your logon password confidential. If the password is lost or forgotten, press the reset button on your device once to reset the password.

3. Log on to the Web configuration page.

5.2 Web configurations for SAG-100WM devices

SAG-100WM Smart Access Gateway devices supports dynamic and static IP addresses, PPPoE connections, and SNAT forwarding. You can modify the WAN port and LAN port configurations as needed, or keep the default configurations.

Default configurations

After you power on your Smart Access Gateway device, you need to connect the WAN and LAN ports of the device to allow your local clients to access Alibaba Cloud. To do so, we recommend that you perform the following actions: Connect the WAN port of the gateway device to your network cable, and then connect the LAN ports to the local clients that require communication. You do not need to modify the WAN port and LAN port configurations for the gateway device.

By default, the WAN port accesses the Internet by using an IP address allocated from the router by the DHCP server. If the LAN port of the Smart Access Gateway device uses a dynamic IP address and DHCP is enabled on the client, the IP address used by the local client is allocated from the first CIDR block that you specified.

WAN configuration

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

To configure the WAN port, follow these steps:

1. Log on to the web configuration page of the Smart Access Gateway device.
2. Click Next to configure the WAN port.
3. Select whether to enable SNAT forwarding.

Once SNAT forwarding is enabled, packets sent from Local Area Network to Wide Area Network are subjected to NAT forwarding by default.

4. Select a connection mode:

- **Dynamic IP:**

To use an IP address allocated by a DHCP server from an Internet router to access the Internet, select this mode.

- **Static IP:**

To use a specified IP address to access the Internet, select this mode. If this mode is selected, you must configure the static IP, the subnet mask and the gateway.



Note:

Make sure that the specified static IP address and the uplink router device are in the same CIDR block.

- **PPPoE:** If you want to access the Internet through dialing, select this mode. Then enter the PPPoE account and password provided by the operator.

LAN configurations (Wi-Fi mode)

LAN ports are used to connect local clients. If you select to enable Wi-Fi, configure LAN ports according to the following information.

Configuration	Description
SSID	The name of the LAN. It is used to differentiate networks and can be customized.
SSID broadcast	You need to enable SSID broadcast for Wi-Fi devices to detect the Wi-Fi network.
Authentication type	WPA-PSK and WPA2-PSK authentication are supported. The WPA2-PSK authentication features higher security.
Encryption algorithm	<ul style="list-style-type: none">· 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.
Password	Set the Wi-Fi password.

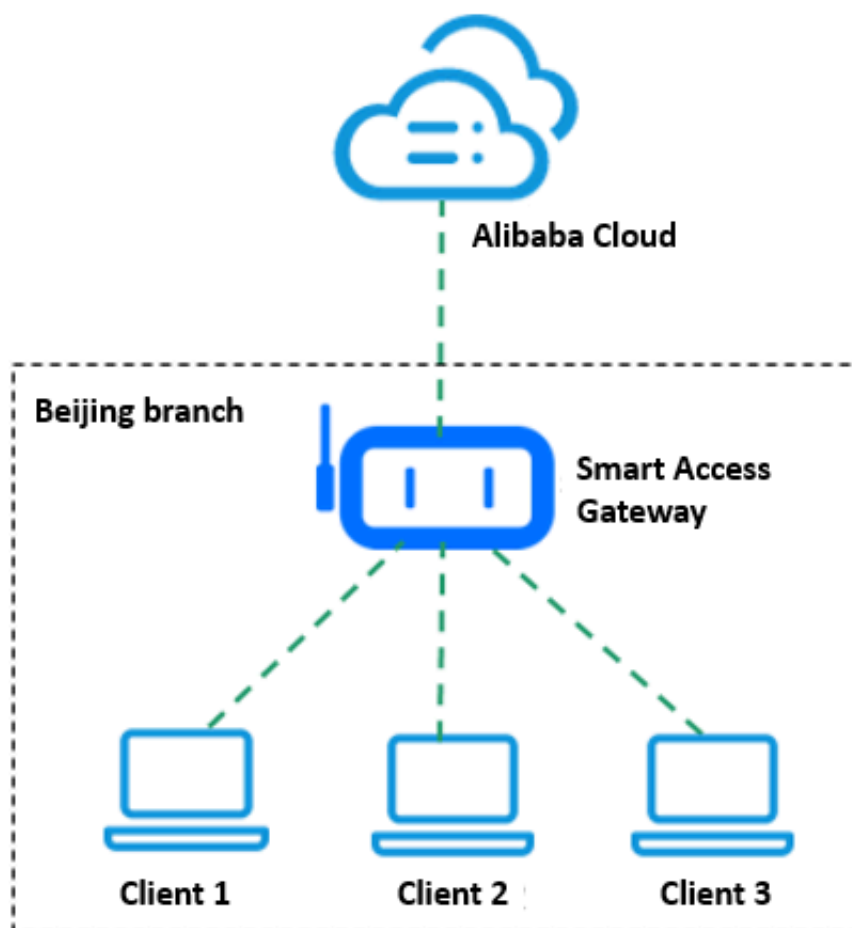
LAN configurations (broadband mode)

LAN ports on the SAG device are used to connect local clients to Alibaba Cloud. If you connect LAN ports of the SAG device to local clients by using network cables, you need to select the method for IP address allocation:

- **Dynamic IP address:**

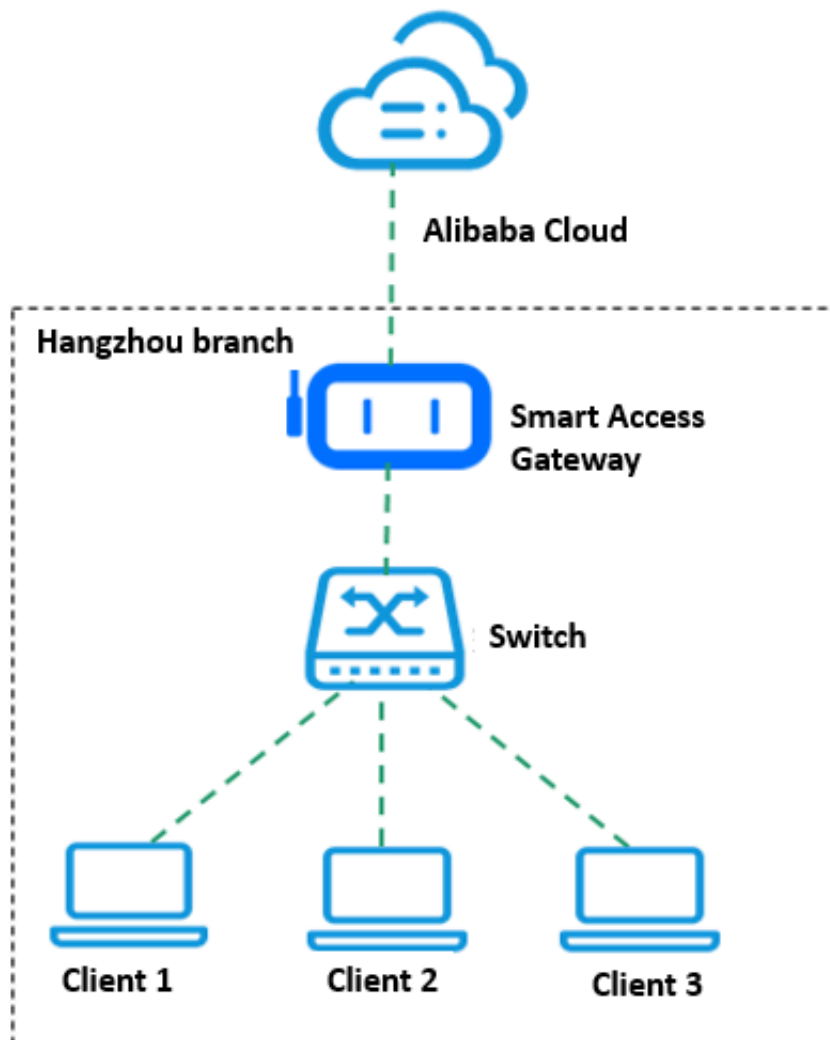
The IP addresses used by the LAN ports are allocated from the first CIDR block configured on Alibaba Cloud console.

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



- Static IP address:

If the IP addresses of the local clients have been configured through a local switch as shown in the following figure, select to use static IP addresses.



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

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

If the specified static IP address and the IP address of the switch are in the same CIDR block, we recommend that you set the gateway address of the switch to the specified static IP address so that no route configuration is required.



Note:

Make sure the static IP address does not conflict with any network to which the gateway device will connect in the future.

Route configurations

If you use static IP addresses as the method for IP address allocation for the LAN ports on the SAG device, you must add routes for the Smart Access Gateway device and to the switch.

- Route configuration for the device

On the LAN configuration page, click Route Configuration, and then add a route. Set the IP address of the local client as the destination CIDR block and set the IP address of the switch as the next hop.

If you have multiple clients, you must configure a route for each client.


- Route configuration for the switch
 - If local clients are to communicate with a VPC, add a route to the switch. The destination CIDR block is the CIDR block of the VPC, and the next hop is the static IP address of the LAN ports.
 - If local branches want to connect with each other through Smart Access Gateway devices, add the respective 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.

5.3 Web configurations for SAG-1000 devices

You can configure service and administration ports for an SAG-1000 device. You can also configure static or OSPF routing for the device.


Configure the service IP address and the administration port

After you log on to the Web configuration page of the SAG-1000 device, you can configure the service IP address and the administration port. Descriptions about the configuration items are provided in the following table.

Configuration	Description
Service IP address	<p>The service IP address is used to establish the VPN tunnel.</p> <div> Note: 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 clients to access the Web configuration page. Port 2 is the administration port.
Administration IP address	The administration IP address is used for local clients to access the Web configuration page..
Whether to isolate	<p>You can 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.

Configure ports

There are six ports on the SAG-1000 device. Port 1 and Port 2 are optical module ports, and port 2 to port 5 are device ports. Descriptions about the configuration items are provided in the following table.

Configuration	Description
Connection method	<p>You can choose to use static or dynamic routing to access the switch.</p> <div> Note: If dual-device one-arm mode is used, only dynamic routing is supported.</div>

Configuration	Description
Port	<p>You can 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 administration port.</p>

Configure OSPF routing

Configuration	Description
Area ID	<p>The ID of the area.</p> <p>Make sure that area IDs of Smart Access Gateway device 1 and Smart Access Gateway device 2 are different.</p>
Hello_time	The interval at which hello packets are sent, in seconds.
dead_time	The dead time interval of the OSPF neighbor, in seconds. The neighbor relationship stops if no hello packet is received during the dead time interval.
Authentication method	<p>You can select the required 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 algorithm to perform authentication. Enter the MD5 key ID and the MD5 key.
Routerid	The ID of the OSPF router. We recommend that you directly use the service IP address.
Area Type	By default, the area type is NSSA.