

Alibaba Cloud Smart Access Gateway

Smart Access Gateway

Issue: 20190917

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 Configuration Guide.....	1
1.1 Links to SAG configuration documentation.....	1
1.2 SAG-100WM configurations.....	2
1.2.1 SAG-100WM overview.....	2
1.2.2 Configuration process.....	6
1.2.3 Web configurations for SAG-100WM devices.....	7
1.3 SAG-1000 configurations.....	12
1.3.1 SAG-1000 overview.....	13
1.3.2 Install an SAG-1000 device.....	16
1.3.3 Configuration process.....	20
1.3.4 Web configurations for SAG-1000 devices.....	20
1.4 Device management.....	24
1.4.1 Update the software of an SAG device.....	24
1.4.2 Restart an SAG remotely.....	25
1.5 Network configurations.....	26
1.5.1 Synchronize the routes between an SAG instance and the corresponding on-premises SAG device.....	26
1.5.2 Associate an SAG instance with a network instance.....	27
1.5.3 Add a SNAT entry.....	28
1.5.4 Add a DNAT entry.....	29
1.5.5 View the networking structure of an SAG instance.....	30
1.6 SAG instance management.....	31
1.6.1 Renew an SAG instance.....	31
1.6.2 Renew an SAG instance and change its configuration.....	31
1.6.3 Upgrade the configuration of an SAG instance temporarily.....	32
1.6.4 Disassociate an SAG instance from a network instance.....	33
1.6.5 Add an ECC link.....	34
1.6.6 Add an Internet link.....	34
1.7 Access to cloud services.....	35
1.7.1 Overview of accessing cloud services.....	35
1.7.2 Set AnyTunnel services.....	35
1.7.3 Set PrivateZone access.....	36
1.7.4 Grant permissions to CCN.....	38
2 SAG Monitoring.....	46
2.1 View the monitoring data of an SAG instance.....	46
2.2 Create an event alert.....	47
2.3 Event protocols.....	48
2.3.1 AccessGatewayFailover.....	48

2.3.2 DeviceWanLinkSwitched.....	48
2.3.3 DeviceOnline.....	49
2.3.4 DeviceWanLinkUp.....	49
2.3.5 DeviceOffline.....	49
2.3.6 ConnectionDisconnect.....	50
2.3.7 DeviceSwitched.....	50
2.3.8 DeviceLinkDown.....	51
2.3.9 DeviceWanLinkDown.....	51
2.3.10 DeviceHacked.....	52
3 SAG Troubleshooting.....	53
3.1 Troubleshooting process.....	53
3.2 SAG status.....	54
3.2.1 SAG indicators.....	54
3.2.2 View the status of an SAG device.....	55
3.2.3 View the link status of an SAG instance.....	56
3.2.4 View the OSPF status.....	56
3.3 System maintenance.....	60
3.3.1 Restart an SAG device.....	60
3.3.2 Update the software of an SAG device.....	61
3.4 Hardware troubleshooting.....	62
3.4.1 Locate the cause of power failure.....	63
3.4.2 The SAG cannot be powered on.....	63
3.4.3 The optical module is faulty.....	64
3.4.4 The Ethernet interface cannot be connected.....	65
3.4.5 The Ethernet interface frequently goes up or down.....	68
3.5 Connectivity faults between SAG-100WM and Alibaba Cloud.....	72
3.5.1 The SAG is offline.....	72
3.5.2 Cannot successfully ping an ECS instance in the same CEN instance or a PC in the same CCN instance.....	73
3.6 Connectivity faults between SAG-1000 and Alibaba Cloud.....	73
3.6.1 The SAG is offline.....	74
3.6.2 A PC cannot ping an ECS instance.....	75
3.6.3 SAG-1000 cannot connect to a local client.....	76
3.7 Link failure between SAG-1000 and the switch.....	77
3.8 FAQ.....	78
3.8.1 What can I do if a service failure occurs?.....	78
3.8.2 What can I do if my SAG is offline?.....	78
3.8.3 What can I do if I forget my password?.....	78
3.8.4 What is the default Wi-Fi password of SAG-100WM?.....	78
4 High availability configurations.....	79
4.1 View the HA configuration of an SAG.....	79
4.2 View the WAN + 4G backup of an SAG.....	79
4.3 View leased line backup.....	80

1 Configuration Guide

1.1 Links to SAG configuration documentation

This topic provides links to all SAG configuration documentation.

The following table describes the configuration items of SAG.

Configuration item	Description
Device management through the console	<p>You can remotely manage physical devices through the Smart Access Gateway console. For more information, see the following documentation:</p> <ul style="list-style-type: none">• #unique_5• #unique_6
Network configurations	<p>You must configure the corresponding network before you can access Alibaba Cloud through an SAG. For more information, see the following documentation:</p> <ul style="list-style-type: none">• #unique_7• #unique_8• #unique_9• #unique_10
SAG instance management	<p>You can manage SAG instances in the Smart Access Gateway console. For more information, see the following documentation:</p> <ul style="list-style-type: none">• #unique_11• #unique_12• #unique_13• #unique_14

Configuration item	Description
Access to cloud services	<p>You can enable network instances attached to your CEN instances to access cloud services deployed in your VPC. For more information, see the following documentation:</p> <ul style="list-style-type: none"> • #unique_15 • #unique_16

1.2 SAG-100WM configurations

1.2.1 SAG-100WM overview

The SAG-100WM device is designed to connect small branches and outlets to Alibaba Cloud. As a plug-and-play device, SAG-100WM does not require Web configuration.

Specifications

Property	SAG-100WM Specification
Operating environment	Indoor environment (no fan provided)
Operating temperature	0°C–45°C
Storage temperature	–40°C–70°C
Power supply	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 300 Mbps, 20 terminals, 100 m2 coverage
4G LTE (Mainland China)	LTE FDD: B1, B3, B5, and B8 LTE TDD: B38, B39, B40, and B41 WCDMA: B1, B5, and B8 TD SCDMA: B34 and B39 GSM: B3 and B8 CDMA EVDO/1X: 800M
4G LTE (Outside Mainland China)	LTE FDD: B1, B3, B5, and B8

Property	SAG-100WM Specification
	WCDMA: B1, B5, and B8
	GSM: B3 and B8
USB	USB 2.0, 500 mA

SAG components

The Smart Access Gateway (SAG) device is shipped with the following components:

- An SAG device
- A power cable



Note:

If any component is missing or damaged, contact Alibaba Cloud after-sales personnel. Two types of SAG-100WM devices are available.

Type 1 (dimensions: 180 mm × 110 mm × 30 mm)

- Front panel
- Rear panel

Type 2 (dimensions: 275 mm × 175 mm × 44.4 mm)

- Front panel
- Side panel
- Rear panel

Front panel and rear panel

The front panel and the rear panel of a Type 1 SAG-100WM device are described as follows:

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

LED indicator	Description
LTE	Indicates whether the device communication is normal. <ul style="list-style-type: none">- Flashing: Data is being transmitted.- Off: No card is inserted.
WAN	Indicates the Ethernet status of the device. <ul style="list-style-type: none">- On: The device is connected to the Ethernet.- Flashing: Data is being transmitted.- Off: The device is not connected to the Ethernet.
Wi-Fi	Indicates the Wi-Fi connection status of the device. <ul style="list-style-type: none">- On: The WLAN is enabled.- Flashing: Data is being transmitted.- Off: The WLAN is disabled.
RUN	Indicates the status of the SAG device. <ul style="list-style-type: none">- On: The device is powered on.- Flashing: Data is being transmitted.- Off: The device is powered off.
CLOUD	Indicates whether the device is connected to Alibaba Cloud. <ul style="list-style-type: none">- 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 the SAG device.

- **RESET button**

To restore the SAG device to its default settings, press and hold the RESET button for five seconds when the device is powered on.

The default administration IP address of the SAG device is 192.168.0.1.

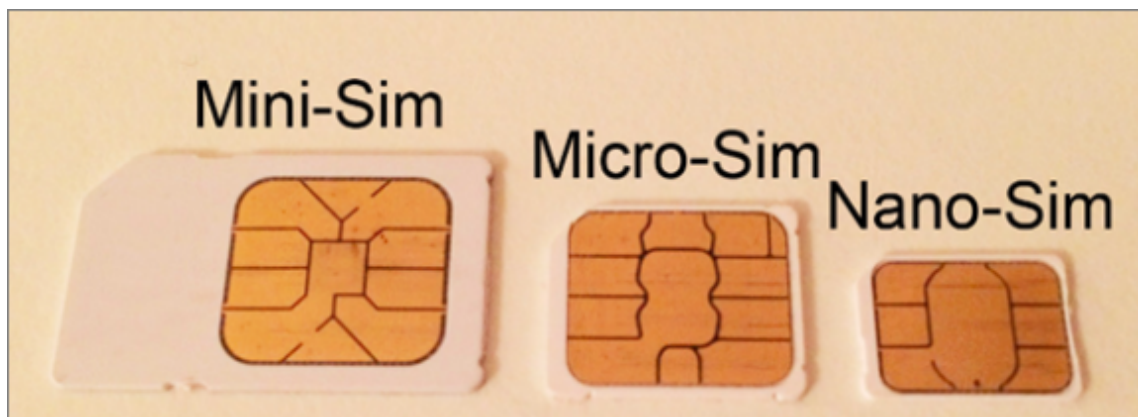
- **SIM card slot**

A SIM card is inserted into the slot. Only Mini-SIM cards, Micro-SIM cards, and Nano-SIM cards are supported. If you use a Micro-SIM or Nano-SIM card, we

recommend that you use a card frame rather than a card sleeve. Otherwise, it may be difficult to pull out the card.

The SAG device is equipped with a SIM card frame that matches Mini-SIM, Micro-SIM, and Nano-SIM cards. You can use the card frame if you want to change the SIM card.

Mini-SIM cards, Micro-SIM cards, and Nano-SIM cards are also called 2FF cards, 3FF cards, and 4FF cards respectively.



- USB interface

Access to the Internet by using the 4G USB interface is not supported.

- WAN ports

The WAN ports are used to access the Internet. These ports support SNAT forwarding, dynamic IP addresses, static IP addresses, and PPPoE.

- LAN ports

The LAN ports are used to connect local clients and can be connected to the switch by configuring routes.

- DC power interface

The power interface is on the rightmost of the panel. The power supply must be 12 V DC.

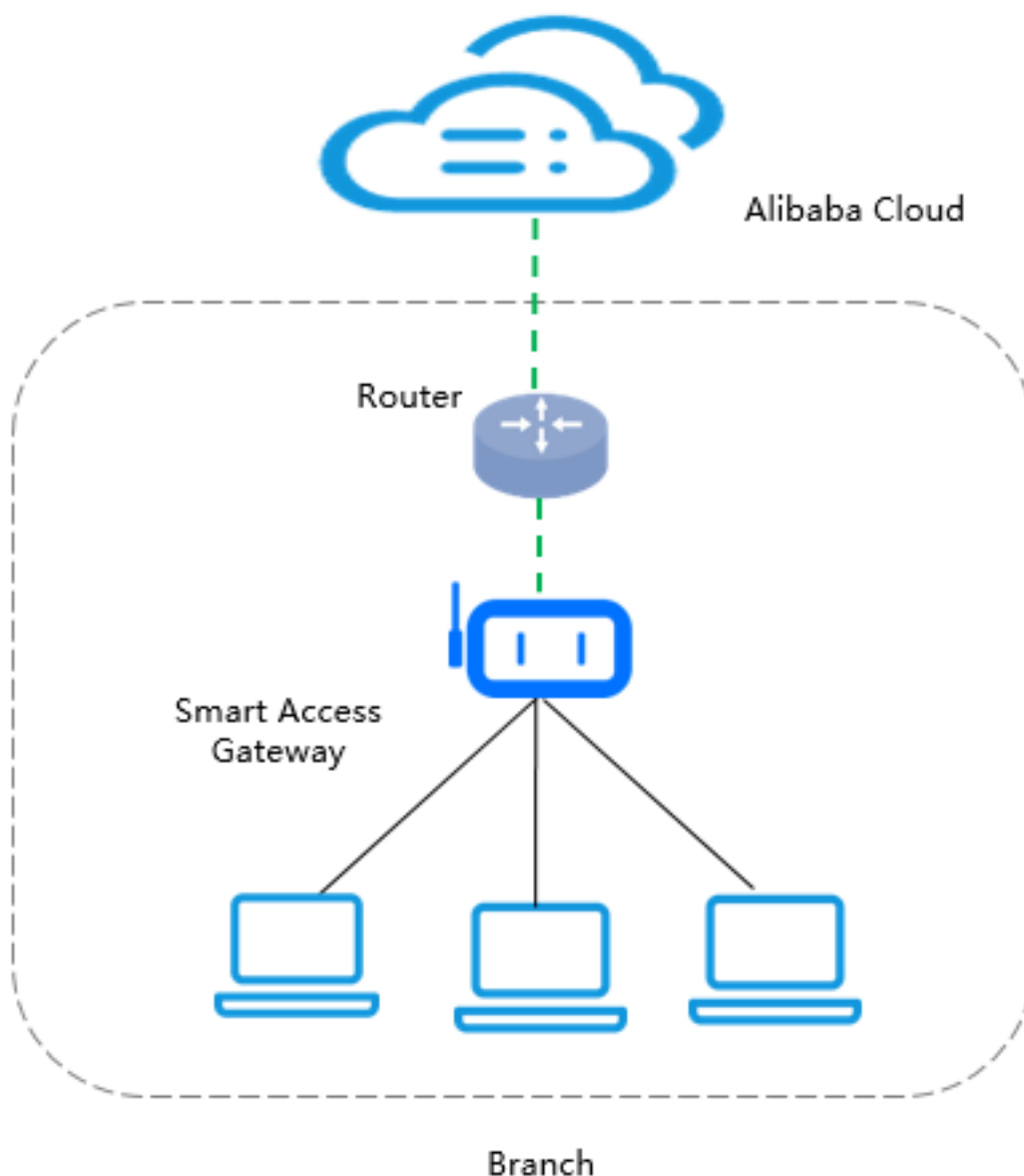


Note:

We recommend that you use the original power cable.

Networking mode

The SAG-100WM device connects local clients to Alibaba Cloud through inline mode, which means that the network topology is unchanged.



1.2.2 Configuration process

Before you can use your Smart Access Gateway (SAG) device, you must power it on and complete the Web configurations and network configurations.

The following figure shows the process that you can use to access Alibaba Cloud with an SAG-100WM device.

When you receive the device after you [#unique_20](#), follow these steps to access Alibaba Cloud through the SAG-100WM device:

1. [#unique_7](#)
2. [#unique_21](#)
3. [#unique_22](#)

1.2.3 Web configurations for SAG-100WM devices

This topic describes the steps that you must follow to complete Web configurations for SAG-100WM devices. Before you access Alibaba Cloud through Smart Access Gateway (SAG) devices, you must complete Web configurations for the SAG devices.

Step 1: Configure the local client

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

- Windows client configuration

1. In the lower-right corner, right-click the network connection icon and then click Open Network and Sharing Center.
2. In the left-side panel, click Change Adapter Settings.
3. Right-click the connected network, and then click Properties.
4. Double-click Internet Protocol Version 4 (TCP/IPv4).
5. Select Obtain an IP Address Automatically and Obtain DNS Server Address Automatically.
6. Click OK.

- Mac client configuration

1. On the desktop, click the System Preferences icon, and then click Network in the Internet and Network section.
2. Click the connected network and then click Advanced.
3. On the Ethernet configuration page, click the TCP/IP tab.
4. From the Configure IPv4 drop-down list, select Using DHCP.

Step 2: Set the password upon your first logon

After you power on the SAG device for the first time, you must go to the Web console to set the logon password.

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

- The SAG device is powered on.
- A LAN port of the SAG device is connected to the local client.
- The local client has DNS enabled to automatically obtain an IP address.

1. Open the browser on the connected local PC and enter `192 . 168 . 0 . 1` in the address bar.

`192 . 168 . 0 . 1` is the default Web configuration address of the SAG device.



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 in the console, the WAN port has DHCP enabled, and the CLOUD status indicator light turns on when the network cable is connected), log on by using the first IP address in the first CIDR block configured in the console.

For example, if the first CIDR block you specified 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, enter the new password, and log on to the Web console.

Keep your logon password securely. 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.



Notice:

- To clear all configurations of the SAG device, power the device on and press and hold the RESET button for five seconds until the CLOUD indicator light starts to flicker.
- To restore the SAG device to its default configurations, power off the device, and then press and hold the RESET button while powering the device back on. When the CLOUD indicator light is on, which means the device is restoring, release the RESET button.

After two to three minutes, the CLOUD indicator light goes off, which means the default configurations are restored.

Step 3: Configure the WAN ports

The WAN ports of the Smart Access Gateway (SAG) device are used for configuring Internet access and support dynamic IP addresses, static IP addresses, and PPPoE connections.

1. Log on to the Web configuration page of the SAG device.
2. Enter the logon password and click OK.
3. Click WAN Port Management. On the WAN Port Management page, configure the WAN ports.
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:

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

- Static IP:

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: Select this mode if you want to access the Internet by using dial-up. You need to enter the PPPoE account name and password provided by the service provider.

5. Click OK.

Step 4: Configure the LAN ports

The LAN ports are used for connecting the local clients.

1. Log on to the Web configuration page of the SAG device.
2. After the WAN ports are configured, click LAN Port Management.

3. On the LAN Port Management page, configure the LAN ports.

- **Wireless mode**

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 to differentiate 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.
Wireless 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 device.
Authentication Method	WPA-PSK authentication and WPA2-PSK authentication are supported. WPA2-PSK authentication features higher security.
Encryption Algorithm	<ul style="list-style-type: none">- TKIP is a temporal key integrity protocol and is not secure. We do not recommend this encryption algorithm.- AES is an efficient encryption standard for Wi-Fi authorization.

Configuration	Description
Password	Set the Wi-Fi password.

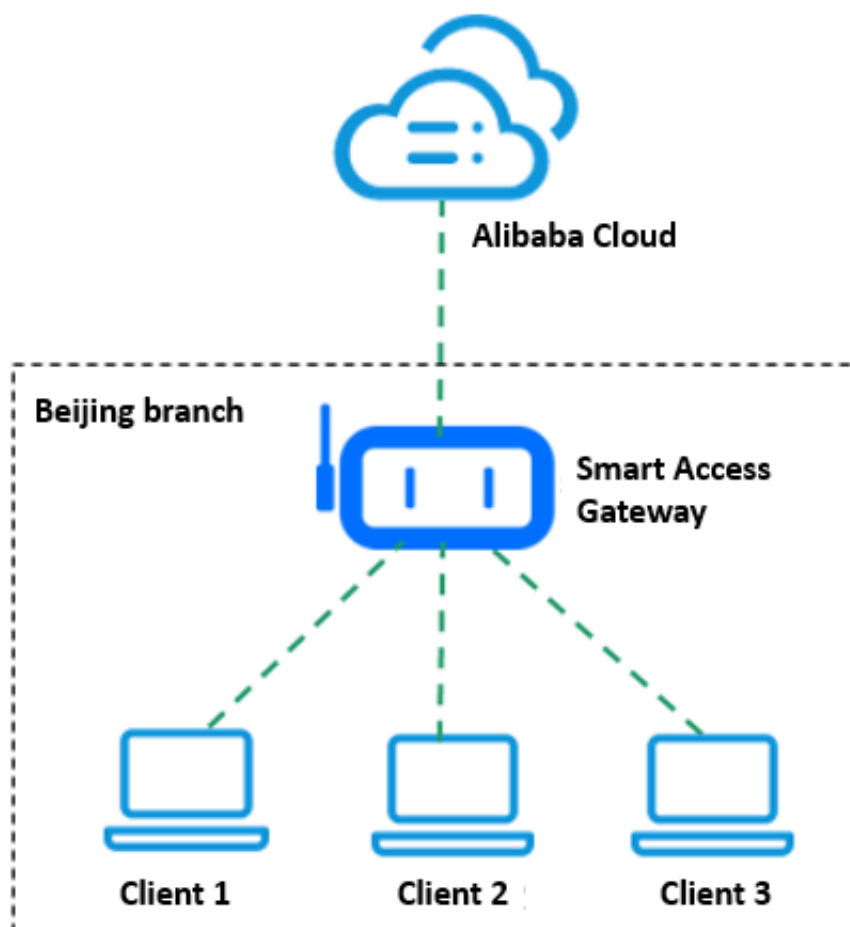
- Ethernet mode

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 configured in Alibaba Cloud console.

If your local clients directly access Alibaba Cloud by using an SAG device as shown in the following figure, use the default configurations.



- Static IP address:

If the IP address of the local client has been configured through 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 routes:

- Static IP address: the IP address of the SAG device.



Note:

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

- If the LAN ports are connected through static IP, you need to add a route to the SAG device and the switch separately.

- **Route configuration for the SAG device**

On the LAN configuration page, select Configure routes, 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 SAG 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.

1.3 SAG-1000 configurations

1.3.1 SAG-1000 overview

The SAG-1000 device is used to connect headquarters and large branches to Alibaba Cloud through one-arm mode.

Specifications

Property	SAG-1000
Casing	Metal, matte black, mountable
Size	1 U, halfwidth
Operating environment	Indoor environment
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
Interfaces	Two SFP optical ports
	The number of electric ports varies according to the manufacturer. Generally , four or six GE/FE RJ45 electric ports are provided.

Accessories

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

- An SAG device
- A power cable

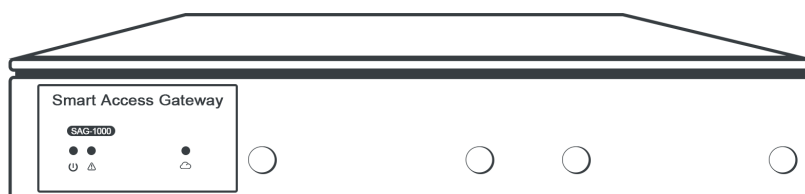


Note:

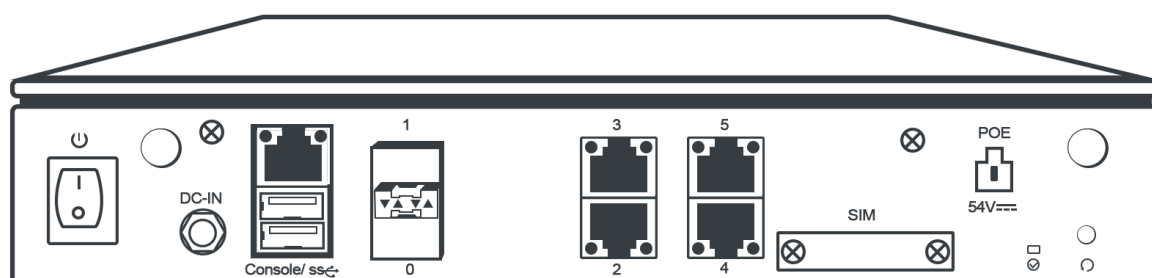
If any item is missing or damaged, contact Alibaba Cloud after-sales personnel. Two types of SAG-1000 devices are provided.

Type 1 (size: 250×193×44 mm)

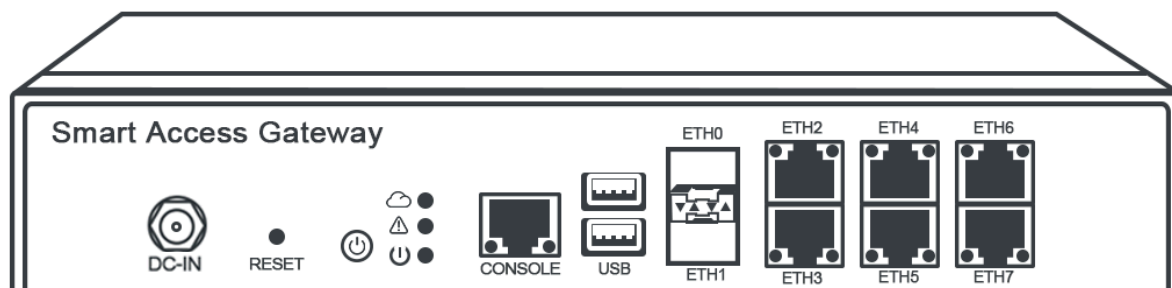
- Front panel



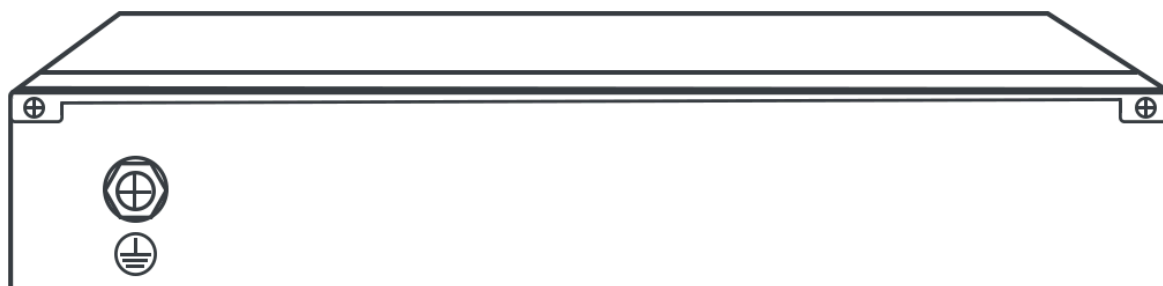
- Rear panel

**Type 2 (size: 241×220×44 mm)**

- Front panel



- Rear panel



The following is an overview about the components of an SAG-1000 device of the Type 1 category. Types 2 device, although different in appearance, have the same functions as Type 1 devices.

- **Front panel**

There is a power LED indicator, an alarm LED indicator, and a cloud connection status LED indicator on the front panel of the SAG device:

LED indicator	Description
Power	On: The device is running normally.
Alarm	The status of the alarm LED indicator includes the following: <ul style="list-style-type: none">- Green: The device is normal.- Yellow: The device is faulty.
Cloud connection status	The status of the cloud connection status LED indicator includes the following: <ul style="list-style-type: none">- Green: The connection to the cloud is normal.- Yellow: The connection to the cloud is faulty.

- **Rear panel**

There is one RESET button, two USB interfaces, six ports, one power socket, and one switch on the rear panel of the SAG device.

- **Ports**

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

The default administration IP address of the SAG device is 192.168.0.1.

- **Reset button**

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

- **USB interface**

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.

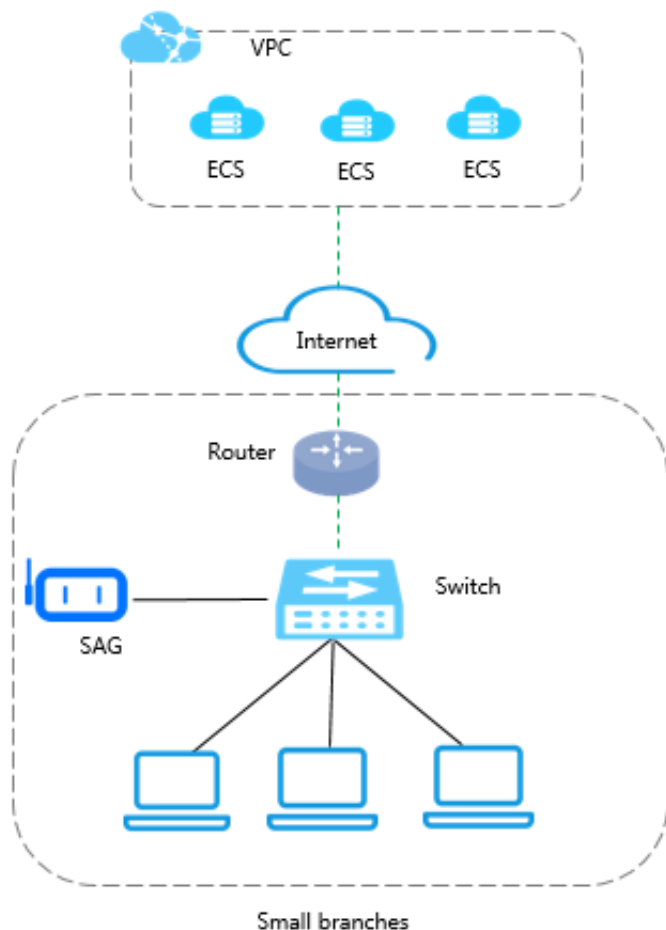


Note:

We recommend that you use the original power cable.

Networking mode

The SAG-1000 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.



1.3.2 Install an SAG-1000 device

This topic describes how to install an SAG-1000 device. The SAG-1000 device can be installed on a workbench or in a cabinet.

Preparations

Before the installation, prepare the following tools:

- Cross screwdriver
- ESD wrist strap
- Screws

Install an SAG-1000 device on a workbench

When you install an SAG-1000 device on a workbench, make sure that:

- The workbench is stable and is correctly grounded.
- Sufficient spacing is reserved around the SAG-1000 device to ensure good heat dissipation.
- No heavy loads are placed on the SAG-1000 device.

Install an SAG-1000 device in a cabinet

You can install the SAG-1000 device on the cabinet shelf, or attach the device to the cabinet.

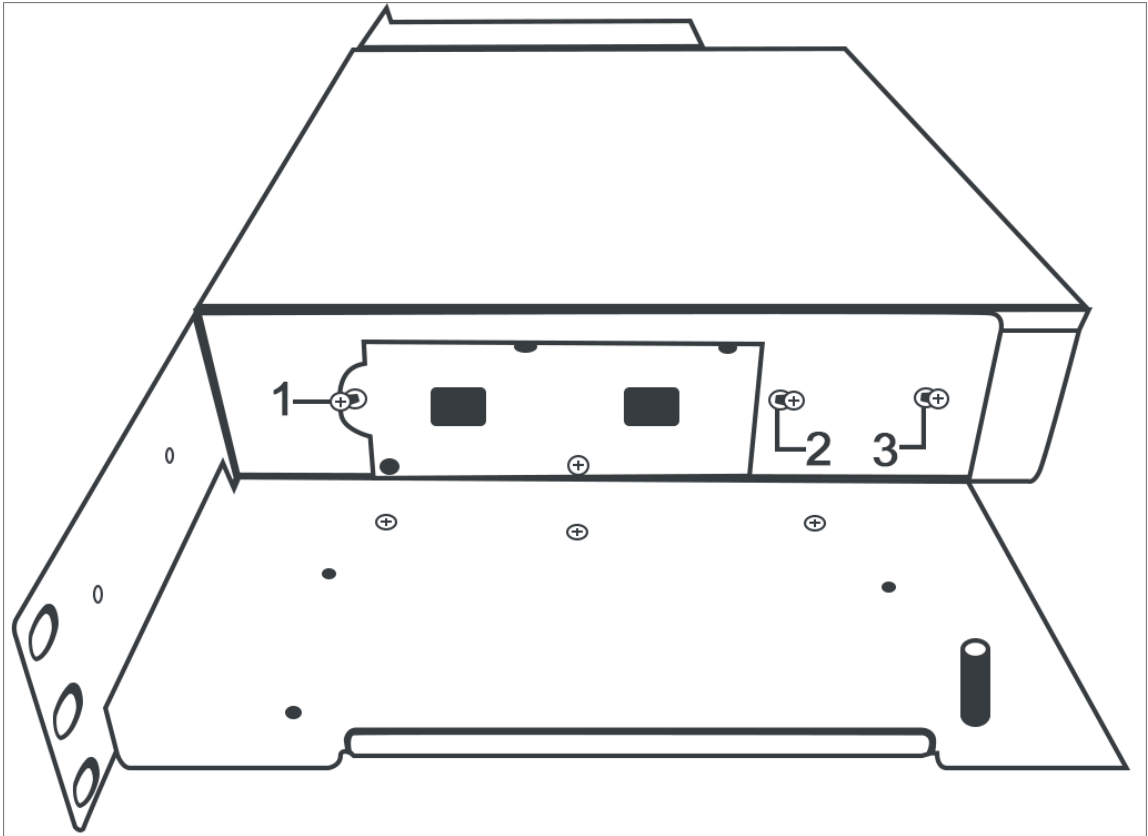
- Install the device on the cabinet shelf
 1. Install the shelf on the cabinet by using screws.
 2. Place the device on the shelf.
- Attach the device to the cabinet



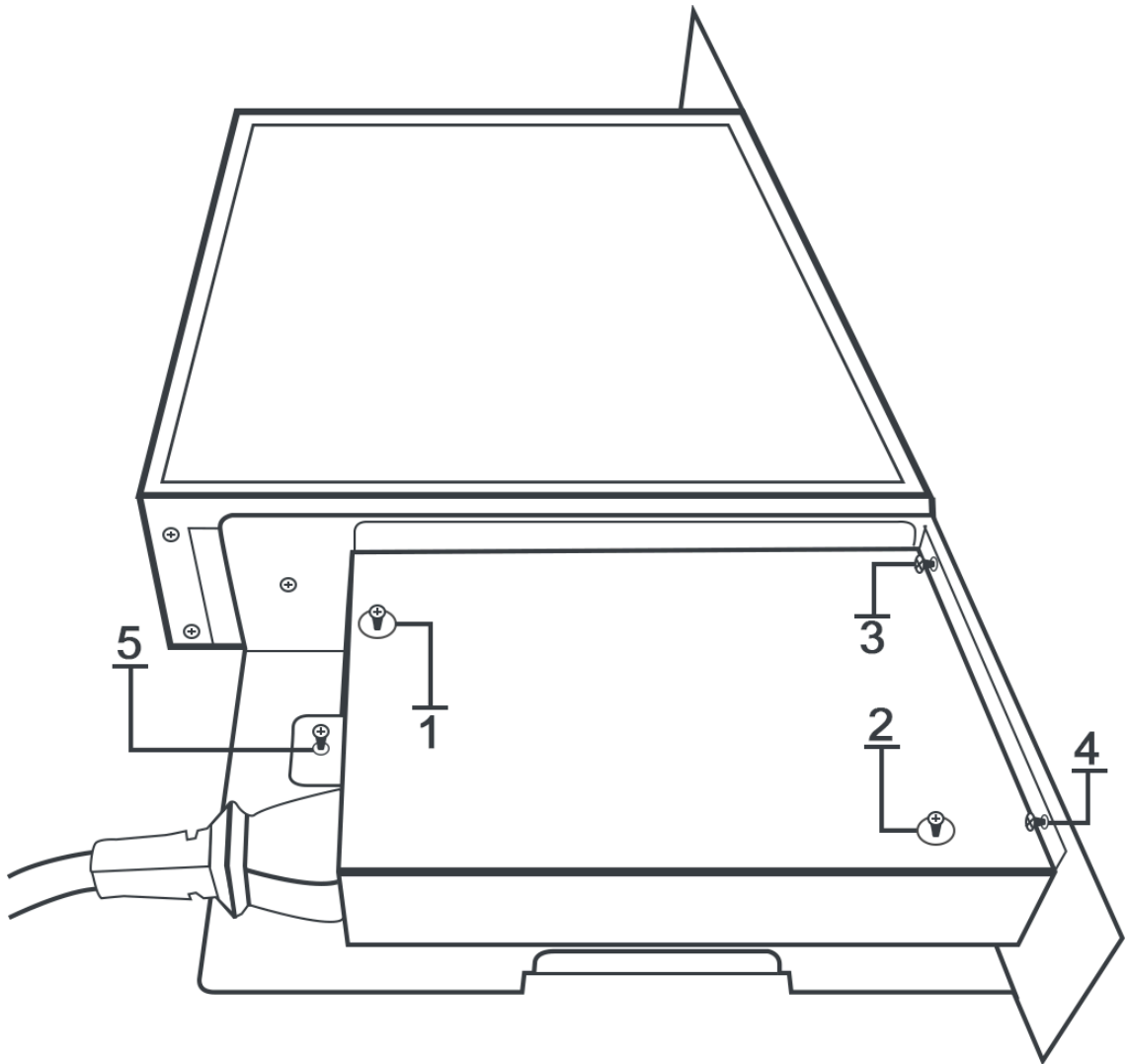
Note:

Before the installation, you must purchase the installation assemblies from the specified manufacturer.

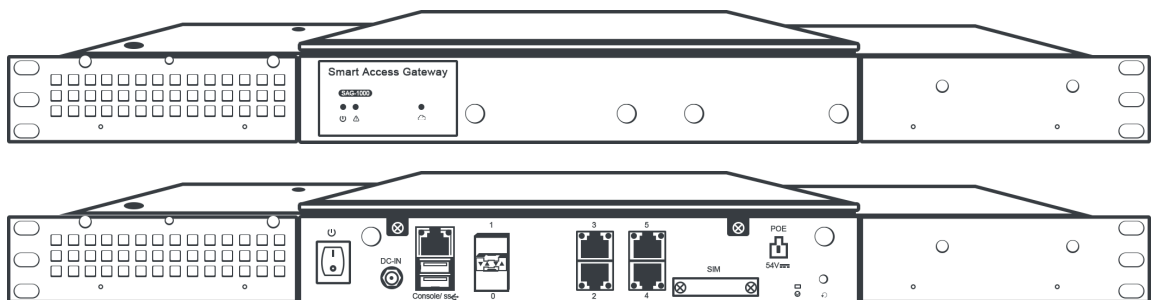
1. Attach one side of the adapter holder to the SAG-1000 device, as shown in the following figure.



2. Attach the cover to the adapter holder by using screws, as shown in the following figure.



3. Attach the other side of the adapter holder to the SAG-1000 device, as shown in the following figure.



4. Use screws to attach the SAG-1000 device to the cabinet horizontally.

1.3.3 Configuration process

Before you can use your Smart Access Gateway (SAG) device, you must power it on and complete the Web configurations and network configurations.

The following figure shows the process that you can use to access Alibaba Cloud with an SAG-1000 device.

When you receive the device after you [#unique_20](#), follow these steps to access Alibaba Cloud through the SAG-1000 device:

1. [#unique_28](#)
2. [#unique_7](#)
3. [#unique_29](#)
4. [#unique_30](#)

1.3.4 Web configurations for SAG-1000 devices

This topic describes the steps that you must follow to complete Web configurations for SAG-1000 devices. Before you access Alibaba Cloud through Smart Access Gateway (SAG) devices, you must complete Web configurations for the SAG devices.

Step 1: Configure the local client

Before performing Web configurations on an SAG-1000 device, you must configure the static IP address of the local client to access the Web configurations.

- Windows client configuration

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



Notice:

Ensure that the IP address is in the management CIDR block of the SAG device (the default management 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

1. On the desktop, click the System Preferences icon, and then click Network in the Internet and Network section. 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.
4. From the Configure IPv4 drop-down list, select Manually, and enter the static IP address and subnet mask to use.



Notice:

Ensure that the IP address is in the management CIDR block of the SAG device (the default management 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.

Step 2: Set the password upon your first logon

After you power on the SAG device for the first time, you must go to the Web console and set a logon password.

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

- The SAG device is powered on.
 - The static IP address is configured on the local client.
 - The local PC is connected to Port 2 of the SAG device through a network cable.
1. Open the browser on the connected local PC and enter 192 . 168 . 0 . 1 in the address bar.

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

2. Enter a logon password.

We recommend that you securely store your logon password and keep it strictly confidential. If the password is lost or forgotten, press the RESET button to clear the old password. Then, log on to the Web console and set a new password.



Notice:


If you press the RESET button for three times or more within 10 seconds, all configurations are cleared.

3. Log on to the Web console.

Step 3: Configure the service IP address and the management IP address

After you configure the username and password and log on to the Web configuration page, you can configure the service IP address and management IP address of the SAG device. Port 2 is the management port by default.

1. On the Web configuration page, click Service IP.
2. Configure the service IP address and management IP address according to the following information, and then click OK.


Configuration	Description
Configure Service IP:	<p>The service IP address is used to establish the VPN tunnel.</p> <div> Notice: Make sure that the specified service IP address can access the Internet.</div>
Management Interface:	<p>The management port is used for local clients to access the Web console. By default, port 2 is the management port.</p>
Isolate or not:	<p>Select whether to isolate the service port from the management port:</p> <ul style="list-style-type: none">· Yes: This port can only be used as a local Web management port and cannot be used as a service port. <p>In the isolation mode, the service traffic and the management traffic do not communicate with each other, achieving a high level of security.</p> <ul style="list-style-type: none">· No: This port is used as both the local Web management port and the service port.

Configuration	Description
Management port IP:	The management IP address is used for Web access of the local client.
Next Hop:	If you choose to isolate the service port from the management port, specify the next hop of the management port.

Step 4: Configure ports and routes

There are six ports on an SAG-1000 device. Port 0 and Port 1 are SFP optical ports, and Port 2 to Port 5 are RJ45 electrical ports. You can configure a static route or Open Shortest Path First (OSPF) routes for port connection.

1. Log on to the Web console of the SAG device and on the Configuration page, click Port Management.
2. Configure the ports of the SAG device according to the following information, and then click OK.

Configuration	Description
Connection Type	Select whether to access the switch by using static routes or dynamic routes.  Notice: When dual-device one-arm mode is used, only dynamic routing is supported.
Port	Click Edit in the Configurations section, enter the IP address of the port used for communication and select whether to enable OSPF. Port 2 is the default management port.
OSPF routing configuration	
Area ID	The ID of the area. Make sure that area IDs of SAG device 1 and SAG device 2 are different and the area ID of each SAG device is the same as that of the corresponding peer switch.


Configuration	Description
Hello_time	The interval in which hello is sent. Unit: seconds. Default value: 3.
Dead_time	The dead interval of OSPF neighbor. Unit: seconds. The neighbor relation stops if no hello packet is received during the dead time. Default value: 10.
Authentication Method	Select an authentication method. <ul style="list-style-type: none">· Not: Do not perform authentication.· Plain Text: Enter a clear text password.· MD5: Use the MD5 method 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	The area type is nssa by default.

1.4 Device management

1.4.1 Update the software of an SAG device

This topic describes how to update the software of a Smart Access Gateway (SAG) device in the SAG console. We recommend that you update your software in off-peak hours to avoid possible network disconnections.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or choose  > Manage Device.
3. In the left-side pane of the SAG instance details page, click Device Management.
4. Select the device whose software you want to update, and then click Update Version.

5. In the Update Version dialog box, select the target version and view the description of previous versions.



Note:


We recommend that you update your software to the latest version. The update takes about 10 minutes.

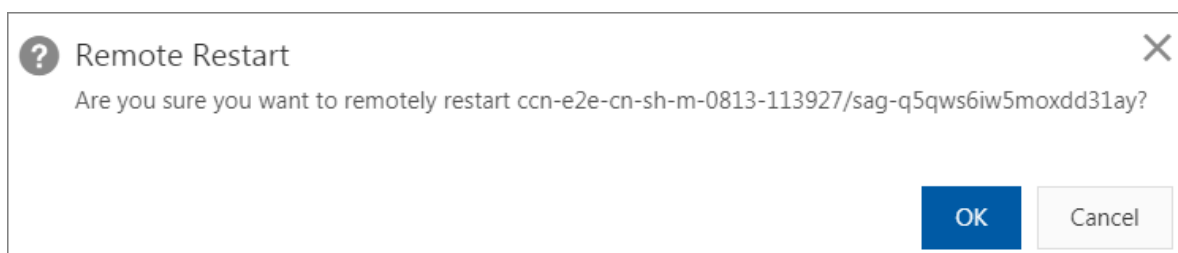
6. Click OK.

1.4.2 Restart an SAG remotely

This topic describes how to restart a Smart Access Gateway (SAG) 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, and then click the target instance ID or choose  > Manage Device.
3. In the left-side navigation pane of the SAG details page, click Device Management.
4. Select the SAG device that you want to restart, and then click Remote Restart.
5. In the displayed Remote Restart dialog box, click OK.



1.5 Network configurations

1.5.1 Synchronize the routes between an SAG instance and the corresponding on-premises SAG device

This topic describes how to synchronize the routes between a Smart Access Gateway (SAG) instance and the corresponding on-premises SAG device.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or click Configure Network in the Actions column.
3. On the SAG instance details page, click Method to Synchronize with On-premises Routes.

4. Select the method to synchronize the SAG instance routes with the on-premises device routes.

The following two methods are available:

- **Static Routing:** The SAG instance and the on-premises SAG device are interconnected through static routing. After you add the on-premises static routes, they are automatically published to the CEN.
 - a. Click Add Static Routing.
 - b. In the Add Static Routing dialog box, set the private CIDR block that is used by the on-premises SAG device to access Alibaba Cloud.



Note:

By default, up to five static routing CIDR blocks can be configured. However, you can open a ticket to increase the quota to 20.

- c. Click OK.
- **Dynamic Routing:** The SAG instance and the on-premises SAG device are interconnected through dynamic routing. After you add the on-premises dynamic routes, the BGP or OSPF protocol is run to automatically learn the on-premises routes.

Method to Synchronize with On-premises Routes	Network Instance Details	SNAT	DNAT	Networking Structure		
<p><input checked="" type="radio"/> Static Routing ?</p> <p><input type="radio"/> Dynamic Routing ?</p> <p>Add Static Routing</p> <table><thead><tr><th>CIDR Block</th><th>Actions</th></tr></thead><tbody></tbody></table>					CIDR Block	Actions
CIDR Block	Actions					

1.5.2 Associate an SAG instance with a network instance

This topic describes how to associate a Smart Access Gateway (SAG) instance with a network instance. You must associate an SAG instance with a network instance if you want to connect the SAG to Alibaba Cloud. You can connect an SAG to Alibaba Cloud through a leased line, the Internet, or the active and standby links.

Procedure

1. Log on to the [Smart Access Gateway console](#).

2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or click Configure Network in the Actions column.
3. On the SAG instance details page, click Network Instance Details.
4. Click Add Network Instance.
5. In the Add Network Instance dialog box, configure the network instance to be associated with the SAG instance.

The parameters are described as follows:

- **Network Type:** the type of the network associated with the SAG instance.

To connect the SAG to Alibaba Cloud through a leased line, associate the SAG with the VBR. To connect the SAG to Alibaba Cloud through the Internet, associate the SAG with a CCN instance.

The CCN is a device access matrix that consists of Alibaba Cloud distributed access gateways. After an SAG instance is associated with a CCN instance, the SAG can communicate with other gateways associated with the CCN instance.



Note:

The CCN instance and the SAG instance must be in the same area.

- **Network Instance:** the network instance to be associated with.

6. Click OK.

1.5.3 Add a SNAT entry

This topic describes how to add a SNAT entry to enable the SNAT function. The SNAT function can hide internal IP addresses and resolve private IP address conflicts.

With this function, on-premises sites can access internal IP addresses, but cannot be accessed by internal IP addresses. If you do not add a SNAT entry, on-premises sites can access each other only when all related IP addresses do not conflict.

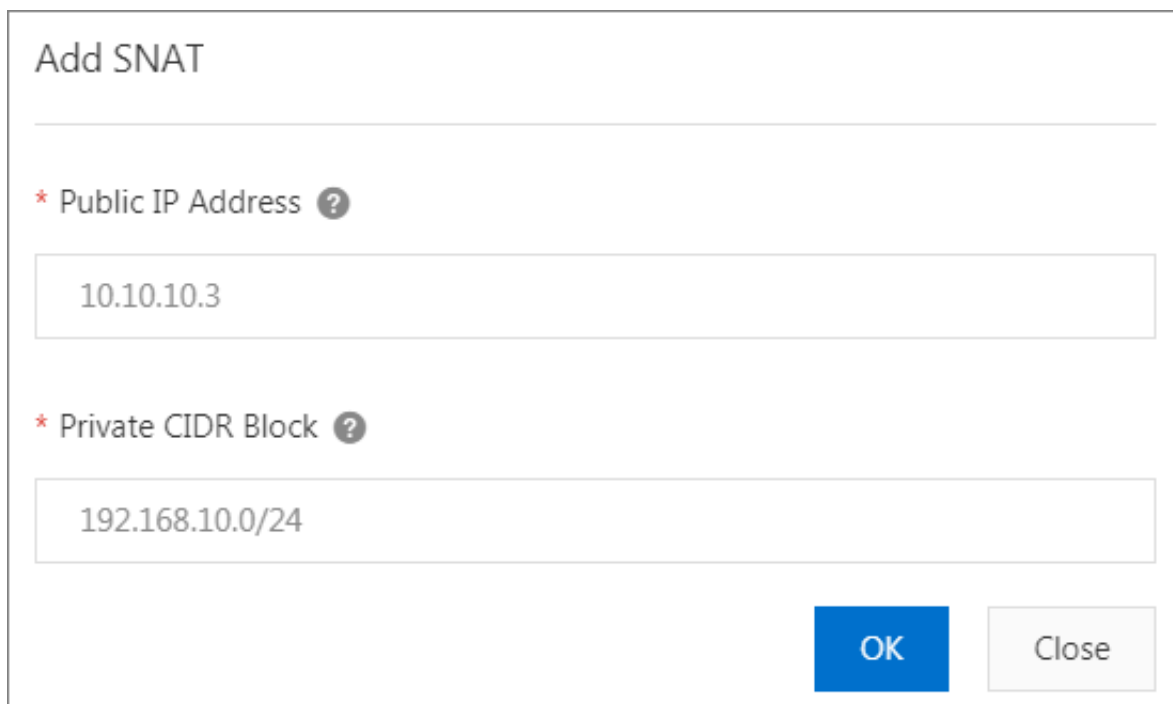
Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or click Configure Network in the Actions column.
3. On the SAG instance details page, click SNAT.
4. On the SNAT tab page, click Add SANT.

5. In the Add SNAT dialog box, set the SNAT parameters.

The SANT parameters are described as follows:

- **Public IP Address:** An IP address in the SNAT CIDR block of the CCN instance.
- **Private CIDR Block:** The private CIDR block used by on-premises terminals to access Alibaba Cloud. The private CIDR blocks cannot conflict with each other.



The image shows a dialog box titled "Add SNAT". It contains two required fields, each marked with a red asterisk and a help icon. The first field is "Public IP Address" with the value "10.10.10.3". The second field is "Private CIDR Block" with the value "192.168.10.0/24". At the bottom right, there are two buttons: "OK" (blue) and "Close" (gray).

1.5.4 Add a DNAT entry


This topic describes how to add a DNAT entry to a Smart Access Gateway (SAG) instance to enable the DNAT function. By using the DNAT function, you can forward requests received by public IP addresses to Alibaba Cloud instances according to custom mapping rules.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or click Configure Network in the Actions column.
3. On the SAG instance details page, click DNAT.
4. On the DNAT tab page, click Add DNAT.

5. In the Add DNAT Rule dialog box, configure the mapping rules.

The following table describes the DNAT rule parameters.

Parameter	Description
Connection Type	Select the DNAT mapping method. Options: <ul style="list-style-type: none">· All Ports: IP mapping, which associates an EIP with the target ECS instance. If this method is used, all requests destined for the specified public IP address are forwarded to the target ECS instance.· Specified Port: port mapping. If this method is used, the NAT Gateway forwards the requests from the specified protocol and port to the specified port of the target ECS instance. If you select this method, you must also specify the corresponding public port, internal port, and protocol.
Public IP Address	Enter a public IP address. <div> Note: A public IP address that is already used in a SNAT entry cannot be used to create a DNAT entry.</div>
Internal IP Address	Enter the private IP address of the ECS instance that will use the DNAT entry to access the Internet.
Public Port	The external port for traffic forwarding.
Internal Port	The internal port for traffic forwarding.
Protocol	The protocol type of the forwarding port.

6. Click OK.

1.5.5 View the networking structure of an SAG instance

This topic describes how to view the networking structure of a Smart Access Gateway (SAG) instance. You can view the networking structure of an SAG instance only after you complete network configurations for the SAG instance.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or click Configure Network in the Actions column.

3. Click the Networking Structure tab. The networking structure of the SAG instance is displayed.

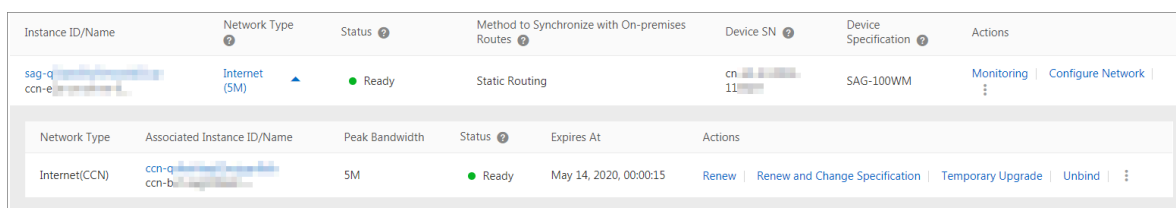
1.6 SAG instance management

1.6.1 Renew an SAG instance

This topic describes how to renew an SAG instance. Before an SAG instance expires, you must renew it to avoid service disruptions.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway. On the displayed page, find the target instance, and then click the drop-down list arrow in the Network Type column.



Instance ID/Name	Network Type	Status	Method to Synchronize with On-premises	Device SN	Device Specification	Actions
sag-q ccn-e	Internet (SM)	Ready	Static Routing	cn 11	SAG-100WM	Monitoring Configure Network

Network Type	Associated Instance ID/Name	Peak Bandwidth	Status	Expires At	Actions
Internet(CCEN)	ccn-q ccn-b	5M	Ready	May 14, 2020, 00:00:15	Renew Renew and Change Specification Temporary Upgrade Unbind

3. Click Renew in the Actions column.
4. On the Renew page, set the renewal duration and complete the payment.

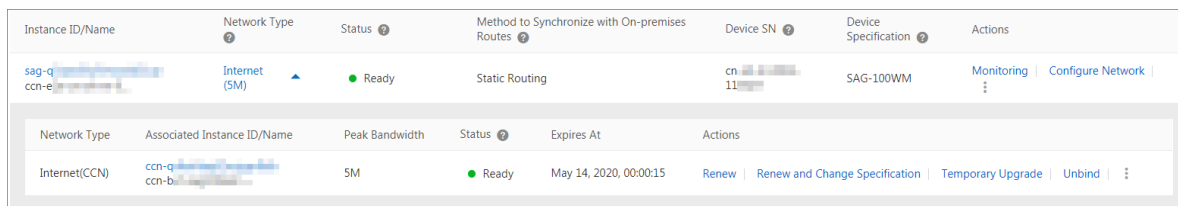
1.6.2 Renew an SAG instance and change its configuration

This topic describes how to renew an SAG instance and change its configuration. After an SAG instance expires, you can renew it and upgrade or downgrade its configuration. Configuration changes take effect within the renewal period.

Procedure

1. Log on to the [Smart Access Gateway console](#).

2. In the left-side navigation pane, click Smart Access Gateway. On the displayed page, find the target instance, and then click the drop-down list arrow in the Network Type column.



Instance ID/Name	Network Type	Status	Method to Synchronize with On-premises	Device SN	Device Specification	Actions
sag-d-ccn-e	Internet (5M)	Ready	Static Routing	cn-11	SAG-100WM	Monitoring Configure Network

Network Type	Associated Instance ID/Name	Peak Bandwidth	Status	Expires At	Actions
Internet(CCN)	ccn-q-ccn-b	5M	Ready	May 14, 2020, 00:00:15	Renew Renew and Change Specification Temporary Upgrade Unbind

3. Click Renew and Change Specification in the Actions column.
4. Set the peak bandwidth and the renewal duration, and then complete the payment.

1.6.3 Upgrade the configuration of an SAG instance temporarily

This topic describes how to temporarily upgrade the configuration of a Subscription Smart Access Gateway (SAG) instance.

Context

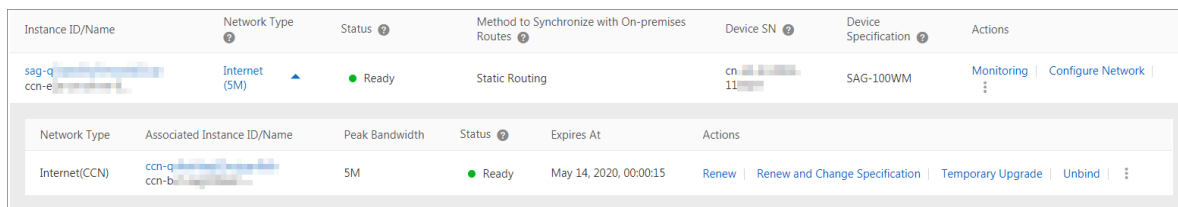
A temporary configuration upgrade can be applied to increase the bandwidth of an SAG to handle the traffic generated during public holidays or sales promotions. After the temporary configuration upgrade expires, the instance automatically restores the previous bandwidth and specifications.



- The minimum duration of a temporary configuration upgrade is two hours. The temporary configuration upgrade is billed by the hour. The upgraded bandwidth takes effect as soon as the payment is completed. Temporary configuration upgrades do not interrupt current services.
- When the restoration time specified for the SAG instance arrives, the instance automatically restores the previous bandwidth.


Procedure

1. Log on to the [Smart Access Gateway console](#).

2. In the left-side navigation pane, click Smart Access Gateway. On the displayed page, find the target instance, and then click the drop-down list arrow in the Network Type column.



Instance ID/Name	Network Type	Status	Method to Synchronize with On-premises Routes	Device SN	Device Specification	Actions
sag-q ccn-e	Internet (SM) 	Ready	Static Routing	cn 11	SAG-100WM	Monitoring Configure Network 

Network Type	Associated Instance ID/Name	Peak Bandwidth	Status	Expires At	Actions
Internet(CCN)	ccn-q ccn-b	5M	Ready	May 14, 2020, 00:00:15	Renew Renew and Change Specification Temporary Upgrade Unbind 

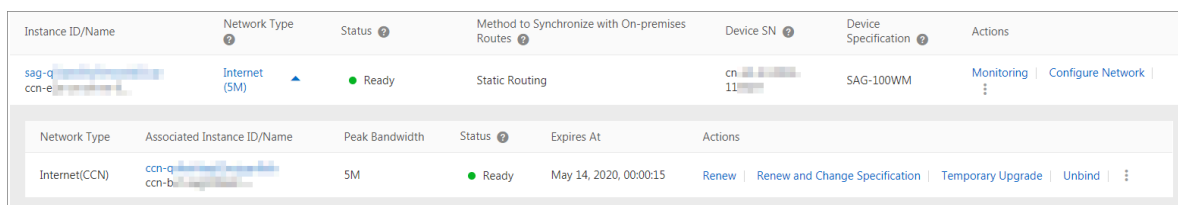
3. Click Temporary Upgrade in the Actions column.
4. On the Temporary Upgrade page, set the peak bandwidth and the restoration time, and then complete the payment.



1.6.4 Disassociate an SAG instance from a network instance


This topic describes how to disassociate an SAG instance from a network instance. After you disassociate an SAG instance, you can associate it with a new CCN or VBR instance.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway. On the displayed page, find the target instance, and then click the drop-down list arrow in the Network Type column.



Instance ID/Name	Network Type	Status	Method to Synchronize with On-premises Routes	Device SN	Device Specification	Actions
sag-q ccn-e	Internet (SM) 	Ready	Static Routing	cn 11	SAG-100WM	Monitoring Configure Network 

Network Type	Associated Instance ID/Name	Peak Bandwidth	Status	Expires At	Actions
Internet(CCN)	ccn-q ccn-b	5M	Ready	May 14, 2020, 00:00:15	Renew Renew and Change Specification Temporary Upgrade Unbind 



3. Click Unbind in the Actions column.
4. In the displayed dialog box, click OK.

You can also click the SAG instance ID, and then click Network Configuration on the SAG instance details page. On the Network Instance Details tab page, click Unbind in the Actions column.

1.6.5 Add an ECC link

This topic describes how to add an Express Cloud Connect (ECC) link to a Smart Access Gateway (SAG) instance. By adding an ECC link, you can connect to Alibaba Cloud at a high speed with improved reliability and security.

Procedure


1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway. On the displayed Smart Access Gateway page, find the target SAG instance, and click  in the Network Type column.
3. Click  in the Actions column and then click Add ECC link.
4. On the Express Cloud Connect page, apply for the ECC service. For more information, see [#unique_47](#).

More information
[#unique_48](#)

1.6.6 Add an Internet link

This topic describes how to add an Internet link. After you connect an on-premises data center to Alibaba Cloud by using an ECC link, you can purchase an Internet link and use it as a standby link to improve the reliability of your service. Also, you can configure latency-sensitive service to the ECC link and other services to the Internet link by using load balancing routing to reduce costs.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway. On the Smart Access Gateway page, find the target SAG instance and click  in the Network Type column.
3. Click Add Internet link in the Actions column.

4. On the Smart Access Gateway Bandwidth page, select a region, enter an instance name, set the peak bandwidth, and select a validity period for the instance.
5. Check the purchase information and click Buy Now.
6. On the Confirm Order page, click Pay.
7. On the Pay page, click Pay.

More information

[#unique_47](#)

1.7 Access to cloud services

1.7.1 Overview of accessing cloud services

PrivateZone is a VPC-based resolution and management service for private domain names. Networks attached to CEN can access the PrivateZone service through CEN. For more information, see [#unique_15](#).

1.7.2 Set AnyTunnel services

If you need to access the cloud services deployed in a VPC through a network in Cloud Enterprise Network (CEN), you need to set domain names for the services, the regions of the services, and the access region. Cloud services are the Alibaba Cloud products that are deployed in VPCs and use AnyTunnel addresses (100.64.0.0/10) to provide services, such as OSS, log service, and DNS.

Prerequisites

Make sure that the host region and the access region have networks (VPC, VBR, or CCN) attached to CEN.

Procedure

1. Log on to the [CEN console](#).
2. Click the ID of the target CEN instance.
3. Click the AnyTunnel tab, and then click SetAnyTunnelService.

4. In the SetAnyTunnelService dialog box, set the following parameters:

- a) Domain Name or IP: Enter the intranet domain name or IP address of the cloud service to be accessed.

For example, if you want to access the OSS service deployed in Hangzhou, enter

`oss - cn - hangzhou - internal . aliyuncs . com` , or the IP address or CIDR block of the OSS service, for example, 100.64.0.1 or 100.64.1.0/24.

- b) Host Region: Select the region to which the cloud service to be accessed belongs.



Note:

Make sure that the host region is the same as the region specified for the intranet domain name.

- c) Access Region: Select the region where the access is initiated.



Note:

Make sure that the network in the access region has been attached to the CEN instance.

- d) Click OK.

1.7.3 Set PrivateZone access

PrivateZone is a VPC-based resolution and management service for private domain names. Networks in a Cloud Enterprise Network (CEN) instance can access the PrivateZone service through CEN.

Prerequisites

Make sure that the host region and access region have networks (VPC, VBR, and CCN) attached to the CEN instance.

Procedure

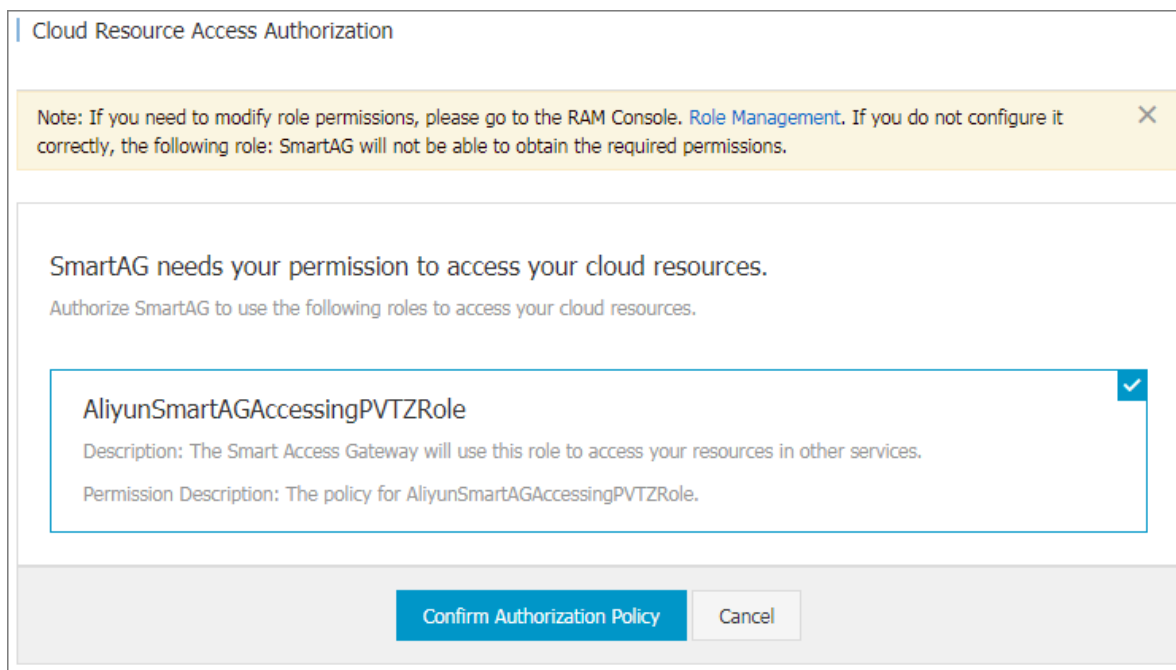
1. Log on to the [CEN console](#).
2. Click the ID of the target CEN instance.
3. Click the PrivateZone tab, and then click Authorization.



Note:

You need to grant permissions to Smart Access Gateway only for the first time you configure PrivateZone access.

4. In the Cloud Resource Access Authorization dialog box, click **Confirm Authorization Policy** to allow local branches associated with a CCN (a component of Smart Access Gateway) in the CEN instance to access PrivateZone.



Cloud Resource Access Authorization

Note: If you need to modify role permissions, please go to the RAM Console. [Role Management](#). If you do not configure it correctly, the following role: SmartAG will not be able to obtain the required permissions.

SmartAG needs your permission to access your cloud resources.
Authorize SmartAG to use the following roles to access your cloud resources.

AliyunSmartAGAccessingPVTZRole ✓

Description: The Smart Access Gateway will use this role to access your resources in other services.
Permission Description: The policy for AliyunSmartAGAccessingPVTZRole.

Confirm Authorization Policy Cancel

5. Click **Set Private Zone** and then in the **Set Private Zone** dialog box, set the following parameters:

- Host Region:** Select the region to which the VPC configured with PrivateZone belongs.
- Host VPC:** Select the VPC that is configured with PrivateZone.

The PrivateZone service can be selected only by selecting the VPC in the host region.

- Access Region:** Select the region where the access is initiated.



Note:

- The access region can be CCN, or the same region as the host region. Make sure that the network in the selected access region has been attached to the CEN instance.
- If you select a CCN instance and the CCN instance account is different from that of the VPC instance or CEN instance, you must authorize the instance. For more information, see [#unique_16](#).

- Click **OK**.

1.7.4 Grant permissions to CCN

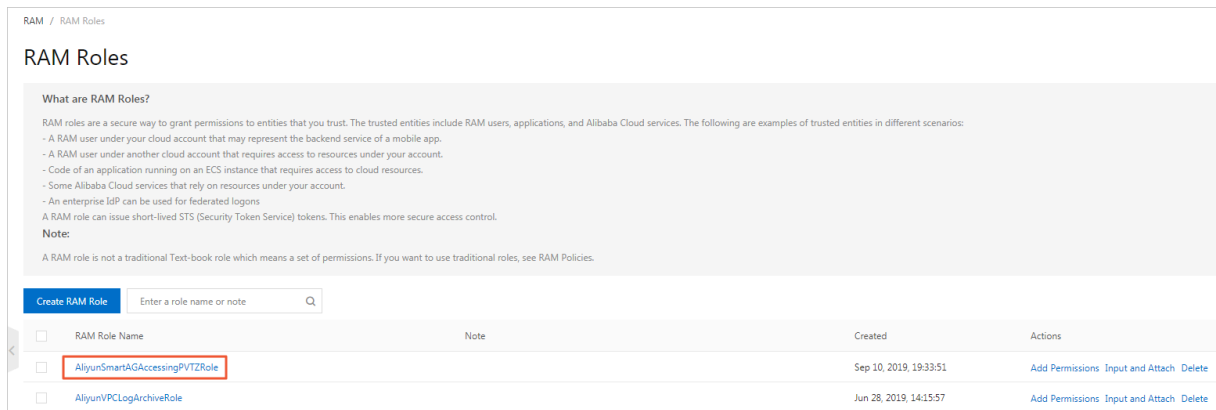
If you need to access the PrivateZone service through local branches of a Cloud Connect Network (CCN) in a Cloud Enterprise Network (CEN) instance, you must grant permissions to the CCN.

Same CEN, VPC, and CCN account

If the CCN, the VPC that is configured with PrivateZone, and the CEN instance all belong to the same account, you need to click **Authorization** on the PrivateZone tab, and grant permissions to CCN by following the prompts. The following table provides example information of this scenario.

Resource	User ID
CEN	111111
VPC	111111
CCN	111111

After you grant permissions to the CCN, the system automatically creates a RAM role named `AliyunSmartAGAccessingPVTZRole`. You can view the RAM role on the RAM Roles page of the [RAM console](#).



Same CEN and VPC account, but different CCN account

If the CEN instance and the VPC that is configured with PrivateZone belong to the same account, but the CCN belongs to a different account, you need to modify the authorization policy. The following table provides example information of this scenario.

Resource	User ID
CEN	111111

Resource	User ID
VPC	111111
CCN	333333

To grant permissions to the CCN, follow these steps:

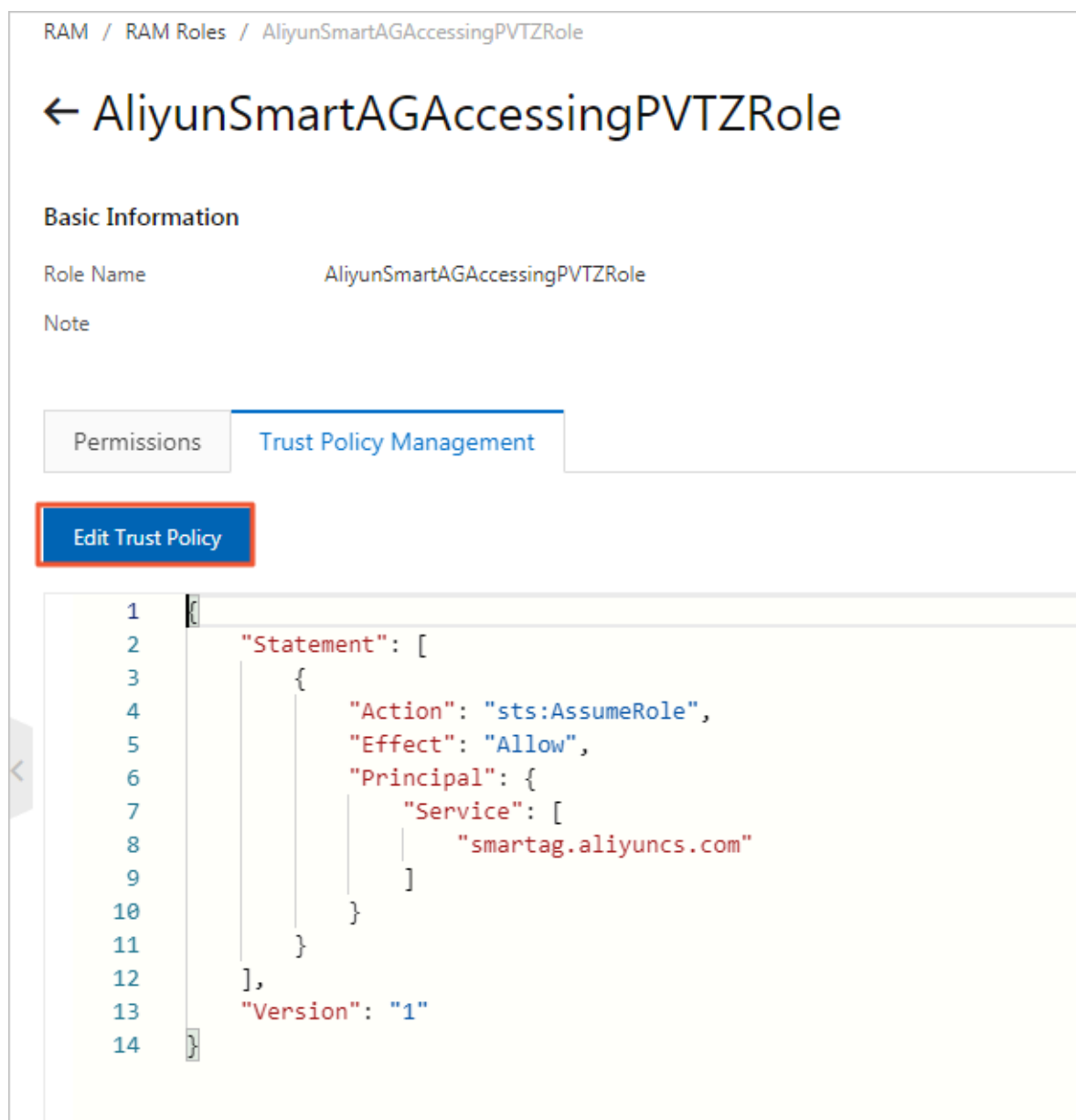


Notice:

You need to use the account to which the VPC belongs.

1. Log on to the [CEN console](#).
2. Click the ID of the target CEN instance.
3. Click the PrivateZone tab, and then click Authorization. Grant permissions to the CCN by following the prompts.
4. Go to the [RAM console](#).
5. In the left-side navigation pane, click RAM Roles.
6. In the search box, enter AliyunSmartAGAccessingPVTZRole and click the displayed role name.

7. Click the Trust Policy Management tab and then click Edit Trust Policy.



8. In Service , add a record of account ID of the CCN@smartag.aliyuncs.com and click OK.

Same CCN and VPC account, but different CEN account

If the CCN and the VPC that is configured with PrivateZone belong to the same account, but the CEN instance belongs to a different account, you need to create a RAM role and grant it permissions by using the account of the VPC. The following table provides example information of this scenario.

Resource	User ID
CEN	333333

Resource	User ID
VPC	111111
CCN	111111

To grant permissions to the CCN, follow these steps:

1. Log on to the [RAM console](#) by using the credentials of the account to which the VPC belongs.
2. In the left-side navigation pane, click RAM Roles.
3. Click Create RAM Role, configure it by referring to the following description, and then click OK.
 - Select type of trusted entity: Select Alibaba Cloud Service.
 - Select Trusted Service: Select smartag Smart Access Gateway.
 - RAM Role Name: Enter AliyunSmartAGAccessingPVTZRole.
4. Click the created RAM role name.
5. On the Permissions tab, click Add Permissions.
6. In the search box, enter pvtz and click the displayed AliyunPvtzReadOnlyAccess policy.

Add Permissions

Principal

AliyunPvtzReadOnlyAccess@role.aliyun-document.onaliyunservice.com

Select Policy

System Policy

pvtz

Selected (0)

Clear

Policy Name	Note
AliyunPvtzFullAccess	Provides full access to Cloud DNS Private Zone via Management Console.
AliyunPvtzReadOnlyAccess	Provides read-only access to Cloud DNS Private Zone via Management Console.

7. Go back to the RAM role details page, and click the Trust Policy Management tab to view the permission information.

RAM / RAM Roles / AliyunPvtzReadOnlyAccess

← AliyunPvtzReadOnlyAccess

Basic Information

Role Name	AliyunPvtzReadOnlyAccess	Created	Feb 15, 2019, 17:22:42
Note		ARN	acs:ram::1231579085529123:role/aliyunpvtzreadonlyaccess

Permissions Trust Policy Management

Edit Trust Policy

```
1 {
2   "Statement": [
3     {
4       "Action": "sts:AssumeRole",
5       "Effect": "Allow",
6       "Principal": {
7         "Service": [
8           "smartag.aliyuncs.com"
9         ]
10      }
11    }
12  ],
13  "Version": "1"
14 }
```

Three different accounts

If the CCN, the VPC that is configured with PrivateZone, and the CEN instance belong to three different accounts, you need to complete the following tasks:

Resource	User ID
CEN	111111
VPC	222222
CCN	333333

1. Use the account of the VPC to create a RAM role and grant it permissions. For more information, see [Same CCN and VPC account, but different CEN account](#).

RAM / RAM Roles / AliyunPvtzReadOnlyAccess

← AliyunPvtzReadOnlyAccess

Basic Information

Role Name	AliyunPvtzReadOnlyAccess	Created	Feb 15, 2019, 17:22:42
Note		ARN	acs:ram::1231579085529123:role/aliyunpvtzreadonlyaccess

Permissions Trust Policy Management

Edit Trust Policy

```
1 {
2   "Statement": [
3     {
4       "Action": "sts:AssumeRole",
5       "Effect": "Allow",
6       "Principal": {
7         "Service": [
8           "smartag.aliyuncs.com"
9         ]
10      }
11    }
12  ],
13  "Version": "1"
14 }
```

2. Use the account of the VPC to modify the policy associated with the corresponding RAM role by adding the CCN service in the format of `CCN account ID @`

aliyuncs . com . For more information, see [Same CEN and VPC account, but different CCN account](#).



To allow multiple CCNs to access the PrivateZone service, add all the CCNs to the trust policy, as shown in the following figure.

Resource	User ID
CEN	111111
VPC	222222
CCN	333333
CCN	444444
CCN	555555

Edit Trust Policy

×

RAM Role Name

AliyunSmartAGAccessingPVTZRole

```
1  {
2    "Statement": [
3      {
4        "Action": "sts:AssumeRole",
5        "Effect": "Allow",
6        "Principal": {
7          "Service": [
8            "smartag.aliyuncs.com",
9            "333333@smartag.aliyuncs.com",
10           "444444@smartag.aliyuncs.com",
11           "555555@smartag.aliyuncs.com"
12         ]
13       }
14     ]
15   },
16   "Version": "1"
```

2 SAG Monitoring

2.1 View the monitoring data of an SAG instance

This topic describes how to view the monitoring data of an SAG instance by using the CloudMonitor service.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or click View Monitoring in the Actions column.
3. In the left-side navigation pane of the SAG instance details page, click Monitoring.
4. View the monitoring data of the SAG instance.

The following table describes the monitoring metrics of the SAG instance.

Metric	Description
Traffic Trends	
Bandwidth	The following data is displayed: <ul style="list-style-type: none">· Inbound bandwidth (bit/s): the traffic consumed to access the SAG from the Internet.· Outbound bandwidth (bit/s): the traffic consumed by the SAG to access the Internet.
Packets	The following data is displayed: <ul style="list-style-type: none">· Incoming packets (packet/s): the number of request packets that the SAG receives per second.· Outgoing packets (packet/s): the number of packets sent by the SAG per second.
Packet loss	Packet loss (packet/s): the number of dropped packets per second.
Detection Trends	
Latency	Detected latency (ms): the response latency of the link test.
Packet loss	Detected lost packets (packet/s): The number of dropped packets per second in the link test.

2.2 Create an event alert

You can set alarm rules for system events of a Smart Access Gateway (SAG) device on the CloudMonitor console. In this way, you can be notified of any system events that occur in a timely manner.

Procedure

1. Log on to the [CloudMonitor console](#).
2. In the left-side navigation pane, click Event Monitoring.
3. On the Event Monitoring page, click the Alarm Rules tab.
4. Click Create event alerts to set the event information to receive and the contact.

If a contact is selected, the contact will be informed of events occurred to instances under the account. If an application group is selected, contacts associated with the application group will be informed of events occurred to instances in the group.

System events of an SAG device include the following:

Type	Name	Description
Event	DeviceOnline	#unique_58
	AccessGatewayFailover	#unique_59
	DeviceWanLinkUp	#unique_60
	DeviceWanLinkSwitched	#unique_61
Alert	DeviceHacked	#unique_62
	DeviceLinkDown	#unique_63
	DeviceSwitched	#unique_64
	DeviceOffline	#unique_65
	DeviceWanLinkDown	#unique_66
	ConnectionDisconnect	#unique_67

2.3 Event protocols

2.3.1 AccessGatewayFailover

The AccessGatewayFailover event indicates that the active IPSEC link of the Smart Access Gateway has failed.

Alarm information

Event name	Event level	Status code	Status description
AccessGatewayFailover	INFO	agwfailover	Access Gateway Failover

Causes

The IPSEC link has failed.

Actions

No action is required.

2.3.2 DeviceWanLinkSwitched

The DeviceWanLinkSwitched event indicates that a switchover occurs between the broadband link and the 4G link. This event is only supported by SAG-100WM.

Alarm information

Event name	Event level	Status code	Status description
DeviceWanLinkSwitched	CRITICAL	WanLinkSwitched	Device Wan Link Switched

Causes

The active link failed and traffic is switched to the standby link.

Actions

No action is required.

2.3.3 DeviceOnline

The DeviceOnline event indicates that the Smart Access Gateway is online.

Alarm information

Event name	Event level	Status code	Status description
DeviceOnline	INFO	online	Device Online

Causes

The Smart Access Gateway is online.

Actions

No action is required.

2.3.4 DeviceWanLinkUp

The DeviceWanLinkUp event indicates that a broadband link or 4G link recovers. This event is only supported by SAG-100WM.

Alarm information

Event name	Event level	Status code	Status description
DeviceWanLinkUp	INFO	WanLinkUp	Device Wan Link Up

Causes

The link has recovered.

Actions

Determine whether to switch to the recovered link.

2.3.5 DeviceOffline

The DeviceOffline event indicates that the Smart Access Gateway is offline.

Alarm information

Event name	Event level	Status code	Status description
DeviceOffline	CRITICAL	offline	Device Offline

Causes

The egress of the Smart Access Gateway to the Internet is disabled, or the Smart Access Gateway is powered off.

Actions

Follow these actions:

1. Check the egress to the Internet.

If you use a laptop to access the Internet, check whether you can visit the official website of Alibaba Cloud.

2. Check whether the Smart Access Gateway is powered off.

2.3.6 ConnectionDisconnect

The ConnectionDisconnect event indicates that the active and standby IPSEC links of the Smart Access Gateway have failed.

Alarm information

Event name	Event level	Status code	Status description
Connection Disconnect	CRITICAL	disconnect	Connection Disconnected

Causes

Both the active and standby IPSEC links of the Smart Access Gateway have failed.

Actions

Check whether the service provider network at the customer side is normal.

2.3.7 DeviceSwitched

The DeviceSwitched event indicates that a switchover has occurred between the active device and the standby device.

Alarm information

Event name	Event level	Status code	Description
DeviceSwitched	CRITICAL	switched	Device Role Changed

Causes

- The active Smart Access Gateway has failed.

- The OSPF neighbor of the active Smart Access Gateway has failed.

Actions

No action is required.

2.3.8 DeviceLinkDown

The DeviceLinkDown event indicates that the branch-side OSPF neighbor or the static route link has failed.

Alarm information

Event name	Event level	Status code	Status description
DeviceLink Down	CRITICAL	linkdown	Device Link State Change

Causes

- The customer-side switch has failed.
- The customer-side switch is incorrectly configured.
- The connection between the customer-side switch and the Smart Access Gateway has failed.

Actions

Check the customer-side switch. For more information, see [#unique_77](#).

2.3.9 DeviceWanLinkDown

The DeviceWanLinkDown event indicates that the broadband link or the 4G link has failed. This event is only supported by SAG-100WM.

Alarm information

Event name	Event level	Status code	Status description
DeviceWanLinkDown	CRITICAL	WanLinkDown	Device Wan Link Down

Causes

A link failure has occurred.

Actions

If the active and standby links are enabled, no action is required.

2.3.10 DeviceHacked

The DeviceHacked event indicates that the Smart Access Gateway has been attacked.

Alarm information

Event name	Event level	Status code	Status description
DeviceHacked	CRITICAL	hacked	Device Hacked

Causes

The serial number of the Smart Access Gateway is stolen.

Actions

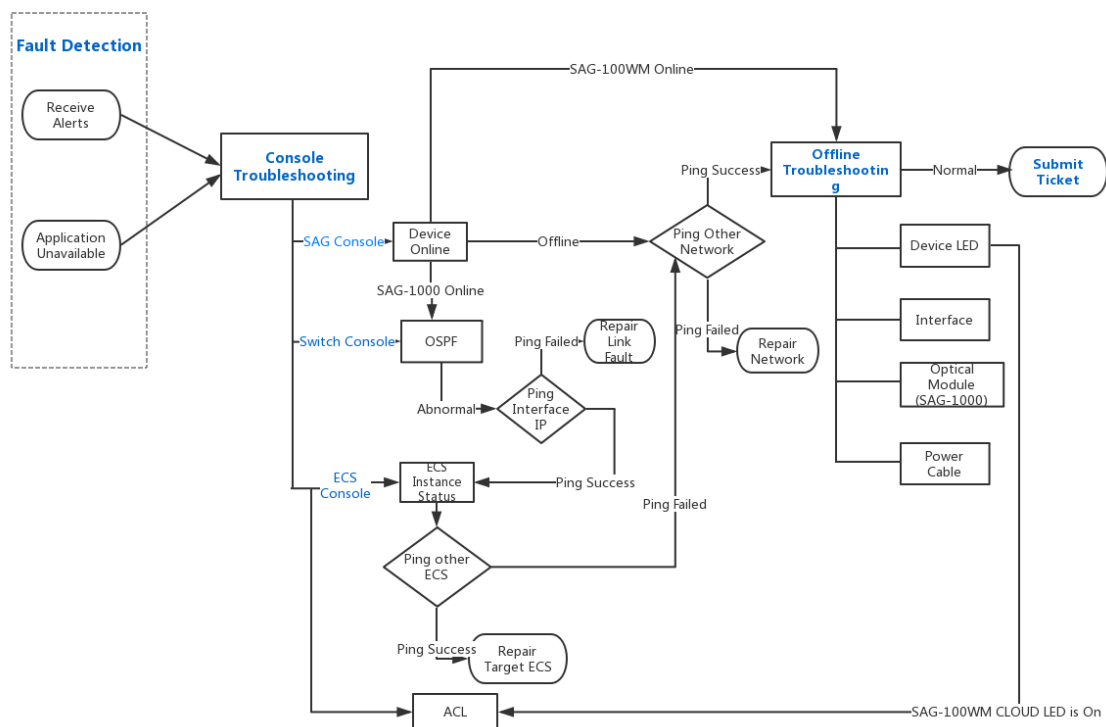
Open a ticket.

3 SAG Troubleshooting

3.1 Troubleshooting process

When a network failure occurs to the Smart Access Gateway (SAG) device, you need to troubleshoot according to the alert information and other information of the device.

The troubleshooting flow diagram is as follows:



SAG-100WM troubleshooting process

If you access Alibaba Cloud through a SAG-100B device, the troubleshooting process is as follows. For more information, see [#unique_82](#):

1. You receive an alert or find that the application is not available.
2. Log on to the Smart Access Gateway console to check the device status.
3. Visit other websites to check the status of the service provider network.
4. Troubleshoot the SAG device.
5. Check security group rule configurations.
6. Open a ticket.

SAG-1000 troubleshooting process

If you access Alibaba Cloud through an SAG-1000 device, the troubleshooting process is as follows. For more information, see [#unique_83](#) and [#unique_84](#):

1. You receive an alert or find that the application is not available.
2. Log on to the Smart Access Gateway console to check the device status.
3. Log on to the switch console to check the OSPF data link status.
4. Log on to the ECS console to check the status of the target instance.
5. Visit other websites to check the status of the service provider network.
6. Troubleshoot the device.
7. Open a ticket.

3.2 SAG status

3.2.1 SAG indicators

This topic identifies the indicators associated with the Smart Access Gateway (SAG).

You can check the status of a Smart Access Gateway (SAG) by checking its indicators.

SAG model	Indicator	Status description
SYS (system indicator)	If the indicator is on, the system runs normally. After you press the RST key (Reset key), the indicator goes off.	
SAG-100WM	LTE	Indicates whether the SAG communication is normal. <ul style="list-style-type: none">· On: The SAG is registered on the network.· Flashing: Data is being transmitted.· Off: The SAG is not registered on the network.

SAG model	Indicator	Status description
	WAN	Indicates the Ethernet status of the SAG. <ul style="list-style-type: none"> On: The SAG is connected to the network through the Ethernet. Flashing: Data is being transmitted. Off: The SAG is not connected to the Ethernet.
	WIFI	Indicates the Wi-Fi connection status of the SAG. <ul style="list-style-type: none"> On: The WLAN is enabled. Flashing: Data is being transmitted. Off: The WLAN is not enabled.
	RUN	Indicates the status of the SAG. <ul style="list-style-type: none"> On: The SAG is powered on. Flashing: The system operates normally. Off: The SAG is powered off.
	CLOUD	Indicates whether the SAG is connected to Alibaba Cloud. <ul style="list-style-type: none"> Flashing: The SAG is connected to Alibaba Cloud. Flashing quickly: The SAG is restoring the default settings or restoring the system. Off: The SAG is not connected to Alibaba Cloud.
SAG-1000	Power supply	On: The SAG is powered on.
	Alarm	The alarm indicator has the following statuses: <ul style="list-style-type: none"> Green: The SAG operates normally. Yellow: A fault has occurred.
	Cloud	The alarm indicator has the following statuses: <ul style="list-style-type: none"> Green: The connection to the cloud is normal. Yellow: The connection to the cloud is faulty.

3.2.2 View the status of an SAG device

This topic describes how to view the status of a Smart Access Gateway (SAG) device in the Smart Access Gateway console.

Procedure

1. Log on to the [Smart Access Gateway console](#).

2. Click the ID of the target SAG instance, and then view the SAG status on the SAG instance details page.

The SAG can be in one of the following states:

- Ready: The SAG is normal.
- Offline: The SAG is not connected to the controller.
- Not bound: The SAG is not associated with a CCN instance.
- Ordered: The SAG has been ordered but has not been shipped.
- Shipped: The SAG has been shipped.
- Locked: The fee associated with the SAG is overdue.

3.2.3 View the link status of an SAG instance

This topic describes how to view the link status of a Smart Access Gateway (SAG) instance in the Smart Access Gateway console. If a link failure occurs, you can conduct a link switchover.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Click the ID of the target SAG instance, and then view the link status on the SAG instance details page.
 - Green indicator: The link is normal.
 - Red indicator: The link has failed. You can click Switch to switch the failed link to a normal link.

3.2.4 View the OSPF status

This topic describes how to view your OSPF status by using the switch console. In case of a connection failure, you can view your OSPF status to check the connectivity between the Smart Access Gateway (SAG) and the switch.

Procedure

1. Run the following command to log on to the switch console:

```
telnet switch IP
```

2. Run the following command to check the status of the OSPF neighbor:

```
show ip ospf neighbor
```

The system output is displayed as follows. Check the value of `State`.

```
OSPF process 1, 8 Neighbors, 8 is Full :
Neighbor ID Pri State BFD State
Dead Time Address Interface
10.10.10.10 0 Full / - -
00:00:10 192.168.10.5 GigabitEthernet 0 / 13
10.10.10.10 0 Full / - -
00:00:10 192.168.10.21 GigabitEthernet 0 / 46
```

3. Run the following command to check OSPF configurations:

```
configure terminal
router ospf
show this
```

The system output is displayed as follows. Check the `area` and the IP address of the network:

```
Building configuration ...
!
router id 1.1.1.1
area 1 nssa translator always default-information originate no-summary
area 2 nssa translator always default-information originate no-summary
area 3 nssa translator always default-information originate no-summary
area 17 nssa translator always default-information originate no-summary
area 18 nssa translator always default-information originate no-summary
area 81 nssa translator always default-information originate no-summary
area 90 nssa translator always default-information originate no-summary
area 91 nssa translator always default-information originate no-summary
network 192.168.10.0 0.0.0.3 area 1
network 192.168.10.4 0.0.0.3 area 1
network 192.168.10.20 0.0.0.3 area 1
network 192.168.20.0 0.0.0.3 area 2
network 192.168.20.4 0.0.0.3 area 2
network 192.168.30.0 0.0.0.3 area 0
network 192.168.67.0 0.0.0.3 area 81
network 192.168.67.4 0.0.0.3 area 81
network 192.168.68.4 0.0.0.3 area 81
network 192.168.68.16 0.0.0.3 area 81
network 192.168.90.0 0.0.0.3 area 90
network 192.168.90.4 0.0.0.3 area 90
network 192.168.91.0 0.0.0.3 area 91
network 192.168.91.4 0.0.0.3 area 91
network 192.169.17.0 0.0.0.3 area 17
```

```

network 192 . 169 . 17 . 4 0 . 0 . 0 . 3 area 17
network 192 . 169 . 18 . 0 0 . 0 . 0 . 3 area 18
network 192 . 169 . 18 . 4 0 . 0 . 0 . 3 area 18
!
end

```

4. Run the following command to check the interface status of the connected SAG:

```
show ip interface brief
```

- up : The interface is normal.
- administratively down : Shutdown is configured on the interface. Run the no shutdown command to enable shutdown.
- down : The network cable is not connected properly. Check the network cable connection.

The system output is displayed as follows:

Interface	Address (Sec)	Status	IP - Address (Pri)	IP - Protocol
GigabitEthernet	0 / 2	no address	down	down
GigabitEthernet	0 / 7	up	192 . 168 . 2 . 7 / 24	up
GigabitEthernet	0 / 11	down	9 . 9 . 9 . 1 / 24	down
GigabitEthernet	0 / 12	up	192 . 168 . 11 . 2 / 24	up
GigabitEthernet	0 / 13	up	192 . 168 . 10 . 6 / 30	up
GigabitEthernet	0 / 15	up	192 . 168 . 40 . 2 / 24	down
GigabitEthernet	0 / 20	up	192 . 168 . 30 . 1 / 30	up
GigabitEthernet	0 / 22	up	192 . 168 . 20 . 2 / 30	up
192 . 169 . 81 . 2 / 30		up	192 . 168 . 12 . 2 / 24	
GigabitEthernet	0 / 23	up	192 . 168 . 20 . 6 / 30	up
192 . 169 . 81 . 6 / 30		up	192 . 169 . 80 . 2 / 30	up
GigabitEthernet	0 / 27	up	192 . 169 . 80 . 6 / 30	up
GigabitEthernet	0 / 28	up	192 . 169 . 17 . 2 / 30	up
GigabitEthernet	0 / 29	up	192 . 168 . 170 . 2 / 30	up
192 . 168 . 170 . 2 / 30		up	192 . 169 . 17 . 6 / 30	up
GigabitEthernet	0 / 30	up	192 . 168 . 67 . 6 / 30	down
GigabitEthernet	0 / 33	down	192 . 168 . 68 . 6 / 30	down
GigabitEthernet	0 / 35	up	192 . 169 . 18 . 2 / 30	up
GigabitEthernet	0 / 36	up	192 . 169 . 18 . 6 / 30	up
GigabitEthernet	0 / 37	up	192 . 168 . 90 . 2 / 30	down
192 . 169 . 90 . 2 / 30		down		

```

192 . 168 .
90 . 29 / 30
GigabitEth ernet 0 / 38
192 . 169 . 90 . 6 / 30 down
GigabitEth ernet 0 / 39
192 . 169 . 91 . 2 / 30 administatively down
down
192 . 168 .
91 . 29 / 30
GigabitEth ernet 0 / 40
192 . 169 . 91 . 6 / 30 up
GigabitEth ernet 0 / 43 up
no address up
GigabitEth ernet 0 / 45
no address down
GigabitEth ernet 0 / 46
no address up
GigabitEth ernet 0 / 48
no address down
Loopback 0 no address no
address up down
VLAN 1 no address no
address up down
VLAN 4
no address up
VLAN 19
no address up
VLAN 47
no address up
VLAN 148
no address up
192 . 168 . 41 . 1 / 24
192 . 168 . 19 . 2 / 30
192 . 168 . 140 . 2 / 24
172 . 16 . 18 . 1 / 24

```

5. Run the following command to check whether the OSPF negotiation time and authentication parameter values match those configured on the SAG:

```

interface GigabitEth ernet 0 / 39
show this

```

Check whether the values of the `ospf authentication` and `ospf message - digest - key` parameters match those configured on the SAG. If not, the SAG has not completed authentication and the neighbor cannot be established.

The system output is displayed as follows:

```

Building configuration ...
!
poe enable
no switchport
ip ospf network point-to-point
ip ospf authentication message-digest
ip ospf message-digest-key 23 md5 888
ip ospf hello-interval 3
ip ospf dead-interval 10
ip ospf priority 0
no ip proxy-arp
ip address 192 . 168 . 91 . 2 255 . 255 . 255 . 252
ip address 192 . 169 . 91 . 2 255 . 255 . 255 . 252
secondary

```

```
ip address 192 . 168 . 91 . 29 255 . 255 . 255 . 252
secondary
!
end2 secondary
```

3.3 System maintenance

3.3.1 Restart an SAG device

This topic describes how to restart a Smart Access Gateway (SAG) device. If a network failure occurs when an SAG device is active, you can restart the device to eliminate any software faults that may be causing the network failure.

You can restart an SAG device by using either of the following methods:

- Power off the device and then power it on. We recommend that you save your current configurations before power off the device.
- Log on to the Smart Access Gateway console to restart the device remotely.


Power off the device and then power it on

Power off the device and then power it on to restart the device. This method is also called cold restart.

For some SAG models, the power switch is on the left of the front panel or on the right of the rear panel. For other SAG models, no power switch is provided. For SAG devices without a power switch, you can remove or connect the power plug to power off or power on the device.

Restart an SAG device remotely

To restart an SAG device remotely by using the Smart Access Gateway console, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID, or choose  > Manage Device in the Actions column.


3. Select the target SAG, and then click Remote Restart.

4. In the displayed dialog box, click OK.

3.3.2 Update the software of an SAG device

This topic describes how to update the software of a Smart Access Gateway (SAG) device in the SAG console. We recommend that you update your software in off-peak hours to avoid possible network disconnections.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or choose  > Manage Device.
3. In the left-side pane of the SAG instance details page, click Device Management.
4. Select the device whose software you want to update, and then click Update Version.
5. In the Update Version dialog box, select the target version and view the description of previous versions.



Note:

We recommend that you update your software to the latest version. The update takes about 10 minutes.

Update Version

提示说明

The current version is 1.5.0. The latest version is 1.7.0. We recommend that you update your device to the latest version. The update may take a few minutes and cause network disconnections. Update your device during the off-peak hours of your business.

Select Version

* Select Target Version

1.5.0

Version Description

> 1.7.0 Release Notes

> 1.6.0 Release Notes

> 1.5.0 Release Notes

> 1.4.1 Release Notes

> 1.4.0 Release Notes

> 1.3.0 Release Notes

Contact Us

6. Click OK.

3.4 Hardware troubleshooting

3.4.1 Locate the cause of power failure

You can locate and troubleshoot the cause of a power failure according to the following method.

Procedure

1. Measure the input voltage. Use a multimeter to measure the input voltage, and determine if the input voltage is abnormal according to the working voltage range of the power adapter.
2. Re-connect the power adapter. Disconnect and reconnect the power adapter and the power cable and then check if the gateway device can be powered on.
3. Cross-validate the power adapter against other power adapters. Use the gateway device with other power adapters to cross-check where any causes of power failure occur.
 - If the power adapter is considered faulty, send it back to the manufacturer for repair.
 - If the gateway device is considered faulty, please open a ticket for further consultation.

3.4.2 The SAG cannot be powered on

Symptoms

The SYS indicator and the power supply indicator of the Smart Access Gateway (SAG) are off.

Causes

- The power switch of the SAG is turned off.
 - The power cable connection is loose.
 - The power supply of the SAG is faulty.
 - The power adapter on the SAG is faulty.
1. Check whether the power switch is turned on.
 2. Check whether the power cable is connected securely.
 3. Check whether the power supply is faulty.

Use a normal power supply instead and check whether the SAG can be powered on.

4. Check whether the power adapter is faulty.

Use a normal power adapter instead and check whether the SAG can be powered on

.

5. If the problem persists, open a ticket for technical support.

3.4.3 The optical module is faulty

This topic explains why an optical module fault occurs and how to troubleshoot it.

Symptoms

After the SAG is connected to an optical module, the interface indicator is not lit green.

Causes

The optical module is incompatible with the SAG or is damaged.

SAGs support optical modules of the following models:

- FORMERICAOE TSD-S1CH1-C11(1.25GB SR 550m 3.3V)
- FORMERICAOE TSD-S2CA1-F11(1.25GB LX 10Km 3.3V)
- Eoptolink EOLS-8512--02-D (1000BASE-SX 850nm)
- Eoptolink EOLS-1312--10-D (1000BASE-LX 1310nm)
- FINISAR FTLF1318P3BTL (1000BASE-LX1310nm)
- H3C SFP-GE-SX-MM850-A (1000BASE-SX 850nm)
- HUAWEI SFP-GE-SX-MM850 (1000BASE-SX 850nm)
- Gigalight GSS-MDO100-007CO (10G SFP+_SFP+AOC Cable 7M)
- H3C SFP-1000BaseT (1250Mbps-100m-RJ45-xx-SFP)
- HUAWEI SFP-1000BaseT (SFP-1000BASE-T-RJ45-100m)

1. Check the sending port on the left of the optical module. If a red laser is visible, the module is operating normally. Do not look directly into the sending port.

Single-mode optical modules give out invisible light. You can use a jumper to connect the sending port and the receiving port. If the status indicator is on, the optical module is operating normally.

2. If the fault persists, make sure that the optical module is compatible with the SAG.

3.4.4 The Ethernet interface cannot be connected

This topic explains why the Ethernet interface cannot be connected and how to troubleshoot it.


Symptoms

The Ethernet interface cannot be physically connected.

Causes

- The devices are not powered on or the cable is incorrectly connected.
 - The twisted pair or the optical fiber is too long or the link loss is too high.
 - A fault has occurred to the interfaces, interface modules, or devices.
1. Check whether the local and peer devices are powered on and whether the cables and modules are connected correctly.
 2. Check whether the links and interface modules of the devices are faulty.

If the devices are connected by a twisted pair, check the items listed in the following table.

Check item	Criteria	Action
Check whether the twisted pair is faulty.	The twisted pair is normal.	Replace the twisted pair if it is faulty.
Check whether the length of the twisted pair between the two devices meets requirements.	<p>The length of the cable between the two devices is less than 100 meters.</p> <div> Note: For 10/100/1000-M electrical interfaces, RJ45 connectors and category 5 twisted pair cables (or higher) are used, with a transmission distance of 100 meters.</div>	<p>If the cable is longer than 100 meters, use the following methods:</p> <ul style="list-style-type: none">· Shorten the distance between the devices to shorten the length of the twisted pair.· If the distance between the devices cannot be changed, the devices can be connected in series through a repeater , hub, or switch.

Check item	Criteria	Action
Check whether the twisted pair is used correctly.	<p>Twisted pairs are classified into straight-through twisted pairs and crossover twisted pairs.</p> <p>Straight-through twisted pairs are used to connect Ethernet interfaces between the following devices:</p> <ul style="list-style-type: none"> • A router and a hub • A router and an Ethernet switch • A computer and an Ethernet switch • A computer and a hub <p>Crossover twisted pairs are used to connect Ethernet interfaces between the following devices:</p> <ul style="list-style-type: none"> • Two routers • A router and a computer • A hub and a hub • A hub and a switch • Two switches • Two computers 	If the type of twisted pair used is incorrect, change it to the correct type.

If the devices are connected through an optical fiber, check the items listed in the following table.

Check item	Criteria	Action
Check whether the optical module corresponds to the optical fiber.	<p>Check whether the optical module matches the optical fiber according to the following information:</p> <ul style="list-style-type: none"> • A multi-mode optical fiber can be used with a multi-mode optical module. • A single-mode optical fiber can be used with a single-mode optical module, but cannot be used with a multi-mode optical module. Single-mode optical fibers are yellow and multi-mode optical fibers are orange. • The wave length of two connected optical modules must be consistent. 	If the optical fiber and the optical module do not match, replace the optical module or the optical fiber as needed.
Check whether the length of the optical fiber matches the transmission distance supported by the optical module.	The length of the optical fiber must be shorter than the transmission distance supported by the optical module.	Shorten the length of the optical fiber or use an optical module that supports greater transmission distance.
Check whether the signal attenuation is within the allowed range.	The range of optical signal attenuation is less than - 28 dB.	If the attenuation exceeds the allowed range, replace the optical fiber. If the problem persists, shorten the length of the optical fiber.

Check item	Criteria	Action
Check whether the two ends of the link are faulty by using the loopback method or a tester.	<p>If you use a tester, the results indicate that the sending and the receiving data flows are normal.</p> <p>If you use the loopback method, the interface is in the up state after you connect the two ends of the optical fiber to an optical module.</p>	If a cable is faulty, replace the cable. If the fault persists, replace the optical modules at the two ends.

3. Check whether the hardware of the local device and the peer device is faulty.

3.4.5 The Ethernet interface frequently goes up or down

This topic explains why the Ethernet interface frequently goes up or down and how to troubleshoot it.

Symptom

The Ethernet interface frequently goes up or down.


Causes

- The cable is incorrectly connected.
- The twisted pair or the optical fiber is too long or the link loss is too high.
- A fault has occurred to the interfaces, interface modules, or devices.

1. Check whether the cable and modules of the local and peer devices are connected correctly.
2. Check whether the links and interface modules of the devices are faulty.

If the devices are connected by a twisted pair, check the items listed in the following table.

Check item	Criteria	Action
Check whether the twisted pair is faulty.	The twisted pair is normal.	Replace the twisted pair if it is faulty.

Check item	Criteria	Action
Check whether the length of the twisted pair between the two devices meets requirements.	<p>The length of the cable between the two devices is less than 100 meters.</p> <div> Note: For 10/100/1000-M electrical interfaces, RJ45 connectors and category 5 twisted pair cables (or higher) are used, with a transmission distance of 100 meters.</div>	<p>If the cable is longer than 100 meters, use the following methods:</p> <ul style="list-style-type: none">· Shorten the distance between the devices to shorten the length of the twisted pair.· If the distance between the devices cannot be changed, the devices can be connected in series through a repeater , hub, or switch.

Check item	Criteria	Action
Check whether the twisted pair is used correctly.	<p>Twisted pairs are classified into straight-through twisted pairs and crossover twisted pairs.</p> <p>Straight-through twisted pairs are used to connect Ethernet interfaces between the following devices:</p> <ul style="list-style-type: none"> • A router and a hub • A router and an Ethernet switch • A computer and an Ethernet switch • A computer and a hub <p>Crossover twisted pairs are used to connect Ethernet interfaces between the following devices:</p> <ul style="list-style-type: none"> • Two routers • A router and a computer • A hub and a hub • A hub and a switch • Two switches • Two computers 	If the type of twisted pair used is incorrect, change it to the correct type.

If the devices are connected through an optical fiber, check the items listed in the following table.

Check item	Criteria	Action
Check whether the optical module corresponds to the optical fiber.	<p>Check whether the optical module matches the optical fiber according to the following information:</p> <ul style="list-style-type: none"> • A multi-mode optical fiber can be used with a multi-mode optical module. • A single-mode optical fiber can be used with a single-mode optical module, but cannot be used with a multi-mode optical module. Single-mode optical fibers are yellow and multi-mode optical fibers are orange. • The wave length of two connected optical modules must be consistent. 	If the optical fiber and the optical module do not match, replace the optical module or the optical fiber as needed.
Check whether the length of the optical fiber matches the transmission distance supported by the optical module.	The length of the optical fiber must be shorter than the transmission distance supported by the optical module.	Shorten the length of the optical fiber or use an optical module that supports greater transmission distance.
Check whether the signal attenuation is within the allowed range.	The range of optical signal attenuation is less than - 28 dB.	If the attenuation exceeds the allowed range, replace the optical fiber. If the problem persists, shorten the length of the optical fiber.

Check item	Criteria	Action
Check whether the two ends of the link are faulty by using the loopback method or a tester.	<p>If you use a tester, the results indicate that the sending and the receiving data flows are normal.</p> <p>If you use the loopback method, the interface is in the up state after you connect the two ends of the optical fiber to an optical module.</p>	If a cable is faulty, replace the cable. If the fault persists, replace the optical modules at the two ends.

3. Check whether the hardware of the local and peer devices is faulty.

3.5 Connectivity faults between SAG-100WM and Alibaba Cloud

3.5.1 The SAG is offline

This topic explains why SAG-100WM is offline and how to troubleshoot it.

Symptoms

In the [Smart Access Gateway console](#), the SAG is in the Offline state.

Causes

- The SAG has a software failure.
 - The connection between the SAG and Alibaba Cloud has failed.
1. Ping other websites in the same network environment of the service provider to make sure that the network is normal.
 - If the network is abnormal, solve the network problem.
 - If the network is normal, proceed to [2](#).
 2. Check whether the SAG is powered on.
 - Check whether the RUN indicator on the SAG is on.
 - Check whether the indicators of connected network interfaces are lit green.
 - If the SAG cannot be powered on, see [#unique_100](#) for troubleshooting.
 - If the SAG can be powered on, proceed to [3](#).
 3. Restart the SAG, or open a ticket for technical support.

3.5.2 Cannot successfully ping an ECS instance in the same CEN instance or a PC in the same CCN instance

This topic describes causes as to why you cannot successfully ping an ECS instance in the same CEN instance or a PC in the same CCN instance from the SAG-100WM device, and the troubleshooting methods.

Symptoms:

The terminal cannot connect to Alibaba Cloud. Specifically, you cannot successfully ping an ECS instance in the same CEN instance or another PC in the same CCN instance.

Causes:

- The link between the terminal and the device has failed.
- The VPN link between the device and Alibaba Cloud has failed.
- The target ECS instance has failed.
- The network of the service provider has failed.

1. Log on to the [Smart Access Gateway console](#).
2. Click the ID of the target Smart Access Gateway instance and check if the status of the device is Ready.
 - If the device is offline, see [#unique_102](#) to troubleshoot.
 - If the device is ready, proceed to [3](#).
3. Check whether the cloud LED light of the device is on.
 - If the cloud LED light is on, the VPN tunnel between the device and Alibaba Cloud is normal. Log on to the ECS console to check if the security group rules of ECS instances allow traffic to pass through.
 - If the cloud LED light is not on, the VPN tunnel between the device and Alibaba Cloud is not established. In this case, proceed to [4](#).
4. The software of the device may have failed. You can restart the device to see if the problem persists or open a ticket for further consultation.

3.6 Connectivity faults between SAG-1000 and Alibaba Cloud

3.6.1 The SAG is offline

This topic explains why SAG-1000 is offline and how to troubleshoot it.

Symptom

In the [Smart Access Gateway console](#), the SAG is in the Offline state.

Causes

- The SAG has a software failure.
 - The connection between the SAG and Alibaba Cloud has failed.
1. Ping other websites in the same network environment of the service provider to make sure that the network is normal.
 - If the network is abnormal, solve the network problem.
 - If the network is normal, proceed to [2](#).
 2. Check whether the device is powered on.
 - Check whether the power supply indicator is lit green.
 - Check whether the indicators of connected network interfaces are lit green.
 - If the SAG cannot be powered on, see [#unique_100](#) for troubleshooting.
 - If the SAG can be powered on, proceed to [3](#).
 3. Log on to the switch console to check the connectivity between the SAG and the switch.
 - If access is provided through static routes, ping the IP address of each interface on the SAG from the switch. If you cannot successfully ping an interface, see [#unique_77](#) to restore the connection to the interface.
 - If the SAG is stand-alone, check whether the second or third indicator on the right is lit yellow or flashing.
 - If the second indicator is lit yellow or flashing, the SAG has a software fault. Open a ticket for technical support.
 - If the third indicator is lit yellow or flashing, the VPN tunnel between the SAG and Alibaba Cloud is unavailable. Open a ticket for technical support.

For more information, see [#unique_105](#).

3.6.2 A PC cannot ping an ECS instance

This topic explains why you cannot ping an ECS instance from a PC and how to troubleshoot it.

Symptoms

A PC cannot connect to Alibaba Cloud through an SAG-1000 device. For example, you cannot ping an ECS instance in the same CEN from the PC.

Causes

- The link between the PC and the SAG-1000 is faulty.
- The VPN link between the SAG and Alibaba Cloud is faulty.
- The target ECS instance is faulty.
- The network of the service provider is faulty.

1. Log on to the [Smart Access Gateway console](#).

2. Click the ID of the target Smart Access Gateway instance and check whether the device is in the Ready state.

- If the device is offline, see [#unique_107](#) for troubleshooting.
- If the device is ready, proceed to [3](#).

3. Log on to the switch console to check the connectivity between the device and the switch.

- If access is provided through static routes, ping the IP address of each interface on the SAG from the switch. If you cannot ping an interface, see [#unique_77](#) to restore the connection to the interface.
- If the SAG is stand-alone, check whether the second or third indicator on the right is lit or flashing.
 - If the second indicator is lit yellow or flashing, the SAG has a software fault. Open a ticket for technical support.
 - If the third indicator is lit yellow or flashing, the VPN tunnel between the SAG and Alibaba Cloud is unavailable. Open a ticket for technical support.
 - If both the second and the third indicators are lit green, proceed to [4](#).

For more information, see [#unique_105](#).

4. Check the status of the ECS instance. Ping other VPC ECS instances or configure an EIP for the target ECS instance to check the connectivity by using the Internet.
 - If you can ping other ECS instances, the target ECS instance is faulty. Resolve the fault.
 - If you cannot ping other ECS instances, proceed to 5.
5. Ping other websites from the PC. If the ping action fails, check whether the network of the service provider is normal.

3.6.3 SAG-1000 cannot connect to a local client

This topic explains why an SAG-1000 device cannot connect to a local client in the same CCN instance and how to troubleshoot it.

Symptoms

An SAG-1000 device cannot connect to a local client in the same CCN instance.

Causes

- The link between the terminal and the SAG is faulty.
 - The VPN link between the SAG and Alibaba Cloud is faulty.
 - The network environment of the target PC is faulty.
 - The network of the service provider is faulty.
1. Log on to the [Smart Access Gateway console](#).
 2. Click the ID of the target Smart Access Gateway (SAG) instance and check whether the SAG is the Ready state.
 - If the SAG is offline, see [#unique_107](#) for troubleshooting.
 - If the SAG is ready, proceed to 3.

3. Log on to the switch console to check the connectivity between the SAG and the switch.

- If access is provided through static routes, ping the IP address of each interface on the SAG from the switch. If you cannot ping an interface, see [#unique_77](#) to restore the connection to the interface.
- If the SAG is stand-alone, check whether the second or third indicator on the right is lit yellow or flashing.
 - If the second indicator is lit yellow or flashing, the SAG has a software fault. Open a ticket for technical support.
 - If the third indicator is lit yellow or flashing, the VPN tunnel between the SAG and Alibaba Cloud is unavailable. Open a ticket for technical support.

For more information, see [#unique_105](#).

4. Repeat the preceding steps to check the SAG in the network environment of the target PC. If the problem persists, open a ticket for technical support.

3.7 Link failure between SAG-1000 and the switch

This topic explains why the link between an SAG-1000 device and the corresponding switch fails and how to troubleshoot it.

Symptoms

- You cannot ping the switch from the device.
 - On the web port configuration page of the device, the port indicator is lit red.
 - When OSPF access is used, the port indicator on the web port configuration page is lit red.
 - The route entry of the corresponding interface IP cannot be found on the web status query page of the device.
 - The physical connection between the device and the switch is incorrect.
 - The interface on the switch is not enabled.
 - The IP address of the device or the switch is incorrectly configured.
1. Check the physical connection between the device and the switch and make sure that the port indicators are on at both ends.
 2. Check the interface configurations of the switch and make sure that the interface is enabled.

3. Check the IP address of the switch interface and make sure that the IP address is in the same CIDR block as the IP address of the device interface.
4. If OSPF access is used, make sure that the OSPF port configurations are the same as the device port configurations.

These configurations include the area ID, hello time, dead time, authentication method, password of plaintext authentication, key ID of MD5 authentication, and router ID. Additionally, you must make sure that all directly connected CIDR blocks are advertised.

3.8 FAQ

3.8.1 What can I do if a service failure occurs?

- If a service failure occurs to your SAG-100WM device, see [#unique_112](#) for troubleshooting.
- If a service failure occurs to your SAG-1000, see [#unique_113](#) and [#unique_114](#) for troubleshooting.

3.8.2 What can I do if my SAG is offline?

- If your SAG-100WM device is offline, see [#unique_116](#) for troubleshooting.
- If your SAG-1000 device is offline, see [#unique_107](#) for troubleshooting.

3.8.3 What can I do if I forget my password?

- If you forget the password of your SAG-100WM device, press the RESET button to clear the password when the device is powered on, and then log on to the Web console and reset the password.
- If you forget the password of your SAG-1000 device, press the RESET button when the device is powered on.

3.8.4 What is the default Wi-Fi password of SAG-100WM?

The default Wi-Fi password of an SAG-100WM device is the serial number of the device, with the first letter being capitalized.

4 High availability configurations

4.1 View the HA configuration of an SAG

This topic describes how to view the high availability (HA) configuration of a Smart Access Gateway (SAG).

Prerequisites

Before you can view the HA configuration of an SAG, the following conditions must be met:

- The standby usage mode is selected when you purchase the SAG.
- The active SAG and standby SAG have the same configurations.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the instance ID of the SAG for which you want to perform an active/standby switchover.
3. In the left-side navigation pane of the SAG details page, click HA Configuration.
4. On the HA Configuration page, view the SN of the active SAG and standby SAG.

The active/standby switchover of SAG-100WM differs from that of SAG-1000 in the following aspects:

- If you switch an SAG-100WM device to its standby device in the console, you must also connect the physical WAN port of the standby device to the Internet.
- SAG-100WM devices support manual active/standby switchover, while SAG-1000 devices support automatic active/standby switchover.

4.2 View the WAN + 4G backup of an SAG

This topic describes how to view the WAN + 4G backup of a Smart Access Gateway (SAG). By default, WAN + 4G backup is enabled for SAG-100WM and SAG-1000 to use wired broadband as the active link and wireless 4G-LTE as the standby link. If the active link fails, the system automatically switches 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, and then click the instance ID of the SAG for which you want to perform an active/standby switchover.
3. In the left-side navigation pane of the SAG details page, click HA Configuration.
4. On the HA Configuration page, view the current active and standby links of the SAG in the WAN + 4G area.

The HA structure of SAG-100WM and SAG-1000 is displayed, as shown in the following figure.

4.3 View leased line backup

This topic describes how to view leased line backup. SAG-1000 supports link-level leased line backup. If the active link fails, the system automatically switches to the backup link.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click Smart Access Gateway, and then click the instance ID of the SAG for which you want to perform an active/standby switchover.
3. In the left-side navigation pane of the SAG details page, click HA Configuration.
4. On the HA Configuration page, view the active and standby leased lines of the SAG instance in the Standby Leased Line area.