

ALIBABA CLOUD

Alibaba Cloud

智能接入网关 Configuration Guide

Document Version: 20220107

 Alibaba Cloud

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions









Style	Description	Example
 Danger	A danger notice 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.
 Warning	A warning notice 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 restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Deploy an SAG-100WM device	07
2. Deploy an SAG-1000 device	08
3. Manage devices	09
3.1. Associate SAG devices with SAG instances	09
3.1.1. View basic information	09
3.1.2. Add a device	11
3.1.3. Upgrade an SAG device to a later version	13
3.1.4. Disassociate an SAG device from the SAG instance	15
3.1.5. Remotely restart an SAG device	15
3.1.6. Remotely access an SAG device	16
3.1.7. Activate an SAG device	17
3.2. Manage devices	17
3.2.1. Assign a role to a port	17
3.2.2. Configure a WAN port	18
3.2.3. Configure a leased line port	22
3.2.4. Configure a LAN port	24
3.2.5. Configure HA for SAG devices	26
3.2.6. Configure the management port	27
3.2.7. Quick diagnosis	29
3.2.8. Manage routes	31
3.2.8.1. Add a static route	31
3.2.8.2. Configure BGP routing	32
3.2.8.3. Configure OSPF routing	34
3.2.8.4. Enable wireless connections	36
4. Configure networks in the cloud	38
4.1. Advertise routes to Alibaba Cloud	38

4.2. Configure an SNAT rule	39
4.3. Add a DNAT rule	39
4.4. Attach a network instance	40
4.5. Authorize cross-account association	42
4.6. Advertise routes	43
4.7. Configure health check	44
4.8. Cancel health check	46
4.9. Detach a network	46
5. Health check	48
5.1. Create a health check instance	48
5.2. Modify a health check instance	50
5.3. Delete a health check instance	51
6. High availability	52
6.1. Use two SAG devices to implement HA	52
6.2. Use wired and wireless connections to implement HA	52
6.3. Use leased lines and SAG to implement HA	53
6.4. Switch the active-standby mode to the active-active mode	54
7. QoS policies	57
7.1. What is a QoS policy?	57
7.2. Manage QoS policies	58
7.3. Associate with or disassociate from an SAG instance	62
7.4. Check the status of a QoS rule	63
8. Access control	64
8.1. Overview	64
8.2. Manage ACLs	65
8.3. Manage ACL rules	65
8.4. Manage SAG instances associated with ACLs	68
9. Flow logs	69

9.1. Overview	69
9.2. Create a flow log	70
9.3. Associate a flow log with SAG instances	72
9.4. Query flow log data	72
9.5. Enable a flow log	73
9.6. Disable a flow log	74
9.7. Disassociate from an SAG instance	74
9.8. Delete a flow log	75
10. Access cloud services	76
10.1. Configure AnyTunnel	76
10.2. Configure PrivateZone	78
10.2.1. Configure PrivateZone	78
10.2.2. Acquire or grant permissions	80
11. DPI	87
11.1. Overview	87
11.2. Manage DPI	88
12. Application acceleration	90
12.1. Overview	90
12.2. Work with application acceleration plans	91
12.3. Associate an application acceleration plan with an SAG i...	93
12.4. Manage an application acceleration rule	95
12.5. Throttle bandwidth for application acceleration from mul...	97
12.6. Throttle bandwidth resources for a client account	99
13. Grant a RAM user the permissions to use QoS policies and flo...	100

1. Deploy an SAG-100WM device

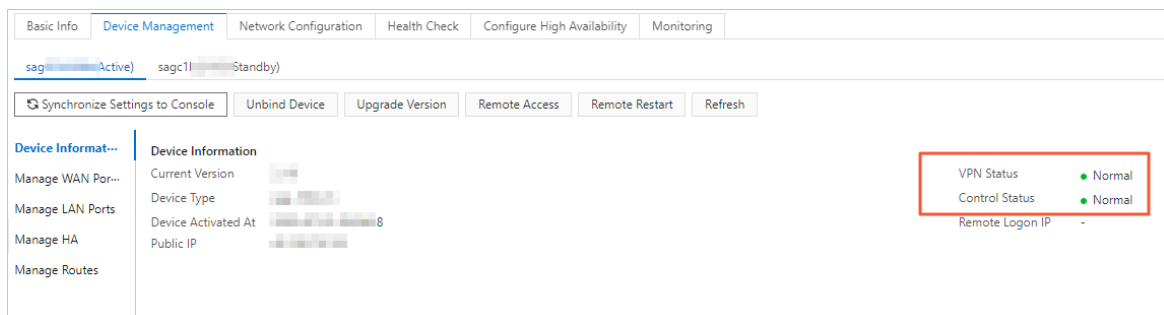
This topic describes how to deploy an SAG-100WM device.

The procedure to deploy an SAG-100WM device is as follows:



You can purchase SAG-100WM devices in the Smart Access Gateway (SAG) console or from a third-party vendor. For more information, see [Purchase SAG devices](#). After you receive the device, you must start, activate, and configure it and set up network connections to connect the device to Alibaba Cloud.

1. Connect the device to your private network. For more information, see [Descriptions of SAG-100WM](#).
2. Activate the device and associate it with the SAG instance. For more information, see [Activate an SAG device](#) and [Add a device](#).
3. Configure the device in the web console. For more information, see [Configure SAG-100WM in the web console](#).
4. Select a method to advertise routes to Alibaba Cloud. For more information, see [Advertise routes to Alibaba Cloud](#).
5. Associate the SAG instance with a Cloud Connect Network (CCN) instance. For more information, see [Associate a CCN instance with an SAG instance](#) or [Attach a network instance](#).
6. You can check the connectivity status in the SAG console.



2. Deploy an SAG-1000 device

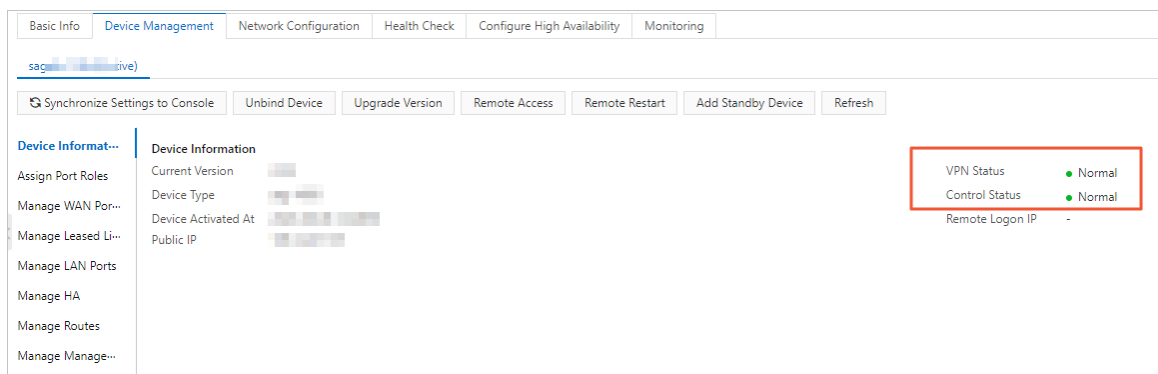
This topic describes how to deploy an SAG-1000 device.

The procedure to deploy an SAG-1000 device is as follows:



You can purchase SAG-1000 devices in the Smart Access Gateway (SAG) console. For more information, see [Purchase SAG devices](#). After you receive the device, you must start, activate, and configure it and set up network connections to connect the device to Alibaba Cloud.

1. Activate the device and associate it with the SAG instance. For more information, see [Activate an SAG device](#) and [Add a device](#).
2. Optional. Assign roles to the device ports. For more information, see [Assign a role to a port](#).
3. Connect the device to your private network. For more information, see [Descriptions of SAG-1000](#).
4. Configure the device in the web console. For more information, see [Configure the SAG-1000 device in the web console](#).
5. Select a method to advertise routes to Alibaba Cloud. For more information, see [Advertise routes to Alibaba Cloud](#).
6. Associate the SAG instance with a Cloud Connect Network (CCN) instance. For more information, see [Associate a CCN instance with an SAG instance](#) or [Attach a network instance](#).
7. You can check the connectivity status in the SAG console.



3. Manage devices

3.1. Associate SAG devices with SAG instances

3.1.1. View basic information

After you purchase a Smart Access Gateway (SAG) device, the system creates an SAG instance that allows you to manage the SAG device. This topic describes how to view basic information about an SAG device through the SAG instance.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the top navigation bar, select the region.
3. On the **Smart Access Gateway** page, click the ID of the SAG instance.
4. On the instance details page, you can view the basic information about the SAG instance on the **Basic Info** tab.

The **Basic Info** tab displays the basic information and advanced features:


- o **Basic Info**: displays information such as the model of the SAG device associated with the current SAG instance, upstream bandwidth, and route advertisement methods.

Parameter	Description
SAG instance ID	The ID of the SAG instance.
SAG Instance Name	The name of the SAG instance. You can click Edit to modify the name. The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
Description	The description of the SAG instance. You can click Edit to modify the description. The description must be 2 to 256 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
WAN Upstream Bandwidth	The maximum upstream bandwidth of the SAG device when the SAG device is connected to the Internet through a WAN port. Unit: Mbit/s. You can click Edit to modify the maximum upstream bandwidth.
Upstream Bandwidth of Cellular Port	The maximum upstream bandwidth of the SAG device when the SAG device is connected to the Internet through 4G networks. Unit: Mbit/s. You can click Edit to modify the maximum upstream bandwidth.

Parameter	Description
Method to Synchronize with On-premises Routes	The method that the SAG device uses to advertise routes to Alibaba Cloud. For more information, see Advertise routes to Alibaba Cloud .
Controller Status	<p>The status of the SAG device.</p> <ul style="list-style-type: none"> Order Placed: The order of the SAG device has been placed and the package has not been dispatched. Order Shipped: The package has been dispatched. After you receive the package, sign for it. Not Associated with CCN: The SAG instance is not associated with a Cloud Connect Network (CCN) instance or virtual border router (VBR). Disconnected: The SAG device is not connected to Alibaba Cloud. Ready: The SAG device is working as expected. Overdue Payment: The SAG device is unavailable due to overdue payments.
VPN Status	<p>The status of the VPN connection through which the SAG device is connected to Alibaba Cloud.</p> <ul style="list-style-type: none"> Normal: The VPN connection is working as expected. If the VPN connection is working as expected, you can place the pointer over Normal to view the protocol that the VPN connection uses, including: <ul style="list-style-type: none"> ipsecVPN: uses Internet Protocol Security (IPsec). By default, the SAG device uses IPsec to establish the VPN connection. aliVPN: uses the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to provide an enhanced VPN connection, encapsulate data packets on any port, minimize packet loss, and improve data transmission efficiency. You can submit a ticket to enable aliVPN. Abnormal: The VPN connection is not working as expected.
Created At	The time when the SAG instance was created.
Expires At	The date when the SAG instance expires.
Device Model	The model of the SAG device that is associated with the SAG instance.

- o **Advanced Features:** displays advanced features such as quality of service (QoS) policies, access control lists (ACLs), and deep packet inspection (DPI).


Parameter	Description
-----------	-------------


Parameter	Description
DPI	<p>Indicates whether DPI is enabled.</p> <p>You can turn on or turn off the switch to enable or disable DPI.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p> Note</p> <ul style="list-style-type: none"> ▪ Before you can associate the SAG instance with an application-aware QoS policy or ACL, you must enable DPI first. ▪ If the SAG instance is associated with an application-aware QoS policy or ACL, you cannot disable DPI. Before you can disable DPI, you must disassociate the application-aware QoS policy or ACL from the SAG instance. For more information, see Associate with or disassociate from an SAG instance and Manage SAG instances associated with ACLs. </div>
QoS Policy	The QoS policy that is associated with the SAG instance. For more information about QoS policies, see What is a QoS policy? .
Transmission Optimization	<p>Indicates whether transmission optimization is enabled.</p> <p>Transmission optimization uses forward error correction (FEC) to minimize packet loss. This makes data transmission more reliable.</p> <p>To enable transmission optimization, submit a ticket.</p>
Flow Log	The flow log that is associated with the SAG instance. For more information about flow logs, see Overview .
ACL	The ACL that is associated with the SAG instance. For more information about ACLs, see Overview .

3.1.2. Add a device

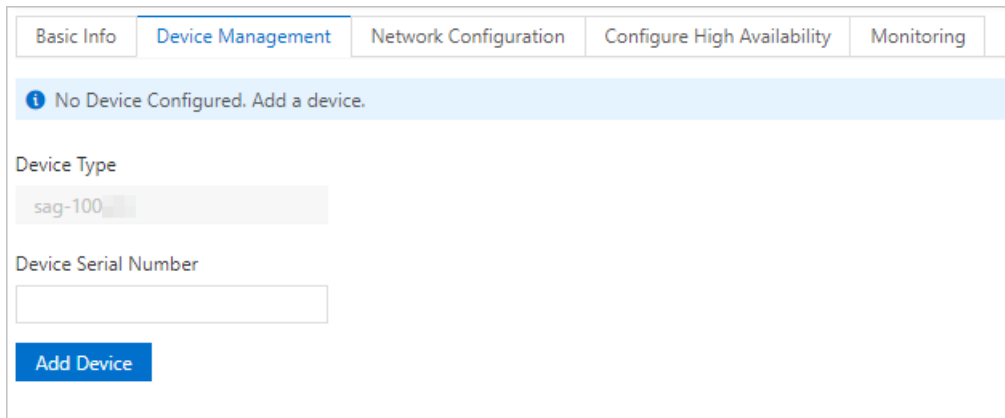
This topic describes how to add a Smart Access Gateway (SAG) device in the SAG console to associate the device with the SAG instance. You can manage SAG devices in the SAG console.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the SAG instance. On the instance details page, click **Device Management**.
 - Find the SAG instance and choose  > **Device Management** in the **Actions** column.

 **Note** If the SAG instance is not associated with any SAG device, after you open the **Device Management** tab, a message appears requiring you to add a device.

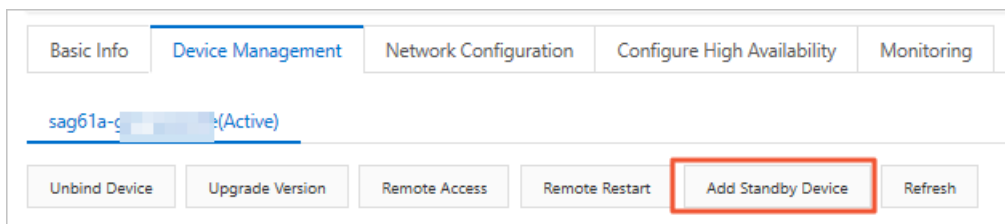
3. On the **Device Management** tab, enter the serial number of the active device.



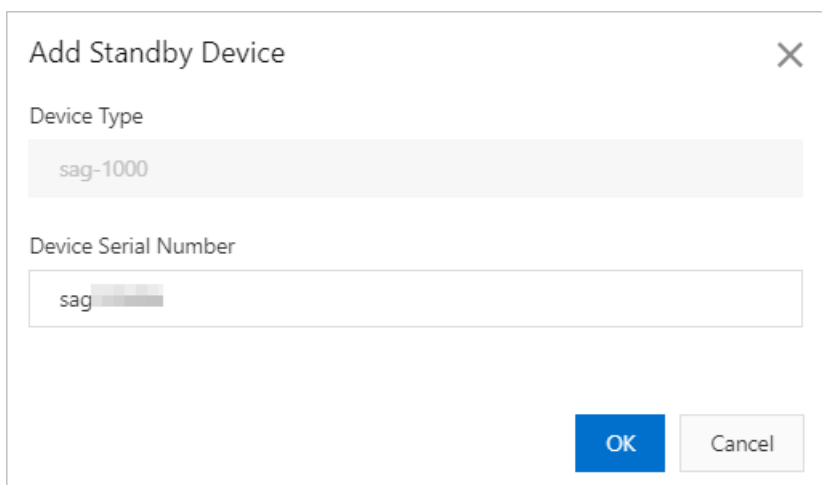
4. Click **Add Device**.
5. After you add the device, click **Add Standby Device** on the **Device Management** tab to add a standby device.

Note

- You can add a standby device only after you add the active device.
- An SAG instance can be associated with at most two SAG devices.

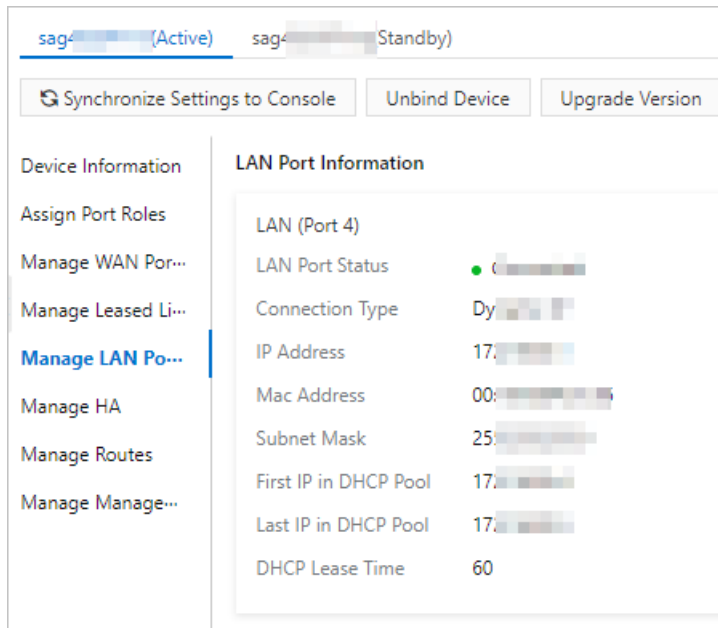


6. In the **Add Standby Device** dialog box, enter the serial number of the standby device.



7. Click **OK**.

After you add the standby device, the devices are displayed:




3.1.3. Upgrade an SAG device to a later version

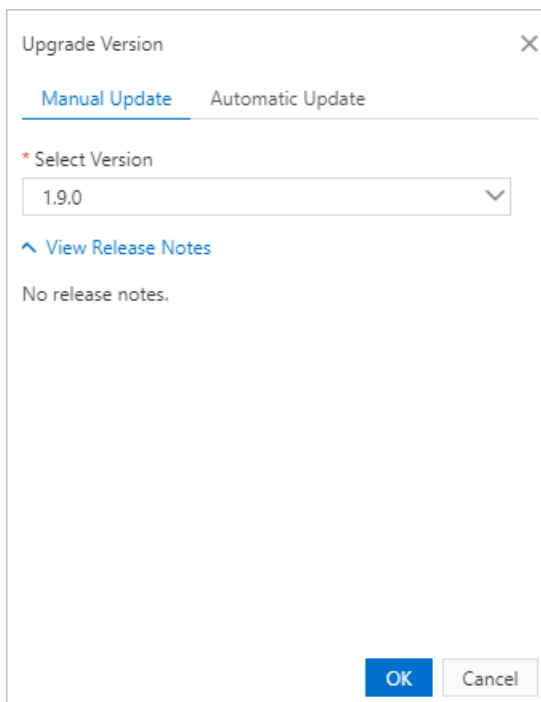
This topic describes how to upgrade a Smart Access Gateway (SAG) device to a later version. We recommend that you upgrade your SAG device to the latest version.

Context

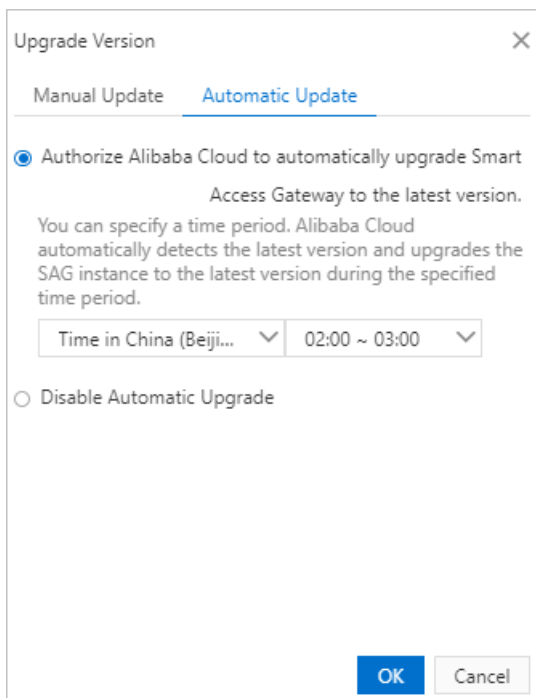
- The upgrade process takes about 10 minutes.
- The upgrade may cause network disconnections. We recommend that you upgrade your SAG device during off-peak hours.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Device Management** tab.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.
3. If both the active and standby devices are associated with the SAG instance, select the target device and click **Upgrade Version**.
4. In the **Upgrade Version** dialog box that appears, select one of the following methods to perform an upgrade.
 - Click the **Manual Update** tab, select the target version, and then click **OK**. Your device is upgraded to the selected version.



- o Click the **Automatic Update** tab, select the **Authorize Alibaba Cloud to automatically upgrade Smart Access Gateway to the latest version** check box, select a time zone and time period, and then click **OK**. The device is upgrade to the latest version during the specified time period.




Note You can also choose to **Disable Automatic Upgrade**.

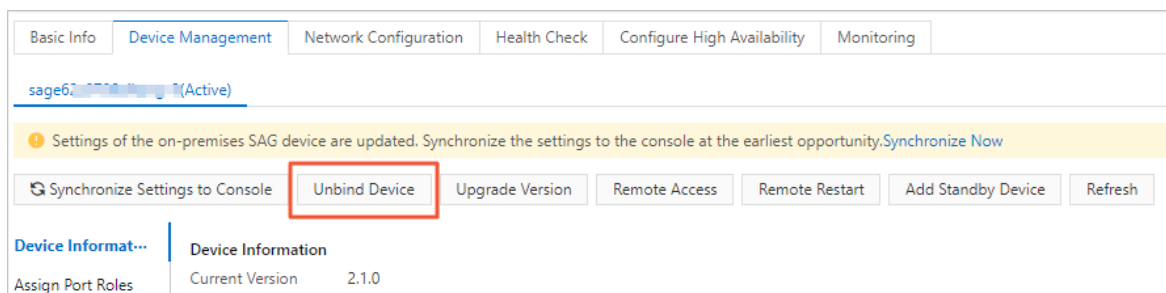
3.1.4. Disassociate an SAG device from the SAG instance

This topic describes how to disassociate a Smart Access Gateway (SAG) device from the SAG instance. After an SAG device is disassociated from the SAG instance, you can no longer use the SAG instance to manage the SAG device.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page, click the **Device Management** tab.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.

3. Select the target device and click **Unbind Device**.




4. In the **Unbind Device** message that appears, click **OK**.

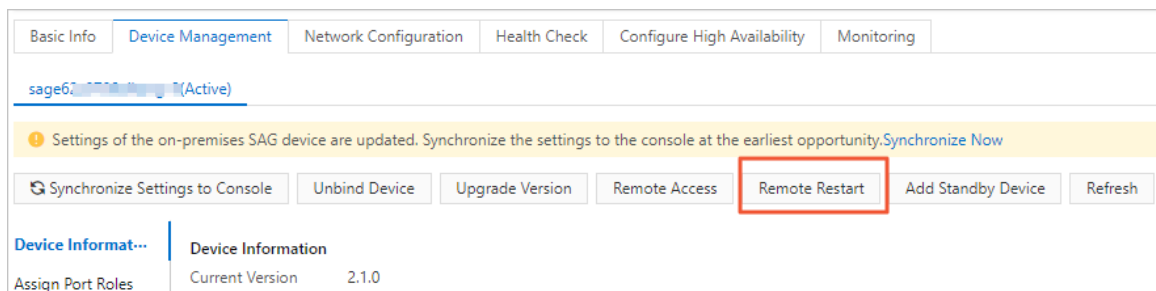
3.1.5. Remotely restart an SAG device

This topic describes how to remotely restart a Smart Access Gateway (SAG) device.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Device Management** tab.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.


3. If both the active and standby devices are associated with the SAG instance, select the target device and click **Remote Restart**.
4. In the **Remote Restart** dialog box that appears, click **OK** to restart the device.




3.1.6. Remotely access an SAG device

This topic describes how to specify an IP address used to remotely log on to the web console of a Smart Access Gateway (SAG) device. You must specify the IP address in the SAG console. Remote access allows you to log on to the web console over a secure and private connection.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click **Smart Access Gateway**.
3. In the top menu bar, select the region.
4. On the **Smart Access Gateway** page, find the SAG instance.
5. Use one of the following methods to go to the **Device Management** tab.
 - Click the ID of the SAG instance. On the instance details page, click the **Device Management** tab.
 - Find the SAG instance and choose  > **Device Management** in the **Actions** column.
6. (Optional) If the SAG instance is associated with an active and a standby SAG device, click the serial number of the SAG device that you want to remotely log on to.

By default, the **Device Management** displays information about the active SAG device.
7. Click **Remote Access**.
8. In the **Remote Access from Private Network** dialog box, enter the private IP address used to log on to the web console and click **OK**.

 Note

- SAG allows only remote access to the web console over a private connection. Therefore, the terminal where access is initiated must be connected to the SAG device over a private network.
- If the SAG device needs to communicate with other networks over Cloud Enterprise Network (CEN), the private IP address used to log on to the web console must not conflict with those of other networks. Otherwise, you cannot remotely log on to the web console.
- If the private IP address used to log on to the web console is not specified, you can use the default management IP address. For SAG-1000 devices, the management IP address is the IP address of the management port by default. For SAG-100WM devices, the management IP address is the IP address of the LAN port by default. For more information, see [Configure SAG-100WM in the web console](#) and [Configure the SAG-1000 device in the web console](#).

9. Open your browser, enter the IP address specified in [Step 8](#) in the address bar, and then press Enter to remotely log on to the web console.

Related information

- [DescribeSagRemoteAccess](#)
- [ModifySagRemoteAccess](#)

3.1.7. Activate an SAG device

After you receive a Smart Access Gateway (SAG) device, you must activate it.

Procedure

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

3.2. Manage devices

3.2.1. Assign a role to a port

SAG-1000 allows you to assign roles to device ports. This helps you assign ports based on business requirements. This topic describes how to modify port roles in the Smart Access Gateway (SAG) console.


Prerequisites

An SAG-1000 device is used.


Context

SAG devices support five port roles: WAN, LAN, leased line, management (MGT), and not assigned. By default, port 5 is the WAN port and port 2 is the management port. The management port cannot be modified. For more information about the management port, see [Configure the management port](#). The other ports are described in the following section.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click **Device Management**.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.
3. On the **Device Management** tab, click **Assign Port Roles** in the left-side navigation tree.
4. Find the target port and click **Edit** in the **Actions** column.
5. In the **Change Port Role** dialog box that appears, select a role for the port.

Port role	Description
Not Assigned	No role is assigned to the port.
WAN	The port is used as a WAN port to connect to the Internet through dynamic IP addresses, static IP addresses, or PPPoE. For more information, see Configure a WAN port .
LAN	The port is used as a LAN port to connect to local clients or switches through dynamic or static IP addresses. For more information, see Configure a LAN port .
Leased Line	The port is used to connect to a leased line. For more information, see Configure a leased line port .

 **Notice** After you modify the port roles in the SAG console, the port roles of both the active and standby devices are updated accordingly. The devices are restarted.

6. Click **OK**.

3.2.2. Configure a WAN port

A WAN port can connect a private network to Alibaba Cloud. This topic describes how to configure a WAN port for a Smart Access Gateway (SAG) device in the SAG console.

Features of a WAN port

- SNAT

After you enable SNAT, private source IP addresses are converted into public IP addresses that can access the Internet. By default, SNAT is disabled.

In inline mode, you must enable SNAT for an SAG device to connect on-premises networks to the Internet. In one-arm mode, we recommend that you disable SNAT.

- FAQ about custom DNS servers

By default, the WAN port directly accesses Alibaba Cloud DNS servers. You can specify a custom DNS server for the WAN port.

- Bandwidth throttling

You can set **bandwidth** throttling for the WAN port. You can use quality of service (QoS) policies and bandwidth throttling to improve bandwidth utilization.

- High-availability connections over WAN ports

You can configure multiple WAN ports for an SAG device. The WAN ports can be used to establish high-availability connections, balance loads, and improve the network availability.

- By default, port 5 of an SAG-1000 device serves as a WAN port. You can also specify other ports as WAN ports.
- The number of WAN ports supported by an SAG-100WM device is based on the device type. Type 2 devices support multiple WAN ports. Type 1 devices support only one WAN port. The exterior of Type 1 and Type 2 devices is different.

You can specify the **priority**, **ISP**, and **weight** properties to manage priorities of WAN ports. The priorities of the properties in descending order: **priority>ISP>weight**.

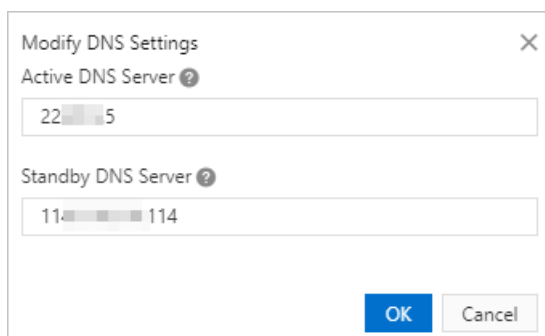
Manage properties	Description	Scenarios
Priority	<p>If you have configured multiple WAN ports for an SAG device, you can set a priority for each WAN port.</p> <p>The port that has the highest priority is used as the active port. Ports that have lower priorities are used as standby ports. An SAG device preferentially uses the active port to forward traffic. If the active port is not working as expected, standby ports automatically take over.</p>	<ul style="list-style-type: none"> ○ If the WAN ports are assigned different priorities, the SAG device can establish high-availability connections by using the active port and standby ports. ○ If the WAN ports are assigned the same priority, the SAG device can implement load balancing for the WAN ports based on the ISP and weight properties.
ISP	<p>If the WAN ports are assigned the same priority, the SAG device matches data packets with Internet service provider (ISP) connections based on the destination IP addresses specified in the data packets. This implements load balancing.</p>	
Weight	<p>If the ISP configurations of the WAN ports are the same or the SAG device cannot find ISPs that match the data packets, the SAG device implements load balancing based on the weights of the WAN ports.</p>	

Note

- You can specify an ISP for each WAN port only if the SAG instance is deployed in the mainland China area.
- The WAN ports can be used to balance only the load of network traffic transmitted over public networks.


Configure a WAN port

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. On the **Smart Access Gateway** page, use one of the following methods to go to the **Device Management** tab.
 - Click the ID of the SAG instance. On the instance details page, click the **Device Management** tab.
 - Find the SAG instance and choose **⋮** > **Device Management** in the **Actions** column.
4. On the **Device Management** tab, click the serial number of the SAG device that you want to manage if the SAG instance is associated with both an active device and a standby device.
5. In the left-side navigation pane of the **Device Management** tab, click **Manage WAN Ports**.
6. If you want to enable SNAT for a WAN port, click **Edit** in the **SNAT Information** section. In the **Edit SNAT** dialog box, enable SNAT and click **OK**.
7. If you want to configure a custom DNS server for a WAN port, click **Edit** in the **DNS information** section. In the **Modify DNS Settings** dialog box, enter a custom DNS server address and click **OK**.



8. In the **WAN-Wired** section, find the WAN port and click **Edit**.
9. In the dialog box that appears, set the following parameters and click **OK**.

Parameter	Description
-----------	-------------

Parameter	Description
<p>Connection Type</p>	<p>Select a connection type for the WAN port.</p> <p>SAG devices support the following connection types:</p> <ul style="list-style-type: none"> ○ Static IP: If the peer port of the WAN port is assigned a static IP address, select this type. <p>If you select Static IP, you must set the following parameters:</p> <ul style="list-style-type: none"> ■ IP: Enter the IP address of the WAN port. ■ Subnet Mask: Enter the subnet mask of the WAN port IP address. ■ Gateway: Enter the gateway IP address of the SAG device. <div style="background-color: #e0f2f1; padding: 10px; margin: 10px 0;"> <p> Note</p> <ul style="list-style-type: none"> ■ Make sure that the IP addresses of the WAN port and the peer port fall within the same CIDR block. ■ After you set Gateway, the SAG device generates a default route. </div> <ul style="list-style-type: none"> ○ Dynamic IP: If the peer port uses Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, select this type. The WAN port uses DHCP to obtain a dynamic IP address. ○ PPPoE: If the WAN port needs to access the Internet through dial-up connections, select this type. <p>You must enter the username and password of the PPPoE account provided by the ISP.</p> <ul style="list-style-type: none"> ■ Account: Enter the username of the PPPoE account. <p>The username must be 6 to 30 characters in length, and can contain digits and letters.</p> <ul style="list-style-type: none"> ■ Password: Enter the password of the PPPoE account. <p>The password must be 6 to 30 characters in length, and can contain digits and letters.</p>
<p>Priority</p>	<p>Set a priority for the WAN port.</p> <p>Valid values: 1 to 50 and -1. Default value: 1. A smaller value represents a higher priority. A value of -1 indicates that the port is not used to forward network traffic.</p>

Parameter	Description
ISP	<p>Select an ISP for the WAN port.</p> <p>SAG devices support the following ISPs:</p> <ul style="list-style-type: none"> ◦ China Telecom ◦ China Mobile ◦ China Unicom ◦ Other
Bandwidth	<p>Set a bandwidth cap for the WAN port. Unit: Mbit/s.</p> <p>Before you set a bandwidth cap, take note of the following rules:</p> <ul style="list-style-type: none"> ◦ If you set a bandwidth cap for the WAN port, you cannot set WAN Upstream Bandwidth or Upstream Bandwidth of Cellular Port for the SAG device. ◦ If you have configured multiple WAN ports for an SAG device and the WAN ports are assigned a QoS policy, the QoS policy is applied based on the following rules: <ul style="list-style-type: none"> ▪ If the WAN ports are assigned different priorities, the QoS policy throttles network traffic based on the bandwidth of the active port. ▪ If the WAN ports are assigned the same priority, the QoS policy throttles network traffic based on the lowest bandwidth cap value of the WAN ports. ◦ If the bandwidth cap of the WAN port is set to 0 Mbit/s, it indicates that traffic forwarding on the WAN port is not throttled.
Weight	<p>Set a weight for the WAN port.</p> <p>Valid values: 1 to 100. Default value: 100.</p> <p>The weight of each WAN port determines the amount of network traffic forwarded on each WAN port. For example, the weight of a WAN port is set to 50 and that of another is set to 100. The ratio of the weights of these two ports is 1:2. If the SAG devices receive three data packets, one packet is forwarded from the WAN port whose weight is 50 and two packets are forwarded from the WAN port whose weight is 100.</p>

References

- [What is a QoS policy?](#)
- [Deployment modes](#)
- [Descriptions of SAG-100WM](#)
- [ModifySagWan](#): modifies configurations for WAN ports of SAG devices.
- [ModifySagWanSnat](#): modifies SNAT configurations for WAN ports of SAG devices.
- [ModifySagUserDns](#): modifies DNS configurations for WAN ports of SAG devices.

3.2.3. Configure a leased line port

A Smart Access Gateway device (SAG) device can connect to Alibaba Cloud through a leased line. You can connect private networks to Alibaba Cloud through leased lines or Internet connections established by SAG devices. The Internet connection and leased line connection of an SAG device can back up each other to enhance the network reliability. This topic describes how to configure a leased line port in the SAG console.

Prerequisites


An SAG-1000 device is used.

Context


You can connect private networks to Alibaba Cloud through leased lines. Leased lines can bypass the Internet service provider (ISP) to keep the network stable and prevent data theft during data transmission. This provides a more secure and faster network connection with lower latency. For more information, see [What is Express Connect?](#).


After you connect a private network to an SAG device, the SAG device connects the private network to Alibaba Cloud through a leased line or over the Internet. This maintains network connections between your private network and Alibaba Cloud. If an SAG device is connected to a leased line, the leased line provides active network connections. When an error occurs in the leased line, the SAG device switches to the Internet to maintain network connections between the private network and Alibaba Cloud.


Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Choose one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click **Device Management**.
 - Find the target SAG instance. In the **Actions** column, choose  > **Device Management**.

3. On the **Device Management** tab, click **Manage Leased Lines**.

 **Note** Make sure that the leased line role is assigned to a port of the SAG device. For more information, see [Assign a role to a port](#).


4. On the **Manage Leased Lines** tab, find the target port and click .
5. Configure the port and click **OK**.
 - If you do not need to configure a sub port, you can click **Edit** in the **Actions** column to configure the leased line port.

 **Note**

The default VLAN code of the leased line port is 0. This indicates that the leased line port is a physical port and you cannot assign sub ports to it.

- If you want to add multiple sub ports to the leased line port, click **Add** in the **Actions** column. Set the following parameters.

Parameter	Description
IP	The IP address of the leased line port. For example: 192.168.1.1.
Subnet Mask	The subnet mask of the IP address of the leased line port. For example: 255.255.255.0.
Port	By default, the port assigned in the preceding step is used. You cannot modify this parameter.
VLAN	The VLAN code of the leased line port. Valid values: 1 to 4094. Default value: 0.


 **Note** If you want to enable the Border Gateway Protocol (BGP) for the leased line port, follow these steps:

6. After you configure the leased line port, select a routing method for the port.
 - o Static routing: uses static routing after the port is configured. In this case, you must add a static route to transmit data through a leased line. For more information, see [Add a static route](#).
 - o Dynamic routing: You can enable BGP for the target port.
 - a. Click the **Manage Routes** tab. In the **BGP Protocol Settings** section, set the parameters. For more information, see [Configure BGP routing](#).
 - b. In the **Leased Line Dynamic Routing Settings** section, find the target port and click **Edit** in the **Actions** column.
 - c. On the **Modify Leased Line Dynamic Routing Settings** page that appears, select **Enable BGP** and enter the IP address and autonomous system (AS) code of the peer port. Click **OK**.

3.2.4. Configure a LAN port

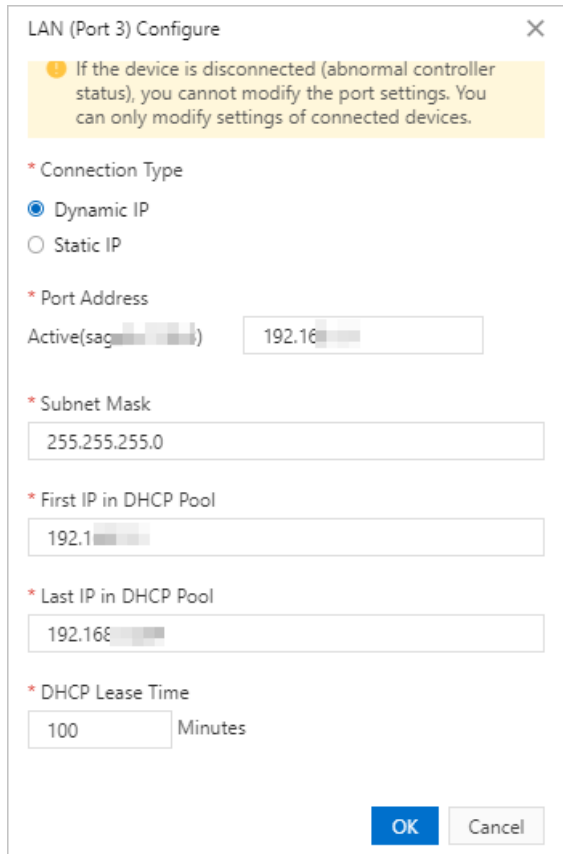
A Smart Access Gateway (SAG) device connects to a local terminal or switch through a LAN port. The SAG device then connects your private network to Alibaba Cloud. This allows you to access resources deployed on Alibaba Cloud. This topic describes how to configure a LAN port of an SAG device in the SAG console.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Choose one of the following methods to open the **Device Management** tab.
 - o Click the ID of the target SAG instance. On the instance details page that appears, click **Device Management**.
 - o Find the target SAG instance. In the **Actions** column, choose  > **Device Management**.
3. On the **Device Management** tab, click **Manage LAN Ports**.
4. Find the target port and click **Edit**.
5. On the configuration page that appears, select a connection type for the LAN port.
 - o **Dynamic IP**: The LAN port dynamically assigns an IP address through DHCP to the connected

device.

If the local network connected to the LAN port has a large number of unspecified users, and you must assign IP addresses for them, we suggest that you select this option. This connection type uses DHCP to dynamically manage and assign IP addresses. This improves IP address utilization and reduces your operation and maintenance workload.



Parameter	Description
Connection Type	In this example, Dynamic IP is selected.
Port Address	The IP address of the LAN port.
Subnet Mask	The subnet mask of the LAN port IP address.
First IP in DHCP Pool	The first IP address of the DHCP pool. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>? Note The DHCP pool must not contain the IP address of the LAN port or the broadcasting address of the CIDR block.</p> </div>
Last IP in DHCP Pool	The last IP address of the DHCP pool.
DHCP Lease Time	The time duration that the IP address is retained after it is assigned through DHCP. Valid values: 1 to 43200. Unit: minute.

- **Static IP:** specifies a static IP address for the LAN port.

If the LAN port is connected to a switch deployed in the private network, and the local terminal does not need to assign IP addresses through the SAG device, we recommend that you select this option. You can specify a static IP address for the LAN port to facilitate management.

Parameter	Description
Connection Type	In this example, Static IP is selected.
Port Address	The IP address of the LAN port.
Subnet Mask	The subnet mask of the LAN port IP address.

6. Click **OK**.

3.2.5. Configure HA for SAG devices

Smart Access Gateway (SAG) supports high availability (HA). This topic describes how to configure HA for SAG devices in the SAG console to prevent single point of failures (SPOFs).

Prerequisites


- Two SAG devices are purchased and the version of the SAG instance is 1.8.0 or later.
- The two SAG devices used to implement HA are of the same device type.
- The ports of the two SAG devices used to implement HA are assigned the same role.
- The IP addresses of the peer ports used to connect the two SAG devices fall into the same CIDR block.

Context

Static HA combines multiple routers into one virtual router. The IP address of the virtual router is used as the default gateway address for hosts in the LAN to establish connections with external networks. When an error occurs in the active gateway device, the HA feature chooses a standby device as the new active device to forward network traffic. HA maintains connections between networks. Dynamic HA does not require virtual IP addresses. The system runs health checks on the gateway devices. When an error occurs in the active gateway device, connections are automatically switched to a standby device.


SAG supports HA pairs that consist of two SAG devices. The active and standby devices are specified by the system. You can check the active and standby SAG devices in the SAG console. If an error occurs in the active device, network connections are automatically switched to the standby device. When the active device becomes functional again, connections are switched back to the active device.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Device Management** tab.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.

3. On the **Device Management** tab, click **Manage HA**.
4. In the **HA Information** section, click the **Edit** icon.
5. In the Configure HA dialog box that appears, select an HA mode.

The following table describes the parameters.

Parameter	Description
HA Mode	<p>Select whether to enable or disable HA.</p> <ul style="list-style-type: none"> ◦ To disable HA, select Disable. ◦ If you select Static, static HA is enabled. This mode applies to scenarios that use static routing. You must specify the port and virtual IP address. ◦ If you select Dynamic, dynamic HA is enabled. This mode applies to scenarios that use dynamic routing.
Port	This parameter is required if you choose to enable static HA mode. Select the device port that uses static routing.
Virtual IP	<p>Enter the virtual IP address of the SAG devices. Enter the virtual IP address in dotted decimal notation, for example, 192.168.0.2.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p> Note</p> <ul style="list-style-type: none"> ◦ The specified virtual IP address and the IP address of the port must fall into the same CIDR block, and cannot overlap with IP addresses that are already assigned to other ports in the same CIDR block. ◦ The active and standby SAG devices must have the same virtual IP address. ◦ You must set the next hop of the Alibaba Cloud-facing route of the core switch to the specified virtual IP address. </div>

6. Click **Save**.

3.2.6. Configure the management port

You can log on to the web console of a Smart Access Gateway (SAG) device through its management port. In the web console, you can configure the SAG device. This topic describes how to modify the settings of the management port in the SAG console for an SAG device.


Prerequisites

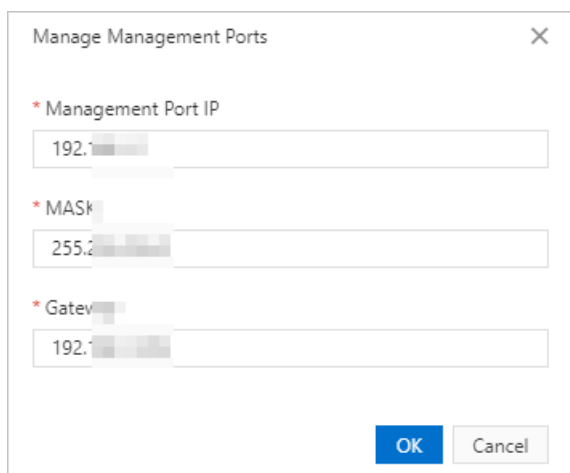
The type of the SAG device is SAG-1000.

Context

- The default CIDR block of the management port of an SAG-1000 device is 192.168.0.0/24 and the default IP address is 192.168.0.1. If you need to use a network cable to connect a local client to the management port of the SAG device, and then log on to the web console from the client, you must configure an IP address within 192.168.0.0/24 on the client. For more information, see [Configure the SAG-1000 device in the web console](#). You can also follow the procedure in this topic to configure the management port.
- Port 2 of an SAG device is the default management port. This port is exclusive and cannot be modified.
- The exclusive management port supports only logons to the web console. This port cannot be used to forward data.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Device Management** tab.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.
3. On the **Device Management** tab, click **Manage Management Ports**.
4. In the **Management Port Information** section, click the **Edit** icon.
5. In the **Manage Management Ports** dialog that appears, set the following parameters.



Parameter	Description
Management Port IP	Enter the IP address of the management port.
MASK	Enter the subnet mask of the IP address of the management port.

Parameter	Description
Gateway	Enter the IP address of the gateway. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> ? Note To access the web console across CIDR blocks, you must specify the gateway IP address. </div>

6. Click OK.

3.2.7. Quick diagnosis

Smart Access Gateway (SAG) provides quick diagnosis to detect and troubleshoot issues in SAG configurations, Internet quality, and workload quality. This allows you to find and handle network issues at the earliest opportunity.

Context

When you connect private networks to Alibaba Cloud through SAG devices, network issues may occur due to poor Internet quality or incorrect configurations. This topic describes how to use quick diagnosis.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to go to the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page, click **Device Management**.
 - Find the target SAG instance and choose **> Device Management** in the **Actions** column.
3. On the **Device Management** tab, click **Quick Diagnosis**.
4. Click **Diagnose** to diagnose the network status. The following table lists the check items.

Type	Item	Description
	LAN port configurations	Checks the status of the LAN port on the SAG device and whether the IP address of the LAN port is correctly configured.
	WAN port configurations	Checks the status of the WAN port on the SAG device, the status of the 4G connection, and whether the IP address of the WAN port is correctly configured.
	Management port configurations	Checks the status of the management port on the SAG device and whether the IP address of the management port is correctly configured.

Type	Item	Description
SAG configurations	Leased line port configurations	Checks the status of the leased line port on the SAG device and whether the IP address of the management port is correctly configured.
	CIDR block configurations	Checks whether the CIDR blocks of the ports on the SAG device have IP addresses that overlap with each other.
	Neighbor device status	Checks whether the SAG device has Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) enabled, and whether the neighbor device is working as expected.
	High availability configurations	Checks whether the SAG device has high availability (HA) enabled and whether the HA feature is working as expected.
Workload quality	Connection status	Checks whether the SAG device is connected to the management and control center.
	Online status	Checks whether the SAG device is connected to Alibaba Cloud.
	Expiration status	Checks whether the SAG device has expired.
	CCN configurations	Checks whether the SAG device is associated with a Cloud Connect Network (CCN) instance, and whether the associated CCN instance is correctly configured.
	CIDR block configurations	Checks whether the CIDR blocks of the ports on the SAG device overlap with the CIDR blocks in the cloud.
	VPN connection	Checks the VPN connection through which the SAG device is connected to Alibaba Cloud. Check items include average latency of data transmission and packet loss.


Type	Item	Description
Internet quality	Internet connection	Checks the quality of the connection between the Internet and the SAG device. The SAG device can be connected to the Internet through a WAN port or 4G networks. Check items include average latency of data transmission and packet loss.
	DNS resolution	Checks whether the SAG device can use DNS to resolve domain names as expected.

5. After the diagnosis is completed, you can view the results and recommended solutions.

The results can be classified into the following types based on the issue severity.

Severity	Description
Error	A major issue is detected on the check item. We recommend that you handle the issue at the earliest opportunity.
Warning	A minor issue is detected on the check item. You can handle the issue as needed.
No Error	No issue is detected on the check item.

What's next


- You can click  in the upper-right corner to download the diagnosis results.
- After you fix the network issues, you can click **Diagnose Again** to verify the fixes.

3.2.8. Manage routes

3.2.8.1. Add a static route

This topic describes how to add a static route to a Smart Access Gateway (SAG) device in the SAG console.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Device Management** tab.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.
3. On the **Device Management** tab, click **Manage Routes** in the left-side navigation tree.

4. In the **Static Routes** section, click **Add Static Route**.
5. In the **Add Static Route** dialog box that appears, set the following parameters.

Parameter	Description
Destination CIDR block	Enter the destination CIDR block for which network traffic is destined. Example: 192.168.1.0/24.
Next Hop	Enter the IP address of the next hop. Example: 192.168.2.1.
Port	Enter the port from which network traffic is originated.
VLAN	Enter the ID of the VLAN. Valid values are from 1 to 4094. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p>Note</p> <ul style="list-style-type: none"> ◦ You can set this parameter only for a leased line port. The default VLAN ID is 0. ◦ Currently, only SAG-1000 devices support leased lines. </div>

6. Click **OK**.

3.2.8.2. Configure BGP routing

Smart Access Gateway (SAG) devices support Border Gateway Protocol (BGP). This topic describes how to configure BGP routing in the SAG console for an SAG device.

Prerequisites

The type of the SAG device is SAG-1000.


Context

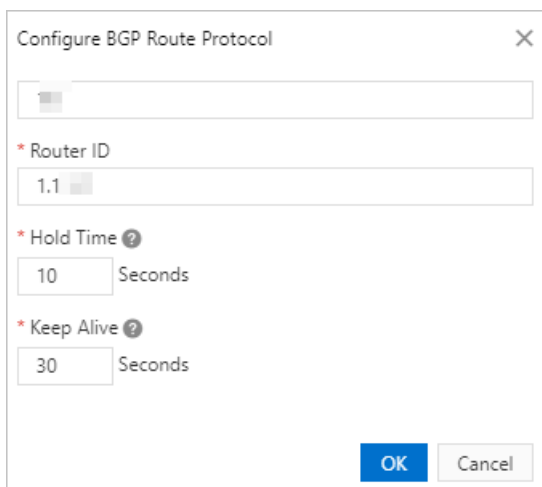
BGP is a standardized exterior gateway protocol that runs between different autonomous systems (AS)

on the Internet. BGP uses Transmission Control Protocol (TCP) as its transport protocol. BGP is designed to exchange routing and reachability information among AS. When an AS needs to exchange routing information with another one, each of them must have a specified border router. BGP ensures network security, flexibility, stability, reliability, and efficiency in many ways.


In a large-scale network, BGP is typically used to exchange and control routing information among multiple AS. SAG devices are typically deployed in one-arm mode if the scale of the network is large. BGP routes network traffic from a private network to Alibaba Cloud without changing the existing network topology and requires simple network configurations.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Use one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Device Management** tab.
 - Find the target SAG instance and choose  > **Device Management** in the **Actions** column.
3. On the **Device Management** tab, click **Manage Routes**.
4. In the **BGP Protocol Settings** section, click the **Edit** icon.
5. In the **Configure BGP Route Protocol** dialog box that appears, set the following parameters.



Parameter	Description
Local AS	Enter the number of the AS to which the SAG device belongs. Valid values: 1 to 2147483647.
Router ID	Enter the BGP router ID of the SAG device. The ID is an IPv4 address, for example, 192.168.1.1.

Parameter	Description
Hold Time	<p>Enter the period of time during which the connection between two peers is maintained.</p> <p>Valid values: 3 to 65535.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note The hold time of the peer-to-peer connection between two peer SAG devices must be set to the same for both devices. If the device does not receive a keep-alive or update message from the peer device within the hold time, the connection between the BGP peers is closed.</p> </div>
Keep Alive	<p>Enter the time interval at which keep-alive messages are transmitted.</p> <p>Valid values: 0 to 65535.</p>

6. In the **Dynamic Routing Settings** section, select **Enable BGP Protocol**.
7. Find the target port and click **Edit** in the **Actions** column.
8. In the **Modify BGP Dynamic Routing Settings** dialog box that appears, select whether to enable BGP and click **OK**.
 - **Enable BGP**: enables BGP. BGP runs between the port and its peer. You must specify the peer IP address and AS number.
 - **Disabled**: disables BGP for the port.

3.2.8.3. Configure OSPF routing

Smart Access Gateway (SAG) supports the Open Shortest Path First (OSPF) protocol. This topic describes how to configure OSPF routing for an SAG device in the SAG console.

Prerequisites

An SAG-1000 device is used.

Context


OSPF uses a link state routing (LSR) algorithm, falls into the group of interior gateway protocols (IGPs), and operates within a single autonomous system. OSPF automatically establishes a link state database and generates a shortest path tree based on the status of network ports. Each OSPF router uses these shortest path trees to construct a routing table, which implements fast convergence of the routing table and reduces network latency.

If your local network structure is constantly changing and networks are frequently added or deleted, we recommend that you use OSPF. OSPF dynamically adjusts routing based on your network changes and reduces network latency. You do not need to manually modify routing configurations. This allows you to manage and maintain your networks in a more efficient way.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Choose one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click **Device**

Management .

- Find the target SAG instance. In the **Actions** column, choose  > **Device Management .**

3. On the **Device Management** tab, click the **Manage Routes** tab.

4. In the **OSPF Protocol Settings** section, click **Edit .**

5. On the **Configure OSPF Protocol** page that appears, set the parameters as described in the following table.

Parameter	Description
Area ID	The area ID. Valid values: 1 to 2147483647.
Hello Time	The time interval at which hello packets are sent. Valid values: 1 to 65535.
Dead Time	The dead time of the OSPF neighbor. If no hello packet is received within the specified dead time, the OSPF neighbor is disconnected. Valid values: 1 to 65535.

Parameter	Description
Authentication Type	Select one of the following authorization types: <ul style="list-style-type: none"> ◦ Disable Authentication: disables authentication. ◦ Plain Text: uses plaintext authentication. A plaintext password is required. The password must be 1 to 8 characters in length, and can contain letters, digits, hyphens (-), and underscores (_). ◦ MD5 Authentication: uses MD5 authentication. An MD5 key ID and an MD5 key are required. Valid values of the MD5 key ID: 1 to 2147483647. Valid values of the MD5 key: 1 to 47.
Router ID	The IP address of the router that has enabled OSPF. Enter an IPv4 address, for example, 192.168.1.1.
Area Type	Default value: NSSA.

6. In the **WAN/LAN Dynamic Routing Settings** section, select **Enable OSPF Protocol**.
7. Find the target port and click **Edit** in the **Actions** column.
8. On the **Modify OSPF Dynamic Routing Settings** page that appears, select whether to enable OSPFs and click **OK**.
 - **Enable OSPF:** enables OSPF for the target port.
 - **Disabled:** disables OSPF for the target port.


3.2.8.4. Enable wireless connections

An SAG-100WM device supports Wi-Fi connections. This enables your mobile terminals to connect private networks to Alibaba Cloud more conveniently. This topic describes how to enable wireless connections for an SAG-100WM device in the Smart Access Gateway (SAG) console.

Prerequisites

An SAG-100WM device is used.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Choose one of the following methods to open the **Device Management** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click **Device Management**.
 - Find the target SAG instance. In the **Actions** column, choose  > **Device Management**.
3. On the **Device Management** tab, click **Manage LAN Ports**.
4. In the **LAN-Wireless** section, click **Edit**.
5. On the **WiFi Settings** page that appears, set the following parameters to enable Wi-Fi

connections.

Parameter	Description
SSID	The name of the LAN. The SSID must be 1 to 31 characters in length, and can contain digits and letters.
SSID Broadcast	You must enable SSID broadcast before other wireless devices can receive the Wi-Fi signals.
Channel	The Wi-Fi channel. Valid values: 0 to 11.
Bandwidth	An SAG-100WM device supports the following channel bandwidth: <ul style="list-style-type: none"> ◦ Automatic. ◦ 20MHz. ◦ 40MHz.
WiFi Security	<ul style="list-style-type: none"> ◦ If this switch is on, you can specify a password to allow specific users to connect to your network over Wi-Fi. ◦ If this switch is off, no password is required. Any user can connect to your network over Wi-Fi.
Authentication Type	An SAG-100WM device supports the following two authentication types. We recommend that you select WPA2-PSK, which is more secure. <ul style="list-style-type: none"> ◦ WPA-PSK. ◦ WPA2-PSK.
Encryption Algorithm	An SAG-100WM device supports the following encryption algorithms: <ul style="list-style-type: none"> ◦ Automatic: the automatic encryption algorithm. ◦ TKIP: Temporal Key Integrity Protocol. ◦ AES: Advanced Encryption Standard.
Password	Specify the password to allow specific users to connect to the Wi-Fi. The password must be 8 to 32 characters in length, and can contain digits and letters.
Confirm Password	Enter the specified password again to confirm it.

6. Click **OK**.

4. Configure networks in the cloud


4.1. Advertise routes to Alibaba Cloud

A routing method specifies how a Smart Access Gateway (SAG) device learns the private CIDR block of the on-premises network. After you configure the routing method, SAG devices can automatically advertise the learned private CIDR block of the on-premises network to Alibaba Cloud.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click **Smart Access Gateway**.
3. In the top menu bar, select the region.
4. On the **Smart Access Gateway** page, find the SAG instance.
5. Use one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the SAG instance. On the instance details page, click the **Network Configuration** tab.
 - Find the SAG instance. In the **Actions** column, click **Network Configuration**.
6. Click the **Method to Synchronize with On-premises Routes** tab.
7. Select a routing method
 - **Static Routing**: Default value. It indicates that the SAG device does not automatically learn the private CIDR block of the on-premises network. You must specify the private CIDR block of the on-premises network. Then, the specified CIDR block will be advertised to Cloud Connect Network (CCN).
 - a. Click **Add Static Route**.
 - b. In the **Add Static Route** dialog box, specify the private CIDR block to be advertised to Alibaba Cloud.

The subnet mask of the CIDR block must be 8 to 32 bits in length, which is based on the private CIDR block that the private network falls within. For example, if the IP address of an on-premises terminal is 192.168.0.100 and the subnet mask is 255.255.0.0, the CIDR block is 192.168.0.0/16.

 **Note** By default, you can add five private CIDR blocks to an SAG device. You can [submit](#) a ticket to increase the quota to at most 50.

- c. Click **OK**.
- **Dynamic Routing**: indicates that the SAG device uses dynamic routing to learn and advertise the private CIDR block of the on-premises network to CCN. In the case of dynamic routing, a dynamic routing protocol, such as BGP and OSPF, is used between the SAG device and the on-premises device (a switch or Internet-facing router). For more information about how to configure a dynamic routing protocol for an SAG device, see [Configure BGP routing](#) and [Configure OSPF routing](#).

Related information

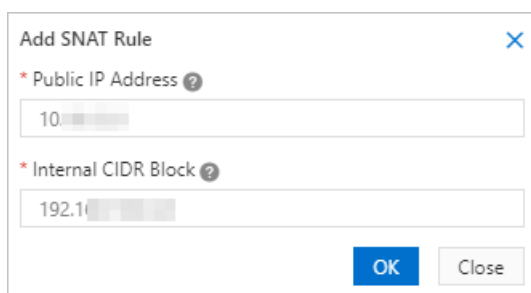
- [Modify Smart Access Gateway](#)

4.2. Configure an SNAT rule

Source Network Address Translation (SNAT) allows you to hide private IP addresses and resolve IP overlapping issues in a private network. SNAT enables a Smart Access Gateway (SAG) device to convert a private IP address to a public IP address. This allows you to access a public network from a private network whereas access from the public network to the private network is denied.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Choose one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click **Network Configuration**.
 - Find the target SAG instance and click **Network Configuration** in the **Actions** column.
3. Click the **Private Network SNAT** tab.
4. Click **Add SNAT Rule**.
5. On the **Add SNAT Rule** page, set the parameters.



The screenshot shows a dialog box titled "Add SNAT Rule" with a close button (X) in the top right corner. It contains two required input fields, each with a red asterisk and a help icon (question mark):
1. "Public IP Address" with the value "10."
2. "Internal CIDR Block" with the value "192.1".
At the bottom right, there are two buttons: a blue "OK" button and a grey "Close" button.

Set the following parameters:

- **Public IP Address:** The target public IP address after conversion.
 - **Internal CIDR Block:** The source CIDR block before conversion, which is used by the local terminal to connect to Alibaba Cloud.
6. Click **OK**.

4.3. Add a DNAT rule

Destination Network Address Translation (DNAT) maps the private IP address of an SAG device to a public IP address. DNAT allows you to access a private network from a public network. This enables the private network to provide services to the public network.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. Choose one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click **Network Configuration**.
 - Find the target SAG instance and click **Network Configuration** in the **Actions** column.
3. Click the **DNAT** tab.

4. Click **Add DNAT Rule**.
5. In the **Add DNAT Rule** dialog box, set the parameters.

The parameters are described in the following table.

Parameter	Description
DNAT Type	<p>Supported DNAT types:</p> <ul style="list-style-type: none"> ◦ Public Network DNAT: maps a private IP address to a public IP address, and automatically identifies the current public IP address. If you want to access a private network over the Internet, select this option. ◦ Private Network DNAT: maps a private IP address to a specified private IP address. Make sure that the specified private IP address does not overlap with another IP address in the private network. Select this option in these scenarios: CIDR blocks overlap with each other in the private network, you also want to access private networks over the Internet when you use SNAT to access Alibaba Cloud resources, or you want to hide the private IP address from Alibaba Cloud.
Connection Type	<p>Supported connection types:</p> <ul style="list-style-type: none"> ◦ All ports: uses IP mapping. Forwards any requests that are destined for the mapped private IP address to the target private address. ◦ Specified Port: forwards the specified protocols and port traffic that are destined for the mapped private IP address to the specified port of the target private IP address. <p>If you select Specified Port, enter the public port, private port, and protocol type based on your workload needs.</p>
Public IP Address	The source IP address before conversion.
Internal IP Address	The target IP address after conversion.
Public Port	The port that provides service after the private IP address is mapped to the public network. Valid values: 1 to 65535.
Private Port	The real port over which services are provided by the private network. Valid values: 1 to 65535.
Protocol	Valid values: TCP and UDP.

6. Click **OK**.

4.4. Attach a network instance

Smart Access Gateway (SAG) allows you to connect a private network to Alibaba Cloud through a leased line, Internet connection, or both. If you choose to use a leased line, you must associate the SAG instance with a virtual border router (VBR). If you choose to use an Internet connection, you must associate the SAG instance with a Cloud Connect Network (CCN) instance.

Prerequisites

- Before you connect your private network to Alibaba Cloud over the Internet, make sure that a CCN instance is created. For more information, see [Create a CCN instance](#).
- If you choose to use a leased line, make sure that the leased line is deployed in your private network and a VBR is created. For more information, see [What is Express Connect?](#).

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the top menu bar, select the region.
3. On the **Smart Access Gateway** page, use one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the SAG instance. On the instance details page, click the **Network Configuration** tab.
 - Find the SAG instance and click **Network Configuration** in the **Actions** column.
4. In the left-side navigation tree, click **Network Instance Details**.
5. In the **Associated Instances Under Current Account** section, click **Attach Network**.

Associated Instances Under Current Account		
Network Type	Instance ID/Name	Actions
Cloud Connect Network(CCN)	ccn- zxte#	Disassociate
Virtual Border Router(VBR)	vbr- zxte#	Disassociate

6. In the **Attach Network** dialog box, set the following parameters.

Attach Network
✕

i You can connect SAG devices to Alibaba Cloud through the Internet or leased lines. You can specify an active link and a standby link to keep your networks connected to Alibaba Cloud. If you use a leased line, you must connect the SAG instance to a VBR. If you use the Internet, you must connect the SAG instance to a CCN instance.

*** Network Type** ?

Virtual Border Router
▼

*** Region**

China (Hangzhou)
▼

*** Network Instance**

test111/vb
9wf
▼

OK

Close

Parameter	Description
Network Type	Select the type of the network instance that you want to attach. <ul style="list-style-type: none"> ◦ Cloud Connect Network: Connect the private network to Alibaba Cloud over the Internet. ◦ Virtual Border Router: Connect the private network to Alibaba Cloud through a leased line.
Region	If you choose to attach a VBR, you must select the region where the VBR is deployed.
Network Instance	Select the network instance.

7. Click **OK**.

4.5. Authorize cross-account association

You can authorize another Alibaba Cloud account to associate its Cloud Connect Network (CCN) instances or virtual border routers (VBRs) with Smart Access Gateway (SAG) instances under your account.

Prerequisites

The UID of the peer account and the ID of the CCN instance or VBR are obtained.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the top menu bar, select the region.
3. In the left-side navigation pane, click **Smart Access Gateway**.
4. On the **Smart Access Gateway** page, find the SAG instance.
5. Use one of the following methods to go to the **Network Configuration** tab of the SAG instance:
 - Click the ID of the SAG instance. On the instance details page, click the **Network Configuration** tab.
 - Find the SAG instance and click **Network Configuration** in the **Actions** column.
6. In the left-side navigation tree, click **Network Instance Details**.
7. In the **Authorized Cross-account Instances** section, click **Authorize CCN Instance**.
8. In the **Authorize CCN Instance** dialog box, set the following parameters and click **OK**.

Parameter	Description
Authorized Account UID	Enter the UID of the account that you want to authorize, for example, 168840159596****.

Parameter	Description
Network Type	Select the type of connection that is allowed to be established between your account and the peer account. Valid values: <ul style="list-style-type: none"> ◦ Cloud Connect Network: If you select this option, you must specify the ID of the CCN instance that is under the peer account. ◦ Virtual Border Router: If you select this option, you must specify the ID of the VBR that is under the peer account.
Target CCN Instance ID	Enter the ID of the peer CCN instance, for example, ccn-6dhj3m2fz7p6og****.
Peer VBR ID	Enter the ID of the peer VBR, for example, vbr-o6w14e21pzziti4tp****.

Related information

- [GrantSagInstanceToVbr](#)
- [GrantSagInstanceToCcn](#)



4.6. Advertise routes

This topic describes how to configure route advertisement policies for Smart Access Gateway (SAG) devices in the SAG console.

Prerequisites

Route advertisement is enabled. Route advertisement is disabled by default. To request the permission to use this feature, [submit a ticket](#).

Procedure

1. Log on to the [SAG console](#).
2. Use one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Network Configuration** tab.
 - Find the target SAG instance and click **Network Configuration** in the **Actions** column.
3. In the left-side navigation tree, click **Routes**.
4. Find the target destination CIDR block.
 - To set the policy for advertising a route to your private network, click  in the **Publish to On-premises** column and select a policy.
 - To set the policy for advertising a route to Alibaba Cloud, click  in the **Health Check Actions** column and select a policy.

Note An Alibaba Cloud-facing route routes network traffic from the private network to Alibaba Cloud. Routes that connect the SAG device to switches are excluded. If network traffic is routed from the private network to Alibaba Cloud through static routing, you can add static routes. For more information, see [Advertise routes to Alibaba Cloud](#).

Route advertisement policy	Description
Publish	<ul style="list-style-type: none"> Private network-facing routes: advertised to the private network through SAG. <p>Note SAG devices and client-premises equipment (CPE) must be connected through dynamic routing.</p> <ul style="list-style-type: none"> Alibaba Cloud-facing routes: advertised to CCN.
Not Publish	<ul style="list-style-type: none"> Private network-facing routes: not advertised to the private network. <p>Note SAG devices and client-premises equipment (CPE) must be connected through dynamic routing.</p> <ul style="list-style-type: none"> Alibaba Cloud-facing routes: not advertised to CCN.

5. Click **OK**.

After you set the advertisement policy for a route, you can find the target destination CIDR block and check the advertisement status in the **Publishing Status** column.

Destination CIDR Block	Route Source	Overlaps with Other CIDR Blocks	Status	Publishing Status	Health Check	Health Check Actions	Actions
10.0.0.0/24	Static Route	No	Running	Published	-	Publish	Set Health Check

4.7. Configure health check

This topic describes how to configure health check for triggering route advertisement policies in the Smart Access Gateway (SAG) console.


Prerequisites



Make sure that the following requirements are met.

- Route advertisement and health check are enabled. To request permissions to use these features, [submit a ticket](#).
- A health check instance is created. For more information, see [Create a health check instance](#).

Procedure

1. Log on to the [SAG console](#).
2. Use one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Network Configuration** tab.
 - Find the target SAG instance and click **Network Configuration** in the **Actions** column.
3. In the left-side navigation tree, click **Routes**.
4. Find the target destination CIDR block and click **Set Health Check** in the **Actions** column.
5. In the **Set Health Check** dialog box that appears, select the target health check instance and click **OK**.

 **Note** After the CIDR block is associated with the health check instance, you must set the advertisement policy again before the settings can take effect.

6. Select an advertisement policy.
 - To set the policy for advertising a route to your private network, click  in the **Publish to On-premises** column and select a policy.
 - To set the policy for advertising a route to Alibaba Cloud, click  in the **Health Check Actions** column and select a policy.

Route advertisement policy	Description
Not Publish - Publish When Health Check Succeeds	Routes are advertised only after network connectivity passes health check. Advertised routes are automatically withdrawn after network connectivity fails health check.
Not Publish - Publish when health check fails	Routes are advertised only after network connectivity fails health check. Advertised routes are automatically withdrawn after network connectivity passes health check.
Publish - Withdraw when health check succeeds	Advertised routes are withdrawn after network connectivity passes health check. Routes are automatically advertised after network connectivity fails health check.
Publish - Publish when health check fails	Advertised routes are withdrawn after network connectivity fails health check. Routes are automatically advertised after network connectivity passes health check.

7. Click **OK**.

After you set the advertisement policy for a route, you can find the target destination CIDR block and check the advertisement status in the **Publishing Status** column.

Destination CIDR Block	Route Source	Overlaps with Other CIDR Blocks	Status	Publishing Status	Health Check	Health Check Actions	Actions
10.3.0.0/28	Static Route	No	Running	Published	hc-2b...7pm	Clear	Set Health Check



4.8. Cancel health check

This topic describes how to cancel health check for a destination CIDR block in the Smart Access Gateway (SAG) console. After health check is canceled, the results of health check no longer effect route advertisement.

Procedure

1. Log on to the [SAG console](#).
2. Use one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the target SAG instance. On the instance details page that appears, click the **Network Configuration** tab.
 - Find the target SAG instance and click **Network Configuration** in the **Actions** column.
3. In the left-side navigation pane, click **Routes**.
4. Find the target destination CIDR block and click **Clear** in the **Health Check** column.
5. In the Clear Health Check Instance message that appears, click **OK**.

Note After you disassociate the health check instance from the CIDR block, you must set the route advertisement policy again before the disassociation can take effect.

6. Select a route advertisement policy. For more information, see [Advertise routes](#).
 - To set the policy for advertising a route to your private network, click  in the **Publish to On-premises** column and select a policy.
 - To set the policy for advertising a route to Alibaba Cloud, click  in the **Health Check Actions** column and select a policy.
7. Click **OK**.

4.9. Detach a network

Before you attach another network to a Smart Access Gateway (SAG) instance, you must detach the existing network.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. On the **Smart Access Gateway** page, use one of the following methods to open the **Network Configuration** tab.
 - Click the ID of the target SAG instance. On the instance details page, click the **Network**

Configuration tab.

- Find the target SAG instance and click **Network Configuration** in the **Actions** column.
3. In the left-side navigation tree, click **Network Instance Details**.
 4. In the **Associated Instances Under Current Account** section, find the target network instance and click **Disassociate** in the **Actions** column.
 5. In the message that appears, click **OK** to detach the network.

5. Health check

5.1. Create a health check instance

Smart Access Gateway (SAG) supports health check. You can create health check instances to test the network connectivity. Health check ensures that workloads can be automatically switched between different network connections. This topic describes how to create a health check instance in the SAG console.

Prerequisites

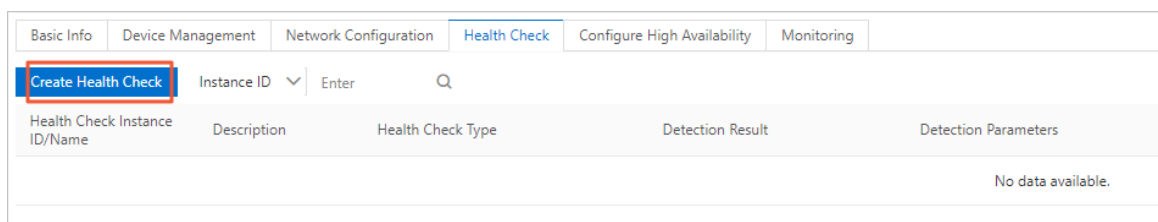
Health check is enabled. Health check is available to selected users only. To request the permission to use this feature, [submit a ticket](#).

Context

Health check tests the network connectivity between the source and destination IP addresses based on the routes associated with the health check instance. This feature ensures that workloads can be automatically switched between different network connections. After you create a health check instance, you must associate the health check instance with routes that point to the target destination CIDR block, and set the route advertisement policy. The SAG instance advertises and withdraws routes based on the result of health check and specified advertisement policy. This ensures that your workloads can be automatically switched between active and standby networks connections. For more information about associating routes with health check, see [Configure health check](#).

Procedure

1. Log on to the [SAG console](#).
2. Click the ID of the target SAG instance.
3. On the instance details page that appears, click the **Health Check** tab.
4. Click **Create Health Check**.



5. In the **Create Health Check** dialog box that appears, set the required parameters.

Create Health Check ✕

* Instance Name ?

Description ?

* Health Check Type ?

* Destination IP ?

Virtual Border Router

* Source IP ?

Parameter	Description
Instance Name	Specify a name for the health check instance. The name must be 2 to 100 characters in length and can contain digits, underscores (_), periods (.), and hyphens (-). It must start with a letter or Chinese character.
Description	Enter a description for the health check instance. The description must be 2 to 256 characters in length and can contain digits, underscores (_), periods (.), and hyphens (-). It must start with a letter or Chinese character.
Health Check Type	Select the type of packet used in health checks. Currently, only ICMP_ECHO is supported.
Destination IP	Enter the destination IP address in health checks. If you need to test the network connectivity of a leased line, select the Virtual Border Router check box and then select the target virtual border router (VBR) from the Destination IP drop-down list. <div style="background-color: #e0f2f7; padding: 5px; border: 1px solid #ccc;"> ? Note The destination IP address must be accessible through the routes used by SAG. </div>

Parameter	Description
Source IP	<p>Enter the source IP address in health checks.</p> <p>If you need to test the network connectivity of a leased line, enter an IP address in the CIDR block from which workloads are routed to the private network through the leased line.</p> <p>Note If you need to test the connectivity to different destination IP addresses, specify a unique source IP address for each destination IP address. Make sure that the source and destination IP addresses are accessible from both directions.</p>
Detection Interval	<p>Enter the health check interval. The next health check does not start only after the current one is complete. Valid values: 1000 to 60000. Default value: 2000. Unit: milliseconds.</p> <p>Note The interval must be longer than the timeout period of health checks.</p>
Detection Times	<p>Enter the number of packets to be transmitted during each health check. Valid values: 1 to 20. Default value: 1.</p>
Health Check Timeout Period	<p>Enter the timeout period of each health check. Valid values: 10 to 30000. Default value: 1000. Unit: milliseconds.</p>
Maximum Detection Failures Allowed	<p>Enter the number of consecutive health check failures that will trigger an alert. Valid values: 1 to 15. Default value: 3.</p>
Maximum RTT Allowed	<p>Enter the maximum round-trip time (RTT) allowed. Value values: -1 and 1 to 5000. Default value: -1, which indicates that no RTT threshold is set. Unit: milliseconds.</p>
Maximum Number of Times RTT Threshold Can be Exceeded	<p>Enter the maximum number of times that the RTT threshold is exceeded before an alert is triggered. Valid values: 1 to 15. Default value: 3.</p>

6. Click OK.

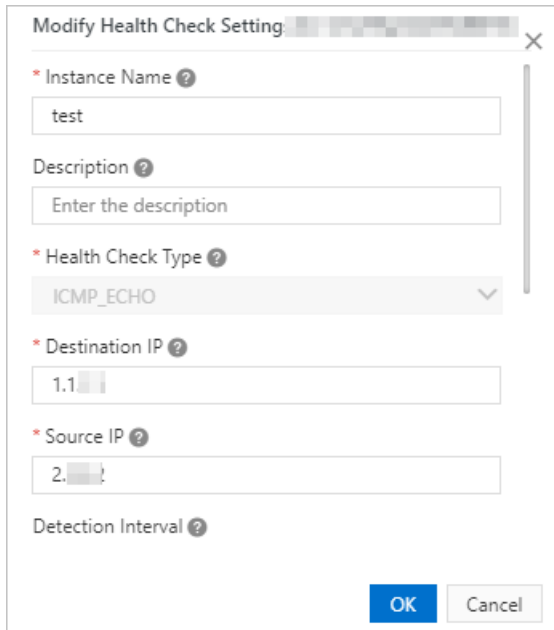
5.2. Modify a health check instance

This topic describes how to modify the settings of a health check instance.

Procedure

1. Log on to the [Smart Access Gateway \(SAG\) console](#).
2. Click the ID of the target SAG instance.
3. On the instance details page that appears, click the **Health Check** tab.
4. Find the target health check instance and click **Configure** in the **Actions** column.

5. In the **Modify Health Check Settings** dialog box that appears, modify the parameters and click **OK**. For more information about the health check parameters, see [Create a health check instance](#).



Modify Health Check Setting

* Instance Name ?
test

Description ?
Enter the description

* Health Check Type ?
ICMP_ECHO

* Destination IP ?
1.1

* Source IP ?
2.

Detection Interval ?

OK Cancel

5.3. Delete a health check instance

This topic describes how to delete a health check instance.

Procedure

1. Log on to the [Smart Access Gateway \(SAG\) console](#).
2. Click the ID of the SAG instance.
3. On the instance details page, click the **Health Check** tab.
4. Find the health check instance and click **Delete** in the **Actions** column.

Note If the health check instance that you want to delete is associated with a route, disassociate it from the route first. For more information, see [Cancel health check](#).

5. In the **Delete Health Check Instance** message that appears, click **OK**.

6.High availability

6.1. Use two SAG devices to implement HA

You can use two Smart Access Gateway (SAG) devices to implement high availability (HA). You can purchase two SAG devices and associate them with the same SAG instance. This way, when one SAG device is malfunctioning, the other SAG device takes over to ensure that your business is not interrupted. This topic describes how to view the HA configuration in the SAG console.

Prerequisites

- Two SAG devices are purchased.
- The gateway configurations of the active and standby devices are the same.

Context

SAG devices support two deployment modes: active-standby mode and active-active mode.

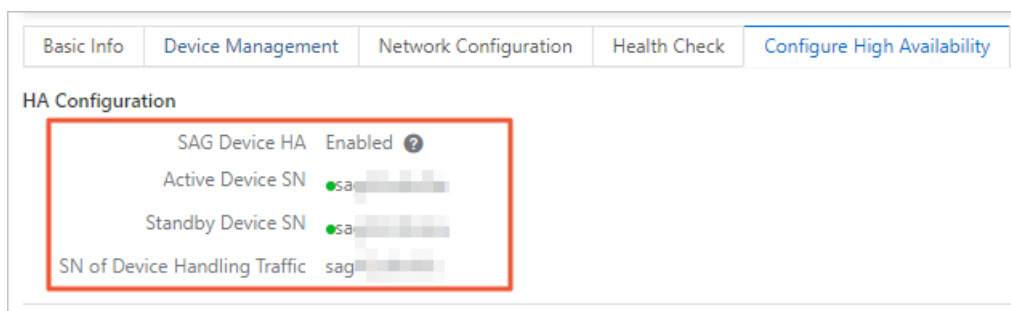
- Active-standby mode: Only the active device is connected to Alibaba Cloud. When the active device is malfunctioning, you must manually switch over to the standby device in the SAG console and connect the standby device to Alibaba Cloud.
- Active-active mode: Both devices are connected to Alibaba Cloud. The system automatically switches over to the other device when one device is malfunctioning.

By default, SAG-100WM devices run in active-standby mode. You can change the active-standby mode to the active-active mode in the SAG console. For more information, see [Switch the active-standby mode to the active-active mode](#).

SAG-1000 devices run only in active-active mode.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the top menu bar, select the region.
3. On the **Smart Access Gateway** page, click the ID of the SAG instance.
4. On the instance details page, click the **Configure High Availability** tab.
5. In the **HA Configuration** section, you can check the HA status of the SAG devices.



6.2. Use wired and wireless connections to implement HA

You can connect Smart Access Gateway (SAG) devices to the Internet through both wired and wireless connection. This implements high availability (HA). The wired connection (active) is established over the WAN port whereas the wireless connection (standby) is established over 4G. When an error occurs in the active connection, the SAG device automatically switches to the standby connection. You can check the connectivity status between your SAG devices and the Internet in the SAG console.

Prerequisites

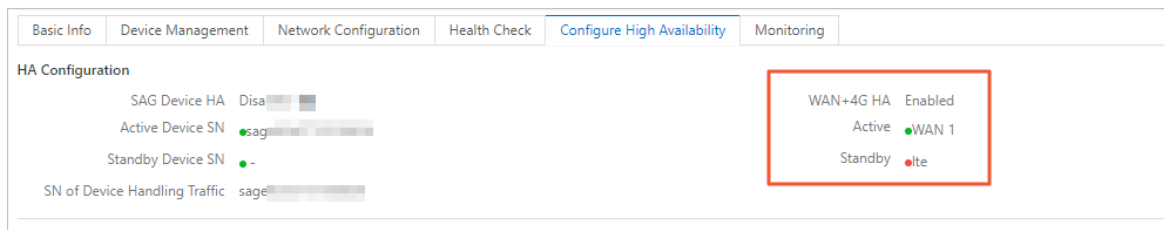
A functional 4G subscriber identity module (SIM) card is purchased from your Internet service provider (ISP) and inserted into the SAG device.

Context

A 4G SIM card is included in the accessories of each SAG device. This card is used to only receive configuration information from Alibaba Cloud, but cannot be used to transmit data. To enable an SAG device to transmit data, we recommend that you purchase a 4G SIM card from an Internet service provider (ISP). After you insert the card into an SAG device, the card can provide standby network connections to the Internet over 4G. When an error occurs in the wired (active) network, the SAG device automatically switches to the standby connection.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click **Smart Access Gateway**.
3. Find the target SAG instance and click the instance ID.
4. On the instance details page, click the **Configure High Availability** tab.
5. In the **HA Configuration** section, you can check the HA status of wired and wireless connections.



- Green: The network connection is available.
- Red: The network connection is unavailable.

6.3. Use leased lines and SAG to implement HA

SAG-1000 can provide standby connections between private networks and Alibaba Cloud. When an error occurs in the leased line, the system automatically switches to the standby connections. You can check the high availability (HA) status of leased lines and SAG devices in the Smart Access Gateway (SAG) console.

Prerequisites

- A leased line and virtual border router (VBR) are deployed. For more information, see [What is Express Connect?](#)

- The VBR is associated with the SAG instance. For more information, see [Attach a network instance](#).

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click **Smart Access Gateway**.
3. Find the target SAG instance and click the instance ID.
4. On the instance details page, click the **Configure High Availability** tab.
5. In the **HA Configuration** section, you can check the HA status of leased lines and SAG devices.



6.4. Switch the active-standby mode to the active-active mode

This topic describes how to switch the active-standby mode to the active-active mode for SAG-100WM devices.

Prerequisites

- Two SAG-100WM devices are purchased.
- The SAG-100WM devices run in active-standby mode.

Context

SAG devices support two deployment modes: active-standby mode and active-active mode.

- **Active-standby mode:** Only the active device is connected to Alibaba Cloud. When the active device is malfunctioning, you must manually switch over to the standby device in the SAG console and connect the standby device to Alibaba Cloud.
- **Active-active mode:** Both devices are connected to Alibaba Cloud. The system automatically switches over to the other device when one device is malfunctioning.

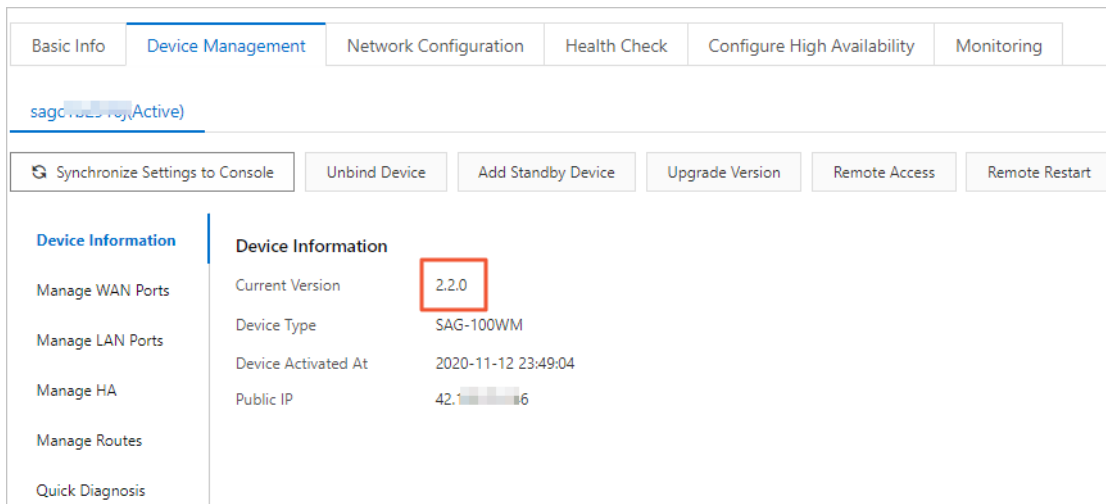
SAG-100WM devices run in active-standby mode by default. To switch to the active-active mode, perform the following steps: When you switch the active-standby mode to the active-active mode for SAG-100WM devices, note that:

- The software versions of both devices must be 1.8.0 or later.
- The software versions of both devices must be the same.

Procedure

1. Perform the following steps to view the software version of the active SAG device:
 - i. Log on to the [SAG console](#).
 - ii. In the top menu bar, select the region.
 - iii. On the **Smart Access Gateway** page, click the ID of the SAG instance.

- iv. On the instance details page, click the **Device Management** tab. In the **Device Information** section, you can view the software version of the active SAG device.



- v. (Optional) If the software version of the active device is earlier than 1.8.0, upgrade the software version. For more information, see [Upgrade an SAG device to a later version](#).

Notice

- The upgrade process takes about 10 minutes.
- The upgrade may cause network disconnections. We recommend that you upgrade your instance during off-peak hours.

2. Perform the following steps to switch over to the standby device and view the software version.
 - i. On the instance details page, click the **Configure High Availability** tab.
 - ii. In the **HA Configuration** section, click **Switch** in the **Standby Device SN** section to connect the standby device to Alibaba Cloud.
 - iii. Return to the **Device Management** tab and click the serial number of the device.
 - iv. In the **Device Information** section, you can view the software version.
 - v. (Optional) If the software version is earlier than 1.8.0, upgrade the software version. For more information, see [Upgrade an SAG device to a later version](#).

Notice


- The upgrade process takes about 10 minutes.
- The upgrade may cause network disconnections. We recommend that you upgrade your instance during off-peak hours.

3. Switch to the active-active mode.
 - i. On the instance details page, click the **Configure High Availability** tab.

- ii. In the **HA Configuration** section, click **Switch** in the **Standby Device SN** section to disconnect the standby device from Alibaba Cloud and connect the active device to Alibaba Cloud.

In active-active mode, the SAG device that is first connected to Alibaba Cloud functions as the active device. The other device that is later connected to Alibaba Cloud functions as the standby device. After you click **Switch**, the standby device is disconnected from Alibaba Cloud and the active device is connected to Alibaba Cloud.

- iii. Click **Switch to Hot Standby** in the **SAG Device HA** section to switch the mode. In the dialog box that appears, click **OK**. After you complete the preceding steps, both SAG devices run in active-active mode. In this mode, both devices are connected to Alibaba Cloud.

 **Note** If you disassociate or reassociate the SAG devices that run in active-active mode, the SAG devices will switch back to the active-standby mode.

7. QoS policies

7.1. What is a QoS policy?

Smart Access Gateway (SAG) supports quality of service (QoS) policies. QoS policies classify network traffic distributed across applications and services. You can use QoS policies to allocate bandwidth resources based on business requirements and improve network quality.

Features

QoS policies can be used to reduce network latency and network congestion. You can apply a QoS policy to an SAG instance to allocate bandwidth resources based on business requirements, reduce network latency, and improve network resource usage.

A QoS policy consists of one or more traffic throttling rules. A traffic throttling rule consists of one or more traffic classification rules. A QoS policy classifies network traffic based on the traffic classification rules and allocates bandwidth resources based on the priorities of the traffic throttling rules.

You can use the following methods to create a QoS policy:


- Create a 5-tuple

A 5-tuple includes the following tuples:

- Protocol: The protocol of the data packets. The supported protocols provided in this topic are for reference only. The actual supported protocols in the console shall prevail.
- Source CIDR block: The source CIDR block from which the data packets are sent.
- Destination CIDR block: The destination CIDR block to which the data packets are sent.
- Source port: The source port from which the data packets are sent.
- Destination port: The destination port to which the data packets are sent.

- Create an application-aware classification rule

QoS policies can use the deep packet inspection (DPI) feature to classify network traffic based on an application or an application group. The supported applications and application groups provided in this topic are for reference only. The actual supported applications and application groups in the console shall prevail.

 **Note** To classify network traffic based on applications or application groups, you must enable the DPI feature first. Only SAG instances that have the DPI feature enabled support application-aware classification rules. For more information about how to enable the DPI feature, see [Manage DPI](#). For more information about the DPI feature, see [Overview](#).

Procedure for using a QoS policy

1. Create a QoS policy.

Create traffic throttling rules and traffic classification rules for the QoS policy. For more information, see [Manage QoS policies](#).

2. Apply the QoS policy to an SAG instance.

Apply the QoS policy to an SAG instance. For more information, see [Associate with or disassociate from an SAG instance](#).

Limits

- QoS policies applied to SAG instances can throttle only outbound traffic.
- When you create a 5-tuple, make sure that the settings of the tuples do not overlap with each other.
- When you create a QoS policy that throttles traffic based on a specific bandwidth range, the system does not check whether the minimum and maximum bandwidth values specified in the policy meet the bandwidth requirements of the SAG instances to which the policy applies.

Limits

Resource	Default limit	Quota increase
The maximum number of QoS policies that can be applied to an SAG instance	1	N/A
The maximum number of traffic throttling rules that can be created in a QoS policy	3	Submit a ticket A QoS policy supports at most four traffic throttling rules.
The maximum number of QoS policies that can be created under an Alibaba Cloud account	10	Submit a ticket
The maximum number of traffic classification rules that can be created for a traffic throttling rule	50	Submit a ticket

7.2. Manage QoS policies

This topic describes how to create or delete a quality of service (QoS) policy.

Create a QoS policy

Create a QoS policy that consists of traffic throttling rules and traffic classification rules. Then, Smart Access Gateway (SAG) classifies network traffic and allocates bandwidth resources based on these rules.


1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region where the SAG instance is deployed.
3. In the left-side navigation pane, click **QoS Policy**.
4. On the **QoS Policy** page, click **Create QoS Policy**.
5. On the **Create QoS Policy** page, specify a name for the policy and create a throttling rule and a classification rule.

Section	Parameter	Description
---------	-----------	-------------

Section	Parameter	Description
Basic Information	QoS Policy Name	Specify a name for the QoS policy. The name must be 2 to 100 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter.
	QoS Policy Description	Enter a description for the QoS policy. The description must be 2 to 100 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter.
Rule	Rule Priority	Specify a priority for the rule. If bandwidth resources are insufficient during data transmission, bandwidth resources are allocated based on the priorities of the throttling rules. Valid values are from 1 to 3. A smaller value represents a higher priority. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> ? Note To set the priority to 4, you must submit a ticket. </div>

Section	Parameter	Description
	Throttling Policy	<p>You can select one of the following options to create a throttling rule:</p> <ul style="list-style-type: none"> ○ By Percentage: ensures that the percentage of bandwidth resources allocated for the specified type of service is not lower than the specified percentage. <p>If you select By Percentage, you must select the bandwidth type and set the minimum and maximum percentages. SAG supports the following bandwidth types:</p> <ul style="list-style-type: none"> ■ CCN Bandwidth: The bandwidth resources used to transfer data from the on-premises network to Alibaba Cloud. ■ Total Internet Bandwidth: The bandwidth resources used to transfer data from the on-premises network to the Internet. <p>For example, the bandwidth used to transfer data from the on-premises network to the Internet is 20 Mbit/s, and the bandwidth resources required for transferring audio data to the Internet is from 10 to 15 Mbit/s. In this case, you can select Total Internet Bandwidth and create a 5-tuple. In the 5-tuple, set the minimum percentage to 50% and the maximum to 75%.</p> <ul style="list-style-type: none"> ○ By Bandwidth: specifies the minimum and maximum bandwidth values for a specified type of service.
	5-Tuple Name	<p>Specify a name for the 5-tuple.</p> <p>The name must be 2 to 100 characters in length, and can contain digits, hyphens (-), and underscores (_). It must start with a letter.</p>
	5-Tuple Description	<p>Enter a description of the 5-tuple.</p> <p>The description must be 1 to 512 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.</p>
	Protocol	<p>Specify the protocol of the data packets.</p> <p>The supported protocols provided in this topic are for reference only. The actual supported protocols in the console shall prevail.</p>
	Source CIDR Block	<p>Specify the source CIDR block from which the data packets are sent.</p>

Section	Parameter	Description
Traffic Classification Rule	Source Port	<p>Specify the source port from which the data packets are sent.</p> <p>Valid values: 1 to 65535 and -1.</p> <p>Set the source port range in one of the following formats: 1/200 and 80/80. A value of -1/-1 specifies all ports.</p>
	Destination CIDR Block	<p>Specify the destination CIDR block to which the data packets are sent.</p>
	Destination Port	<p>Specify the destination port to which the data packets are sent.</p> <p>Valid values: 1 to 65535 and -1.</p> <p>Set the destination port range in one of the following formats: 1/200 and 80/80. A value of -1/-1 specifies all ports.</p>
	Effective Period	<p>Specify the beginning and end of the validity period of the 5-tuple.</p>
	Application Group	<p>Specify the application group to which the 5-tuple applies.</p> <p>An application group may contain multiple applications. After you specify an application group, the 5-tuple applies to all applications in the group.</p> <p>The supported application groups provided in this topic are for reference only. The actual supported application groups in the console shall prevail.</p>
	Application	<p>Specify the application to which the 5-tuple applies.</p> <p>You can select an application from the specified application group.</p> <p>The supported applications provided in this topic are for reference only. The actual supported applications in the console shall prevail.</p>

 Note

- If you specify an **Application Group** or an **Application**, the QoS policy is an application-aware QoS policy. Application-aware QoS policies can be applied to only SAG instances that have the DPI feature enabled. For more information about how to enable the DPI feature, see [Manage DPI](#).
- If you specify both an **Application Group** and an **Application**, the QoS policy is applied to all applications in the specified application group and the specified **Application**.

6. Click **Create**.

Delete a QoS policy

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region where the SAG instance is deployed.
3. In the left-side navigation pane, click **QoS Policy**.
4. On the **QoS Policy** page, find the QoS policy that you want to delete.
5. Click **Delete** in the **Actions** column.
6. In the **Delete QoS Policy** message, confirm the QoS policy and click **OK**.

Related information

- [What is a QoS policy?](#)

7.3. Associate with or disassociate from an SAG instance

This topic describes how to associate a quality of service (QoS) policy with or disassociate a QoS policy from a Smart Access Gateway (SAG) instance.

Associate a QoS policy with an SAG instance

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **QoS Policy**.
4. On the **QoS Policy** page, find the QoS policy and click **Add Instance** in the **Actions** column.
5. On the **Associate with Instance** page, select one or more SAG instances.
6. Click **Confirm Add**.

Disassociate a QoS policy from an SAG instance.

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **QoS Policy**.
4. On the **QoS Policy** page, click the ID of the QoS policy.

5. On the details page, click the **Associated Instances** tab.
6. Find the SAG instance, click **Disassociate** in the **Actions** column.
7. In the dialog box that appears, confirm the information and click **OK**.

7.4. Check the status of a QoS rule

After you create a quality of service (QoS) policy, you can check the status of its rules.

Prerequisites

You must meet the following requirements before you can check the status of QoS rules:

- A QoS policy is created. For more information, see [Manage QoS policies](#).
- The QoS policy is associated with a Smart Access Gateway (SAG) instance. For more information, see [Associate with or disassociate from an SAG instance](#).

Procedure

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region where the QoS policy is created.
3. In the left-side navigation pane, click **QoS Policy**.
4. On the **QoS Policy** page, find the QoS policy and check the status in the **Rule Status** column.
 - **Functioning**: The QoS policy has been applied to the specified SAG devices.
 - **Error**: One or more rules in the QoS policy failed to be applied to the specified SAG devices.
You can click **Learn More** to view detailed information about the error.

8. Access control


8.1. Overview

Smart Access Gateway (SAG) supports access control lists (ACLs). You can create an ACL to allow or deny specific data traffic to improve the security of your networks.

Descriptions of ACLs

An ACL is used to filter traffic based on the specified ACL rule and action policy. An ACL rule consists of match conditions and the action policy:

- Match condition: You can specify the following items as match conditions for an ACL rule: network type, rule direction, protocol type, source CIDR block, source port, destination CIDR block, destination port, application group, and application type. For more information, see [Manage ACL rules](#).

 **Note** Before you create an application-aware ACL rule, you must enable the deep packet inspection (DPI) feature. You can create application-aware ACL rules for only SAG instances that have DPI enabled. For more information about how to enable DPI, see [Manage DPI](#). For more information about DPI, see [Overview](#).

- Action policy: You can specify whether to allow or deny traffic that meets the ACL rule.

You can create one or more ACL rules for an ACL. By default, the system filters traffic based on ACL rules in descending order of rule priorities.

- If traffic meets an ACL rule, the system allows or denies the traffic based on the specified action policy. In this case, the matching process ends immediately and the system stops comparing the traffic with another ACL rule.
- If the traffic does not meet any ACL rule, the system allows the traffic by default.

Procedure

1. Create an ACL.

For more information, see [Manage ACLs](#).

2. Create ACL rules.

For more information, see [Manage ACL rules](#).

3. Associate the ACL with an SAG instance.

Associate the ACL with an SAG instance. For more information, see [Manage SAG instances associated with ACLs](#).

Limits

Item	Default limit	Quota increase
The maximum number of ACLs that can be associated with an SAG instance	1	N/A

Item	Default limit	Quota increase
The number of ACL rules that can be created for an ACL	50	Submit a ticket
The number of ACLs that can be created under an Alibaba Cloud account	10	Submit a ticket

8.2. Manage ACLs

This topic describes how to create or delete an access control list (ACL).

Create an ACL

1. Log on to the [Smart Access Gateway \(SAG\) console](#).
2. In the top navigation bar, select the region where the SAG instance is deployed.
3. In the left-side navigation pane, click **ACL**.
4. On the **ACL** page, click **Create ACL**.
5. In the **Create ACL** dialog box, specify a name for the ACL and click **OK**.

The name must be 2 to 100 characters in length, and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter.

Delete an ACL

1. Log on to the [Smart Access Gateway \(SAG\) console](#).
2. In the top navigation bar, select the region where the SAG instance is deployed.
3. In the left-side navigation pane, click **ACL**.
4. On the **ACL** page, find the ID of the ACL that you want to delete.
5. Click **Delete** in the **Actions** column.
6. In the **Delete ACL** dialog box, confirm the ACL and click **OK**.

8.3. Manage ACL rules

Smart Access Gateway (SAG) implements access control based on access control list (ACL) rules. This topic describes how to create, modify, and delete an ACL rule.

Context

An ACL rule consists of match conditions and an action policy.

- Match conditions: ACL rules can filter network traffic by network type, rule direction, protocol, source CIDR block, source port, destination CIDR block, destination port, application group, and application type. You can set match conditions based on your business requirements.
- Action policy: ACL rules can allow or block network traffic.


Create an ACL rule

1. Log on to the [SAG console](#).

2. In the top navigation bar, select the region where the ACL is deployed.
3. In the left-side navigation pane, click **ACL**.
4. On the **ACL** page, click the ID of the ACL that you want to manage.
5. On the ACL instance details page, click **Add Rule**.
6. In the **Add Rule** dialog box, set the following parameters.

Parameter	Description
Instance Name	Specify a name for the ACL rule. The name must be 2 to 100 characters in length, and can contain digits, periods (.), underscores (_), and hyphens (-).
Network Type	<ul style="list-style-type: none"> ◦ Private Network: The ACL rule controls network traffic originated from and destined for private IP addresses. ◦ Public Network: The ACL rule controls network traffic originated from and destined for public IP addresses.
Rule Direction	<ul style="list-style-type: none"> ◦ Outbound: The ACL rule controls outbound network traffic of the on-premises network that is associated with the SAG instance. ◦ Inbound: The ACL rule controls inbound network traffic of the on-premises network that is associated with the SAG instance.
Policy	Select Allow or Block to allow or block network traffic.
Protocol	Select the protocol to which the ACL rule applies. The supported protocols provided in this topic are for reference only. The actual protocols in the SAG console shall prevail.
Source CIDR Block	<ul style="list-style-type: none"> ◦ For outbound traffic: Enter the source CIDR block that initiates requests from the on-premises network. ◦ For inbound traffic: Enter the source CIDR block from which requests are sent to the on-premises network.
Source Port Range	Specify the range of the source ports. Valid values: 1 to 65535 and -1. Set the source port range in one of the following formats: 1/200, 80/80, and -1/-1. -1/-1 specifies all ports.
Destination CIDR Block	<ul style="list-style-type: none"> ◦ For outbound traffic: Enter the destination CIDR block to which requests are sent. ◦ For inbound traffic: Enter the destination CIDR block of the on-premises network to which requests are sent.

Parameter	Description
Destination Port Range	<p>Specify the range of the destination ports.</p> <p>Valid values: 1 to 65535 and -1.</p> <p>Set the destination port range in one of the following formats: 1/200, 80/80, and -1/-1. -1/-1 specifies all ports.</p>
Rule Priority	<p>Specify the priority of the ACL rule.</p> <p>Valid values: 1 to 100. A smaller value represents a higher priority. If rules have the same priority, whichever applied to the SAG devices earlier takes effect.</p> <p>The system filters requests based on ACL rules in descending order of rule priorities. The system performs the action specified in the matched rule on the requests. Requests that do not match any rule are allowed by default.</p>
Application Group	<p>Select an application group to which you want to apply the ACL rule.</p> <p>An application group may contain multiple applications. The ACL rule is applied to all applications in the selected application group.</p> <p>The supported applications provided in this topic are for reference only. The actual applications in the SAG console shall prevail.</p>
Application	<p>Select applications to which you want to apply the ACL rule.</p> <p>You can select an application from the specified application group.</p> <p>The supported applications provided in this topic are for reference only. The actual applications in the SAG console shall prevail.</p>

 **Note**

- After you select an **Application Group** or **Application**, the ACL rule is applied to the selected application group or application. Application-based ACL rules can be applied to only SAG instances that has deep packet inspection (DPI) enabled. For more information about how to enable DPI, see [Manage DPI](#).
- When you create an ACL rule, if you select an **Application Group** and an **Application**, the rule is applied to all the applications in the selected application group and the selected **Application**.

Modify an ACL rule

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region where the ACL is deployed.
3. In the left-side navigation pane, click **ACL**.
4. On the **ACL** page, click the ID of the ACL that you want to manage.
5. On the ACL instance details page, find the ACL rule that you want to modify.
6. In the **Actions** column, click **Modify**.

7. In the **Edit Rule** dialog box, modify the settings and click **OK**.

For more information about the parameters, see [Create an ACL rule](#).

Delete an ACL rule

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region where the ACL is deployed.
3. In the left-side navigation pane, click **ACL**.
4. On the **ACL** page, click the ID of the ACL that you want to manage.
5. On the ACL instance details page, find the ACL rule that you want to delete.
6. In the **Actions** column, click **Delete**.
7. In the **Delete Rule** message, click **OK**.

8.4. Manage SAG instances associated with ACLs

This topic describes how to associate Smart Access Gateway (SAG) instances with or disassociate SAG instances from access control lists (ACLs).

Associate SAG instances with an ACL

After you create an ACL, you must associate it with SAG instances so that the ACL can be applied to the SAG instances. After you associate an ACL with an SAG instance, the SAG instance can use the ACL to control network traffic that goes through the SAG instance.

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region where the ACL is created.
3. In the left-side navigation pane, click **ACL**.
4. On the **ACL** page, find the ACL that you want to manage and click **Add Instances** in the **Actions** column.
5. On the **Associated Instances** tab, click **Associate with Instance**.
6. In the **Associate with Instance** dialog box, select one or more SAG instances.
7. Click **OK**.

Disassociate instances from an ACL

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region where the ACL is created.
3. In the left-side navigation pane, click **ACL**.
4. On the **ACL** page, find and click the ID of the ACL that you want to manage.
5. On the ACL instance details page, click the **Associated Instances** tab.
6. On the **Associated Instances** tab, find the SAG instance that you want to disassociate and click **Disassociate** in the **Actions** column.
7. In the **Disassociate Instance** message, confirm the instance information and click **OK**.

9.Flow logs

9.1. Overview

Smart Access Gateway (SAG) supports flow logs that capture information about the inbound and outbound traffic of the associated SAG devices. You can monitor network traffic and troubleshoot errors based on this information. You can also analyze workloads and make informed business decisions based on flow logs.

 **Note** Flow logs are supported by only SAG-1000 devices.

Types of flow log

Flows logs are classified into the following types based on the storage location:

- Log Service flow logs

Log Service flow logs store captured traffic information in Alibaba Cloud Log Service. You can query and analyze log data in Log Service. Log Service flow logs are free of charge in public preview. Log Service charges fees for log storage and retrieval.




Log Service flow logs store the captured traffic information as log entries in Log Service. Each log entry includes the traffic information about a specific 5-tuple during a specific time period. You can specify the time period. During the specified time period, data is aggregated and then stored as a log entry.

- NetFlow flow logs

NetFlow flow logs encapsulate the captured traffic information into NetFlow packets, which are transmitted to NetFlow collectors. You can query log data on the NetFlow collectors.

Fields of flow logs

The following table lists the flow log fields and their descriptions.

Field	Description
Instance_id	The ID of the SAG instance.  Note NetFlow flow logs do not support this field.
snid	The serial number of the SAG device.  Note NetFlow flow logs do not support this field.
ali-uid	The UID of the Alibaba Cloud account.  Note NetFlow flow logs do not support this field.

Field	Description
start	The beginning of the validity period of the 5-tuple.
end	The end of the validity period of the 5-tuple.
protocol	The transport layer protocol of the network traffic.
srcaddr	The source CIDR block of the network traffic.
srcport	The source port of the network traffic.
dstaddr	The destination CIDR block of the network traffic.
dstport	The destination port of the network traffic.
packets	The number of packets transmitted during the specified time period.
bytes	The size of the packets.
tcp-flags	The TCP flags.
tos	The type of service (ToS) field in the IP header.
inport	The ID of the port that receives packets.
outport	The ID of the port and transmits packets.

Configuration procedure

The following procedure shows how to configure a flow log.

1. Create a flow log

You can specify the location where log data is stored. The type of flow log is determined by the storage location. For more information, see [Create a flow log](#).

2. Associate the flow log with an SAG instance

After you create a flow log, you must associate it with an SAG instance. The flow log captures traffic information about the associated SAG instance. For more information, see [Associate a flow log with SAG instances](#).

3. Query flow log data

After you create and associate the flow log with an SAG instance, you can query the log data. You can analyze network traffic that flows through the SAG instance, reduce business costs, and troubleshoot network errors based on the captured traffic information. For more information, see [Query flow log data](#).

9.2. Create a flow log

SAG-1000 devices support flow logs. A flow log captures information about the inbound and outbound traffic of the associated SAG-1000 device. You can monitor network traffic and troubleshoot errors based on this information. You must create a flow log before you can capture traffic information.

Prerequisites

- To store flow logs in Alibaba Cloud Log Service, make sure that the following prerequisites are met:
 - Log Service is activated. For more information, visit the [buy page of Log Service](#).
 - A Log Service Logstore and project are created. For more information, see [Create a project](#) and [Create a Logstore](#).
- To store flow logs on a NetFlow collector, make sure that network connections are established between the Smart Access Gateway (SAG) device and NetFlow collector.

Procedure

1. Log on to the [SAG console](#).
2. In the left-side navigation pane, click **Flow Log**. On the **Flow Log** page, click **Create Flow Log**.
3. In the **Create Flow Log** pane that appears, set the following parameters.

You can store captured network information in Logstores of Log Service, NetFlow collectors, or both. The parameters are describes as follows.

Parameter	Description
Name	Specify a name for the flow log.
Output Interval Under Active Connections	Specify the time interval at which log data of active network connections is collected. The default time interval is 300 seconds. We recommend that you set the interval to between 60 and 6,000 seconds.
Output Interval Under Inactive Connections	Specify the time interval at which log data of inactive network connections is collected. The default time interval is 15 seconds. We recommend that you set the interval to between 10 and 600 seconds.
Output Flow Log To	<p>Specify where you want to store the log data.</p> <ul style="list-style-type: none"> ◦ To store log data in Log Service, select sls and set the following parameters. <ul style="list-style-type: none"> ▪ SLS Region: The region where Log Service is deployed. ▪ SLS Project: The project to which the Logstore belongs. ▪ SLS Logstore: The Logstore where log data is stored. ◦ To store log data on a NetFlow collector, select netflow and set the following parameters. <ul style="list-style-type: none"> ▪ NetFlow Server Address: The IP address of the NetFlow collector, for example, 192.168.0.2. ▪ NetFlow Server Port: The port of the NetFlow collector. The default port is 9995. ▪ NetFlow Version: V5, V9, and V10 are supported. The default version is V9. ◦ To store log data both in Log Service and on a NetFlow collector, select all. You must set all the Log Service and NetFlow collector parameters.

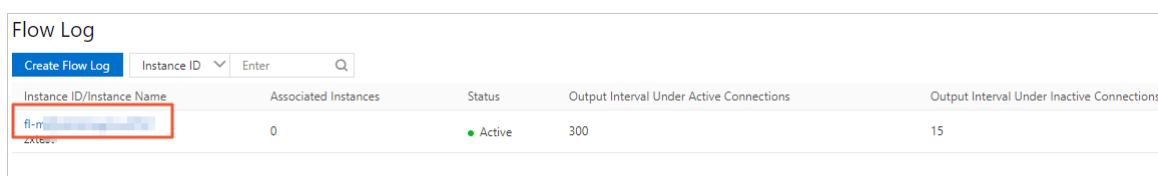
4. Click **OK**.

9.3. Associate a flow log with SAG instances

Flow logs associated with Smart Access Gateway (SAG) instance can capture information about the inbound and outbound traffic of the SAG instances. Log data is stored in Log Service or on NetFlow collectors.

Procedure

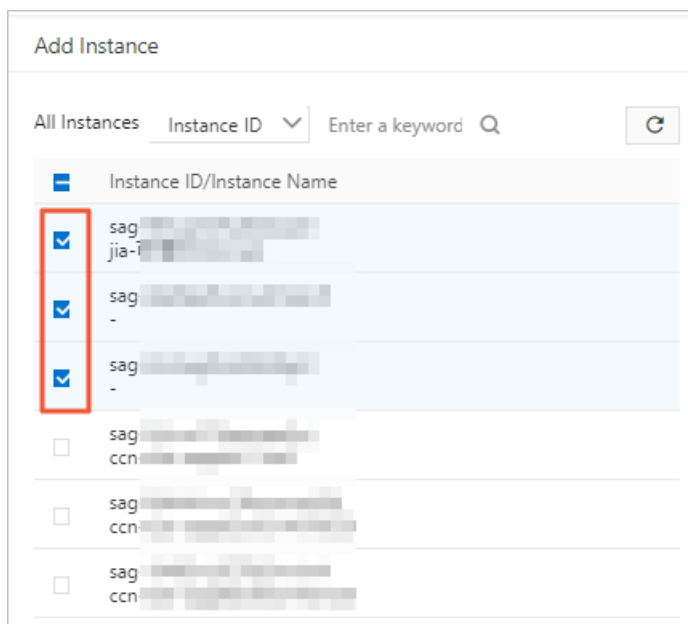
1. Log on to the [SAG console](#).
2. In the left-side navigation pane, click **Flow Log**. On the **Flow Log** page, click the ID of the target flow log.



3. On the flow log details page, click **Add Instance**.



4. In the **Add Instance** pane that appears, select one or more SAG instances and click **OK**.



9.4. Query flow log data

This topic describes how to query the data collected by a flow log associated with Smart Access Gateway (SAG) instances. Flow log data helps you monitor network traffic and troubleshoot network errors. You can also analyze workloads and make informed business decisions based on flow log data.

Query log data in Log Service

To query log data stored in Log Service, you must log on to the Log Service console.

1. Log on to the [Log Service console](#).
2. In the **Projects** list, find and click the name of the target project. Logstores under the project are listed.



3. Find and click the name of the target Logstore. Log Service allows you to query data by field. You can specify a field and click **Search & Analyze** to query and analyze data.

Query log data on NetFlow collectors

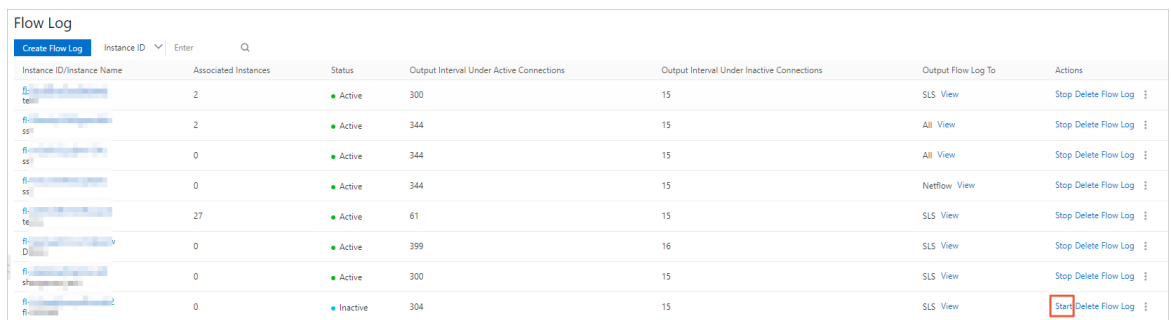
You can query flow log data on NetFlow collectors where flow logs are stored.

9.5. Enable a flow log

This topic describes how to enable an **Inactive** flow log. After a flow log is enabled, it captures the traffic information about specified Smart Access Gateway (SAG) instances.

Procedure

1. Log on to the [SAG console](#).
2. In the left-side navigation pane, click **Flow Log**.
3. On the **Flow Log** page, find the target flow log that is in the **Inactive** state and click **Start** in the **Actions** column.



After the flow log is enabled, its status changes to **Active**.

Instance ID/Instance Name	Associated Instances	Status	Output Interval Under Active Connections	Output Interval Under Inactive Connections	Output Flow Log To	Actions
E-5-tes	2	Active	300	15	SLS View	Stop Delete Flow Log
E-5-ssr	2	Active	344	15	All View	Stop Delete Flow Log
E-5-ssr	0	Active	344	15	All View	Stop Delete Flow Log
E-5-ssr	0	Active	344	15	Netflow View	Stop Delete Flow Log
E-5-tes	27	Active	61	15	SLS View	Stop Delete Flow Log
E-5-DDI	0	Active	399	16	SLS View	Stop Delete Flow Log
E-5-pha	0	Active	300	15	SLS View	Stop Delete Flow Log

9.6. Disable a flow log

This topic describes how to disable a flow log. After a flow log is disabled, it stops capturing the traffic information about specified Smart Access Gateway (SAG) instances.

Context

Disabling a flow log does not delete it. If you need to use a disabled flow log to capture traffic information, you must enable the flow log again.

Procedure

1. Log on to the [SAG console](#).
2. In the left-side navigation pane, click **Flow Log**.
3. On the **Flow Log** page, find the target flow log and click **Stop** in the **Actions** column.

Instance ID/Instance Name	Associated Instances	Status	Output Interval Under Active Connections	Output Interval Under Inactive Connections	Output Flow Log To	Actions
E-5-tes	2	Active	300	15	SLS View	Stop Delete Flow Log
E-5-ssr	2	Active	344	15	All View	Stop Delete Flow Log
E-5-ssr	0	Active	344	15	All View	Stop Delete Flow Log
E-5-ssr	0	Active	344	15	Netflow View	Stop Delete Flow Log
E-5-tes	27	Active	61	15	SLS View	Stop Delete Flow Log
E-5-DDI	0	Active	399	16	SLS View	Stop Delete Flow Log
E-5-pha	0	Active	300	15	SLS View	Stop Delete Flow Log
E-5-pha	0	Inactive	304	15	SLS View	Start Delete Flow Log

After the flow is disabled, its status changes to **Inactive**.

Instance ID/Instance Name	Associated Instances	Status	Output Interval Under Active Connections	Output Interval Under Inactive Connections	Output Flow Log To	Actions
E-5-tes	2	Active	300	15	SLS View	Stop Delete Flow Log
E-5-ssr	2	Active	344	15	All View	Stop Delete Flow Log
E-5-ssr	0	Active	344	15	All View	Stop Delete Flow Log
E-5-ssr	0	Active	344	15	Netflow View	Stop Delete Flow Log
E-5-tes	27	Active	61	15	SLS View	Stop Delete Flow Log
E-5-DDI	0	Active	399	16	SLS View	Stop Delete Flow Log
E-5-pha	0	Active	300	15	SLS View	Stop Delete Flow Log
E-5-pha	0	Inactive	304	15	SLS View	Start Delete Flow Log

9.7. Disassociate from an SAG instance

After a flow log is disassociated from a Smart Access Gateway (SAG) instance, the flow log stops capturing traffic information about the SAG instance.

Procedure

1. Log on to the [SAG console](#).
2. In the left-side navigation pane, click **Flow Log**. On the **Flow Log** page, click the ID of the target flow log.

Instance ID/Instance Name	Associated Instances	Status	Output Interval Under Active Connections	Output Interval Under Inactive Connections
fl-m- zxtbce	0	Active	300	15

3. Disassociate the flow log from one or more SAG instances at a time.
 - o Disassociate the flow log from an individual SAG instance: Find the target SAG instance and click **Remove** in the **Actions** column. In the **Remove** message that appears, click **OK**.

Instance ID/Name	Actions
<input type="checkbox"/> sag- zxtbce	Remove
<input type="checkbox"/> sag- zxtbce	Remove
<input type="checkbox"/> Batch Remove	

- o Disassociate the flow log from multiple SAG instances at a time: Select the target SAG instances and click **Batch Remove** below the instance list. In the **Remove** message that appears, click **OK**.

Instance ID/Name	Actions
<input checked="" type="checkbox"/> sag- zxtbce	Remove
<input checked="" type="checkbox"/> sag- zxtbce	Remove
<input checked="" type="checkbox"/> Batch Remove	

9.8. Delete a flow log

This topic describes how to delete an **Active** or **Inactive** flow log. After a flow log is deleted, you can view traffic information captured by it in the Log Service console or on the specified NetFlow collector.

Prerequisites

If the flow log that you want to delete is associated with a Smart Access Gateway (SAG) instance, disassociate it from the SAG instance first. For more information, see [Disassociate from an SAG instance](#).

Procedure

1. Log on to the [SAG console](#).
2. In the left-side navigation pane, click **Flow Log**.
3. On the **Flow Log** page, find the target flow log and click **Delete Flow Log** in the **Actions** column.
4. In the **Delete Flow Log** message that appears, click **OK**.

10. Access cloud services

10.1. Configure AnyTunnel

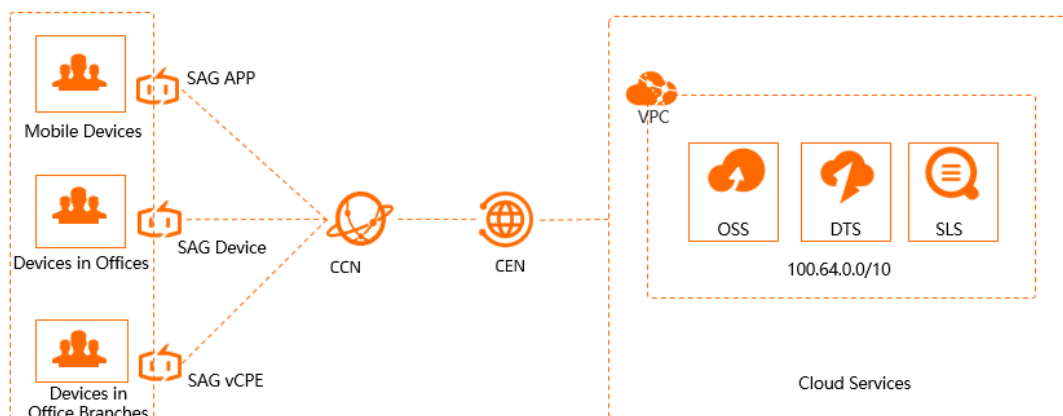
Smart Access Gateway (SAG) can access cloud services deployed in Virtual Private Cloud (VPC) networks through Cloud Enterprise Network (CEN). This topic describes how to configure AnyTunnel in the CEN console.

Prerequisites

- A CEN instance is created and VPC networks connected to the cloud services that you want to access are attached to the CEN instance. For more information, see [Create a CEN instance](#).
- The Cloud Connect Network (CCN) instance connected to your private network is associated with the CEN instance. For more information, see [Attach a network instance](#).

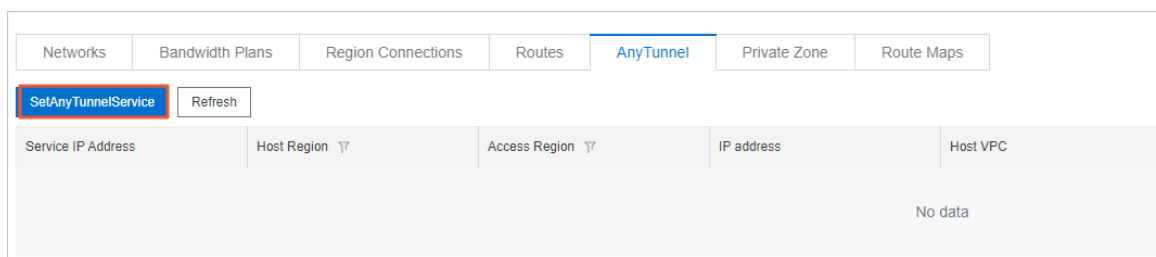
Context

Cloud services refer to Alibaba Cloud services, such as Object Storage Service (OSS), Log Service, and Data Transmission Service (DTS), that use the CIDR block 100.64.0.0/10 to provide services. To enable on-premises clients to access cloud services deployed in VPC networks, you can connect your private network to Alibaba Cloud through SAG. Then, attach the CCN instance associated with the SAG instance to a CEN instance.



Procedure

1. Log on to the [CEN console](#).
2. On the **Instances** page, click the ID of the CEN instance that you want to manage.
3. On the instance details page, click the **AnyTunnel** tab and then click **SetAnyTunnelService**.



4. In the **SetAnyTunnelService** pane, set the following parameters:

- **Service IP address:** Enter an IP address or CIDR block used by the cloud service. This IP address or CIDR block must fall into 100.64.0.0/10. For example, you can enter 100.118.28.52/32.
- **Host Region:** Select the region where the cloud service is deployed.

Note Make sure that at least one VPC network in the selected region is attached to the CEN instance.

- **Host VPC:** From the drop-down list, select the VPC network that is attached to the CEN instance.

After you select a VPC network, networks attached to the CCN instance can access the cloud service through the VPC network.

- **Access Region:** Select the CCN instance that is associated with the CEN instance.

Note Make sure that the selected CCN instance is associated with the CEN instance.

- **Description:** Enter a description for the cloud service. This parameter is optional.

The description is optional. If you enter one, it must be 2 to 256 characters in length, and can contain digits, hyphens (-), underscore (_), and periods (.). It must start with a letter or a Chinese character and cannot start with `http://` or `https://`.

SetAnyTunnelService

- **Service IP Address**
- **Host Region**
- **Host VPC**
- **Access Region**

Mainland China CCN
- Description** ?

0/256

5. Click **OK**.

Note Typically, a cloud service uses multiple IP addresses. Repeat the preceding steps to add routes to all the IP addresses of the cloud service.

Related information

- Use SAG and CEN to access OSS

10.2. Configure PrivateZone

10.2.1. Configure PrivateZone

Alibaba Cloud DNS PrivateZone (PrivateZone) is a VPC-based resolution and management service for private domain names. You can use Smart Access Gateway (SAG) to access PrivateZone through Cloud Enterprise Network (CEN). This topic describes how to configure PrivateZone in the CEN console.

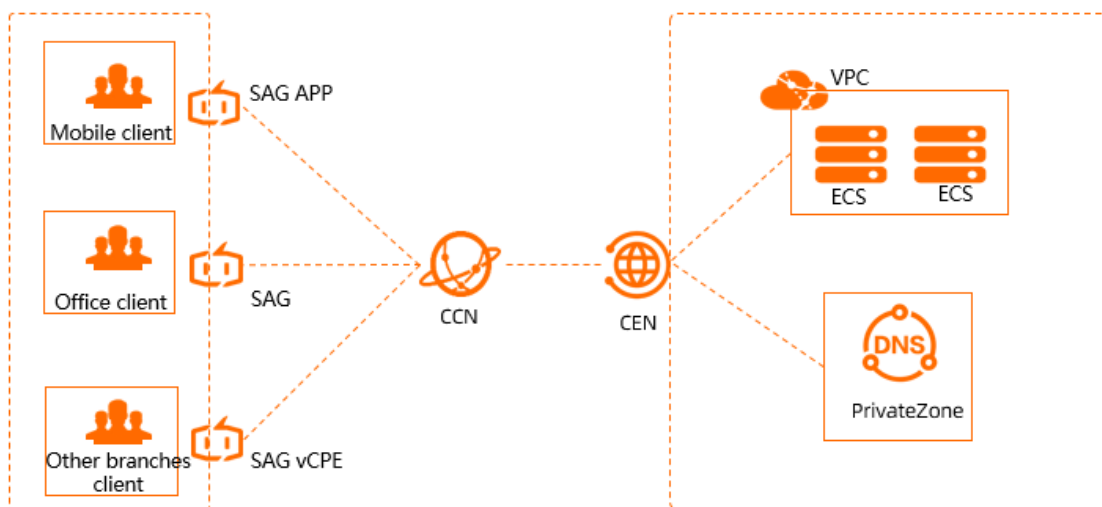
Prerequisites

- PrivateZone is activated. For more information, see [Subscribe Service](#).
- A CEN instance is created and a virtual private cloud (VPC) is attached to the CEN instance. Make sure that the VPC and PrivateZone are deployed in the same region. For more information, see [Create a CEN instance](#).
- The Cloud Connect Network (CCN) instance connected to your on-premises network is attached to the CEN instance. For more information, see [Attach a network instance](#).

Context


PrivateZone is a VPC-based resolution and management service for private domain names. You can use PrivateZone to resolve private domain names to IP addresses in one or multiple specific VPCs.

PrivateZone allows you to access Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, Object Storage Service (OSS) buckets, and other Alibaba Cloud resources by using private domain names. The private domain names are invalid outside VPCs. You can connect your on-premise network to a VPC through SAG and CEN. You can configure PrivateZone in the CEN console to allow the on-premises network and VPC to access each other through private domain names.

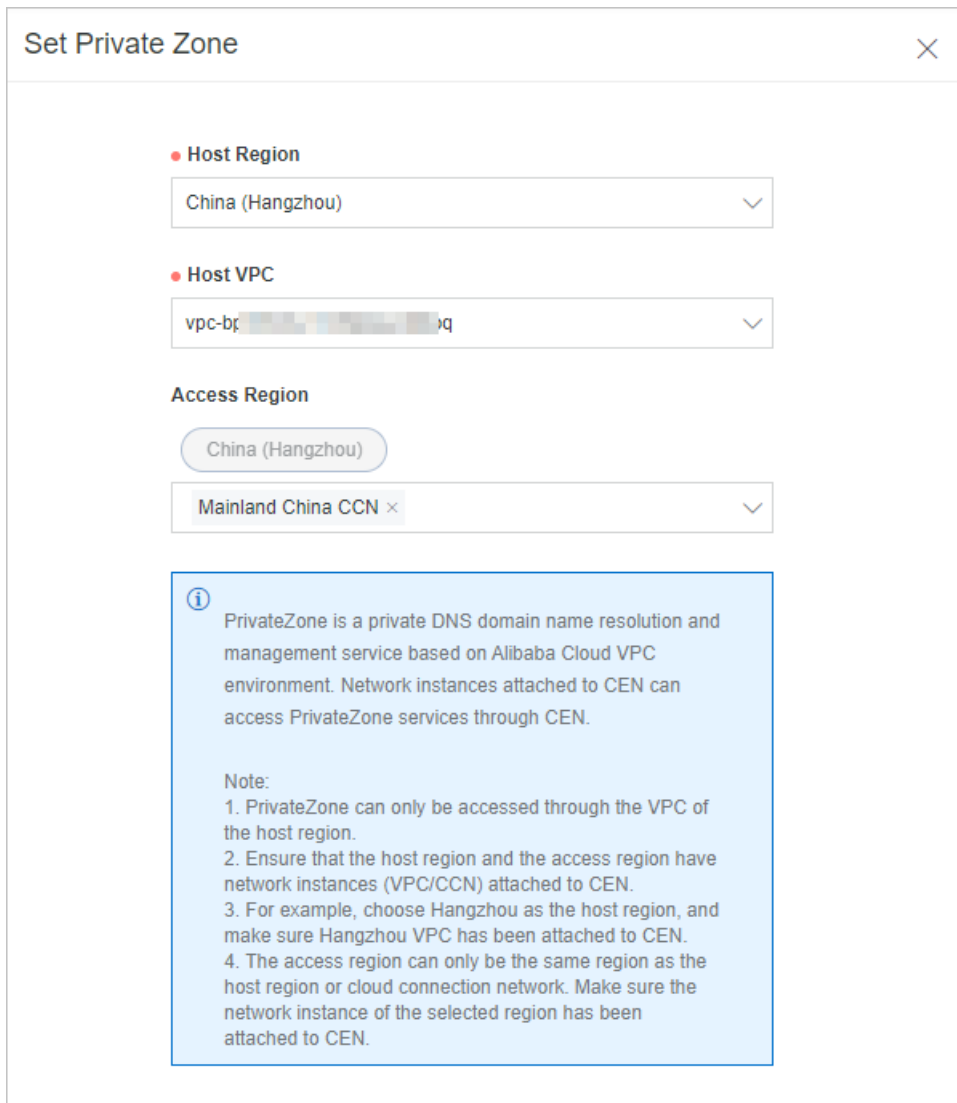


Procedure

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

 **Note** You need to confirm the authorization only when it is your first time configuring PrivateZone.

4. On the **Cloud Resource Access Authorization** page, click **Confirm Authorization Policy** to allow the on-premises network to access PrivateZone. Make sure that the on-premises network is associated with the CCN instance that is attached to the CEN instance.
5. Click **Set Private Zone**. In the **Set Private Zone** pane, set the following parameters:



Set Private Zone [X]

● **Host Region**
China (Hangzhou) [v]

● **Host VPC**
vpc-bj... [v]

Access Region
China (Hangzhou) [v]
Mainland China CCN [x] [v]

Note:
PrivateZone is a private DNS domain name resolution and management service based on Alibaba Cloud VPC environment. Network instances attached to CEN can access PrivateZone services through CEN.

Note:

1. PrivateZone can only be accessed through the VPC of the host region.
2. Ensure that the host region and the access region have network instances (VPC/CCN) attached to CEN.
3. For example, choose Hangzhou as the host region, and make sure Hangzhou VPC has been attached to CEN.
4. The access region can only be the same region as the host region or cloud connection network. Make sure the network instance of the selected region has been attached to CEN.

- i. **Host Region**: Select the region of the VPC for which PrivateZone is enabled.
- ii. **Host VPC**: Select the VPC for which PrivateZone is enabled.

PrivateZone can be accessed only over the specified VPC.

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

Note

- Set Access Region to the CCN instance that is deployed in the same region as that of PrivateZone. Make sure that the specified CCN instance is attached to the CEN instance.
- If the CCN instance, CEN instance, and VPC are under different Alibaba Cloud accounts, you must acquire permissions from the peer accounts. For more information, see [Acquire or grant permissions](#).

iv. Click OK.

10.2.2. Acquire or grant permissions

If you want to access Alibaba Cloud DNS PrivateZone (PrivateZone) through your on-premises network, you must acquire or grant relevant permissions. Make sure that the on-premises network is associated with a Cloud Connect Network (CCN) instance that is attached to a Cloud Enterprise Network (CEN) instance.

Scenario 1: All under the same account

If the CCN instance, CEN instance, and VPC for which PrivateZone is enabled are under the same account, you can click **Authorization** on the **Private Zone** tab to complete authorization.

Note You need to confirm the authorization only when it is your first time configuring PrivateZone.

Item	User ID (UID) of the account
CEN	111111
VPC	111111
CCN	111111

After authorization is completed, the system automatically creates a Resource Access Management (RAM) role named **AliyunSmartAGAccessingPVTZRole**. You can view this role on the **RAM Roles** page of the [RAM console](#).


The screenshot shows the RAM console interface. On the left is a navigation menu with 'Roles' selected. The main content area displays 'Roles' with a 'What are RAM Roles?' section explaining that RAM roles are a secure way to grant permissions to trusted entities. Below this is a 'Create Role' button and a search bar containing 'AliyunSmartAGAccessingPVTZRole'. A table lists the role details:

Role Name	Note	Created
AliyunSmartAGAccessingPVTZRole	智能接入网关(SmartAG)默认使用此角色来访问您在其他云产品中的资源	May 8, 2020, 17:04:13


Scenario 2: CCN instance under a different account

If the CEN instance and VPC are under the same account but the CCN instance is under a different account, you must modify the authorization policy.

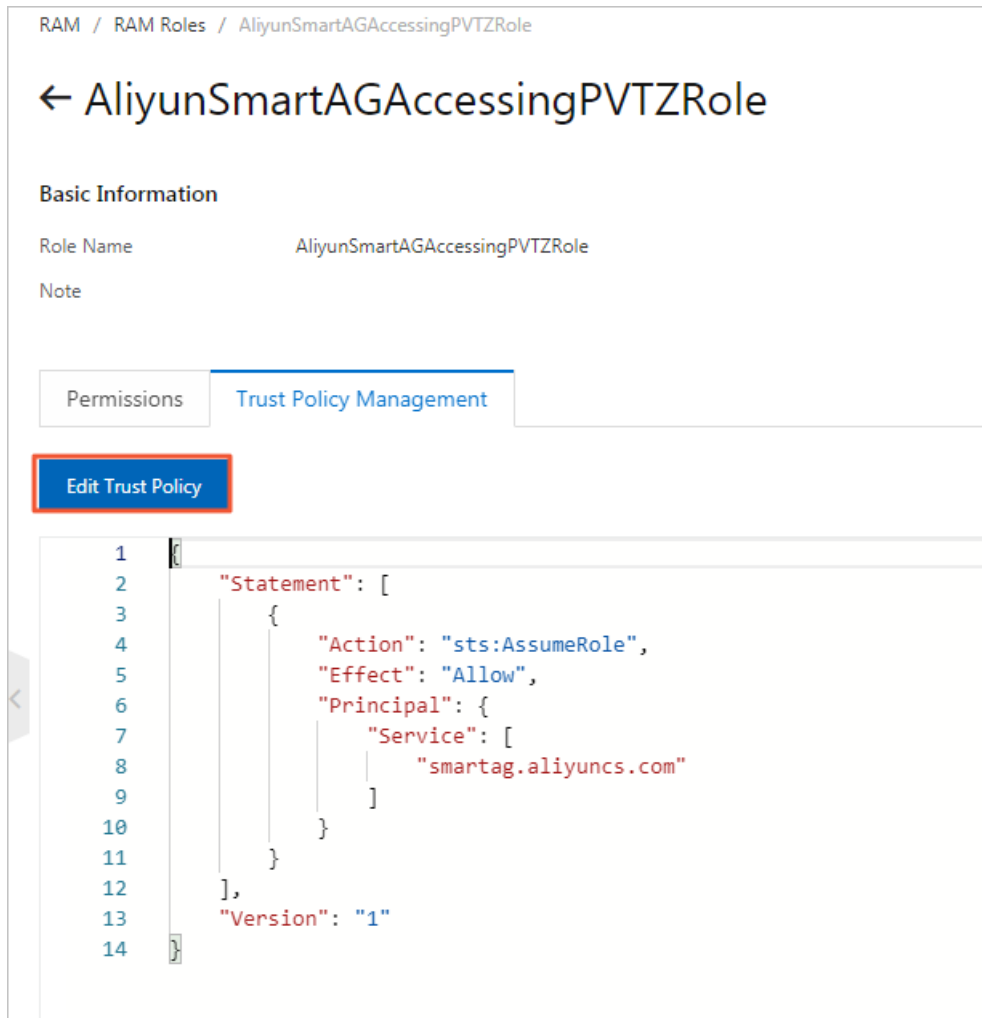
Item	UID of the account
CEN	111111
VPC	111111
CCN	333333

 **Notice** You must perform the following operations with the account to which the VPC belongs.

1. Log on to the [CEN console](#).
2. Click the ID of the CEN instance.
3. Click **Private Zone**, and then click **Authorization** to complete authorization.

 **Note** You need to confirm the authorization only when it is your first time configuring PrivateZone.

4. Log on to the [RAM console](#).
5. In the left-side navigation pane, click **RAM Roles**.
6. Enter **AliyunSmartAGAccessingPVTZRole** in the search box and click the name of the policy that appears.
7. Click the **Trust Policy Management** tab, and then click **Edit Trust Policy**.



8. Add `UID of the CCN account@smartag.aliyuncs.com` to the Service field, and then click OK.

Scenario 3: CEN instance under a different account

If the CCN instance and VPC are under the same account but the CEN instance is under a different account, you must create an authorization policy with the account to which the VPC belongs.

Item	UID of the account
CEN	333333
VPC	111111
CCN	111111

1. Log on to the [RAM console](#) with the account to which the VPC belongs.
2. In the left-side navigation pane, click **RAM Roles**.
3. Set the following parameters and click OK. For more information, see [Create a RAM role for a trusted Alibaba Cloud service](#).
 - **Trusted entity type:** Select **Alibaba Cloud Service**.
 - **Role Type:** Select **Normal Service Role**.

- **RAM Role Name:** Enter **AliyunSmartAGAccessingPVTZRole**.
- **Select Trusted Service:** Select **Smart Access Gateway**.

Create RAM Role

1 Select Role Type — 2 Configure Role — 3 Finish

Select Type of Trusted Entity
Alibaba Cloud Service

Role Type
 Normal Service Role Service Linked Role [?](#)

* RAM Role Name
AliyunSmartAGAccessingPVTZRole
The name can contain a maximum of 64 characters, only English letters, numbers, and hyphens (-) are accepted.

Note

* Select Trusted Service
Smart Access Gateway

4. Click the name of the newly created RAM role.
5. On the **Permissions** tab, click **Add Permissions**.
6. Enter **pvtz** in the search box below **System Policy**, and then click **AliyunPvtzReadOnlyAccess** to add read-only permissions on PrivateZone. For more information, see [Grant permissions to a RAM role](#).

Add Permissions

* Principal
AliyunSmartAGAccessingPVTZRole@... X

* Select Policy
System Policy Custom Policy + Create Policy

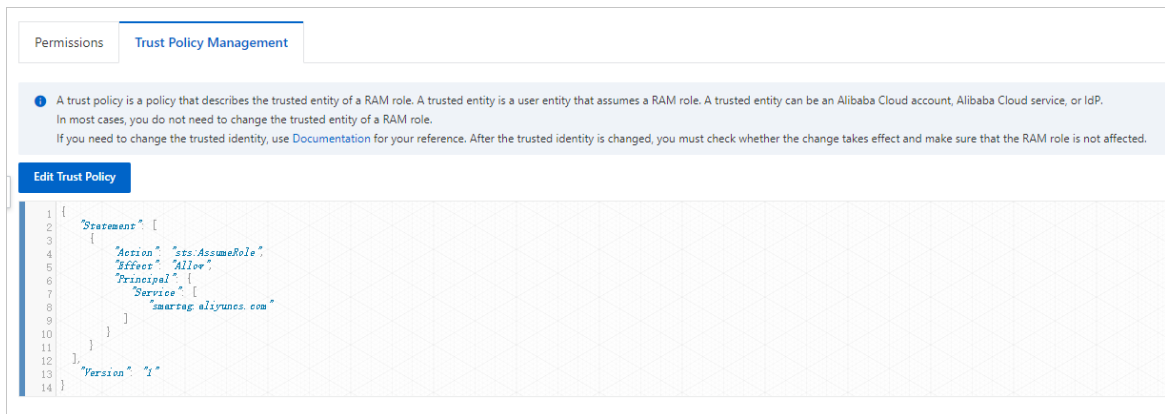
pvtz

Authorization Policy Name	Description
AliyunPvtzFullAccess	Provides full access to Cloud DNS Private Zone via Man...
AliyunPvtzReadOnlyAccess	Provides read-only access to Cloud DNS Private Zone vi...

Select a policy.

Selected (0) Clear

- After the authorization is completed, you can click **Trust Policy Management** to view authorization information.



Scenario 4: All under different accounts

If the CCN instance, CEN instance, and VPC are under different accounts, you must perform the following operations:

Item	UID of the account
CEN	111111
VPC	222222
CCN	333333

- Refer to Scenario 3 and create a RAM role with the account to which the VPC belongs.

For more information, see [Scenario 3: CEN instance under a different account](#).



- Refer to Scenario 2 and add `UID of the CCN account@aliyuncs.com` to an existing policy with

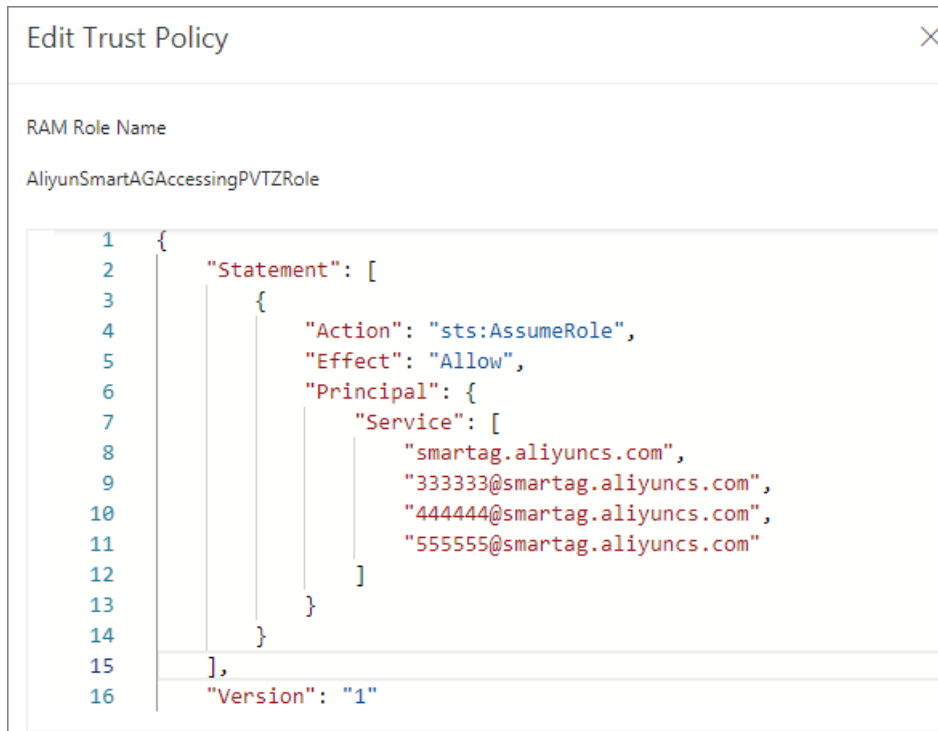
the account to which the VPC belongs.

For more information, see [Scenario 2: CCN instance under a different account](#).



If you have multiple CCN instances and each CCN instance is under a different account, only add the CCN instances that require access to PrivateZone.

Item	UID of the account
CEN	111111
VPC	222222
CCN	333333
CCN	444444
CCN	555555



```
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"
```

11.DPI

11.1. Overview

Smart Access Gateway (SAG) supports the deep packet inspection (DPI) feature. The DPI feature allows you to create application-aware quality of service (QoS) policies and access control lists (ACLs) and view monitoring data of applications. This feature regulates network traffic routes through simple and effective solutions and analyzes traffic distribution to provide a better user experience.

Introduction to DPI

DPI retrieves the payload of data packets to identify and re-organize the application data transmitted through the application layer. This allows DPI to gain full insights into an application and filter data packets based on system control policies. In addition, the system can display the distribution of network traffic based on the application data collected by DPI.

DPI supports the following features:

- Application-aware QoS policies
- Application-aware ACLs
- Traffic monitoring based on applications

When you create a QoS policy or an ACL, you must specify an application. DPI identifies and analyzes network traffic based on the specified application and performs operations based on system control policies. You can choose one of the following methods to specify applications:


- Specify applications: DPI identifies each application. When you create a policy, you can specify an application.
- Specify application groups: DPI classifies applications into groups based on the application characteristics. When you create a policy, you can specify an application group. After you specify an application group, the policy applies to all applications in the group.

Procedure for using DPI

The DPI feature is disabled by default. You must enable and configure the DPI feature before you can use it.

 **Note** The following SAG device models support the DPI feature: SAG-1000.

1. Enable the DPI feature. For more information, see [Manage DPI](#).
2. Create a policy based on your business requirements.
 - Create an application-aware QoS policy. For more information, see [What is a QoS policy?](#).
 - Create an application-aware ACL. For more information, see [Overview](#).
 - View monitoring data of applications. For more information, see [View traffic monitoring data of applications](#).

 **Note** You must enable the DPI-based monitoring feature for the SAG instance before you can view the traffic monitoring data. For more information, see [Manage DPI](#).

11.2. Manage DPI

This topic describes how to enable or disable the deep packet inspection (DPI) feature and the DPI-based monitoring feature for a Smart Access Gateway (SAG) instance.

Prerequisites

The SAG instance for which you want to manage DPI is associated with an SAG-1000 device.

Context


The DPI feature allows you to create application-aware quality of service (QoS) policies and access control lists (ACLs) to manage network traffic. In addition, you can view monitoring data of applications. DPI regulates network traffic routes through simple and effective solutions and analyzes traffic distribution.

Enable DPI


1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. On the **Smart Access Gateway** page, click the ID of the SAG instance.
4. On the **Basic Info** tab, find the **Advanced Features** section and turn on the **DPI** switch.
5. In the **Enable DPI** message, click **OK**.

Enable DPI-based monitoring

SAG is integrated with Log Service to provide the DPI-based monitoring feature. You can use this feature to analyze traffic distribution of different applications.

 **Note** You must activate Log Service before you can enable DPI-based monitoring. You are charged when you activate Log Service. For more information about the billing rules of Log Service, see [Overview](#). For more information about Log Service, see [What is Log Service?](#)

1. Log on to the [Smart Access Gateway console](#).
2. In the top navigation bar, select the region.
3. On the **Smart Access Gateway** page, click the ID of the SAG instance.
4. On the details page of the SAG instance, choose **Monitoring > DPI Statistics on Applications**.
 - i. In the **Enable DPI** section of the **DPI Statistics on Applications** tab, click **Enable**.

 **Note** If DPI is already enabled, skip this step.

- ii. In the **Activate Log Service** section, click **Activate Now**.

After these features are enabled, the traffic monitoring data of the SAG instance is displayed. For more information, see [View traffic monitoring data of applications](#).

Disable DPI-based monitoring

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.

3. On the **Smart Access Gateway** page, click the ID of the SAG instance.
4. On the details page of the SAG instance, choose **Monitoring > DPI Statistics on Applications**.
5. In the upper-right corner of the **DPI Statistics on Applications** tab, click **Disable DPI-based Monitoring**.
6. In the **Disable DPI-based Monitoring** message, click **OK**.

Disable DPI

If you disable DPI for an SAG instance, DPI-based monitoring is also disabled. In addition, the application rules of the QoS policies and ACLs that are associated with the SAG instance become invalid.

1. Log on to the **SAG console**.
2. In the top navigation bar, select the region.
3. On the **Smart Access Gateway** page, click the ID of the SAG instance.
4. On the **Basic Info** tab, find the **Advanced Features** section and turn on the **DPI** switch.
5. In the message that appears, click **OK**.

12. Application acceleration

12.1. Overview

After your on-premises networks are connected to Alibaba Cloud through Smart Access Gateway (SAG), you can use application acceleration plans to quickly and stably access applications that are deployed in regions outside mainland China.

Limits

- Application acceleration plans can be used only in scenarios where clients in mainland China access applications that are deployed in regions outside mainland China.
- SAG vCPE instances do not support application acceleration plans.
- If you use an SAG CPE instance, the version of the SAG device that is associated with the SAG instance must be 2.4.0 or later.

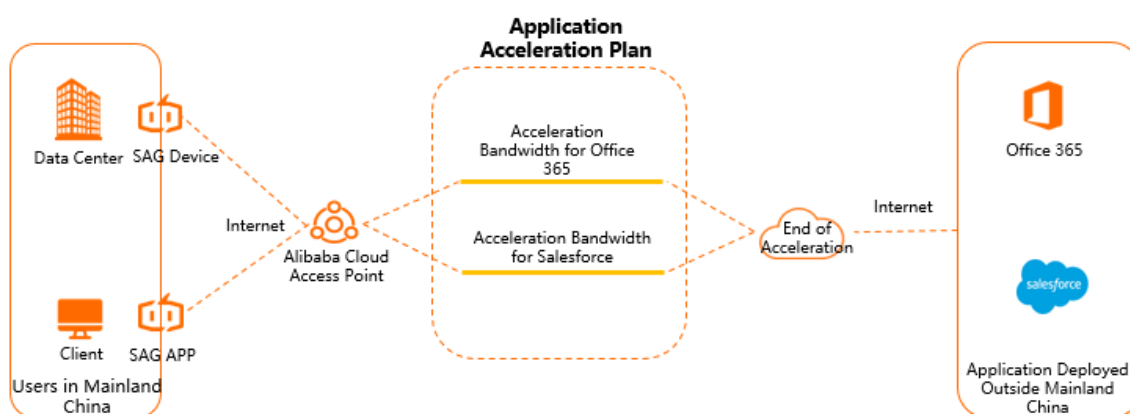
If the version of the SAG device is earlier than 2.4.0, you must upgrade it. For more information, see [Upgrade an SAG device to a later version](#).

- If you use an SAG app instance, the version of the SAG app that is associated with the SAG app instance must be 2.4.0 or later.

If the version of the SAG app is earlier than 2.4.0, you must upgrade it. For more information about the SAG app, see [安装客户端](#).

Scenarios

Based on the high-quality bandwidth resources provided by Alibaba Cloud, application acceleration plans can reduce network latency, jitter, and packet loss during data transfer. After an SAG instance is associated with an application acceleration plan, the bandwidth plan can be applied to your on-premises networks through Alibaba Cloud access points. This accelerates access to one or more applications that are deployed in regions outside mainland China.



Procedure

1. Connect on-premises networks to Alibaba Cloud by using SAG. For more information about how to connect on-premises networks to Alibaba Cloud by using SAG, see the following topics.

- SAG devices: [Deploy an SAG device in inline mode](#) or [Deploy an SAG device in one-arm mode and enable dynamic routing](#).
 - The SAG app: [Get started with SAG APP](#).
2. Purchase an application acceleration plan. For more information, see [Work with application acceleration plans](#).
 3. Associate the application acceleration plan with an SAG instance. For more information, see [Associate an application acceleration plan with an SAG instance](#).

After the application acceleration plan is associated with an SAG instance, the bandwidth plan can be applied to the on-premises networks that are associated with the SAG instance.

4. Add an application acceleration rule. For more information, see [Manage an application acceleration rule](#).

An application acceleration rule is used to allocate bandwidth resources that you can use to access different applications. Access to applications deployed in regions outside mainland China can be accelerated only after you add an application acceleration rule.

Differences between the maximum bandwidth value for an SAG instance and the maximum bandwidth value for an application

When you associate an application acceleration plan with an SAG instance, the value of the **Maximum Bandwidth** parameter refers to the maximum bandwidth that can be used to accelerate access from the on-premises networks associated with the SAG instance. For each SAG instance, the maximum value of the Maximum Bandwidth parameter cannot exceed that of the associated application acceleration plan.

When you add an application acceleration rule, the value of the **Maximum Bandwidth** parameter refers to the maximum bandwidth that can be used to accelerate access from on-premises networks associated with one or more SAG instances to the specified application. For each application acceleration plan, the sum of Maximum Bandwidth values that you set for different applications cannot exceed the maximum bandwidth value of the application acceleration plan.

For more information, see [Throttle bandwidth for application acceleration from multiple dimensions](#).

12.2. Work with application acceleration plans

Based on the high-quality bandwidth resources provided by Alibaba Cloud, application acceleration plans can reduce network latency, jitter, and packet loss during data transfer. After your on-premises networks are connected to Alibaba Cloud through Smart Access Gateway (SAG), you can use application acceleration plans to quickly and stably access applications that are deployed in regions outside mainland China.

Purchase an application acceleration plan

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, click **Purchase Bandwidth Plan**.
5. On the **Application Acceleration Plan** page, set the following parameters, click **Buy Now**, and

then complete the payment.

Parameter	Description
Region	Select the region to which the clients belong.
Type	Select a type for the application acceleration plan. By default, Advanced Application Acceleration Plan is selected.
Maximum Bandwidth	Select a maximum bandwidth value for the application acceleration plan. Unit: Mbit/s.
Duration	Specify a subscription duration for the application acceleration plan.
Name	Enter a name for the application acceleration plan. The name must be 2 to 128 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.

Upgrade an application acceleration plan

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, find the application acceleration plan and click **Upgrade** in the **Actions** column.
5. On the **Upgrade/Downgrade** page, set **Maximum Bandwidth**.
6. In the **Terms of Service** section, read and select Terms of Service, click **Buy Now**, and then complete the payment.

Downgrade an application acceleration plan

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, find the application acceleration plan and click **Downgrade** in the **Actions** column.
5. On the **Downgrade** page, set **Maximum Bandwidth**.
6. In the **Terms of Service** section, read and select Terms of Service, click **Buy Now**, and then complete the payment.

Renew an application acceleration plan

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, find the application acceleration plan and click **Renew** in the **Actions** column.
5. On the **Renew** page, set **Duration**.

6. In the **Terms of Service** section, read and select **Terms of Service**, click **Buy Now**, and then complete the payment.

12.3. Associate an application acceleration plan with an SAG instance

After you associate an application acceleration plan with a Smart Access Gateway (SAG) instance, the on-premises networks associated with the SAG instance can use the bandwidth for application acceleration. This topic describes how to associate an application acceleration plan with an SAG instance.

Prerequisites

Before you associate an application acceleration plan with an SAG instance, make sure that the following requirements are met:

- If you want to associate an application acceleration plan with an SAG CPE instance, the version of the SAG device associated with the SAG CPE instance must be 2.4.0 or later.

If the version of the SAG device is earlier than 2.4.0, upgrade it. For more information, see [Upgrade an SAG device to a later version](#).


- If you want to associate an application acceleration plan with an SAG app instance, the version of the SAG app must be 2.4.0 or later.

If the version of the SAG app is earlier than 2.4.0, upgrade it. For more information, see [安装客户端](#).


- The SAG instance to be associated is in the **Available** state.
- An application acceleration plan is purchased. For more information, see [Work with application acceleration plans](#).

Associate an application acceleration plan with an SAG instance on the Application Acceleration Plan page

1. Log on to the [Smart Access Gateway console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, find the application acceleration plan and click its ID.
5. On the **Associated SAG Instances** tab, click **Associate with SAG Instance**.
6. On the **Associate With SAG Instance** dialog box, click **+ Add**, set the following parameters, and then click **OK**.

 **Note** You can associate an application acceleration plan with up to 20 SAG instances at a time.

Parameter	Description
-----------	-------------

Parameter	Description
SAG Model	<p>Select an SAG type.</p> <p>You can associate an application acceleration plan with an SAG instance of the following types:</p> <ul style="list-style-type: none"> ◦ SAG devices, including the following models: <ul style="list-style-type: none"> ▪ SAG-1000 ▪ SAG-100WM ◦ SAG app
SAG Instance	Select the ID of the SAG instance to be associated.
Maximum Bandwidth	<p>Select a maximum value for the bandwidth for application acceleration of the SAG instance. Unit: Mbit/s.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> Note The maximum bandwidth value of each SAG instance cannot exceed that of the associated application acceleration plan.</p> </div>

Associate an application acceleration plan with an SAG instance on the SAG instance page

You can associate an application acceleration plan with an SAG instance on the **SAG** or **SAG App Instances** page.

1. Log on to the [Smart Access Gateway console](#).
2. In the top navigation bar, select the region.
3. Go to one of the following pages based on the type of the SAG instance.
 - In the left-side navigation pane, click **Smart Access Gateway** to go to the **SAG** page. On the page that appears, you can find SAG CPE instances.
 - In the left-side navigation pane, choose **Smart Access Gateway APP > SAG App Instances** to go to the **SAG App Instances** page. On the page that appears, you can find SAG app instances.
4. Find the SAG instance that you want to associate and click **Associate with Bandwidth Plan** in the **Actions** column.
5. In the **Associate with Bandwidth Plan** dialog box, select an application acceleration plan, set a maximum bandwidth value, and then click **OK**.

For each SAG instance, the maximum value of the Maximum Bandwidth parameter cannot exceed that of the associated application acceleration plan.

What to do next

After you associate an application acceleration plan with an SAG instance, you must add an application acceleration rule to allocate bandwidth resources for different applications. Then, on-premises networks can use the bandwidth for application acceleration to access applications. For more information, see [Manage an application acceleration rule](#).

Related operations

If your on-premises networks no longer need the application acceleration service, you can disassociate the application acceleration plan from the SAG instance.

1. Log on to the [Smart Access Gateway console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, find the application acceleration plan and click its ID.
5. On the **Associated SAG Instances** tab, find the SAG instance and click **Disassociate** in the **Actions** column.
6. In the **Disassociate Application Acceleration Plan** dialog box, confirm the instance ID and click **OK**.

12.4. Manage an application acceleration rule

After you associate an application acceleration plan with a Smart Access Gateway (SAG) instance, you must configure an application acceleration rule. An application acceleration rule is used to allocate bandwidth resources for different applications. This topic describes how to add, modify, or delete an application acceleration rule.

Context

Before you configure an application acceleration rule, take note of the following limits:

- For each application acceleration plan, the sum of bandwidth values that you specify for different application acceleration rules cannot exceed the maximum bandwidth value of the application acceleration plan.
- The combination of **Region** and **Accelerated Application** for each application acceleration rule must be unique.

Assume that you have configured an application acceleration rule named A where Region is set to China (Hong Kong), Accelerated Application is set to Office 365 and Salesforce, and Maximum Bandwidth is set to 2 Mbit/s. In this case, you can configure another application acceleration rule where Region is set to Singapore (Singapore), Accelerated Application is set to Salesforce, and Maximum Bandwidth is set to 2 Mbit/s. However, you cannot create an application acceleration rule where Region is set to China (Hong Kong), Accelerated Application is set to Salesforce, and Maximum Bandwidth is set to 3 Mbit/s. You cannot add this rule because the value of Accelerated Application is the same as that of Rule A.

Add an application acceleration rule

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, find the application acceleration plan and click its ID.


- On the details page, click the **Application Acceleration Rules** tab and click **Add Application Acceleration Rule**.
- In the **Add Application Acceleration Rule** dialog box, click **+ Add**, set the following parameters, and then click **OK**.

Parameter	Description
Region	Select the region where the application that you want to access is deployed.
Maximum Bandwidth	Specify the maximum bandwidth that the on-premises networks can use to access the application. Unit: Mbit/s.
Accelerated Application	Select the application that you want to access.

Copy an application acceleration rule

You can copy an application acceleration rule by performing the following steps.

- Log on to the [SAG console](#).
- In the top navigation bar, select the region.
- In the left-side navigation pane, click **Application Acceleration Plan**.
- On the **Application Acceleration Plan** page, find the application acceleration plan and click its ID.
- On the details page, click the **Application Acceleration Rules** tab.
- Find the application acceleration rule that you want to copy and click **Clone** in the **Actions** column.
- In the **Copy Application Acceleration Rule** dialog box, set **Region** and **Accelerated Application**, and then click **OK**.

 **Note** For the same application acceleration plan, the combination of **Region** and **Accelerated Application** for each application acceleration rule must be unique.

Modify an application acceleration rule

- Log on to the [SAG console](#).
- In the top navigation bar, select the region.
- In the left-side navigation pane, click **Application Acceleration Plan**.
- On the **Application Acceleration Plan** page, find the application acceleration plan and click its ID.
- On the details page, click the **Application Acceleration Rules** tab.
- Find the application acceleration rule that you want to modify and click **Edit** in the **Actions** column.
- In the **Modify Application Acceleration Rule**, modify **Region** and **Accelerated Application**, and then click **OK**.

Delete an application acceleration rule

1. Log on to the [SAG console](#).
2. In the top navigation bar, select the region.
3. In the left-side navigation pane, click **Application Acceleration Plan**.
4. On the **Application Acceleration Plan** page, find the application acceleration plan and click its ID.
5. On the details page, click the **Application Acceleration Rules** tab.
6. Find the application acceleration rule that you want to delete and click **Remove** in the **Actions** column.
7. In the **Delete Application Acceleration Rule** dialog box, confirm the rule ID and click **OK**.

12.5. Throttle bandwidth for application acceleration from multiple dimensions

An application acceleration plan can be shared by multiple on-premises networks that are associated with Smart Access Gateway (SAG) instances. To prevent on-premises networks associated with one SAG instance from consuming a large amount of bandwidth resources, the system allows you to throttle bandwidth from different dimensions. This way, you can use bandwidth resources for application acceleration more flexibly and effectively.

When you use an application acceleration plan, you can throttle bandwidth in the following ways:

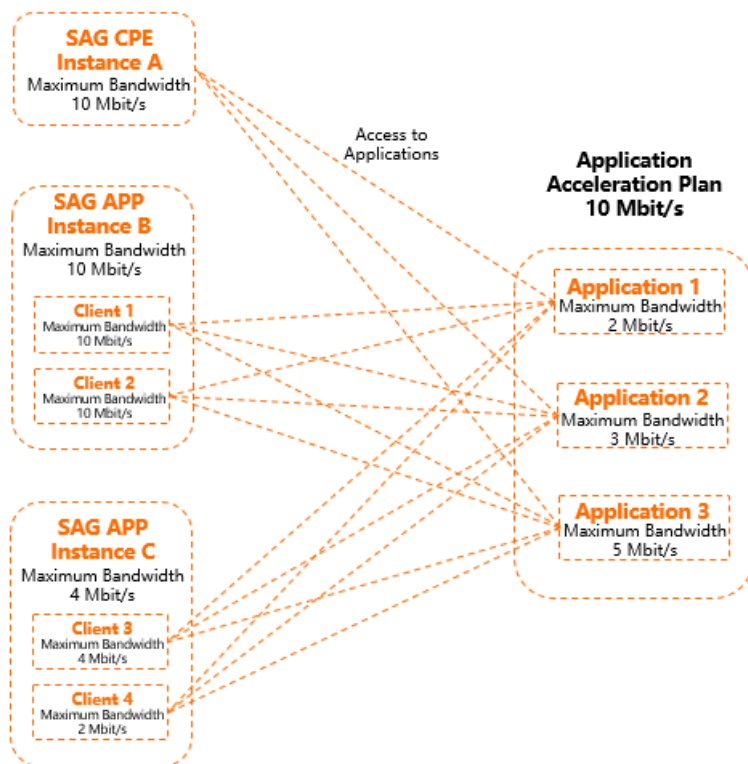
- Set a maximum bandwidth value for an SAG instance to specify the maximum bandwidth that can be used by the associated on-premises networks for application acceleration.

The maximum bandwidth value of each SAG instance cannot exceed that of the associated application acceleration plan.

- Set a maximum bandwidth value for a client account of an SAG app instance to specify the maximum bandwidth that can be used by the client account for application acceleration.

The maximum bandwidth value of each client account cannot exceed that of the SAG app instance to which the client account belongs.

The following figure shows the correlation between the maximum bandwidth value of each application when you throttle bandwidth resources from different dimensions.



For example, to accelerate access to Application 1, Application 2, and Application 3, you have purchased a 10 Mbit/s application acceleration plan. The application acceleration plan is associated with Instance A, Instance B, and Instance C, and the following configurations are made:

- The maximum bandwidth values for Application 1, Application 2, and Application 3 are set to 2 Mbit/s, 3 Mbit/s, and 5 Mbit/s.
- The maximum bandwidth values for Instance A, Instance B, and Instance C are set to 10 Mbit/s, 10 Mbit/s, and 4 Mbit/s.
- The maximum bandwidth values for Client 1, Client 2, Client 3, and Client 4 are set to 10 Mbit/s, 10 Mbit/s, 4 Mbit/s, and 4 Mbit/s.

This topic uses the following examples to help you understand the correlation between the maximum bandwidth value of each application.

At a point in time, only the on-premises networks associated with Instance A access Application 1. In this case, the maximum bandwidth that the on-premises networks can use is 2 Mbit/s.

At a point in time, the on-premises networks associated with Instance A and Client 2 access Application 1 at the same time. In this case, the sum of bandwidth used by the on-premises networks and Client 2 does not exceed 2 Mbit/s.

At a point in time, only Client 3 accesses Application 3. In this case, the maximum bandwidth that Client 3 can use is 4 Mbit/s because the maximum bandwidth of Client 3 is set to 4 Mbit/s.

Related operations

- Set a maximum bandwidth value for an SAG instance. For more information, see [Associate an application acceleration plan with an SAG instance](#).

- Set a maximum value for the bandwidth of a client account. For more information, see [Throttle bandwidth resources for a client account](#).
- Set a maximum bandwidth value for an application. For more information, see [Manage an application acceleration rule](#).

12.6. Throttle bandwidth resources for a client account

To use bandwidth resources for application acceleration in a more effective way, you can set maximum bandwidth values for client accounts of a Smart Access Gateway (SAG) app instance.

Prerequisites


- A client account is created. For more information, see [Create a client account](#).
- An application acceleration plan is associated with the SAG app instance to which the client account belongs, and a maximum bandwidth value is set for the SAG app instance. For more information, see [Associate an application acceleration plan with an SAG instance](#).
- The version of the SAG app is 2.4.0 or later. For more information, see [安装客户端](#).

Context

Before you set a maximum bandwidth value for a client account, take note of the following rules:

- The maximum bandwidth value of a client account cannot exceed that of the SAG app instance to which the client account belongs.
- In scenarios where a maximum bandwidth value is not set for a client account:
 - If the maximum bandwidth value of the SAG app instance is less than 5 Mbit/s, for example, 4 Mbit/s, the maximum bandwidth value of each client account that belongs to the SAG app instance is 4 Mbit/s by default.
 - If the maximum bandwidth value of the SAG app instance is greater than 5 Mbit/s, the maximum bandwidth value of each client account that belongs to the SAG app instance is 5 Mbit/s by default.

Procedure

1. Log on to the [SAG console](#).
- 2.
3. In the left-side navigation pane, choose **Smart Access Gateway APP > SAG APP Instances**.
4. On the **SAG APP** page, click the ID of the SAG app instance that you want to manage.
5. On the details page, click the **Client Accounts** tab.
6. Find the client account that you want to manage and choose  > **Modify Bandwidth** in the **Actions** column.
7. In the **Modify Bandwidth** dialog box, set a maximum bandwidth value and click **OK**.

13. Grant a RAM user the permissions to use QoS policies and flow logs

This topic describes how to grant a RAM user the permissions to use quality of service (QoS) policies and flow logs.

Procedure

1. View the permission policies that have been attached to a RAM user.
 - i. Log on to the [RAM console](#) with your Alibaba Cloud account.
 - ii. In the left-side navigation pane, choose **Permissions > Grants**.
 - iii. On the **Grants** page, find the RAM user that you want to manage and view the permission policies that have been attached.

If the `AliyunSmartAccessGatewayFullAccess` permission policy is attached to the RAM user, the RAM user can use QoS policies and flow logs without other permissions. You can click **AliyunSmartAccessGatewayFullAccess** to view its details. The following code block shows the content of the `AliyunSmartAccessGatewayFullAccess` permission policy:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "smartag:*",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

2. If the `AliyunSmartAccessGatewayFullAccess` permission policy is not attached to the RAM user, you can create a custom permission and attach it to the RAM user. This grants the RAM user the required permissions.

If the RAM user needs to use QoS policies and flow logs, perform the following steps to create and attach a custom permission policy to the RAM user.

- i. Log on to the [RAM console](#).
- ii. In the left-side navigation pane, choose **Permissions > Policies**.
- iii. On the **Policies** page, click **Create Policy**.
- iv. On the **Create Custom Policy** page, set the following parameters and click **OK**.
 - **Policy Name**: Enter a name for the custom permission.
 - **Configuration Mode**: Select a configuration mode. Select **Script**.

- Policy Document : Enter the content.
- QoS policies

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "smartag:AssociateQos",
        "smartag:CreateQos",
        "smartag:CreateQosCar",
        "smartag:CreateQosPolicy",
        "smartag>DeleteQosCar",
        "smartag>DeleteQosPolicy",
        "smartag:DescribeQosCars",
        "smartag:DescribeQosPolicies",
        "smartag:DisassociateQos",
        "smartag:GetQosAttribute",
        "smartag:ModifyQos",
        "smartag:ModifyQosCar",
        "smartag:ModifyQosPolicy"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

- Flow logs

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "smartag:ActiveFlowLog",
        "smartag:AssociateFlowLog",
        "smartag:CreateFlowLog",
        "smartag:DeactiveFlowLog",
        "smartag:DescribeFlowLogSags",
        "smartag:DisassociateFlowLog",
        "smartag:ModifyFlowLogAttribute"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

For more information about the parameters, see [Create a custom policy](#).

- In the left-side navigation pane, choose **Identities > Users**.
- On the **Users** page, find the RAM user and click **Add Permissions** in the **Actions** column.

- vii. In the **Add Permissions** panel, confirm **Authorized Scope** and **Principal**.
- viii. In the **Select Policy** section, click **Custom Policy**, select the permission that you created, and then click **OK**.

After you complete the preceding steps, you can perform [Step 1](#) to view the permission policy that is attached to the RAM user.