ALIBABA CLOUD

Alibaba Cloud

智能接入网关

Tutorials

Document Version: 20220706

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 `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Deploy an SAG device in inline mode

This topic describes how to connect two office branches to Alibaba Cloud virtual private clouds (VPCs). In this example, the office branches are located in Hangzhou and Ningbo, and the VPCs are deployed in the China (Shanghai) and China (Beijing) regions.

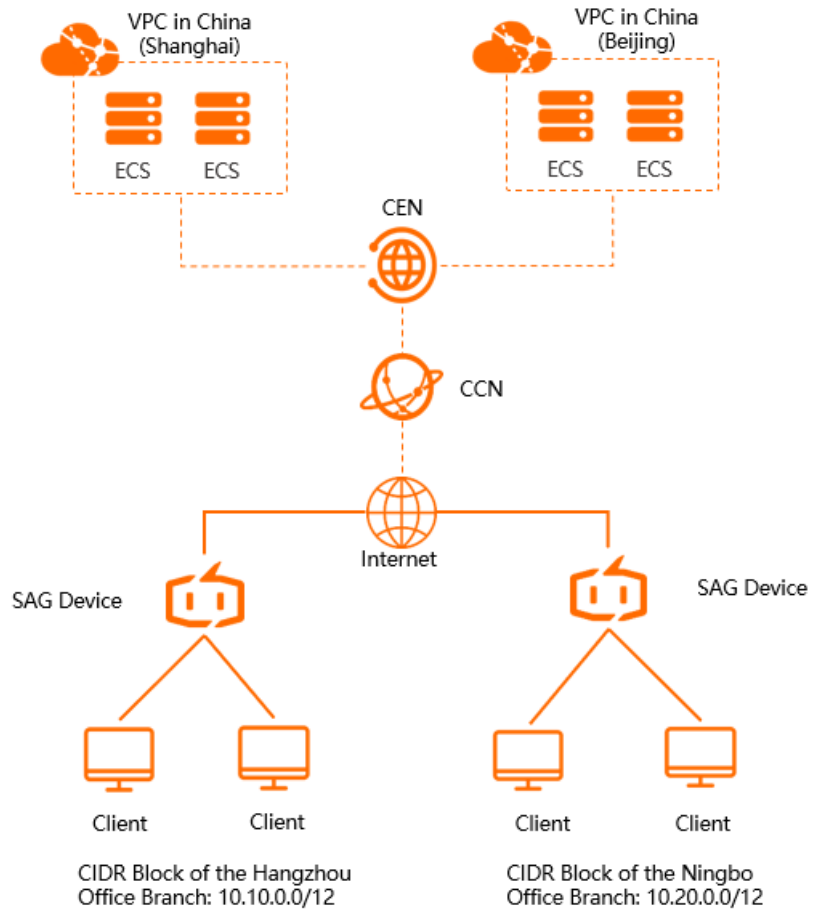
Prerequisites

Before you begin, make sure that the following requirements are met:

- A VPC is deployed in the China (Shanghai) and China (Beijing) regions. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC in the China (Shanghai) region. For more information, see Create a CEN instance.
- The VPCs in the China (Beijing) and China (Shanghai) regions are associated with the same CEN instance. For more information, see Attach a network instance.

Context

In this example, a company has created a VPC in both the China (Shanghai) and China (Beijing) regions. The company needs to connect its Hangzhou and Ningbo office branches to Alibaba Cloud to enable the office branches to access resources on Alibaba Cloud. The CIDR blocks used by the Hangzhou and Ningbo office branches are 10.10.0.0/12 and 10.20.0.0/12. The local clients of the Hangzhou and Ningbo office branches need to connect to Alibaba Cloud through SAG-100WM.



Procedure

The procedure to deploy an SAG device in inline mode is as follows.

Step 1: Purchase SAG devices

After you purchase SAG devices in the SAG console, Alibaba Cloud delivers the devices to the specified address and creates an SAG instance to help you facilitate network management.

To purchase an SAG device, perform the following steps.

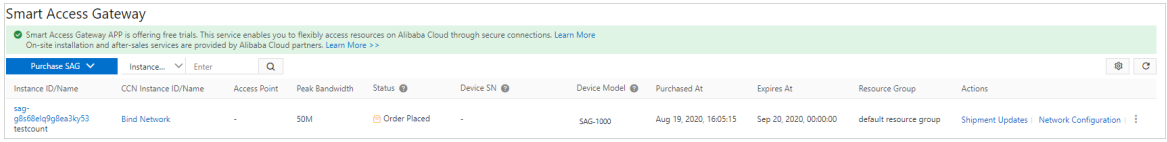
1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Create SAG Instance**.
3. Set the following parameters.
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the type of the SAG device. **SAG-100WM** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have an SAG device. **No** is selected in

this example.

- **Quantity**: Select the number of SAG devices that you want to purchase. **1** is selected in this example.
- **Area**: Select the area where the SAG bandwidth will be used. This area must be the same as that of the SAG devices and cannot be modified.
- **Name**: Specify a name for the SAG instance.

  The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
- **Peak Bandwidth**: Select the maximum bandwidth for network connections. **30Mbps** is selected in this example.
- **Subscription Duration**: Select the duration of the subscription.

4. On the **Confirm Order** page, click **Confirm Purchase**.
5. In the **Shipping Address** dialog box that appears, enter the recipient address and then click **Buy Now**.
6. On the **Pay** page that appears, click **Pay**.
7. Repeat this step to purchase another SAG device. One device is for the Hangzhou office branch, and the other is for the Ningbo office branch.
   You can check whether the order has been placed on the Smart Access Gateway page. The SAG devices will be shipped within two business days. If the order is not shipped within two business days, submit a ticket to query the shipping status.



Step 2: Connect the SAG devices to the private networks of the office branches

1. After you receive the SAG devices, check whether you have received all the accessories. For more information, see Descriptions of SAG-100WM.
2. Start an SAG device and connect its WAN port to the modem and LAN port to the local clients.
3. In this example, the local clients in the Hangzhou and Ningbo office branches need to access Alibaba Cloud through the SAG devices. You can use the default gateway configurations. For more information about configuring the WAN and LAN ports, see Configure a WAN port and Configure a LAN port.
4. Repeat this step to connect the other device to the private network. One device is connected to the Hangzhou office branch and the other is connected to the Ningbo office branch.

Step 3: Activate the SAG devices

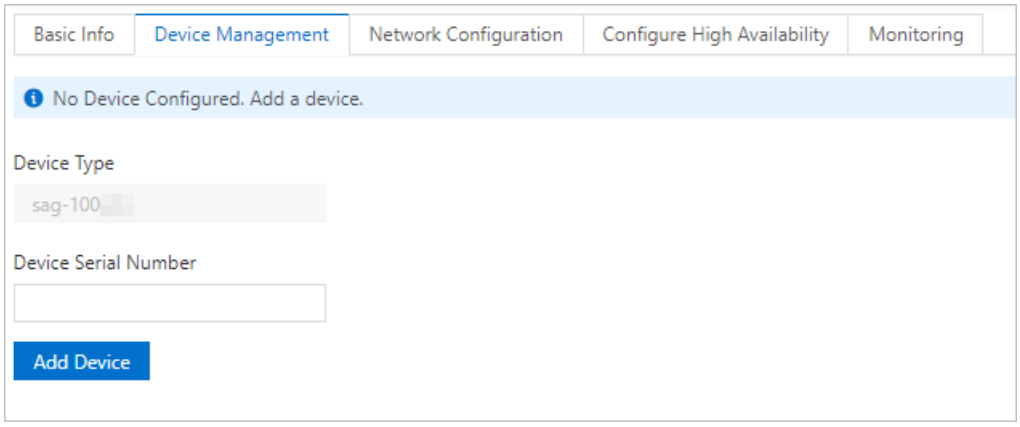
After you receive the SAG devices, you must activate them.

To activate an SAG device, perform the following steps.

1. Log on to the SAG console.
2. In the left-side navigation pane, click **Smart Access Gateway**.
3. On the **Smart Access Gateway** page, find the SAG instance and click **Activate** in the **Actions**

column.

4. Click the ID of the SAG instance. On the instance details page, click the **Device Management** tab, enter the serial number of the device, and then click **Add Device** to associate the SAG device with the SAG instance.



5. Repeat this step to activate the other device and associate it with the SAG instance.

Step 4: Set up network connections

After you activate the SAG devices and connect them to the private networks, you must configure network settings in the SAG console to direct local routes to Alibaba Cloud.

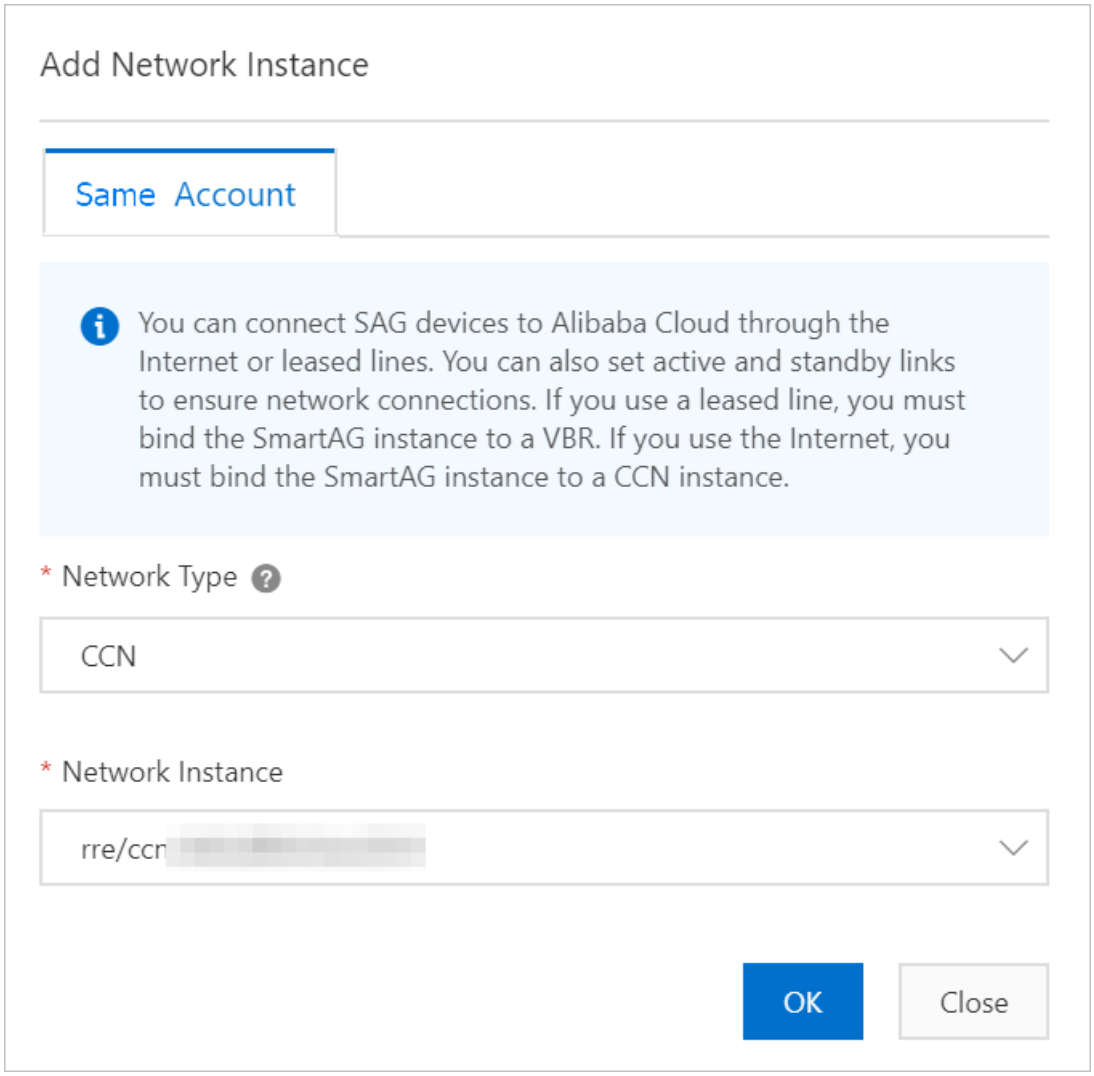
To configure network settings, perform the following steps.

1. Log on to the SAG console.
2. In the left-side navigation pane, click **Smart Access Gateway**. On the **Smart Access Gateway** page, find the SAG instance and click **Network Configuration** in the **Actions** column.
3. Configure a method to synchronize with local routes.
   i. In the left-side navigation tree, click **Method to Synchronize with On-premises Routes**.
   ii. Select **Static Routing** and click **Add Static Route**. In the Add Static Route dialog box that appears, enter the CIDR blocks used by the Hangzhou and Ningbo office branches, respectively.

   The CIDR block 10.10.0.0/12 of the Hangzhou office branch is used in this example. The default gateway configurations are used in this example. Therefore, the IP addresses of local clients are allocated from this CIDR block: 10.10.0.0/12.
   iii. Click **OK**.
4. Associate the SAG vCPE instance with a CCN instance.
   i. Create a CCN instance. For more information about how to create CCN instances, see Create a CCN instance.
   ii. After you create a CCN instance, navigate to the **Network Configuration** tab and click **Network Instance Details** in the left-side navigation tree.

iii. In the **Associated Instances Under Current Account** section, click **Attach Network** to associate the SAG instance with a CCN instance.

- **Network Type**: Select **Cloud Connect Network**.
- **Network Instance**: Select the ID of the CCN created in the preceding step.



iv. Click **OK**.

5. Repeat this step to configure the network settings of the other SAG instance.

   Associate the SAG instances of the Hangzhou and Ningbo office branches with the same CCN instance.

Step 5: Associate the CCN instance with a CEN instance

Perform the following steps to associate the CCN instance with a CEN instance. This connects the office branches to Alibaba Cloud.

1. Log on to the SAG console.
2. In the left-side navigation pane, click **CCN**.
3. Find the CCN instance and click **Bind CEN Instance** in the **Actions** column.
4. In the **Bind CEN Instance** pane that appears, select the CEN instance. After the CCN instance is associated with the CEN instance, SAG devices in the CCN can communicate with VPCs associated

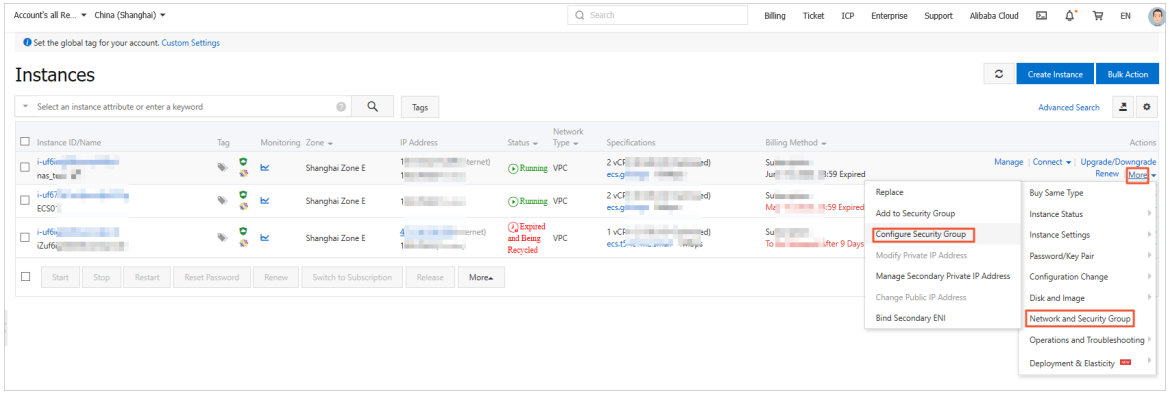
with the CEN.

Step 6: Configure a security group

Configure a security group to allow the office branches to access resources in the VPCs.

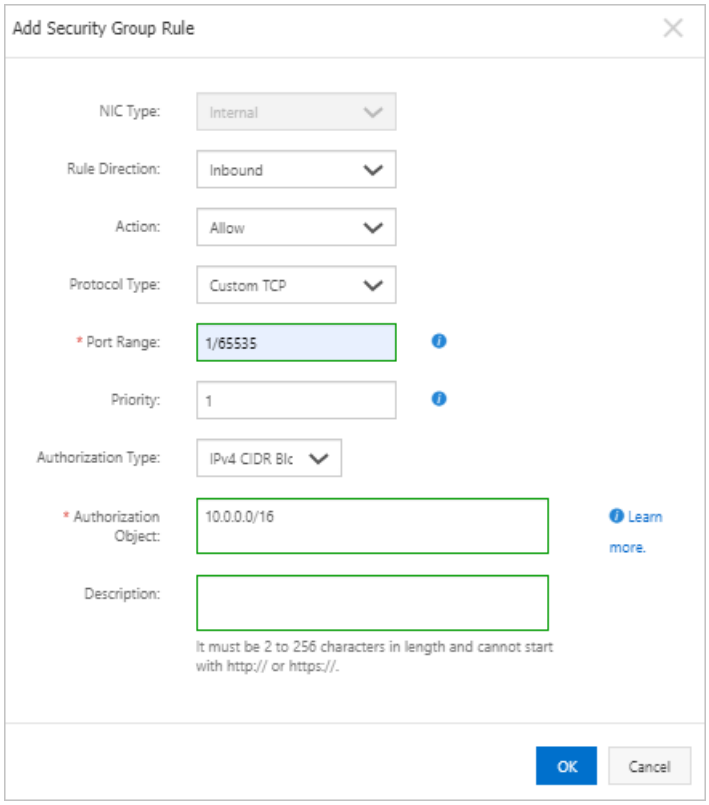
Perform the following steps to configure a security group.

1. Log on to the Elastic Compute Service (ECS) console.
2. In the left-side navigation pane, click **Instances**.
3. Find the ECS instance deployed in the VPC and choose **More > Network and Security Group > Configure Security Group**.



4. Find the security group, click **Add Rules** in the **Actions** column, and then click **Add Security Group Rule**.
5. Create a security group rule that allows access from the private network to the VPC.

   The following figure shows how to add a security group rule. Set **Authorization Object** to the CIDR block of the private network. In this example, this parameter is set to 10.10.0.0/12 and 10.20.0.0/12, which are the CIDR blocks of the Hangzhou and Ningbo office branches.



6. Repeat this step to create another security group rule. One rule allows access from local clients to the VPC network in the China (Shanghai) region, and the other to the VPC network in the China (Beijing) region. These security group rules allow the Hangzhou and Ningbo office branches to access resources in the VPC networks.

Step 7: Test the connectivity

After you complete the configurations in the preceding steps, access cloud resources deployed in the VPC networks from a client in the office branches to test the connectivity.

2.Deploy an SAG device in one-arm mode and enable static routing

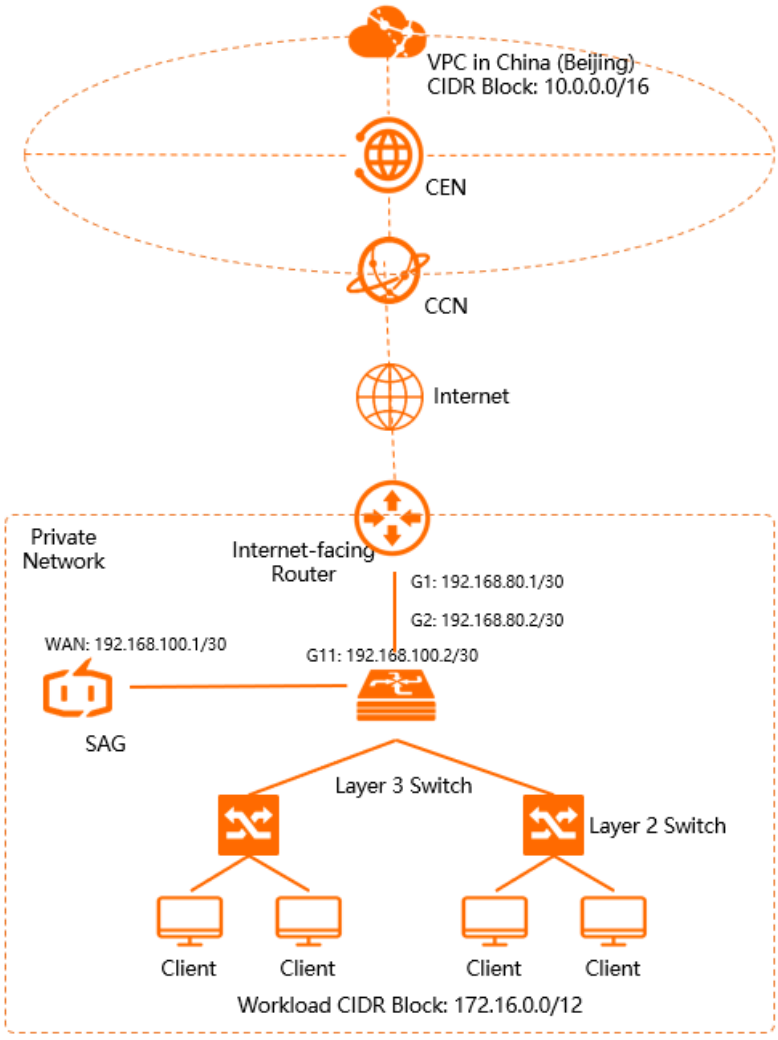
This topic describes how to deploy a Smart Access Gateway (SAG) device in one-arm mode and use the SAG device to connect on-premises networks to Alibaba Cloud.

Prerequisites

- A virtual private cloud (VPC) is created. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and the VPC is attached to the CEN instance. For more information, see Create a CEN instance.

Context

In this example, an enterprise has created a VPC in the China (Beijing) region and deployed services in the VPC. The enterprise needs to connect its on-premises network to Alibaba Cloud to access resources on Alibaba Cloud. In this case, the enterprise can deploy an SAG-1000 device in one-arm mode to meet the business requirements. This deployment mode does not change the existing network topology of the enterprise and allows the enterprise to access resources on Alibaba Cloud by using the SAG device.



Network planning

The following CIDR blocks are used in this example. When you allocate CIDR blocks based on your requirements, make sure that the CIDR blocks do not overlap with each other.

Node	CIDR block
Enterprise network	CIDR block for business: 172.16.0.0/12
	WAN port (port 5) of the SAG device: 192.168.100.1/30. Gateway: 192.168.100.2
	Port G11 of the Layer 3 switch: 192.168.100.2/30
	• Port G1 of the egress router: 192.168.80.1/30 • Port G2 of the Layer 3 switch: 192.168.80.2/30
VPC in the China (Beijing) region	10.0.0.0/16

Procedure

Step 1: Purchase an SAG device

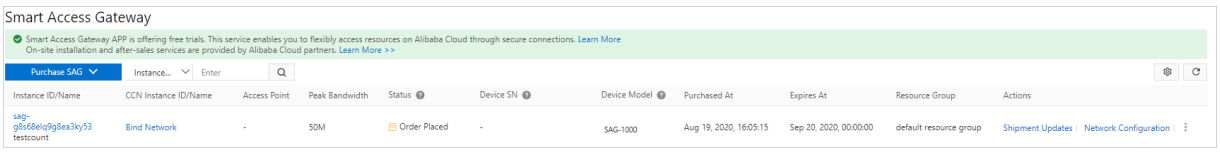
After you place an order in the SAG console, Alibaba Cloud delivers the SAG device to the specified address and creates an SAG instance to facilitate the management of the device.

> **Note** If the area where the SAG device is used is outside mainland China, you must purchase the device from a third-party vendor that is authorized by Alibaba Cloud. For more information, see Purchase SAG devices.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Purchase SAG**.
3. Select **Create SAG (CPE)**.
4. Set the following parameters and click **Buy Now**:
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the model of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have an SAG device. **No** is selected in this example.
   - **Edition**: Select the edition of the SAG device. **Standard** is selected in this example by default.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **1** is selected in this example.
   - **Area**: Select the area where the bandwidth will be used. The area is the same as that of the SAG device and cannot be changed.
   - **Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
   - **Peak Bandwidth**: Specify the maximum bandwidth value. **50 Mbps** is specified in this example.
   - **Subscription Duration**: Specify the subscription duration of the bandwidth resources.
5. Confirm the order information and click **Confirm Purchase**.
6. In the **Shipping Address** dialog box, enter the recipient address and click **Buy Now**.
7. On the **Pay** page, select a payment method and complete the payment.

You can check whether the order has been placed on the Smart Access Gateway page. After the order is placed, it will be shipped within two business days. If your order is not shipped as expected, you can submit a ticket to query the shipping status.



Step 2: Activate the SAG devices

After you receive the SAG device, check whether you have received all the accessories. For more information, see Descriptions of SAG-1000.

1. Log on to the SAG console.
2. In the top navigation bar, select the area of the SAG device.
3. On the **Smart Access Gateway** page, find the SAG instance created for the SAG device.
4. In the **Actions** column, click **Activate**.
5. In the **Activate** dialog box, click **OK**.
6. After the SAG device is activated, connect it to the private network based on the preceding network topology.

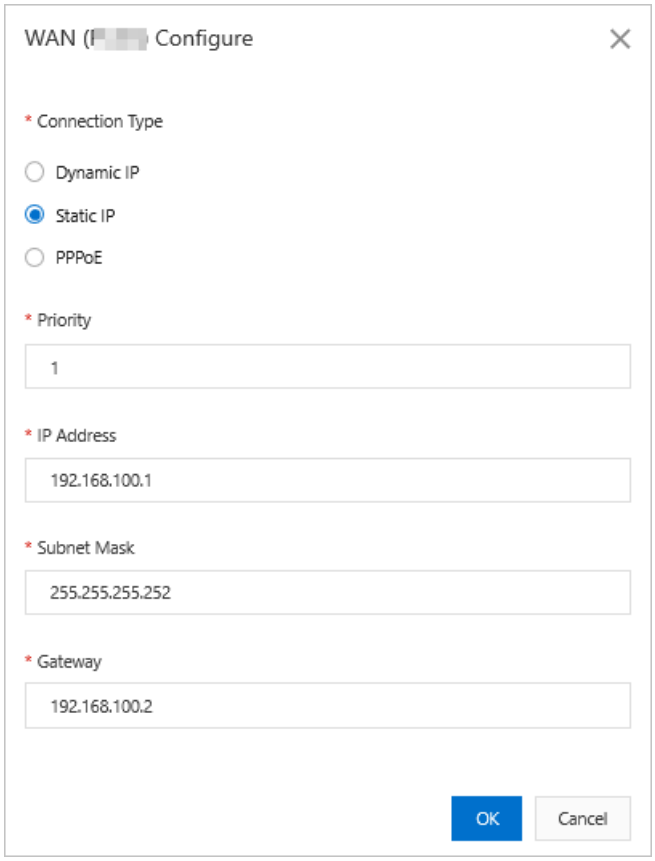
   Use a network cable to connect the WAN port (port 5) of the SAG device to port G11 of the Layer 3 switch.
7. (Optional)If the SAG device was purchased from a third-party vendor, you must manually associate the SAG device with the SAG instance. For more information, see Add a device.

Step 3: Configure the SAG device

After the SAG device is connected to the on-premises network, you can configure the device ports in the SAG console.

Before you begin, make sure that the SAG device is started, the 4G network works as expected, and the SAG device is connected to Alibaba Cloud.

1. Configure the ports.
   i. On the **Smart Access Gateway** page, click the ID of the SAG instance.
   ii. On the instance details page, click the **Device Management** tab.
   iii. In the left-side section, click **Manage WAN Ports**.
   iv. In the **WAN (Port 5)** section, click **Edit**.
   v. In the **Configure WAN (Port 5)** dialog box, set the following parameters and click **OK**.



Parameter	Description
Connection Type	Select **Static IP**.
Priority	Use the default value **1**.
IP Address	The IP address of the WAN port. In this example, *192.168.100.1* is used.
Subnet Mask	The subnet mask of the IP address of the WAN port. In this example, *255.255.255.252* is used.
Gateway	The IP address of the gateway. In this example, *192.168.100.2* is used. **Note** After the gateway is configured, the SAG device automatically adds a default route.

2. Select a method to advertise routes to Alibaba Cloud.

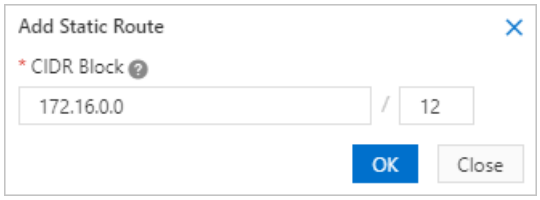
   You must specify how routes are advertised to Alibaba Cloud. These routes are used for network communication between the on-premises network and cloud resources.

   i. On the SAG instance details page, click the **Network Configuration** tab.

   ii. In the left-side navigation tree, click **Methods to Synchronize with On-premises Routes**.

iii. Select **Static Routing**, click **Add Static Route** to add a static route, and then click **OK**.

Enter the CIDR block used to connect the on-premises network to Alibaba Cloud. 172.16.0.0/12 is used in this example.



3. Configure static routes

You must add a route that points to the WAN port for the on-premise network. This way, the backup feature is enabled for the 4G network.

i. On the **Smart Access Gateway** page, click the ID of the SAG instance.

ii. On the instance details page, click the **Device Management** tab.

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

iv. On the **Manage Routes** page, click **Add Static Route**.

v. On the **Add Static Route** page, set the following parameters and use the default values for the other parameters, and then click **OK**.

Example

Parameter	Description
Destination CIDR Block	Enter the destination CIDR block for which network traffic is destined. In this example, *172.16.0.0/12* is used.
Next Hop	Enter the IP address of the next hop. In this example, *192.168.100.2* is used, which is the peer IP address of the WAN port.
Port	Select the egress port of the destination CIDR block. In this example, the WAN port configured in Step is selected.

Step 4: Configure switches and egress routers

You must configure the peer switch and egress router for the SAG device. The switch and router used in this example may be different from yours. For more information, refer to the manuals issued by the providers of your devices.

1. Configure routes for the Layer 3 switch.

```
interface GigabitEthernet 0/11
no switchport
ip address 192.168.100.2 255.255.255.252 #The IP address of the peer switch of the SAG device
ip route 10.0.0.0 255.255.0.0 192.168.100.1 #The route that points to the VPC in the China (Beijing) region
ip route 0.0.0.0 0.0.0.0 192.168.80.1 #The route that points to the Internet
```

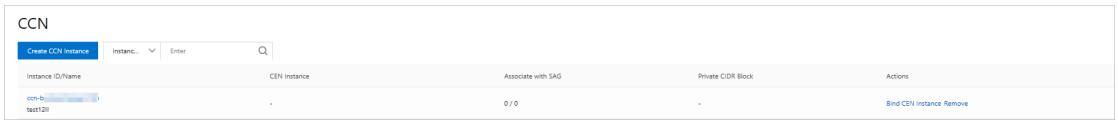
2. Configure routes for the egress router. The following example provides sample configurations.

```
ip route 192.168.100.0 255.255.255.252 192.168.80.2 #The route that points to the SAG device
```

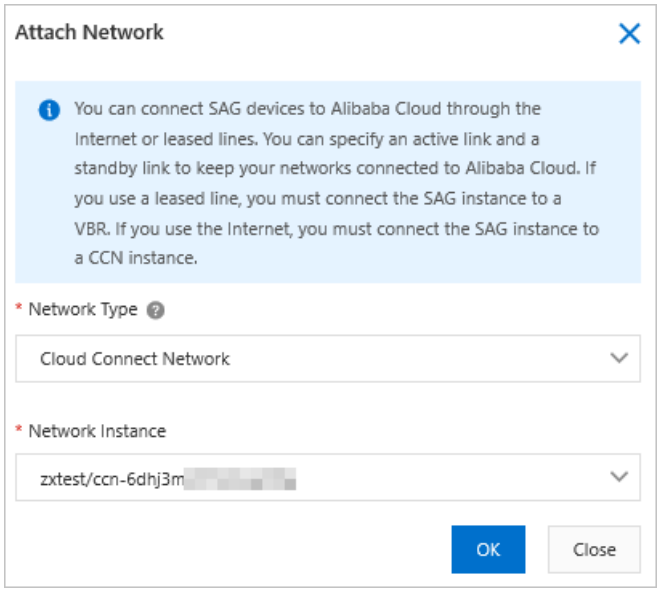
Step 5: Set up network connections

After you configure the SAG device, you must set up network connections to connect the private network to Alibaba Cloud.

1. Create a Cloud Connect Network (CCN) instance.
   i. Log on to the SAG console.
   ii. In the top navigation bar, select **Mainland China**.
   The area of the CCN instance must be the same as that of the SAG device.
   iii. In the left-side navigation pane, click **CCN**.
   iv. On the **CCN** page, click **Create CCN Instance**.
   v. In the **Create CCN Instance** pane, specify a name for the CCN instance and click **OK**.
   The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.



2. Associate the SAG instance with the CCN instance.
   i. In the left-side navigation pane, click **Smart Access Gateway**.
   ii. On the **Smart Access Gateway** page, find the SAG instance that you want to manage and click **Network Configuration** in the **Actions** column.
   iii. In the left-side navigation tree, click **Network Instance Details**.
   iv. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance, and then click **OK**.



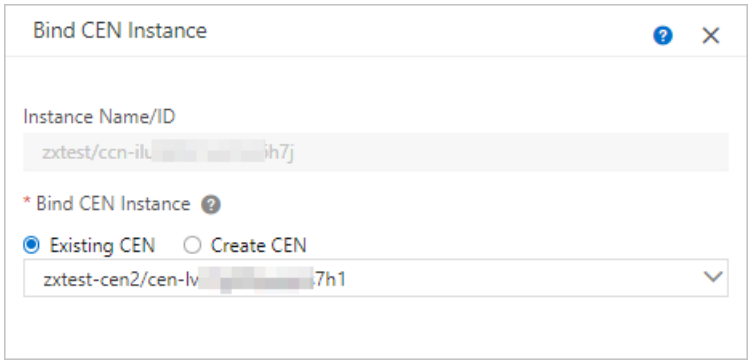
3. Associate the CCN instance with a CEN instance.

After the CCN instance is associated with a CEN instance, SAG devices associated with the CCN instance can communicate with VPC networks associated with the CEN instance.

i. In the left-side navigation pane, click **CCN**.

ii. Find the CCN instance and click **Bind CEN Instance** in the **Actions** column.

iii. In the **Bind CEN Instance** pane, select **Existing CEN**, select the CEN instance that you want to associate with the CCN instance, and then click **OK**.



4. Create a security group rule.

   You must create a security group rule for the Elastic Compute Service (ECS) instance in the VPC network to allow clients in the CIDR block 172.16.0.0/12 of the private network to access resources deployed on the ECS instance. For more information, see Add a security group rule.

Step 6: Test the network connectivity

After you complete the preceding steps, check whether you can access cloud resources deployed in the VPC from a client in the on-premises network.

3.Deploy an SAG device in one-arm mode and enable dynamic routing

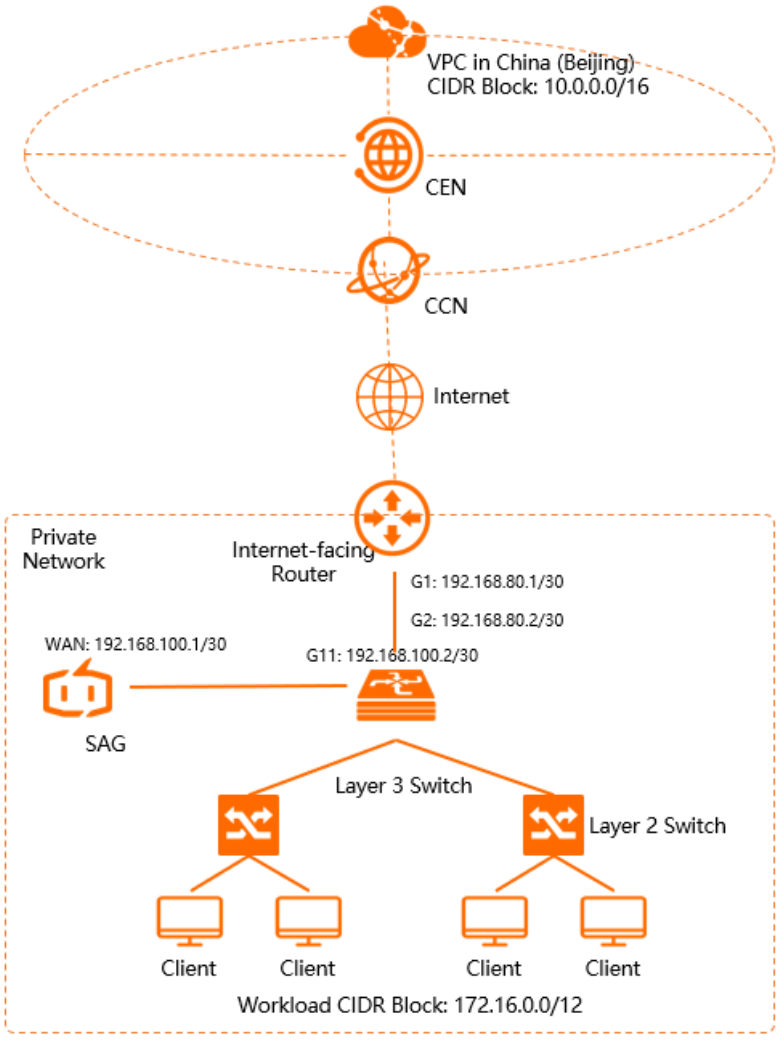
This topic describes how to deploy a Smart Access Gateway (SAG) device in one-arm mode and enable Open Shortest Path First (OSPF) routing to connect a private network to Alibaba Cloud.

Prerequisites

- A Virtual Private Network (VPC) network is created. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC network. For more information, see Create a CEN instance.

Context

In this example, a company needs to connect its private network to Alibaba Cloud. The company has created a VPC network in the China (Beijing) region and deployed application services in the VPC network. The company wants to use SAG to connect the company private network in mainland China to Alibaba Cloud. The model of the SAG device used in this example is SAG-1000. The SAG device is deployed in one-arm mode and OSPF dynamic routing is enabled. This solution connects the private network to Alibaba Cloud without changing the topology of the private network



Subnetting

The following CIDR blocks are used in this example. When you allocate CIDR blocks based on your actual requirements, make sure that the CIDR blocks do not overlap with each other.

Network	CIDR block
Private network of the company	Workloads: 172.16.0.0/12.
	WAN port (port 5) of the SAG device: 192.168.100.1/30. IP address of the gateway: 192.168.100.2.
	Port G11 of the Layer 3 switch: 192.168.100.2/30. Loopback interface: 192.168.100.3/32.
	Port G1 of the Internet-facing router: 192.168.80.1/30. Port G2 of the Layer 3 switch: 192.168.80.2/30.
VPC network in the China (Beijing) region	10.0.0.0/16

Configuration procedure

Step 1: Purchase an SAG device

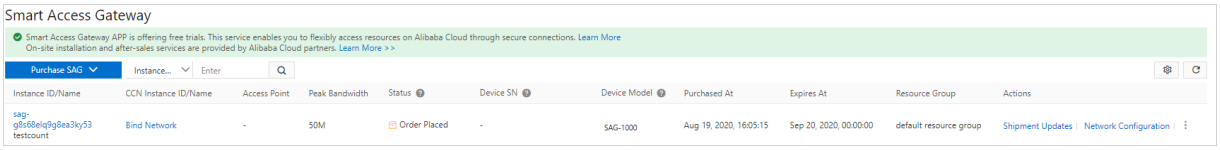
After you place an order in the SAG console, Alibaba Cloud delivers the SAG device to the specified address and creates an SAG instance to facilitate the management of the device.

> **Note** If the area where the SAG device is used is outside mainland China, you must purchase the device from a third-party vendor that is authorized by Alibaba Cloud. For more information, see Purchase SAG devices.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Purchase SAG**.
3. Select **Create SAG (CPE)**.
4. Set the following parameters and click **Buy Now**:
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the model of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have an SAG device. **No** is selected in this example.
   - **Edition**: Select the edition of the SAG device. **Standard** is selected in this example by default.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **1** is selected in this example.
   - **Area**: Select the area where the bandwidth will be used. The area is the same as that of the SAG device and cannot be changed.
   - **Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
   - **Peak Bandwidth**: Specify the maximum bandwidth value. **50 Mbps** is specified in this example.
   - **Subscription Duration**: Specify the subscription duration of the bandwidth resources.
5. Confirm the order information and click **Confirm Purchase**.
6. In the **Shipping Address** dialog box, enter the recipient address and click **Buy Now**.
7. On the **Pay** page, select a payment method and complete the payment.

You can check whether the order has been placed on the Smart Access Gateway page. After the order is placed, it will be shipped within two business days. If your order is not shipped as expected, you can submit a ticket to query the shipping status.



Step 2: Activate the SAG devices

After you receive the SAG device, check whether you have received all the accessories. For more information, see Descriptions of SAG-1000.

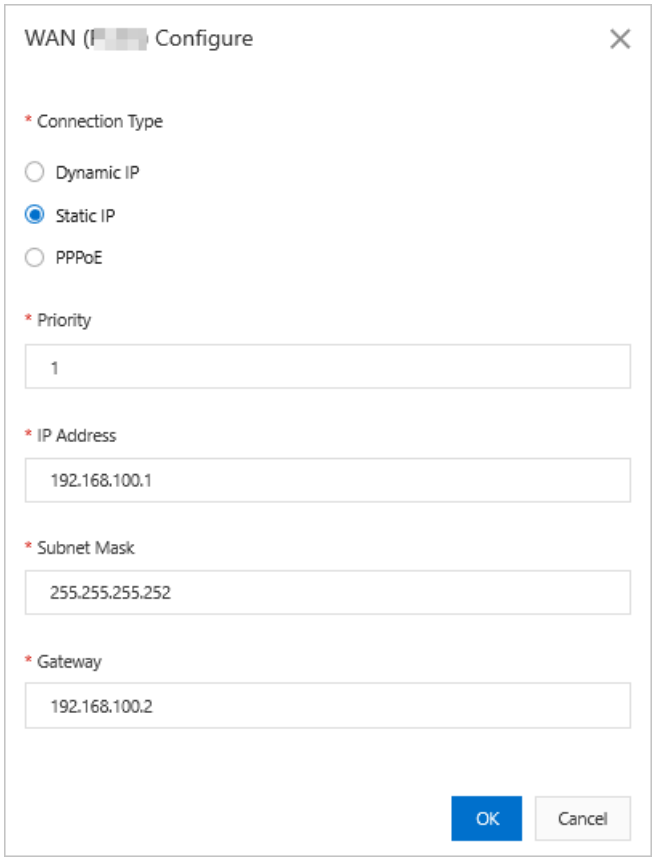
1. Log on to the SAG console.
2. In the top navigation bar, select the area of the SAG device.
3. On the **Smart Access Gateway** page, find the SAG instance created for the SAG device.
4. In the **Actions** column, click **Activate**.
5. In the **Activate** dialog box, click **OK**.
6. After the SAG device is activated, connect it to the private network based on the preceding network topology.

   Use a network cable to connect the WAN port (port 5) of the SAG device to port G11 of the Layer 3 switch.
7. (Optional)If the SAG device was purchased from a third-party vendor, you must manually associate the SAG device with the SAG instance. For more information, see Add a device.

Step 3: Configure the SAG device

After the SAG device is connected to the private network, you can configure the device ports in the SAG console.

1. Configure ports.
   i. On the **Device Management** tab, click **Manage WAN Ports** in the left-side navigation tree.
   ii. In the **WAN (Port 5)** section, click **Edit**.
   iii. In the **Configure WAN (Port 5)** dialog box, set the following parameters and click **OK**.



- **Connection Type**: **Static IP** is selected in this example.
- **Priority**: **1** is selected by default.
- **IP Address**: Enter the IP address of the WAN port. 192.168.100.1 is used in this example.
- **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
- **Gateway**: Enter the IP address of the gateway. 192.168.100.2 is used in this example.

> **Note** After the gateway is configured, the SAG device automatically adds a default route.

2. Configure OSPF dynamic routing.

   Configure OSPF dynamic routing to establish network communication between the SAG device and Layer 3 switch.

   i. On the **Device Management** tab, click **Manage Routes** in the left-side navigation tree.

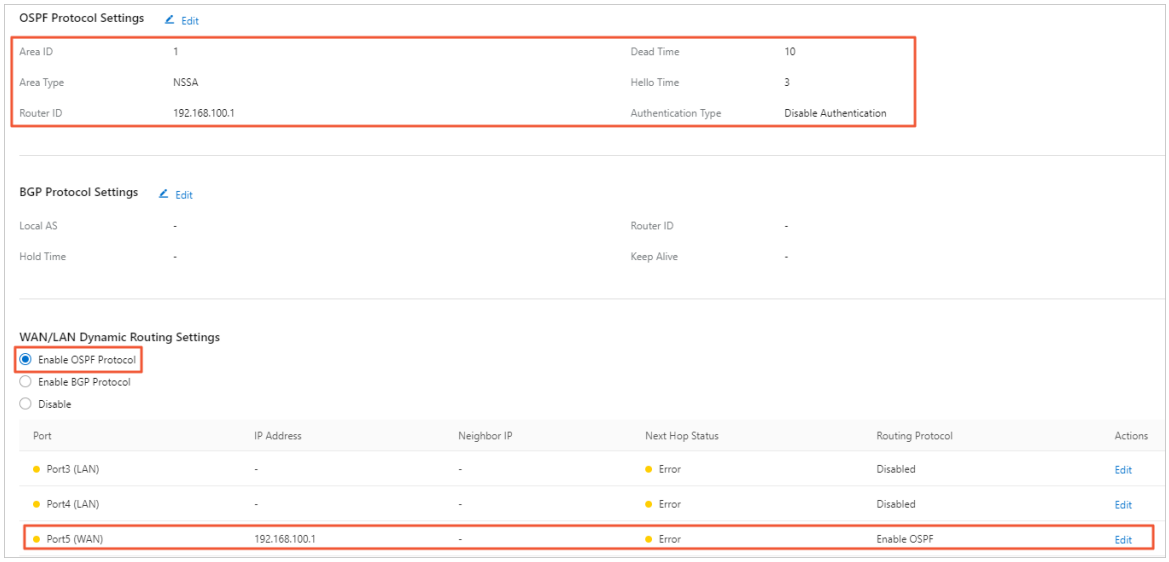
   ii. In the **OSPF Protocol Settings** section, click **Edit**.

iii. In the **Configure OSPF Protocol** dialog box, enter the information about the allocated IP address and click **OK**.

Parameter	Description
Area ID	Set the area ID to 1.
Hello_time	Set the hello time to 3 seconds.
Dead_time	Set the dead time to 10 seconds.
Authentication	Select Disable Authentication.
Router ID	Set the router ID to 192.168.100.1.
Area Type	Default value: NSSA.

iv. In the **WAN/LAN Dynamic Routing Settings** section, select **Enable OSPF Protocol**.

v. Find **Port 5(LAN)**, click **Edit** in the **Actions** column, select Enable OSPF, and then click **OK**.



3. Select a method to advertise routes to Alibaba Cloud.

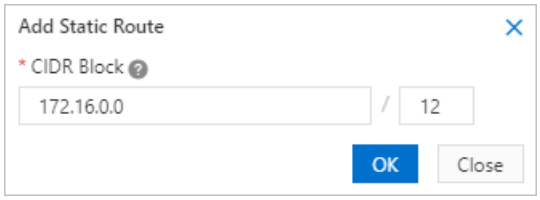
   You must specify how routes are advertised to Alibaba Cloud. These routes are used for network communication between the private network and cloud resources.

   i. On the instance details page, click the **Network Configuration** tab.

   ii. In the left-side navigation tree, click **Methods to Synchronize with On-premises Routes**.

   iii. Select **Static Routing**, click **Add Static Route** to add a CIDR block, and then click **OK**.

   Enter the CIDR block used to connect the private network to Alibaba Cloud. 172.16.0.0/12 is used in this example.



Step 4: Configure switches and Internet-facing routers

In this step, you must configure the peer switch and Internet-facing router for the SAG device. Switches and routers used in this example may be different from yours. For more information, see the manuals issued by your providers.

1. Configure the Layer 3 switch.

```
#a. Set the port IP addresses and OSPF parameters.
interface GigabitEthernet 0/11
 no switchport
 ip ospf network point-to-point                          #The network type of the ports t
hat use the OSPF protocol must be set to peer-to-peer (P2P). Otherwise, the SAG device
cannot calculate routes correctly.
  ip ospf hello-interval 3
 ip ospf dead-interval 10
 ip address 192.168.100.2 255.255.255.252
#b. Configure the loopback IP address and route advertisement information for the switc
h.
interface Loopback 0
ip address 192.168.100.3 255.255.255.255               #The loopback IP address of the
switch.
router ospf 1                                           #Configure OSPF settings and rou
tes.
 router-id 192.168.100.3                                #The router ID of the switch tha
t uses the OSPF protocol.
 network 172.16.0.0 0.15.255.255 area 0                 #The CIDR block of the private n
etwork.
 network 192.168.100.0 0.0.0.4 area 1                        #The CIDR block of the swit
ch port connected to the SAG device.
 network 192.168.100.3 0.0.0.0 area 0                         #The loopback IP address o
f the switch.
 area 1 nssa                                            #The OSPF area is NSSA.
```

2. Configure routes for the Internet-facing router.

```
ip route 192.168.100.0 255.255.255.252 192.168.80.2    #The route to the SAG device.
```

Step 5: Set up network connections

After you configure the SAG device, you must set up network connections to connect the private network to Alibaba Cloud.

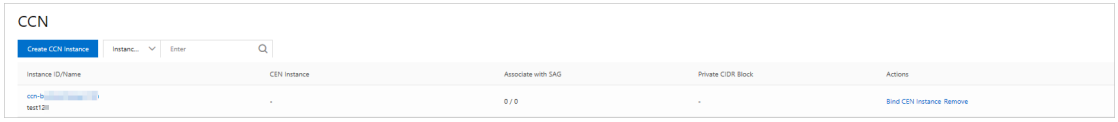
1. Create a Cloud Connect Network (CCN) instance.
   i. Log on to the SAG console.
   ii. In the top navigation bar, select **Mainland China**.

   The area of the CCN instance must be the same as that of the SAG device.

   iii. In the left-side navigation pane, click **CCN**.
   iv. On the **CCN** page, click **Create CCN Instance**.

v. In the **Create CCN Instance** pane, specify a name for the CCN instance and click **OK**.

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



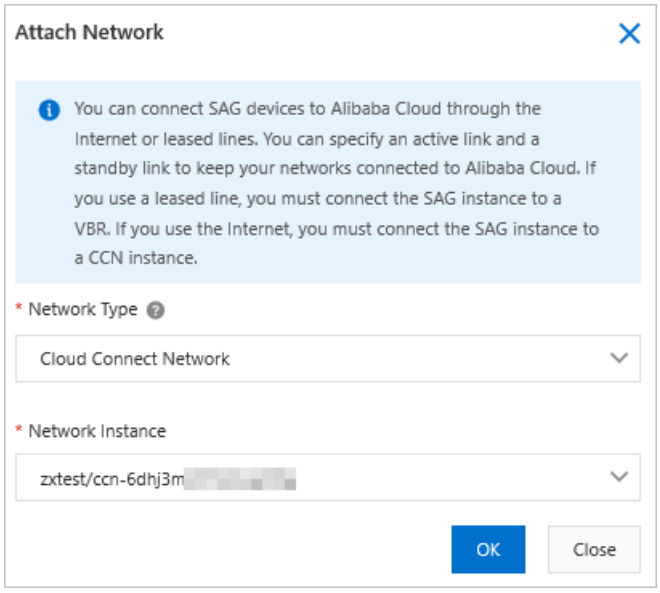
2. Associate the SAG instance with the CCN instance.

i. In the left-side navigation pane, click **Smart Access Gateway**.

ii. On the **Smart Access Gateway** page, find the SAG instance that you want to manage and click **Network Configuration** in the **Actions** column.

iii. In the left-side navigation tree, click **Network Instance Details**.

iv. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance, and then click **OK**.



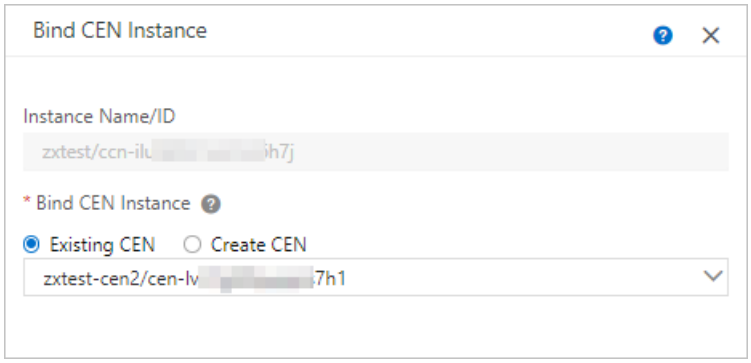
3. Associate the CCN instance with a CEN instance.

After the CCN instance is associated with a CEN instance, SAG devices associated with the CCN instance can communicate with VPC networks associated with the CEN instance.

i. In the left-side navigation pane, click **CCN**.

ii. Find the CCN instance and click **Bind CEN Instance** in the **Actions** column.

iii. In the **Bind CEN Instance** pane, select **Existing CEN**, select the CEN instance that you want to associate with the CCN instance, and then click **OK**.



4. Create a security group rule.

   You must create a security group rule for the Elastic Compute Service (ECS) instance in the VPC network to allow clients in the CIDR block 172.16.0.0/12 of the private network to access resources deployed on the ECS instance. For more information, see Add a security group rule.

Step 6: Test network connectivity

After you complete the preceding steps, test whether you can access cloud resources deployed in the VPC network from a client in the private network.

4.Deploy an SAG device in inline mode and enable DHCP on the LAN port

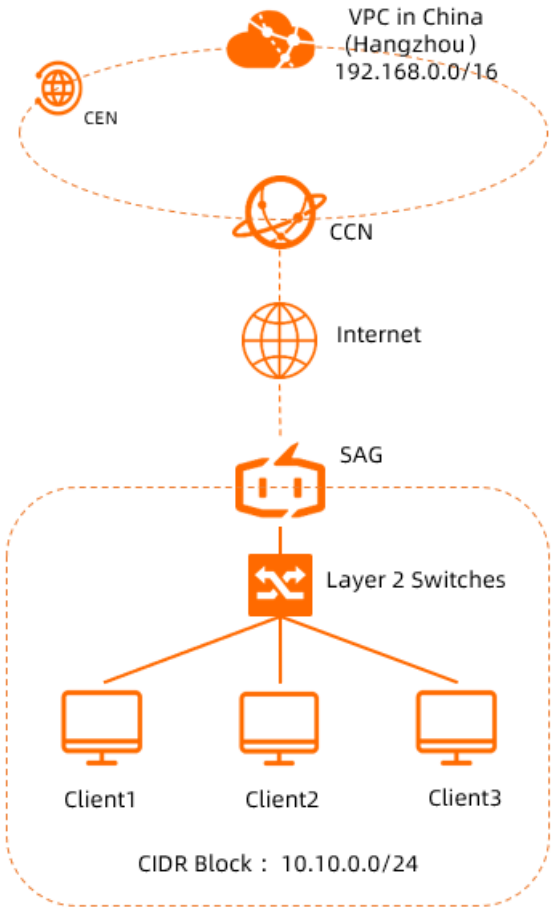
This topic describes how to deploy a Smart Access Gateway (SAG) device and configure Dynamic Host Configuration Protocol (DHCP) on the LAN port to connect private networks to Alibaba Cloud. DHCP is used to dynamically allocate IP addresses and configurations to clients. This facilitates network O&M.

Scenario

The following scenario is used in this topic. An enterprise has created a virtual private cloud (VPC) in the China (Hangzhou) region and cloud services are deployed in the VPC. The enterprise has a new branch (on-premises network) in Hangzhou and wants to connect the on-premises network to Alibaba Cloud. In addition, the enterprise wants the on-premises network to access the DNS server deployed by the enterprise to use the DNS service.

The enterprise plans to deploy an SAG-1000 device in inline mode to connect the on-premises network to Alibaba Cloud. In this scenario, DHCP is enabled on the LAN port of the SAG device to manage and dynamically allocate client IP addresses. In addition, DHCP is also used to allocate the IP address of the DNS server to clients. This facilitates network O&M.

After the enterprise deploys the SAG device, the enterprise can use Cloud Connect Network (CCN) and Cloud Enterprise Network (CEN) to connect the on-premises network to Alibaba Cloud.



Plan networks

Resource	Network planning and configuration
On-premises network	10.10.0.0/24

Resource	Network planning and configuration

SAG device	• Use an SAG-1000 device.
	• Use the inline mode. Connect a modem to the WAN port and connect the LAN port to a Layer 2 switch of the on-premises network.
	• Set port 5 as a WAN port and select the PPPoE connection type.
	  ◦ Username: 33****
	  ◦ Password: 1234****
	  Note The username and password for PPPoE are provided by the Internet service provider (ISP).
	• Set port 4 as a LAN port and enable DHCP.
	  ◦ Set the port IP address to 10.10.0.1/24.
	  ◦ Set the following IP address range for DHCP: 10.10.0.2 to 10.10.0.254.
	  ◦ Enable DHCP options to allocate DNS server addresses to clients.
	  Set the DNS server address to 47.XX.XX.80.

VPC	192.168.0.0/16

Prerequisites

- A VPC is created in the China (Hangzhou) region and cloud services are deployed in the VPC.
- You have read and understand the security group rules that apply to the Elastic Compute Service (ECS) instances in the VPC. Make sure that the security group rules allow the on-premises network to access the ECS instances.

Procedure

Step 1: Purchase an SAG device

Note

1.
2.
3.
4.
5.
6.

Step 2: Activate and connect the SAG device

1.
2.
3.
4.
5. ○ Connect a modem to the WAN port (port 5) of the SAG device by using a network cable.
   ○ Connect the LAN port (port 4) of the SAG device to a Layer 2 switch by using a network cable.
6.

Step 3: Configure the SAG device

You must log on to the web console to configure the SAG devices.

1. Log on to the web console of the SAG device.

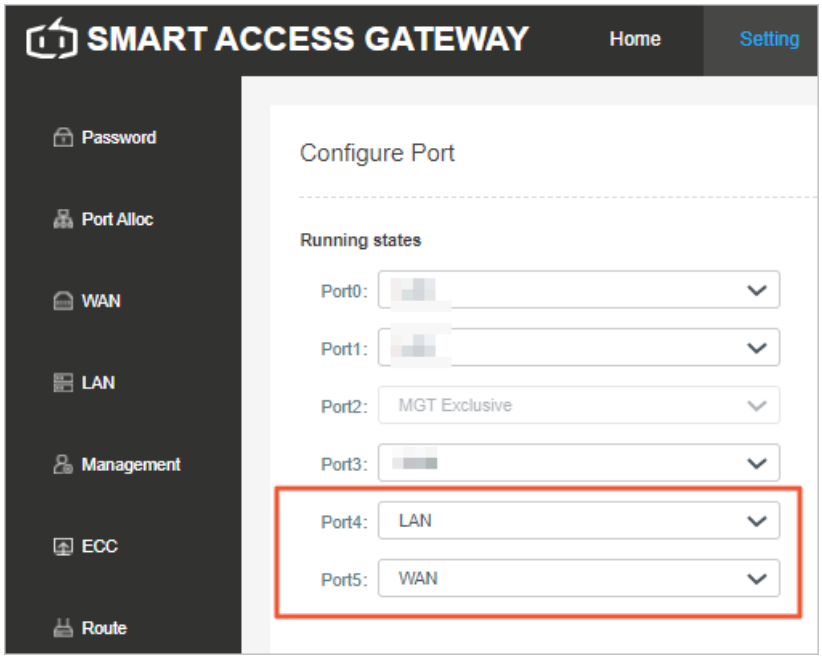
   Use a network cable to connect a computer in the on-premises network to the management port (port 2 by default) of the SAG device. Then, open a browser on the computer and log on to the web console. For more information, see Step 1: Configure the local client and Step 2: Set the password.

2. Assign roles for the ports of the SAG device.

   > **Note** By default, port 5 serves as the WAN port and port 4 serves as the LAN port. If the default setting is used, skip this step and perform Step . Otherwise, perform the following steps to ensure that port 5 serves as the WAN port and port 4 serves as the LAN port.

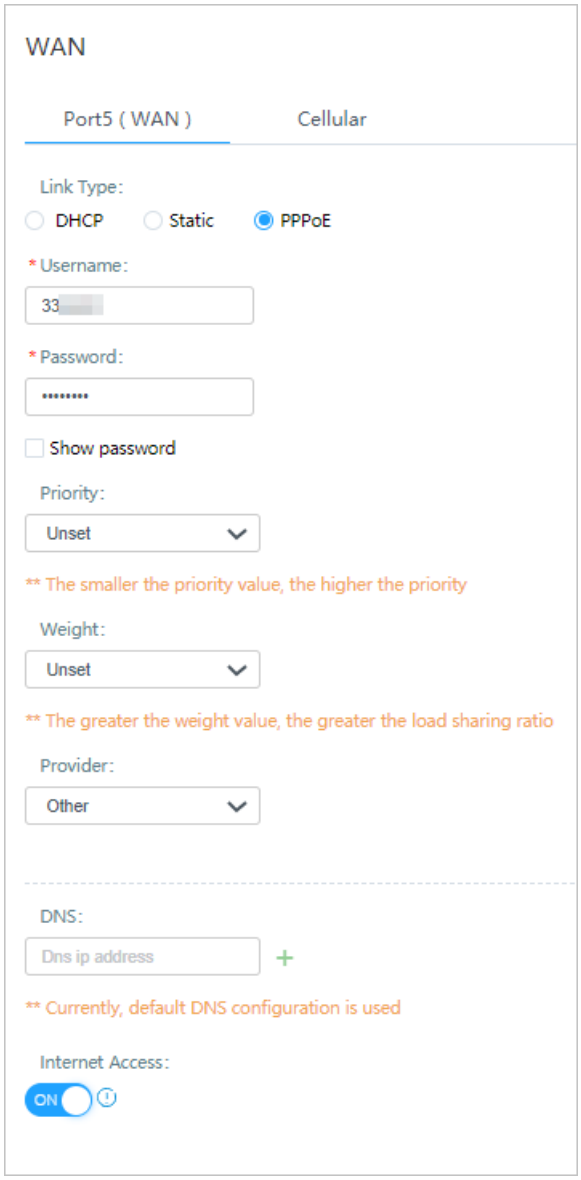
   i. After you log on to the web console, click **Setting** in the top navigation bar.
   ii. In the left-side navigation pane, click **Port Alloc**.

iii. On the **Port Alloc** page, find the port that you want to manage, select a port type, and then click **OK**.



- **Port 4**: Select **LAN**.
- **Port 5**: Select **WAN**.

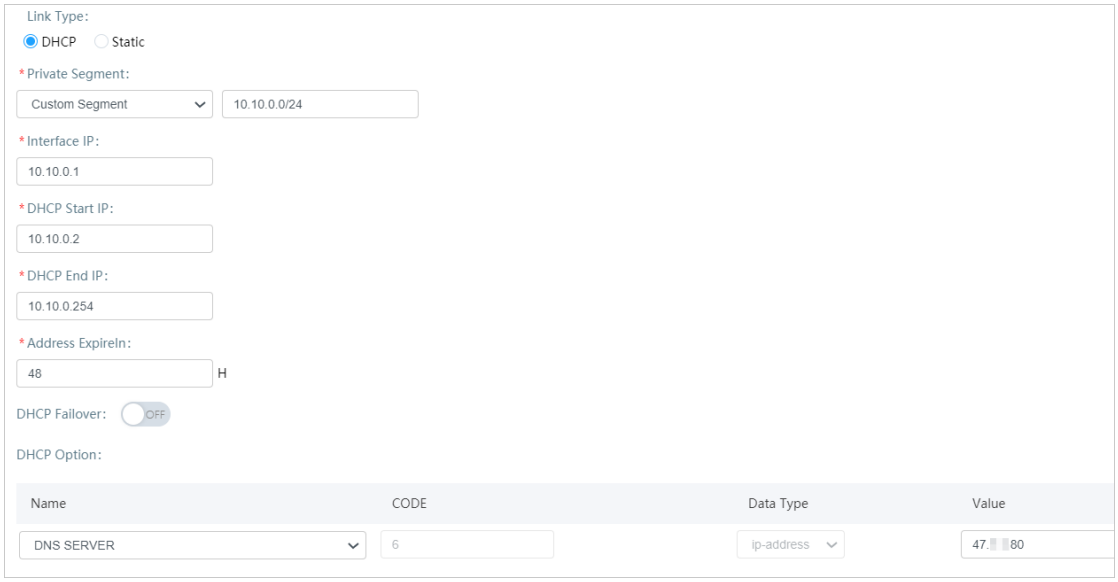
3. Configure the WAN port.
   i. In the left-side navigation pane, click **WAN**.
   ii. On the **WAN** page, click **Port 5 (WAN)**, set the following parameters, and then click **OK**:



- **Link Type**: Select **PPPoE**.
- **Username**: In this example, *33***** is used.
- **Password**: In this example, *1234***** is used.
- **Internet Access**: In this example, this feature is enabled.
- Use the default settings for other parameters.

4. Configure the LAN port.
   i. In the left-side navigation pane, click **LAN**.

ii. On the **LAN** page, click **Port 4 (LAN)**, set the following parameters, and then click **OK**:



- **Link Type**: Select **Dynamic IP**.
- **Private Segment**: Select **Custom Segment** and enter the private CIDR block of the on-premises network: *10.10.0.0/24*.
- **Interface IP**: Enter the IP address of the LAN port. In this example, *10.10.0.1* is used.
- **DHCP Start IP**: In this example, *10.10.0.2* is used.
- **DHCP End IP**: In this example, *10.10.0.254* is used.
- **Address ExpireIn**: In this example, 48 is used. Unit: hours.
- **DHCP Failover**: In this example, this feature is disabled.
- **DHCP Option**: On the right side of the page, click **Add**. Set the following parameters and click **OK** in the **Actions** column:
  - **Name**: Select **DNS SERVER**.
  - **CODE**: The default value is **6**.
  - **Data Type**: The default value is **ip-address**, which indicates the DNS server address to be specified in the **Value** field.
  - **Value**: Enter the DNS server address. In this example, *47.XX.XX.80* is used.

Step 4: Set up network connections

After you configure the SAG device, you must set up network connections in the SAG console to connect the on-premises network to Alibaba Cloud.

1.
2.
3. Select a method to advertise routes to Alibaba Cloud.
   i.
   ii.
   iii.

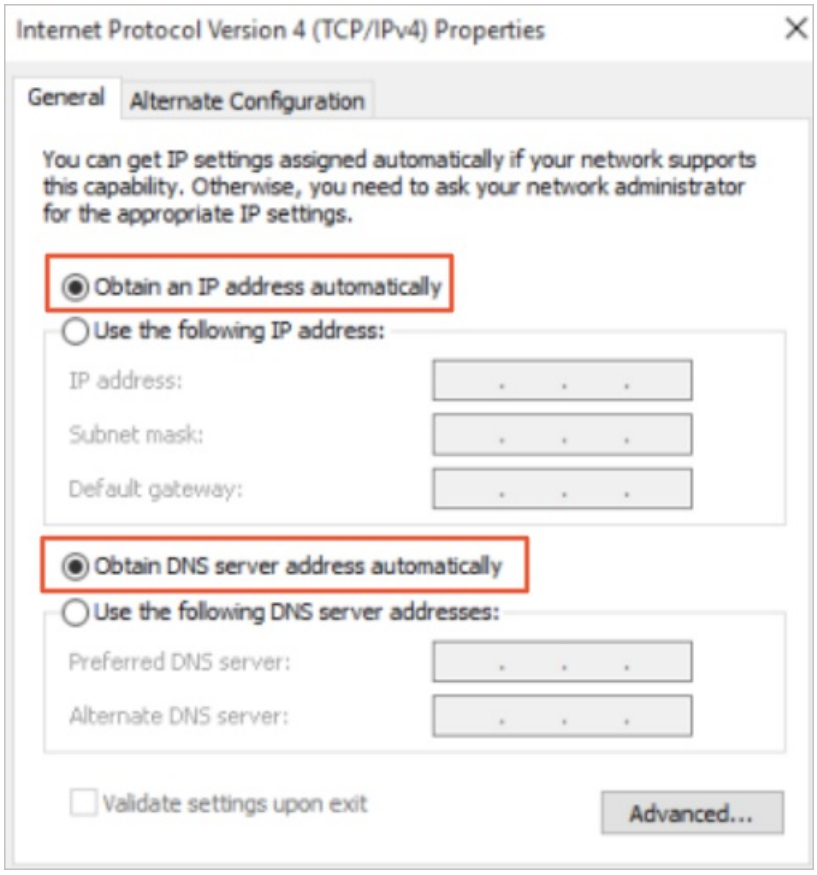
iv. In the **Add Static Route**, enter *10.10.0.0/24*, which is the private CIDR block of the on-premises network, and then click **OK**.

4. Create a CCN instance and associate it with the SAG instance.
   i.
   ii.
   iii.
   iv.
   v.
   vi.
5. Create a CEN instance and attach the VPC and the CCN instance to it.
   i.
   ii.
   iii.
   iv.
   v.
   vi.
   vii.

Step 5: Test the connectivity

1. Find a client in the on-premises network, set the Ethernet network interface controller (NIC) of the client to automatically obtain IP addresses and DNS server addresses. For more information, see the operation guide of the client.

   The Windows operating system is used in the following example.



2. After you complete the configuration, the SAG device automatically allocates IP addresses and DNS server addresses to clients. Run the **ping** command on the client to ping an ECS instance in the VPC. If a response packet is returned, it indicates that the on-premises network is connected to Alibaba Cloud.

```
ping <IP address of an ECS instance>
```

References

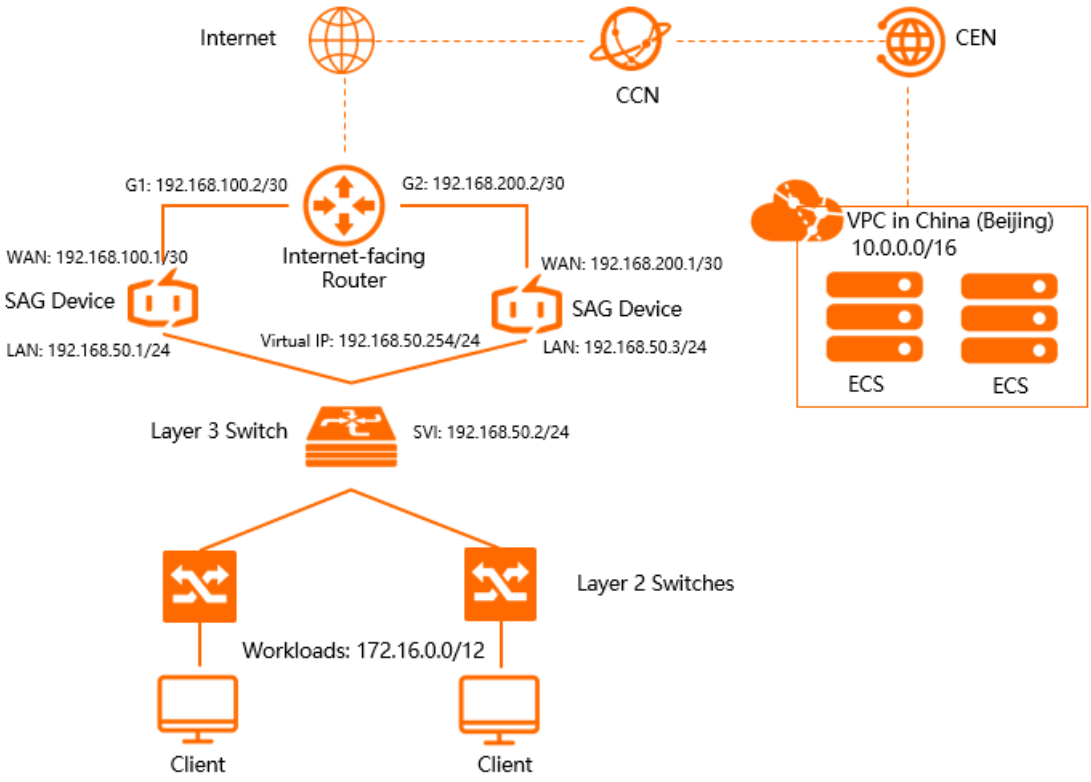
-
-

5.Deploy two SAG devices in inline mode and enable static routing

This topic describes how to deploy two Smart Access Gateway (SAG) devices in inline mode and enable static routing to connect a private network to Alibaba Cloud. This deployment mode improves network availability.

Context

The following figure shows the topology of the private network. A Layer 3 switch is connected to two Layer 2 switches. Local clients and servers are connected to the Layer 2 switches. Two SAG devices are connected to the Layer 3 switch in inline mode to establish network connections between the private network and Alibaba Cloud. The two SAG devices serve as a standby device for each other.



Prerequisites

- A virtual private cloud (VPC) is created in the China (Beijing) region. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC in the China (Beijing) region. For more information, see Create a CEN instance.

Subnetting

The following CIDR blocks are used in this example. When you allocate CIDR blocks based on your actual requirements, make sure that the CIDR blocks do not overlap with each other.

Item	IP address
VPC in the China (Beijing) region	10.0.0.0/16
Internet-facing router	Port G1: 192.168.100.2/30.
	Port G2: 192.168.200.2/30.
SAG Device 1	• WAN port (port 5): 192.168.100.1/30. Next hop: 192.168.100.2. • LAN port (port 4): 192.168.50.1/24. High availability (HA) is enabled and the virtual IP address is 192.168.50.254.
SAG Device 2	• WAN port (port 5): 192.168.200.1/30. Next hop: 192.168.200.2. • LAN port (port 4): 192.168.50.3/24. HA is enabled and the virtual IP address is 192.168.50.254.
Layer 3 switch	• Port G11: assigned to VLAN 10. • Port G12: assigned to VLAN 10. • VLAN 10: 192.168.50.2/24.
Private network	172.16.0.0/12

Step 1: Purchase SAG devices

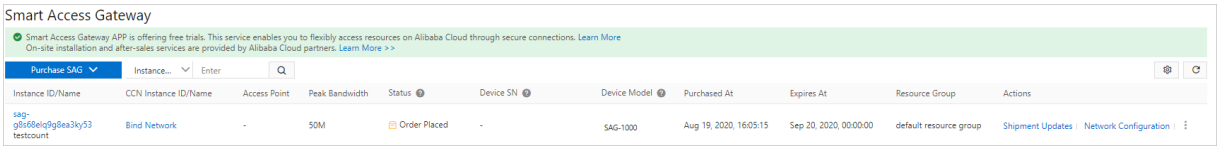
After you purchase SAG devices in the SAG console, Alibaba Cloud delivers the devices to the specified address and creates an SAG instance to help you facilitate network management.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Create SAG Instance**.
3. Set the following parameters and click **Buy Now**:
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the type of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have SAG devices. **No** is selected in this example.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **2** is selected in this example.
   - **Area**: Select the area where the SAG bandwidth will be used. This area must be the same as that of the SAG devices and cannot be modified.
   - **Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter.
   - **Peak Bandwidth**: Specify the maximum bandwidth value. **30Mbps** is selected in this example.
   - **Subscription Duration**: Specify the subscription duration of the bandwidth resources.

4. Confirm the order information and click **Confirm Purchase**.
5. In the **Address** dialog box, enter the recipient address and then click **Order Now**.
6. On the **Pay** page, click **Pay**.

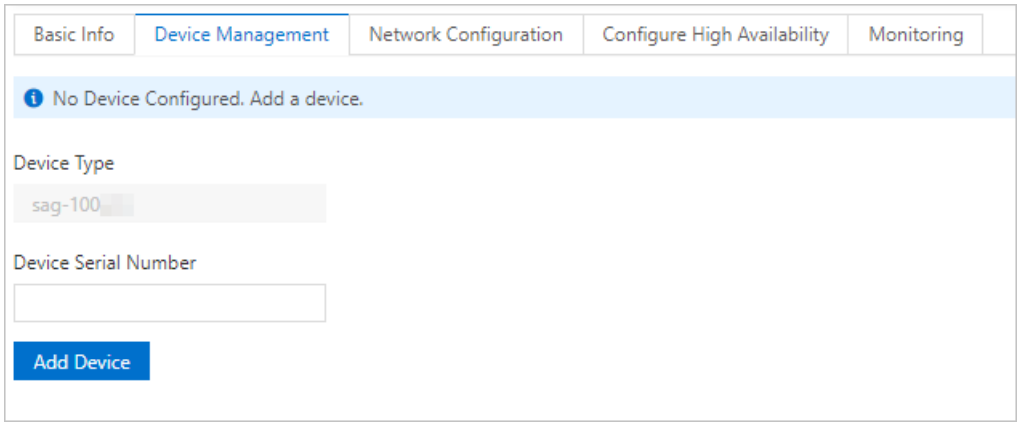
You can check whether the order has been placed on the Smart Access Gateway page. After the order is placed, it will be shipped within two business days. If the order is not shipped within two business days, submit a ticket to query the shipping status.



Step 2: Activate the SAG devices

After you receive the SAG devices, check whether you have received all the accessories. For more information, see Descriptions of SAG-1000.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, find the SAG instance created for the SAG device.
3. In the **Actions** column, click **Activate**.
4. Click the ID of the SAG instance. On the instance details page, click the **Device Management** tab and enter the serial number of the device.



5. Click **Add Device**.
6. Repeat this step to associate the other SAG device with the SAG instance.

Step 3: Connect the SAG devices to your private network

After you activate the SAG devices and associate them with the SAG instance, you must connect the devices to your private network.

Before you begin, make sure that the devices are activated, the 4G networks work as expected, and the devices are connected to Alibaba Cloud. Device 1 is used in this example. Repeat this step to connect Device 2 to your private network.

1. On the **Smart Access Gateway** page, find and click the SAG instance.
2. On the instance details page, click the **Device Management** tab.
3. In the left-side navigation tree, click **Assign Port Roles**.
4. In the **Assign Port Roles** section, find the port and click **Edit** in the **Actions** column. Assign a role

to the port and click **OK**.

The WAN port (port 5) and LAN port (port 4) are used in this example. For more information about ports, see Assign a role to a port.

5. Use a network cable to connect the WAN port (port 5) of the SAG device to port G1 of the Internet-facing router.
6. Use a network cable to connect the LAN port (port 4) of the SAG device to port G11 of the Layer 3 switch.

Step 4: Configure ports

After the SAG devices are connected to your private network, you can configure the device ports in the SAG console.

Device 1 is used in this example. Repeat this step to configure the ports of Device 2.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click the ID of the SAG instance.
3. On the instance details page, click the **Device Management** tab.
4. In the left-side navigation tree, click **Manage LAN Ports**.
5. In the **LAN (Port 4)** section, click **Edit**.
6. In the **Configure LAN (Port 4)** dialog box, set the following parameters and click **OK**.

   Device 1:

   - **Connection Type**: Select **Static IP**.
   - **Port Address**: Enter the IP address of the LAN port. 192.168.50.1 is used in this example.
   - **Subnet Mask**: Enter the subnet mask of the LAN port IP address. 255.255.255.0 is used in this example.

   Device 2:

   - **Connection Type**: **Select Static IP**.
   - **Port Address**: Enter the IP address of the LAN port. 192.168.50.3 is used in this example.
   - **Subnet Mask**: Enter the subnet mask of the LAN port IP address. 255.255.255.0 is used in this example.
7. In the left-side navigation tree, click **Manage WAN Ports**.
8. In the **WAN (Port 5)** section, click **Settings**.
9. In the **Configure WAN (Port 5)** dialog box, set the following parameters and click **OK**.

   Device 1:

   - **Connection Type**: Select **Static IP**.
   - **IP Address**: Enter the IP address of the WAN port. 192.168.100.1 is used in this example.
   - **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
   - **Gateway**: Enter the IP address of the gateway. 192.168.100.2 is used in this example.

   Device 2:

   - **Connection Type**: **Select Static IP**.

- **IP Address**: Enter the IP address of the WAN port. 192.168.200.1 is used in this example.
- **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
- **Gateway**: Enter the IP address of the gateway. 192.168.200.2 is used in this example.

> **Note** After you configure the gateway, the SAG device generates a default route.

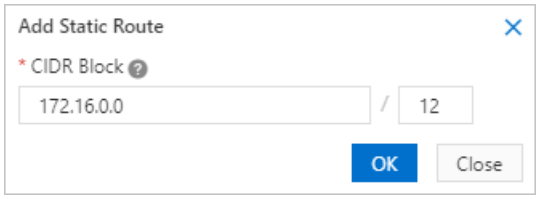
Step 5: Configure routing methods

After you configure the WAN and LAN ports of the SAG devices, you must also configure the routing method that synchronizes local routes with Alibaba Cloud and specify static routes to route traffic from Alibaba Cloud to the private network.

Device 1 is used in this example. Repeat this step to configure a routing method for Device 2.

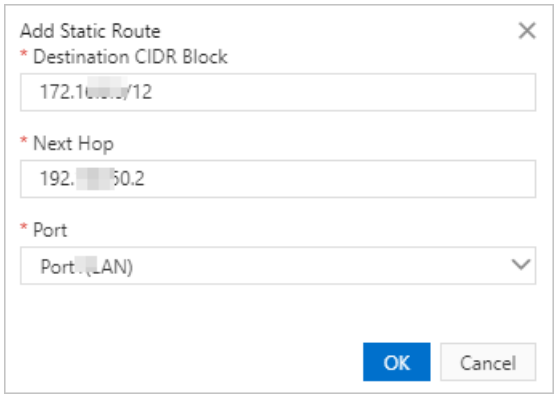
1. On the **Smart Access Gateway** page, click the ID of the SAG instance.
2. On the instance details page, click the **Network Configuration** tab.
3. In the left-side navigation tree, click **Methods to Synchronize with On-premises Routes**.
4. Select **Static Routing**, click **Add Static Route** to add a CIDR block, and then click **OK**.

   Enter the CIDR block used to route network traffic from Alibaba Cloud to the private network. 172.16.0.0/12 is used in this example.

5. On the instance details page, click the **Device Management** tab.
6. In the left-side navigation tree, click **Manage Routes** and then click **Add Static Route**.
7. In the **Add Static Route** dialog box, add a static route that routes traffic from Alibaba Cloud to the private network.

Parameter	Description
Destination CIDR Block	Device 1: 172.16.0.0/12. Device 2: 172.16.0.0/12.
Next Hop	Device 1: 192.168.50.2. Device 2: 192.168.50.2.
Ports	Select Port 4 (LAN) for both Device 1 and Device 2.



Step 6: Configure HA

The HA feature is used in this example to address single point of failures (SPOFs).

Device 1 is used in this example. Repeat this step to configure a routing method for Device 2.

1.
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 the **Device Management** tab.
   - Find the 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 .
5. In the **Configure HA** dialog box, select an HA mode.

   The following table describes the parameters.

Parameter	Description
HA Mode	Select **Static** for both Device 1 and Device 2.
Port	Select LAN 4 for both Device 1 and Device 2.
Virtual IP	Enter a virtual IP address for the SAG devices. 192.168.50.254 is used for both Device 1 and Device 2 in this example.

6. Click **Save**.

Step 7: Configure the Layer 3 switch and Internet-facing router

The commands used to configure switches vary depending on the switch provider. For more information, see the manuals issued by your providers. A switch and router provided by Cisco are used in this example.

- The Layer 3 switch

> **Note** For each SAG device, the network type of ports using the OSPF protocol must be set to peer-to-peer (P2P). Otherwise, the SAG device cannot calculate routes correctly.

```
Configure IP addresses for the ports:
interface GigabitEthernet 0/12
switchport access vlan 10                 Assign the LAN port of Device 1 to VLAN 10
interface GigabitEthernet 0/14
switchport access vlan 10                Assign the LAN port of Device 2 to VLAN 10
interface  vlan 10
ip address 192.168.50.2 255.255.255.0    The gateway IP address of the client
ip route 0.0.0.0 0.0.0.0 192.168.50.254         The route to the Internet
```

- The Internet-facing router

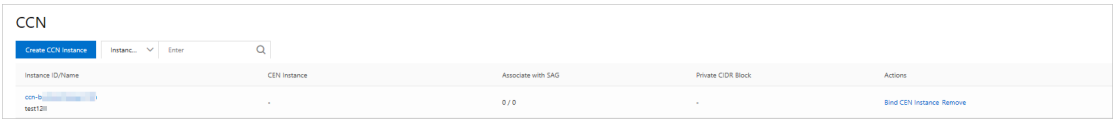
```
Configure static routes
ip route 192.168.100.1 255.255.255.252  192.168.100.2 The route to Device 1.
ip route 192.168.200.1 255.255.255.252  192.168.200.2 The route to Device 2.
```

Step 8: Set up network connections

After you configure the SAG devices, you must set up network connections to connect the private network to Alibaba Cloud.

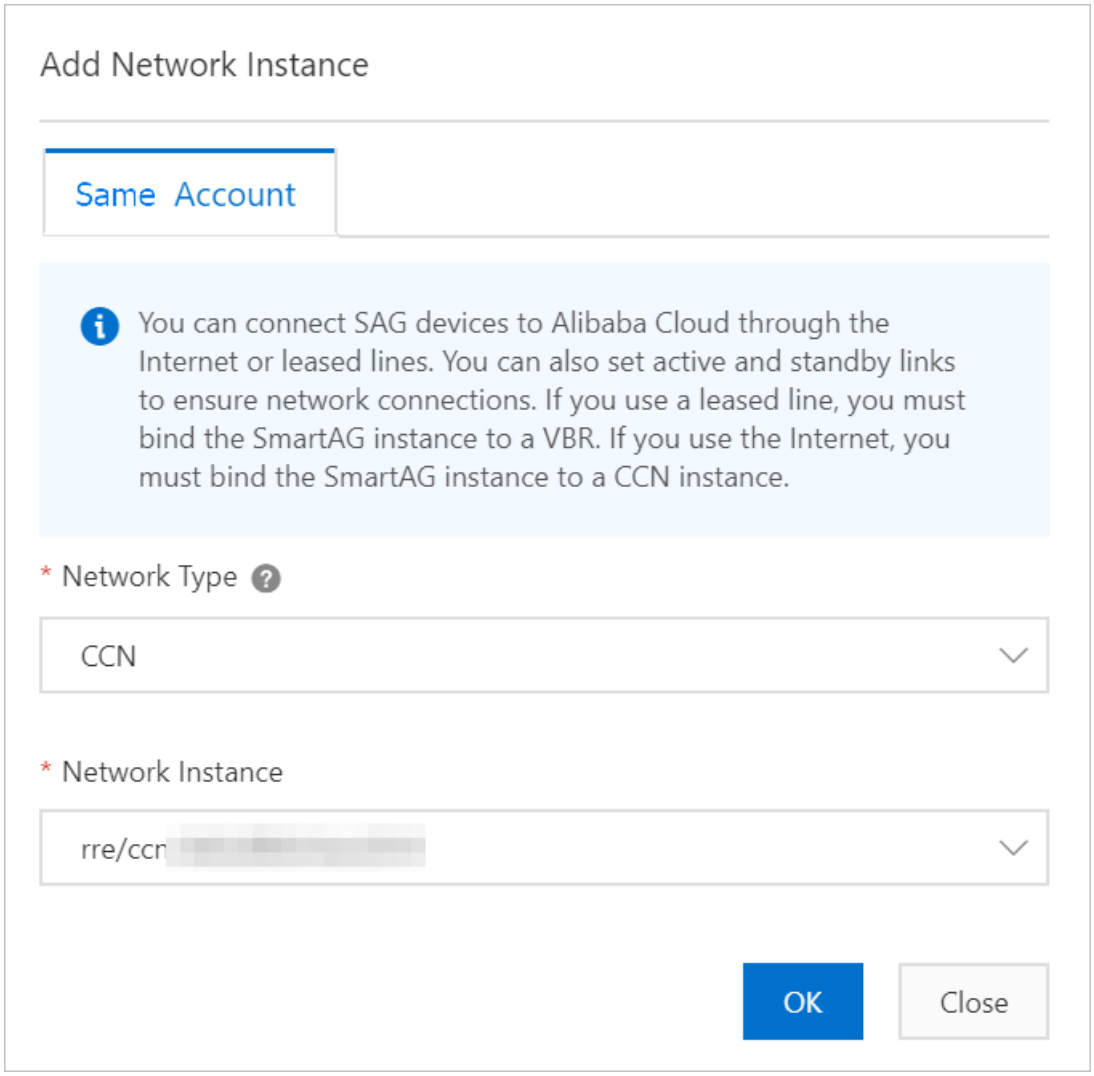
1. Create a CCN instance.
   i. Log on to the SAG console.
   ii. In the left-side navigation pane, click **CCN**.
   iii. On the **CCN** page, click **Create CCN Instance**.
   iv. In the **Create CCN Instance** pane, specify a name for the CCN instance and click **OK**.

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



2. Set up network connections.
   i. Log on to the SAG console.
   ii. On the **Smart Access Gateway** page, find the SAG instance and click **Network Configuration** in the **Actions** column.

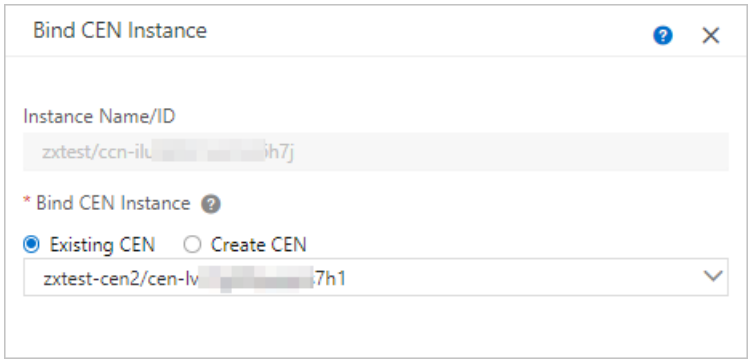
iii. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance, and then click **OK**.



3. Associate the CCN instance with a CEN instance.
   i. Log on to the SAG console.
   ii. In the left-side navigation pane, click **CCN**.
   iii. Find the CCN instance and click **Bind CEN Instance** in the **Actions** column.

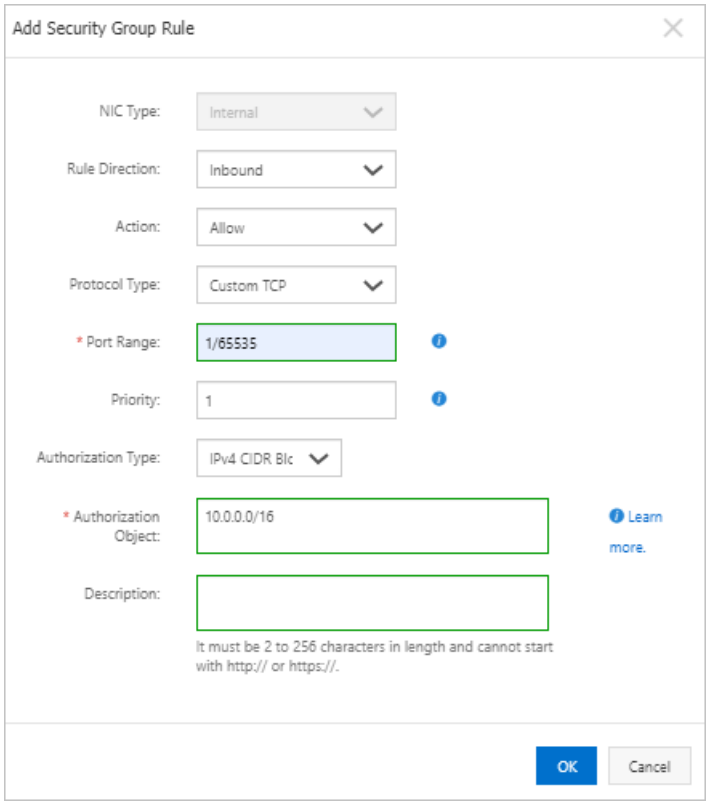
iv. In the **Bind CEN Instance** pane, select the CEN instance and click **OK**.

After the CCN instance is associated with the CEN instance, SAG devices in the CCN can communicate with networks such as VPCs and virtual border routers (VBRs) associated with the CEN.



4. Configure a security group.
   i. Log on to the ECS console.
   ii. In the left-side navigation pane, click **Instance**.
   iii. Find the ECS instance deployed in the VPC and choose **More > Network and Security Group > Configure Security Group**.
   iv. Click **Add Rules** and then click **Add Security Group Rule**.
   v. Create a security group rule that allows access from the private network to the VPC.

   The following figure shows how to configure a security group rule. Set Authorization Object to the CIDR block of the private network.



Step 9: Test the connectivity

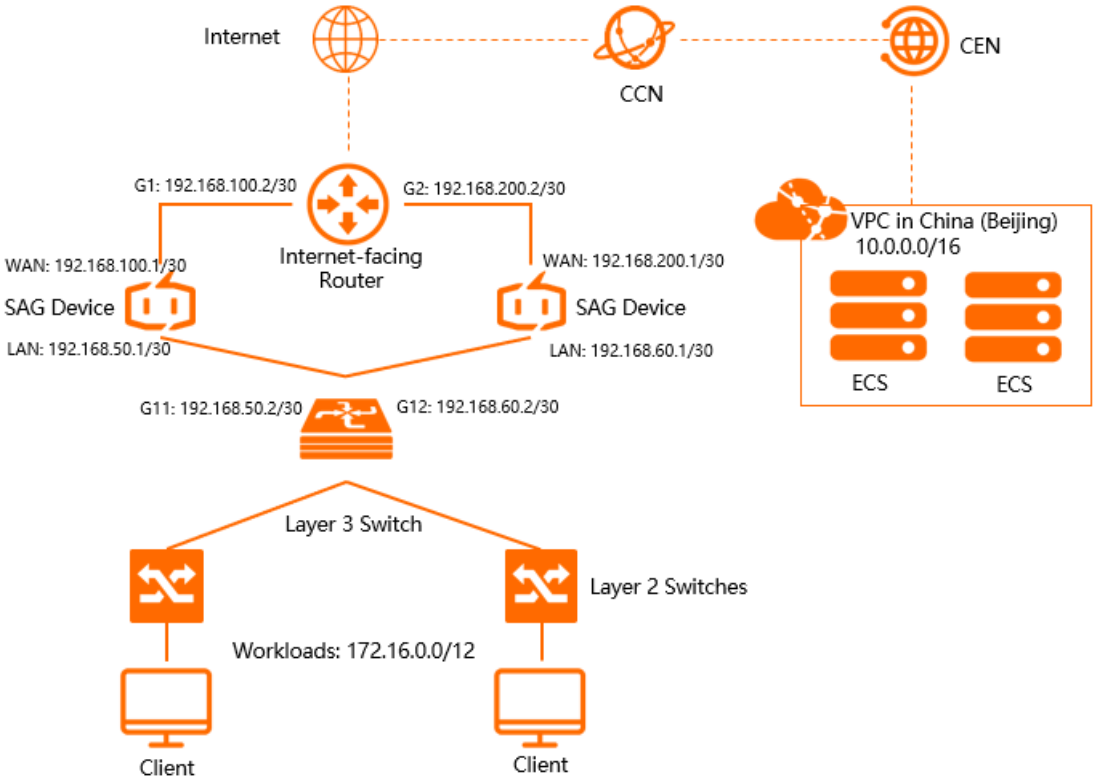
After you complete the configurations in the preceding steps, access cloud resources deployed in the VPC from a client in your private network to test the connectivity.

6.Deploy two SAG devices in inline mode and enable dynamic routing

This topic describes how to deploy two Smart Access Gateway (SAG) devices in inline mode and enable Open Shortest Path First (OSPF)-based dynamic routing to connect a private network to Alibaba Cloud.

Context

The following figure shows the topology of the private network. A Layer 3 switch is connected to two Layer 2 switches. Local clients and servers are connected to the Layer 2 switches. Two SAG devices are connected to the Layer 3 switch in inline mode to establish network connections between the private network and Alibaba Cloud. The two SAG devices serve as a standby device for each other.



Prerequisites

- A Virtual Private Cloud (VPC) network is created in the China (Beijing) region. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC network in the China (Beijing) region. For more information, see Create a CEN instance.

Subnetting

The following CIDR blocks are used in this example. When you allocate CIDR blocks based on your actual requirements, make sure that the CIDR blocks do not overlap with each other.

Object	IP address
VPC network in the China (Beijing) region	10.0.0.0/16.
Internet-facing router	Port G1: 192.168.100.2/30.
	Port G2: 192.168.200.2/30.
SAG Device 1	• WAN port (port 5): 192.168.100.1/30. Next hop: 192.168.100.2. • LAN port 4:192.168.50.1/30.
SAG Device 2	• WAN port (port 5): 192.168.200.1/30. Next hop: 192.168.200.2. • LAN port 4:192.168.60.1/30.
Layer 3 switch	• Port G11: 192.168.50.2/30. • Port G12: 192.168.60.2/30. • Loopback interface: 192.168.100.3/32.
Private network	172.16.0.0/12.

Step 1: Purchase SAG devices

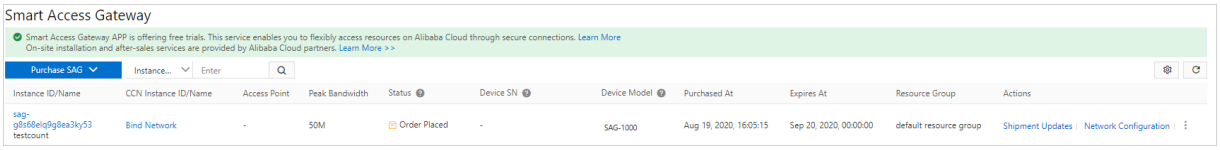
After you purchase SAG devices in the SAG console, Alibaba Cloud delivers the devices to the specified address and creates an SAG instance to help you facilitate network management.

1. Log on to the SAG console.
2. Set the following parameters.
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the type of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have SAG devices. **No** is selected in this example.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **2** is selected in this example.
   - **Area**: Select the area where the SAG bandwidth will be used. This area must be the same as that of the SAG devices and cannot be modified.
   - **Instance Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter or Chinese character.
   - **Peak Bandwidth**: Select the maximum bandwidth for network connections. **30Mbps** is selected in this example.
   - **Subscription Duration**: Select the duration of the subscription.
3. After you set the preceding parameters, click **Buy Now**.
4. Confirm the order information and click **Confirm Purchase**.

5. In the **Shipping Address** dialog box that appears, enter the recipient address and then click **Buy Now**.
6. On the **Pay** page that appears, click **Pay**.

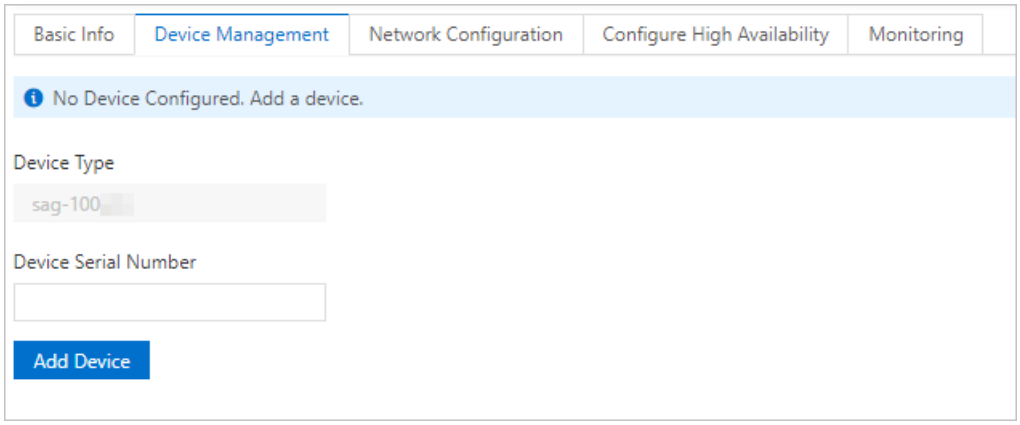
You can check whether the order has been placed on the Smart Access Gateway page. The SAG devices will be shipped within two business days. If the order is not shipped within two business days, submit a ticket to query the shipping status.



Step 2: Activate the SAG devices

After you receive the SAG devices, check whether you have received all the accessories. For more information, see Descriptions of SAG-1000.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, find the target SAG instance.
3. In the **Actions** column, click **Activate**.
4. Click the ID of the target SAG instance. On the instance details page, click the **Device Management** tab and enter the serial number of the device.



5. Click **Add Device**.
6. Repeat this step to associate the other SAG device with the SAG instance.

Step 3: Connect the SAG devices to your private network

After you activate the SAG devices and associate them with the SAG instance, you must connect the devices to your private network.

Before you begin, make sure that the devices are activated, the 4G networks work as expected, and the devices are connected to Alibaba Cloud. Device 1 is used in this example. Repeat this step to connect Device 2 to your private network.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, find and click the target SAG instance.
3. On the instance details page, click the **Device Management** tab.
4. In the left-side navigation tree, click **Assign Port Roles**.

5. In the **Assign Port Roles** section, find the target port and click **Edit** in the **Actions** column. Assign a role to the port and click **OK**.

   The WAN port (port 5) and LAN port (port 4) are used in this example. For more information about ports, see Assign a role to a port.
6. Use a network cable to connect the WAN port (port 5) of the SAG device to port G1 of the Internet-facing router.
7. Use a network cable to connect the LAN port (port 4) of the SAG device to port G11 of the Layer 3 switch.

Step 4: Configure ports

After the SAG devices are connected to your private network, you can configure the device ports in the SAG console.

Device 1 is used in this example. Repeat this step to configure the ports of Device 2.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click the ID of the target SAG instance.
3. On the instance details page, click the **Device Management** tab.
4. In the left-side navigation tree, click **Manage LAN Ports**.
5. In the **LAN (Port 4)** section, click **Edit**.
6. In the **Configure LAN (Port 4)** dialog box that appears, set the following parameters and click **OK**.
   - **Connection Type**: Select **Static IP**.
   - **Port Address**: Enter the IP address of the LAN port. 192.168.50.1 is used in this example.
   - **Subnet Mask**: Enter the subnet mask of the LAN port IP address. 255.255.255.252 is used in this example.
7. In the left-side navigation tree, click **Manage WAN Ports**.
8. In the **WAN (Port 5)** section, click **Edit**.
9. In the **Configure WAN (Port 5)** dialog box that appears, set the following parameters and click **OK**.
   - **Connection Type**: Select **Static IP**.
   - **IP Address**: Enter the IP address of the WAN port. 192.168.100.1 is used in this example.
   - **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
   - **Gateway**: Enter the IP address of the gateway. 192.168.100.2 is used in this example.

     > **Note** After you configure the gateway, the SAG device generates a default route.

Step 5: Configure OSPF-based dynamic routing

You can configure OSPF-based dynamic routing for SAG devices in the SAG console.

Device 1 is used in this example. Repeat this step to configure OSPF-based dynamic routing for Device 2.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click the ID of the target SAG instance.

3. On the instance details page, click the **Device Management** tab.
4. In the left-side navigation tree, click **Manage Routes**.
5. In the **OSPF Protocol Settings** section, click **Edit**.
6. In the **Configure OSPF Protocol** dialog box that appears, enter the information about the allocated IP address and click **OK**.

Parameter	Description
Area ID	Set area IDs as follows: Area ID of the active device: 1. Area ID of the standby device: 1.
Hello Time	Set the hello time to 3 seconds for both devices.
Dead Time	Set the dead time to 10 seconds for both devices.
Authentication Type	Select Disable Authentication for both devices.
Router ID	Set router IDs as follows: Router ID of the active device: 192.168.100.1. Router ID of the standby device: 192.168.200.1.
Area Type	The area type is set to NSSA by default.

7. In the **Dynamic Routing Settings** section, select **Enable OSPF Protocol**.
8. Find **Port 4 (LAN)**, click **Edit** in the **Actions** column, select Enable OSPF, and then click **OK**.

Step 6: Configure the Layer 3 switch and Internet-facing router

The commands used to configure switches vary depending on the switch provider. For more information, see the manuals issued by your providers. A switch and router provided by Cisco are used in this example.

- The Layer 3 switch

- Set the port IP addresses and OSPF parameters.

  > **Note** For each SAG device, the network type of ports using the OSPF protocol must be set to peer-to-peer (P2P). Otherwise, the SAG device cannot calculate routes correctly.

```
interface GigabitEthernet 0/11
 no switchport
 ip ospf network point-to-point          Set the network type to P2P
 ip ospf hello-interval 3
 ip ospf dead-interval 10
 ip address 192.168.50.2 255.255.255.252 The port IP address of the peer switch of Devi
ce 1
interface GigabitEthernet 0/12
 no switchport
 ip address 192.168.60.2 255.255.255.252    The port IP address of the peer switch of D
evice 2
 ip ospf network point-to-point    Set the network type to P2P
 ip ospf dead-interval 10
 ip ospf hello-interval 3
!
```

- Specify the loopback address and route advertisement information.

  > **Note** OSPF requires a not-so-stubby area (NSSA), automatically generates a default route, and advertises it to SAG.

```
interface Loopback 0
ip address 192.168.100.3 255.255.255.255                      The loopback address of
the switch
!
router ospf 1
 router-id 192.168.100.3                                    The router ID of the switc
h
 network 172.16.0.0 0.15.255.255 area 0                       The CIDR block of the lo
cal server
 network 192.168.50.0 0.0.0.4 area 1                      The CIDR block of the switch
port connected to Device 1
 network 192.168.100.3 0.0.0.0 area 0                       The loopback address of th
e switch
 network 192.168.60.0 0.0.0.4 area 1                      The CIDR block of the switch
port connected to Device 2
 area 1 nssa default-information-originate no-summary
!
```

- The Internet-facing router

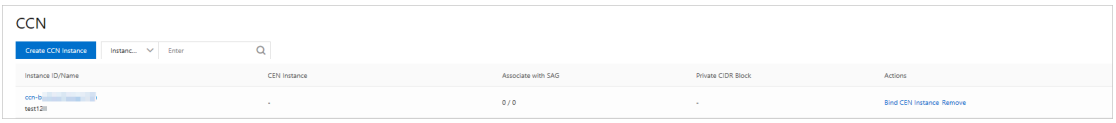
```
Configure static routes
ip route 192.168.100.0 255.255.255.252  192.168.100.2 The route to Device 1
ip route 192.168.200.0 255.255.255.252  192.168.200.2 The route to Device 2
```

Step 7: Set up network connections

After you configure the SAG devices, you must set up network connections to connect the private network to Alibaba Cloud.

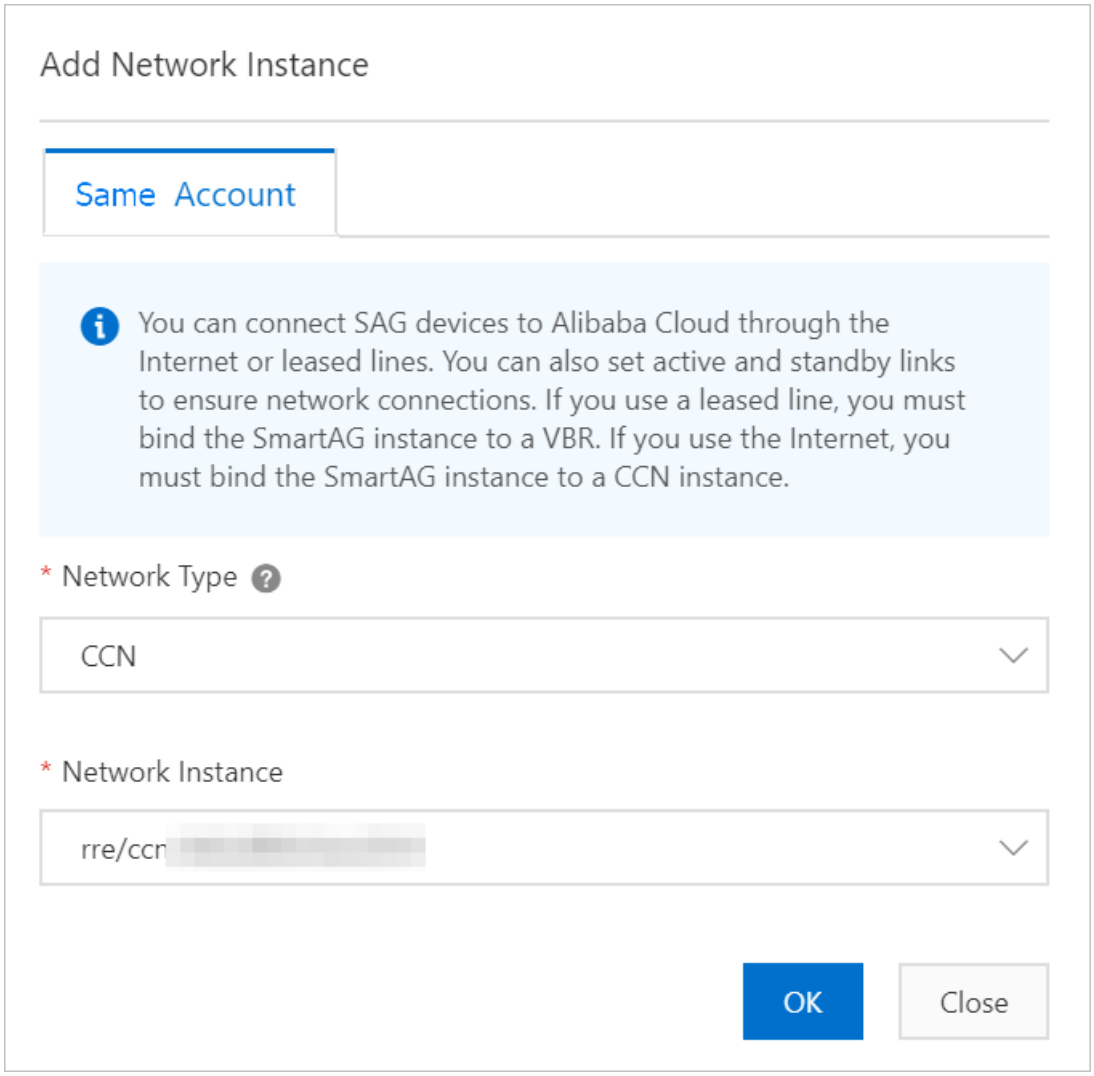
1. Create a Cloud Connect Network (CCN) instance.
   i. Log on to the SAG console.
   ii. In the left-side navigation pane, click **CCN**.
   iii. On the **CCN** page, click **Create CCN Instance**.
   iv. In the **Create CCN Instance** pane that appears, specify a name for the CCN instance and click **OK**.

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



2. Set up network connections.
   i. Log on to the SAG console.
   ii. On the **Smart Access Gateway** page, click the ID of the target SAG instance or click **Network Configuration** in the **Actions** column.
   iii. On the **Method to Synchronize with On-premises Routes** tab, select **Dynamic Routing**.

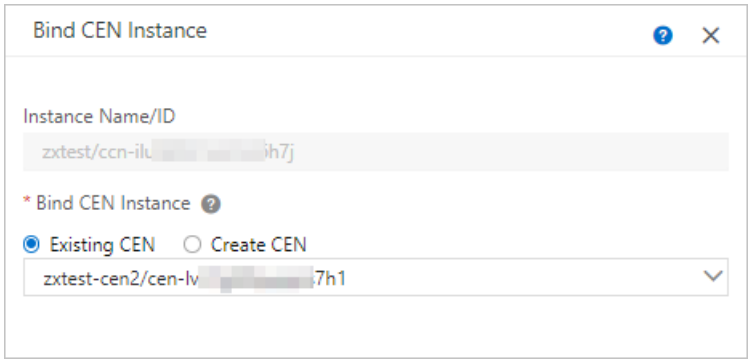
iv. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance, and then click **OK**.



3. Associate the CCN instance with a CEN instance.
   i. Log on to the SAG console.
   ii. In the left-side navigation pane, click **CCN**.
   iii. Find the target CCN instance and click **Bind CEN Instance** in the **Actions** column.

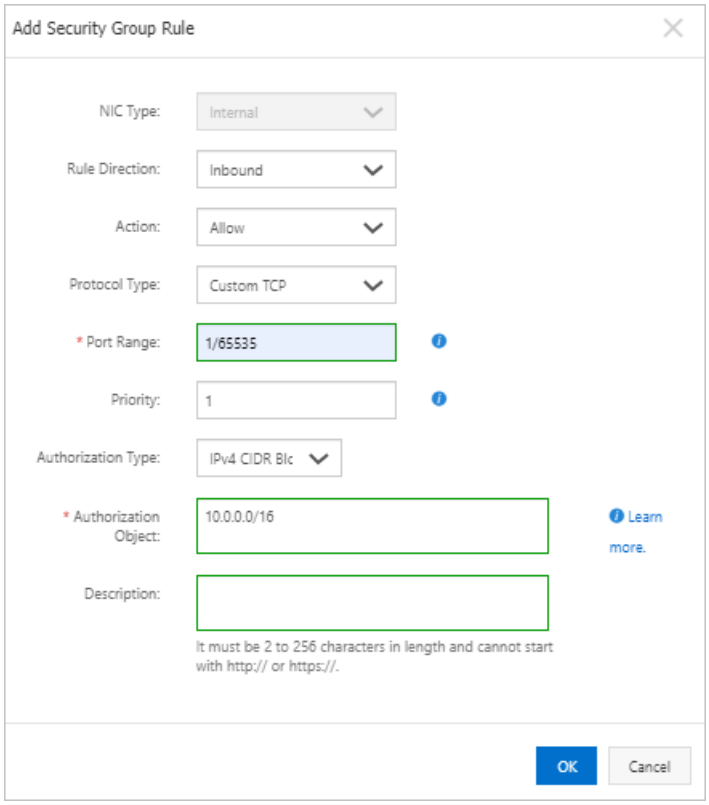
iv. In the **Bind CEN Instance** pane that appears, select the target CEN instance and click **OK**.

After the CCN instance is associated with the CEN instance, SAG devices in the CCN can communicate with networks such as VPC networks and virtual border routers (VBRs) associated with the CEN.



4. Configure a security group.
   i. Log on to the Elastic Compute Service (ECS) console.
   ii. In the left-side navigation pane, click **Instances**.
   iii. Find the ECS instance deployed in the target VPC network and choose **More > Network and Security Group > Configure Security Group**.
   iv. Click **Add Rules** and then click **Add Security Group Rule**.
   v. Create a security group rule that allows access from the private network to the VPC network.

   The following figure shows how to configure a security group rule. Set Authorization Object to the CIDR block of the private network.



Step 8: Test the connectivity

After you complete the configurations in the preceding steps, access cloud resources deployed in the VPC network from a client in your private network to test the connectivity.

7.Deploy two SAG devices in inline mode and enable DHCP on LAN ports

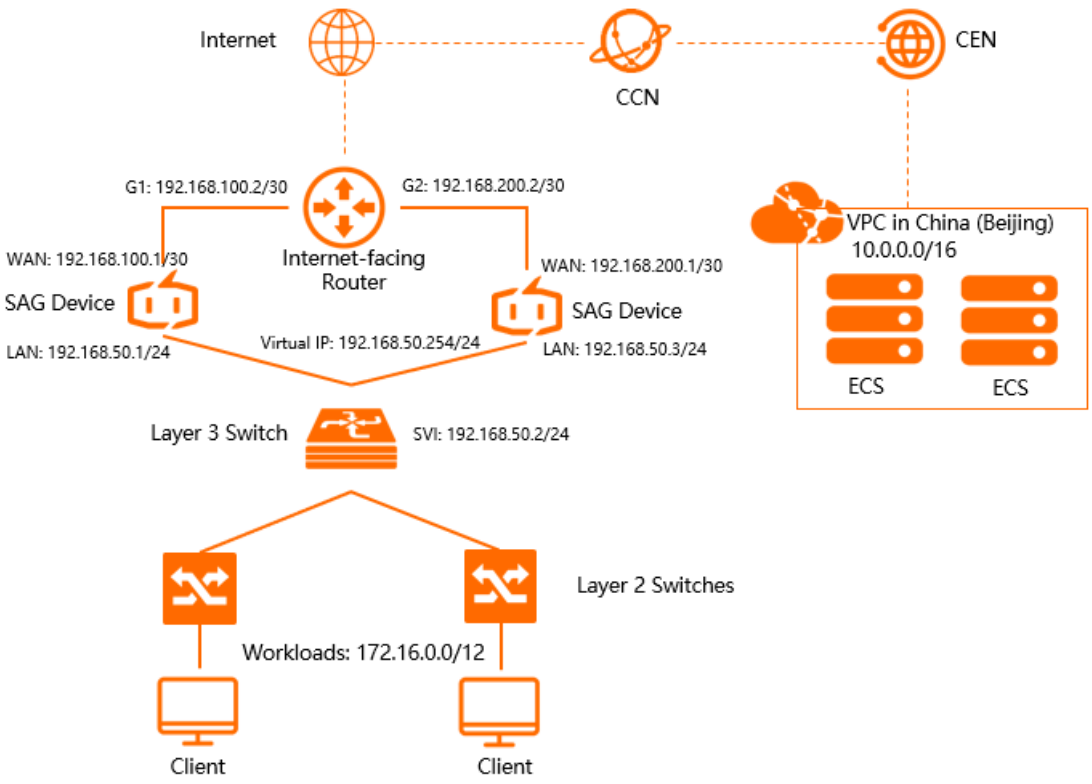
This topic describes how to deploy two Smart Access Gateway (SAG) devices in inline mode and enable Dynamic Host Configuration Protocol (DHCP) on the LAN ports. This way, you can connect private networks to Alibaba Cloud and improve the availability of your networks.

Prerequisites

- A Virtual Private Cloud (VPC) network is created. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC network. For more information, see Create a CEN instance.

Context

In this example, an enterprise has created a VPC network in China (Beijing) and has deployed services in the VPC network. The enterprise wants to connect private networks to Alibaba Cloud through SAG devices. The enterprise wants to deploy two SAG-1000 devices in inline mode. The enterprise also wants to enable DHCP on the LAN ports of the SAG devices. This way, the enterprise can manage and dynamically assign IP addresses to the client side, and operations and maintenance (O&M) workloads are reduced. The enterprise also wants to enable the DHCP failover and high availability (HA) features of the SAG devices. This allows the enterprise to switch over to the standby device when the active device is faulty, which improves the network availability.



Subnetting

The following table describes the IP addresses and CIDR blocks in this example. If you want to use your own IP addresses and CIDR blocks, make sure that the IP addresses or CIDR blocks do not overlap with each other.

Item	Subnetting
VPC network in China (Beijing)	Private CIDR block: 10.0.0.0/16
Internet-facing router	Port G1: 192.168.100.2/30
	Port G2: 192.168.200.2/30

Active SAG device	• WAN port 5: uses a static IP address
	  ◦ Port IP address: 192.168.100.1/30
	  ◦ Gateway: 192.168.100.2
	• LAN port 4: uses a dynamic IP address
	  ◦ Port IP address: 192.168.50.1/24
	  ◦ DHCP IP address pool: 192.168.50.3 to 192.168.50.253
	  ◦ DHCP failover is enabled
	  ◦ HA is enabled: The virtual IP address is 192.168.50.254

Standby SAG device	• WAN port 5: uses a static IP address
	  ◦ Port IP address: 192.168.200.1/30
	  ◦ Gateway: 192.168.200.2
	• LAN port 4: uses a dynamic IP address
	  ◦ Port IP address: 192.168.50.2/24
	  ◦ DHCP IP address pool: 192.168.50.3 to 192.168.50.253
	  ◦ DHCP failover is enabled
	  ◦ HA is enabled: The virtual IP address is 192.168.50.254

Layer 2 switch	• Connect port G11 to LAN port 4 of the active SAG device • Connect port G12 to LAN port 4 of the standby SAG device
Private networks	Private CIDR block: 192.168.50.0/24

Configuration procedure

Step 1: Purchase SAG devices

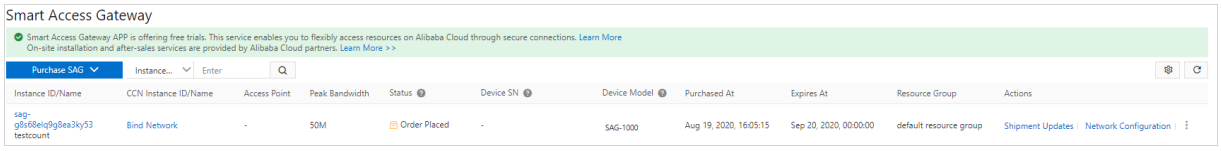
After you purchase SAG devices in the SAG console, Alibaba Cloud delivers the devices to the specified address and creates SAG instances to help you facilitate network management.

> **Note** To use SAG devices outside mainland China, you must purchase SAG devices from third-party vendors. For more information, see Purchase SAG devices.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Purchase SAG**.
3. Select **SAG (CPE)**.
4. Set the following parameters and click **Buy Now**.
   - **Area**: Select the area where the SAG device will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the type of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have SAG devices. **No** is selected in this example.
   - **Edition**: Select the edition of the SAG device. **Standard** is selected in this example.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **2** is selected in this example.
   - **Area**: Select the area where the SAG bandwidth will be used. This area must be the same as that of the SAG devices and cannot be modified.
   - **Instance Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
   - **Peak Bandwidth**: Select the maximum bandwidth for network connections. **50 Mbps** is selected in this example.
   - **Subscription Duration**: Select the duration of the subscription.
5. Confirm the order information and click **Confirm Purchase**.
6. In the **Address** dialog box, enter the recipient address and click **Order Now**.
7. On the **Pay** page, select a payment method and complete the payment.

You can check whether the order has been placed on the Smart Access Gateway page. The SAG devices will be shipped within two business days. If the shipping is overdue, you can submit a ticket to view the shipping status.



Step 2: Activate the SAG devices

After you receive the SAG devices, check whether you have received all the accessories. For more information, see Descriptions of SAG-1000.

1. Log on to the SAG console.
2. In the top navigation bar, select the region where the SAG instance is deployed.

3. On the **Smart Access Gateway** page, find the SAG instance.
4. In the **Actions** column, click **Activate**.
5. In the **Activate** dialog box, click **OK**.
6. Click the instance ID to go to the details page where you can view the serial number of the SAG device.

   > **Note**
   > - The SAG device with a larger serial number is the active device and the other is the standby device. For more information, log on to the SAG console.
   > - If you purchase the SAG devices from a third-party vendor, you must manually associate the SAG devices with the SAG instances. For more information, see Add a device. When you manually associate the SAG devices with the SAG instances, the first associated SAG device is the active device by default.

7. After you activate the SAG devices, you must connect them to your private network based on the following topology:

   For the active SAG device:

   - Use a network cable to connect WAN port 5 of the SAG device to port G1 of the Internet-facing router.
   - Use a network cable to connect LAN port 4 of the SAG device to port G11 of the Layer 2 switch.

   For the standby SAG device:

   - Use a network cable to connect WAN port 5 of the SAG device to port G2 of the Internet-facing router.
   - Use a network cable to connect LAN port 4 of the SAG device to port G12 of the Layer 2 switch.

Step 3: Configure the SAG devices

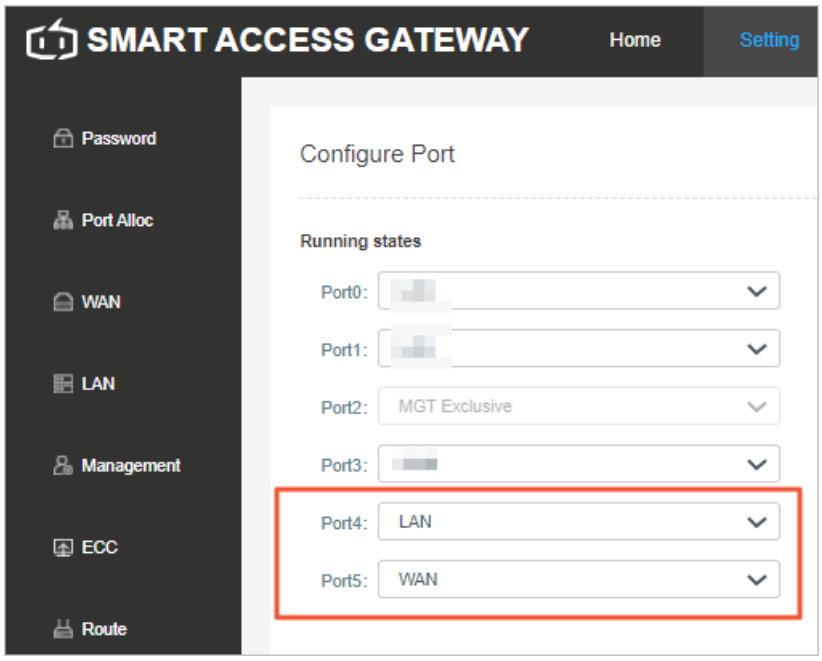
You must log on to the web console to configure the SAG devices. Before you begin, make sure that the devices are started, the 4G networks work as expected, and the devices are connected to Alibaba Cloud.

1. You can use a network cable to connect port 2 of the active SAG device to your computer and log on to the web console. For more information, see Step 1: Configure the local client and Step 2: Set the password.
2. Assign port roles

   > **Note** By default, port 5 is the WAN port and port 4 is the LAN port. If your system uses the default settings, you can skip this step. If the settings are modified, you must perform the following steps to reassign the roles.

   i. In the web console, click **Settings**.
   ii. In the left-side navigation pane, click **Port Alloc**.

iii. On the **Port Alloc** page, find the port and select a role.



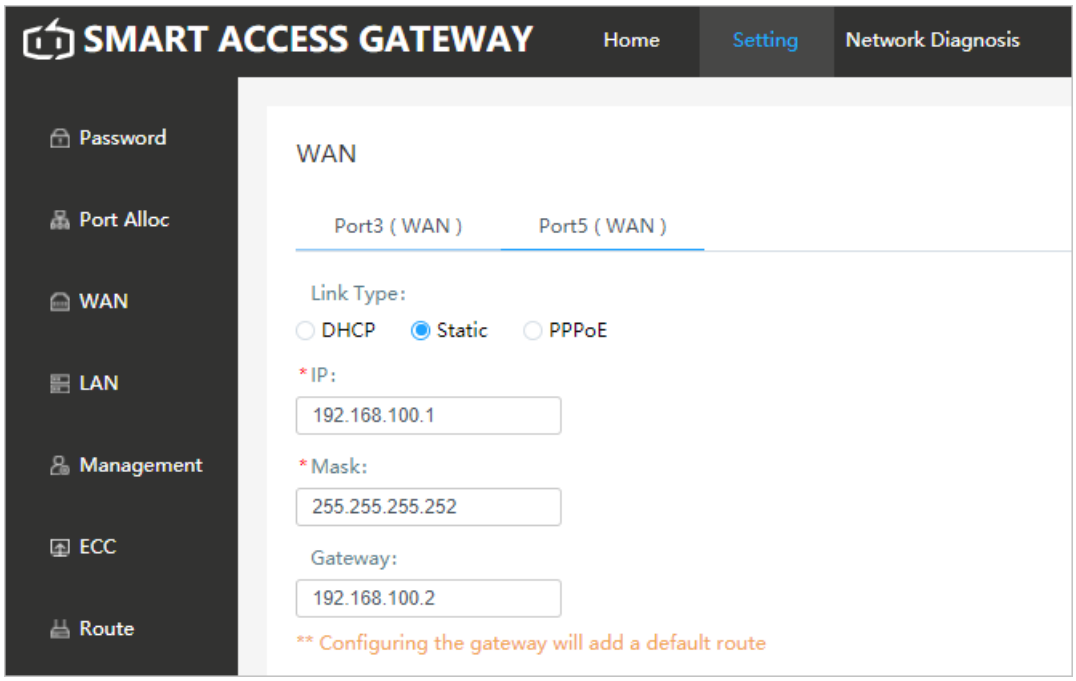
- **Port 5**: Select **WAN**.
- **Port 4**: Select **LAN**.

iv. Click **OK**.

3. Configure the WAN port.

i. In the left-side navigation pane, click **WAN**.

ii. On the **WAN** page, click **Port 5 (WAN)**.



- **Link Type**: Select **Static**.
- **IP**: Enter the IP address of the WAN port. 192.168.100.1 is used in this example.
- **Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
- **Gateway**: Enter the IP address of the gateway. 192.168.100.2 is used in this example.

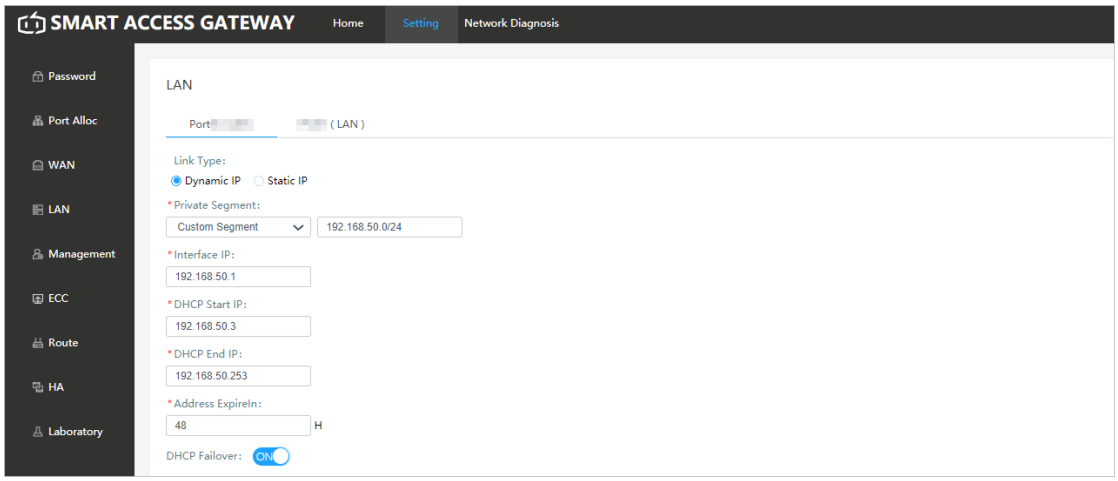
> **Note** After the parameter is set, a default route is added to the SAG device.

iii. Click **OK**.

4. Configure the LAN port.

i. In the left-side navigation pane, click **LAN**.

ii. On the **LAN** page, click **Port 4 (LAN)**.



- **Link Type**: Select **Dynamic IP**.
- **Private Segment**: Select **Custom Segment** and enter 192.168.50.0/24.
- **Interface IP**: Enter the IP address of the LAN port. 192.168.50.1 is used in this example.
- **DHCP Start IP**: 192.168.50.3 is used in this example.
- **DHCP End IP**: 192.168.50.253 is used in this example.
- **Address ExpireIn**: 48 hours.
- **DHCP Failover**: enabled.

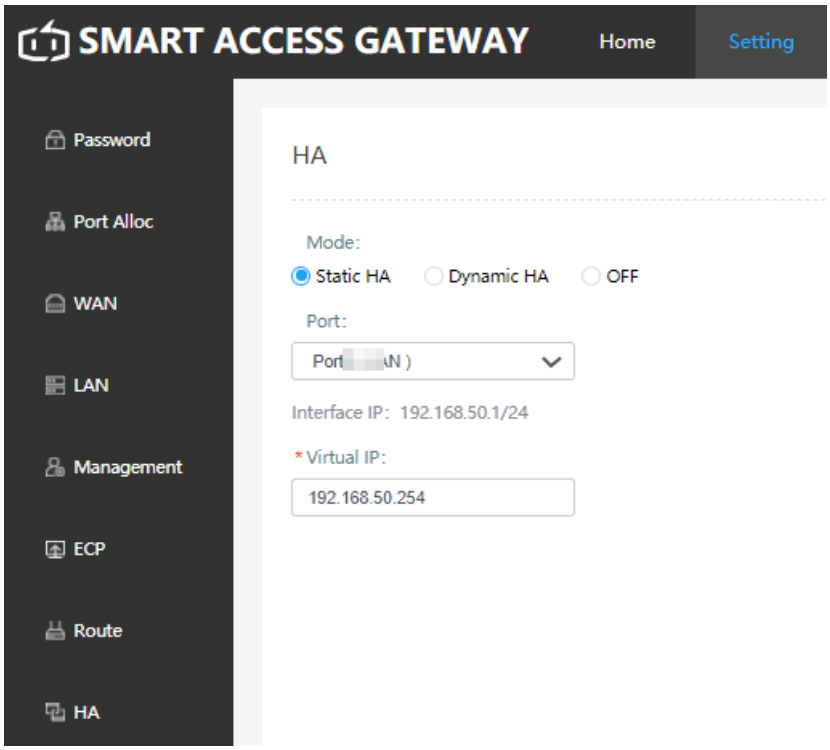
> **Note** To use the DHCP failover feature, you must also enable the HA feature. The HA virtual IP address functions as the IP address of the gateway and is automatically advertised to the client side. After you enable the DHCP failover and HA features for both the active and standby devices, you can switch over to the standby device when the active device is faulty. This enables the availability of your networks.

iii. Click **OK**.

5. Enable the HA feature.

i. In the left-side navigation pane, click **HA**.

ii. On the **HA** page, select **Static HA**.



- **Port**: **Port 4 (LAN)** is used in this example.
- **Virtual IP**: the virtual IP address. 192.168.50.254 is used in this example.

iii. Click **OK**.

6. Configure the standby SAG device.

   Refer to the logon configurations of the active SAG device and configure the standby SAG device based on the following information:

   - Configure WAN port 5:
     - **Link Type**: Select **Static**.
     - **IP**: The IP address of the WAN port. 192.168.200.1 is used in this example.
     - **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
     - **Gateway**: Enter the IP address of the gateway. 192.168.200.2 is used in this example.

       > **Note** After the parameter is set, a default route is added to the SAG device.

   - Configure LAN port 4:
     - **Connection Type**: Select **Static IP**.
     - **Private Segment**: Select **Custom Segment** and enter 192.168.50.0/24.
     - **Interface IP**: the IP address of the LAN port. 192.168.50.2 is used in this example.
     - **DHCP Start IP**: 192.168.50.3 is used in this example.
     - **DHCP End IP**: 192.168.50.253 is used in this example.
     - **Address ExpireIn**: 48 hours.

- **DHCP Failover**: enabled.

- Configure HA: Select **Static HA**.
  - **Port**: **Port 4 (LAN)** is used in this example.
  - **Virtual IP**: the virtual IP address. 192.168.50.254 is used in this example.

Step 4: Advertise routes to Alibaba Cloud

To connect private networks to Alibaba Cloud, you must advertise routes to Alibaba Cloud.

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 page that appears, click the **Network Configuration** tab.
5. In the left-side navigation tree, click **Methods to Synchronize with On-premises Routes**.
6. Select **Static Routing**, click **Add Static Route** to add a CIDR block, and then click **OK**.

   192.168.50.0/24 is used in this example.

Step 5: Set up network connections in the console

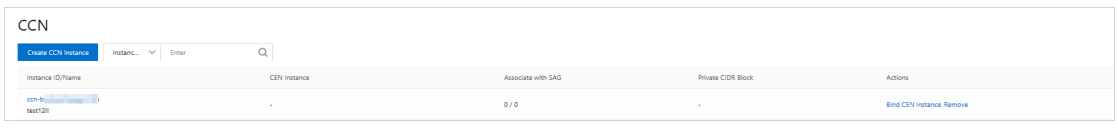
After you complete the preceding steps, you must set up network connections in the cloud.

1. Create a Cloud Connect Network (CCN) instance.
   i. Log on to the SAG console.
   ii. In the top navigation bar, select **Mainland China**.

   The CCN instance and SAG instance must be deployed in the same region.

   iii. In the left-side navigation pane, click **CCN**.
   iv. On the **CCN** page, click **Create CCN Instance**.
   v. In the **Create CCN Instance** pane, specify a name for the CCN instance and click **OK**.

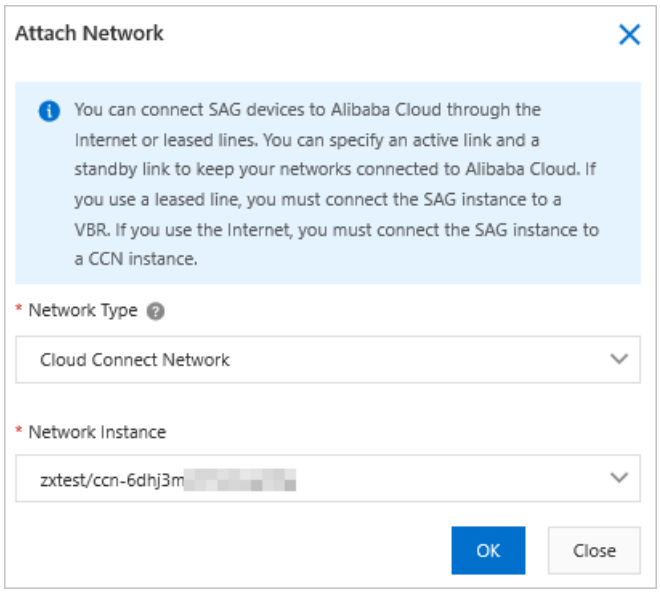
   The name must be 2 to 100 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.



2. Associate the SAG instance with a CCN instance.
   i. In the left-side navigation pane, click **Smart Access Gateway**.
   ii. On the **Smart Access Gateway** page, find the SAG instance and click **Network Configuration** in the **Actions** column.

iii. In the left-side navigation tree, click **Network Instance Details**.

iv. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance you created, and then click **OK**.



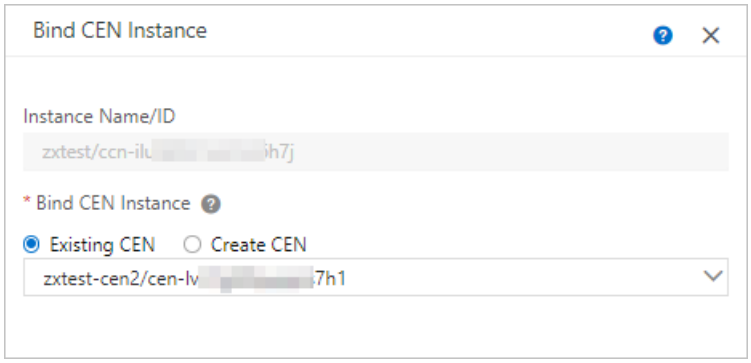
3. Associate the CCN instance with a CEN instance.

   After the CCN instance is associated with the CEN instance, SAG devices associated with the CCN instance can communicate with VPC networks associated with the CEN instance.

   i. In the left-side navigation pane, click **CCN**.

   ii. Find the CCN instance and click **Bind CEN Instance** in the **Actions** column.

   iii. In the **Bind CEN Instance** pane, select **Existing CEN**, select the CCN instance from the drop-down list, and then click **OK**.



4. Create a security group rule.

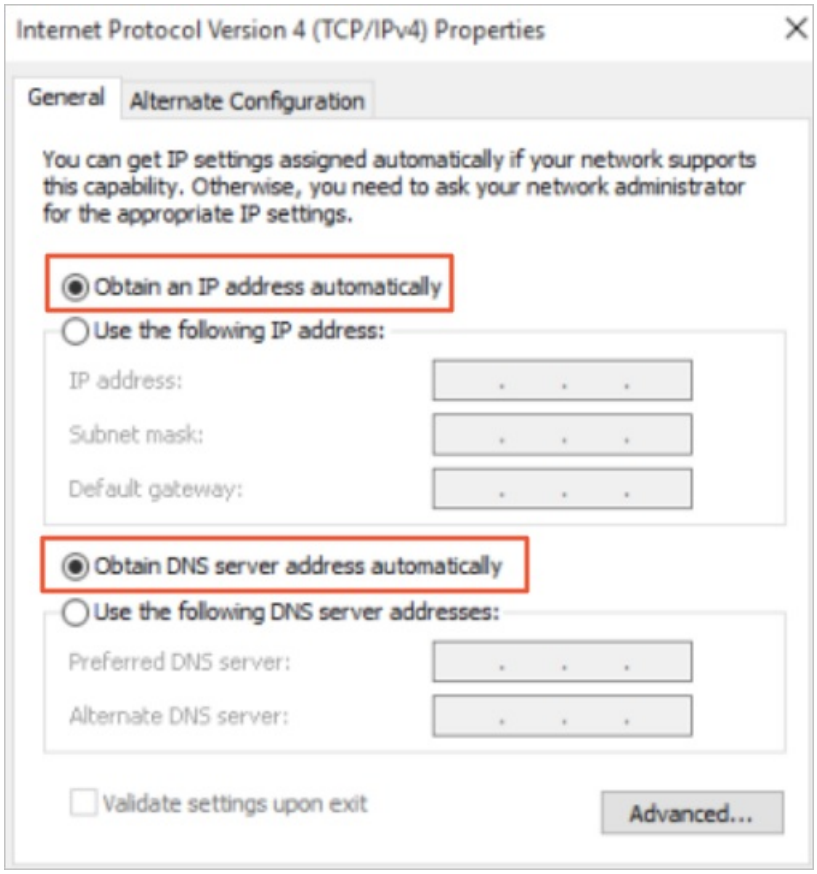
   You must create a security group rule for the Elastic Compute Service (ECS) instance to allow the private CIDR block 192.168.50.0/24 to access resources on the CES instance. For more information, see Add a security group rule.

Step 6: Test the connectivity

After you complete the preceding steps, you can test the connectivity between the VPC network and your private networks.

1. Before you test the connectivity, you must configure the network interface controller (NIC) of your on-premises computer to automatically obtain an IP address. For more information, see the system

manuals of your on-premises computer. The Windows operating system is used in the following example.



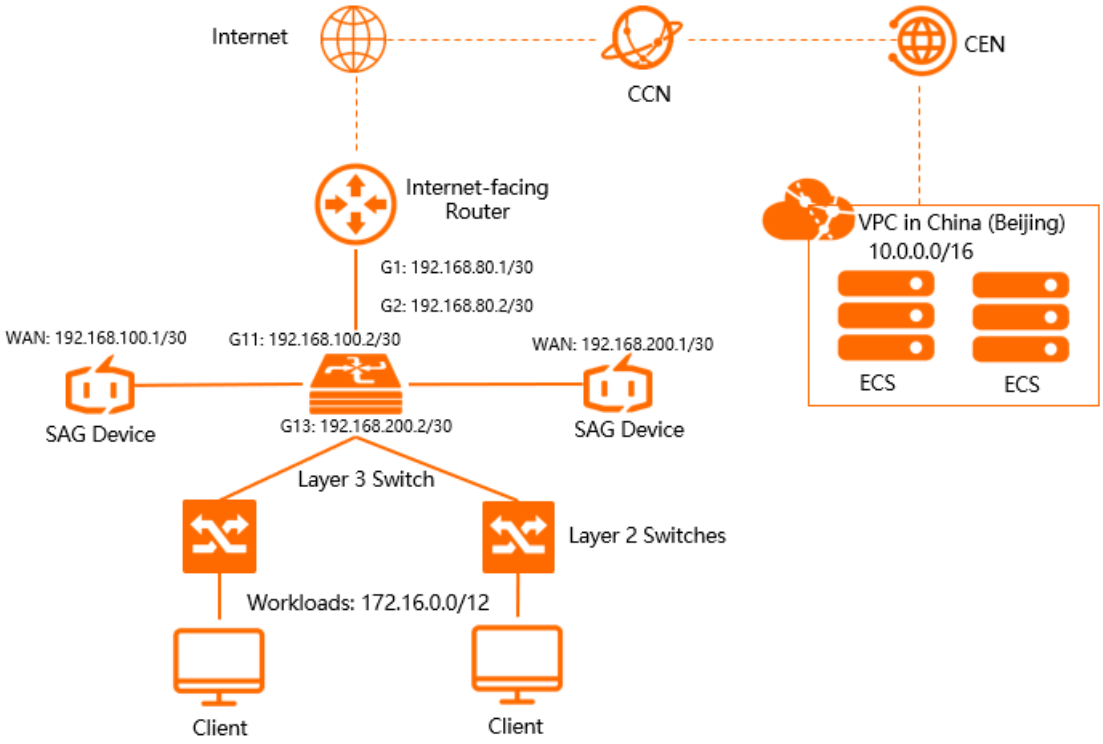
2. Select Automatically obtain an IP address. Then, the SAG device automatically assigns an IP address to your on-premises computer. After the SAG device assigns an IP address to your on-premises computer, you can test the connectivity between the VPC network and your private networks.

8.Deploy two SAG devices in one-arm mode and enable dynamic routing

This topic describes how to deploy two Smart Access Gateway (SAG) devices in one-arm mode and enable Open Shortest Path First (OSPF)-based dynamic routing to connect a private network to Alibaba Cloud.

Context

The following figure shows the topology of the private network. A Layer 3 switch is connected to two Layer 2 switches. On-premises clients and servers are connected to the Layer 2 switches. Two SAG devices are connected to the Layer 3 switch in inline mode to establish network connections between the private network and Alibaba Cloud. When one device is malfunctioning, the other device takes over.



Prerequisites

- A virtual private cloud (VPC) is created in the China (Beijing) region. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC in the China (Beijing) region. For more information, see Create a CEN instance.

Subnetting

Set IP addresses as shown below:

Item	CIDR block
VPC in the China (Beijing) region	10.0.0.0/16
Internet-facing router	192.168.80.1/30
Uplink port of the Layer 3 switch	192.168.80.2/30
SAG Device 1	WAN port (port 5): 192.168.100.1/30. Next hop: 192.168.100.2.
SAG Device 2	WAN port (port 5): 192.168.200.1/30. Next hop: 192.168.200.2.
Layer 3 switch	• Port G11: 192.168.100.2/30 • Port G13: 192.168.200.2/30 • Loopback interface: 192.168.100.3/32
Private network	172.16.0.0/12

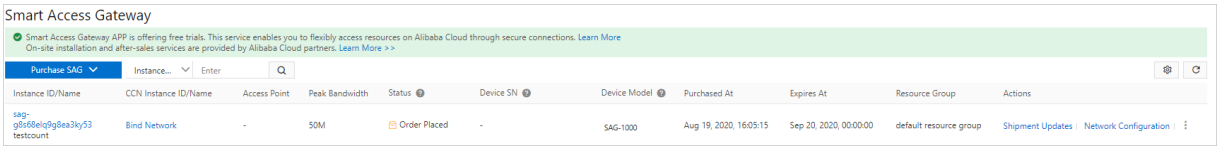
Step 1: Purchase SAG devices

After you purchase SAG devices in the SAG console, Alibaba Cloud delivers the devices to the specified address and creates an SAG instance to help you facilitate network management.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Create SAG** Instance.
3. Set the following parameters and click **Buy Now**:
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the model of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have SAG devices. **No** is selected in this example.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **2** is selected in this example.
   - **Area**: Select the area where the SAG bandwidth will be used. This area must be the same as that of the SAG devices and cannot be modified.
   - **Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter.
   - **Peak Bandwidth**: Specify the maximum bandwidth value. **30Mbps** is selected in this example.
   - **Subscription Duration**: Specify the subscription duration of the bandwidth resources.
4. Confirm the order information and click **Confirm Purchase**.
5. In the **Address** dialog box, enter the recipient address and then click **Order Now**.
6. On the **Pay** page, click **Pay**.

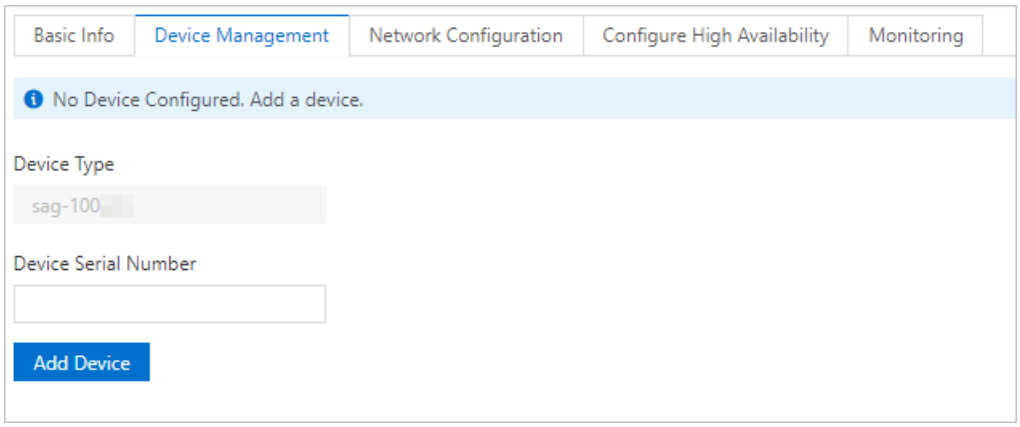
You can check whether the order has been placed on the Smart Access Gateway page. After the order is placed, the package will be shipped within two business days. If the package is not shipped within two business days, submit a ticket to query the shipping status.



Step 2: Activate the SAG devices

After you receive the SAG devices, check whether you have received all the accessories. For more information, see Descriptions of SAG-1000.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, find the SAG instance.
3. In the **Actions** column, click **Activate**.
4. In the **Activate** dialog box, click **OK**.
5. Click the ID of the SAG instance. On the instance details page, click the **Device Management** tab and enter the serial number of the device.



6. Click **Add Device**.
7. Repeat this step to associate the other SAG device with the SAG instance.

Step 3: Connect the SAG devices to your private network

After you activate the SAG devices and associate them with the SAG instance, you must connect the devices to your private network.

Before you begin, make sure that the devices are activated, the 4G networks work as expected, and the devices are connected to Alibaba Cloud. The active device is used in this example. Repeat this step to connect the standby device to your private network.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, find and click the SAG instance ID.
3. On the instance details page, click the **Device Management** tab.
4. In the left-side navigation tree, click **Assign Port Roles**.
5. In the **Assign Port Roles** section, find the port and click **Edit** in the **Actions** column. Assign a role to the port and click **OK**.

   The WAN port (port 5) is used in this example. For more information about ports, see Assign a role to a port.
6. Use a network cable to connect the WAN port (port 5) of the SAG device to port G11 of the Layer 3

switch.

Step 4: Configure ports

After the SAG devices are connected to your private network, you can configure the device ports in the SAG console.

The active device is used in this example. Repeat this step to configure the ports of the standby device.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click the ID of the SAG instance.
3. On the instance details page, click the **Device Management** tab.
4. In the left-side navigation tree, click **Manage WAN Ports**.
5. In the **WAN (Port 5)** section, click **Settings**.
6. In the **Configure WAN (Port 5)** dialog box, set the following parameters and click **OK**.
   - **Connection Type**: Select **Static IP**.
   - **IP Address**: Enter the IP address of the WAN port. 192.168.100.1 is used in this example.
   - **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
   - **Gateway**: Enter the IP address of the gateway. 192.168.100.2 is used in this example.

     Note After the parameter is set, a default route is added to the SAG device.

Step 5: Configure OSPF-based dynamic routing

You can configure OSPF-based dynamic routing for SAG devices in the SAG console.

The active device is used in this example. Repeat this step to configure OSPF-based dynamic routing for the standby device.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click the ID of the SAG instance.
3. On the instance details page, click the **Device Management** tab.
4. In the left-side navigation tree, click **Manage Routes**.
5. In the **OSPF Protocol Settings** section, click **Edit**.
6. In the **Configure OSPF Protocol** dialog box, enter the information about the allocated IP address and click **OK**.

Parameter	Description
Area ID	Set area IDs as shown before: Area ID of the active device: 1. Area ID of the standby device: 1.
Hello Time	Set the hello time to 3 seconds for both devices.
Dead Time	Set the dead time to 10 seconds for both devices.

Parameter	Description
Authentication Type	Select Disable Authentication for both devices.
Router ID	Set router IDs as shown below: Router ID of the active device: 192.168.100.1. Router ID of the standby device: 192.168.200.1.
Area Type	Default value: NSSA.

7. In the **WAN/LAN Dynamic Routing Settings** section, select **Enable OSPF Protocol**.
8. Find **Port 5 (WAN)**, click **Edit** in the **Actions** column, select Enable OSPF, and then click **OK**.

Step 6: Configure the Layer 3 switch and Internet-facing router

The commands used to configure switches vary based on the switch provider. For more information, see the manuals issued by your providers. A switch and router provided by Cisco are used in this example.

- The Layer 3 switch
  - Set the port IP addresses and OSPF parameters.

> **Note** For each SAG device, the network type of ports that use the OSPF protocol must be set to peer-to-peer (P2P). Otherwise, the SAG device cannot calculate routes correctly.

```
interface GigabitEthernet 0/11
 no switchport
 ip ospf network point-to-point           Set the network type to P2P
 ip ospf hello-interval 3
 ip ospf dead-interval 10
 ip address 192.168.100.2 255.255.255.252   The port IP address of the peer switch of D
evice 1

 interface GigabitEthernet 0/13
 no switchport
 ip address 192.168.200.2 255.255.255.252     The port IP address of the peer switch of
Device 2
 ip ospf network point-to-point                Set the network type to P2P
 ip ospf dead-interval 10
 ip ospf hello-interval 3
!
```

- Specify the loopback address and route advertisement information.

  > **Note** OSPF requires a not-so-stubby area (NSSA), automatically generates a default route, and advertises it to SAG.

```
interface Loopback 0
ip address 192.168.100.3 255.255.255.255                    The loopback address of
the switch
!
router ospf 1
 router-id 192.168.100.3                                   The router ID of the switc
h
 network 172.16.0.0 0.15.255.255 area 0                     The CIDR block of the on
-premises server
 network 192.168.100.0 0.0.0.4 area 1                     The CIDR block of the switc
h port connected to Device 1
 network 192.168.100.3 0.0.0.0 area 0                      The loopback address of th
e switch
 network 192.168.200.0 0.0.0.4 area 1                     The CIDR block of the switc
h port connected to Device 2
 area 1 nssa default-information-originate no-summary
!
```

- The Internet-facing router

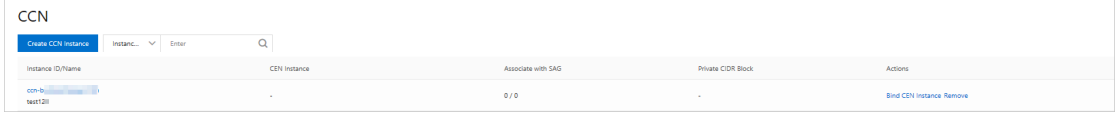
```
Add a static route
ip route 192.168.100.1 255.255.255.252  192.168.80.2 The route to Device 1
ip route 192.168.200.1 255.255.255.252  192.168.80.2 The route to Device 2
```

Step 7: Set up network connections

After you configure the SAG devices, you must set up network connections to connect the private network to Alibaba Cloud.

1. Create a CCN instance.
   i. Log on to the SAG console.
   ii. In the left-side navigation pane, click **CCN**.
   iii. On the **CCN** page, click **Create CCN Instance**.
   iv. In the **Create CCN Instance** pane, specify a name for the CCN instance and click **OK**.

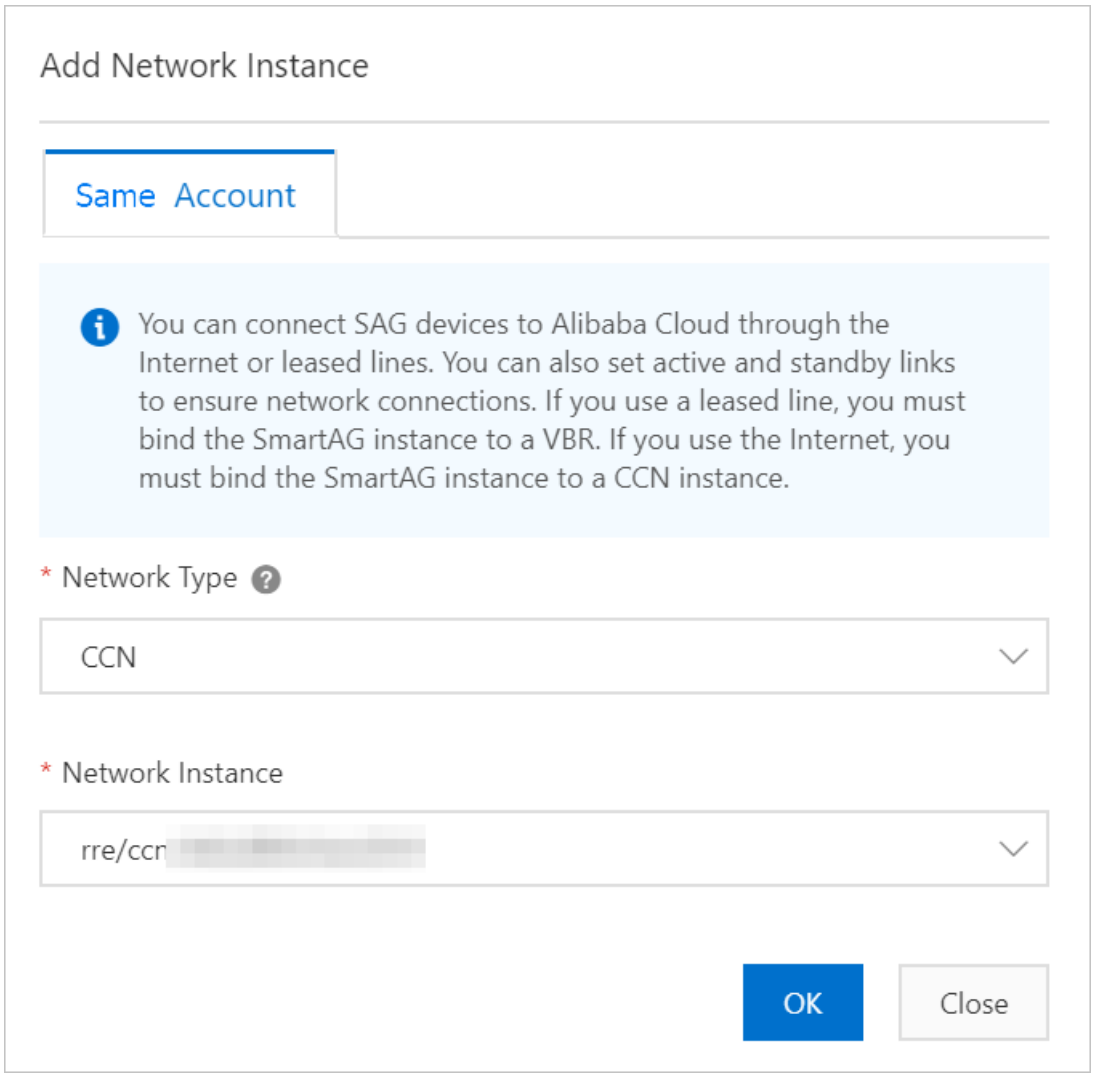
   The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.



2. Set up network connections.
   i. Log on to the SAG console.
   ii. On the **Smart Access Gateway** page, click the ID of the SAG instance or click **Network Configuration** in the **Actions** column.

iii. On the **Method to Synchronize with On-premises Routes** tab, select **Dynamic Routing**.

iv. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance, and then click **OK**.



3. Associate the CCN instance with a Cloud Enterprise Network (CEN) instance.

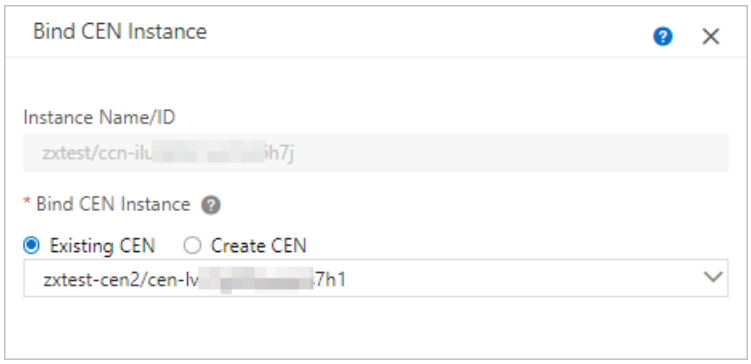
i. Log on to the SAG console.

ii. In the left-side navigation pane, click **CCN**.

iii. Find the CCN instance and click **Bind CEN Instance** in the **Actions** column.

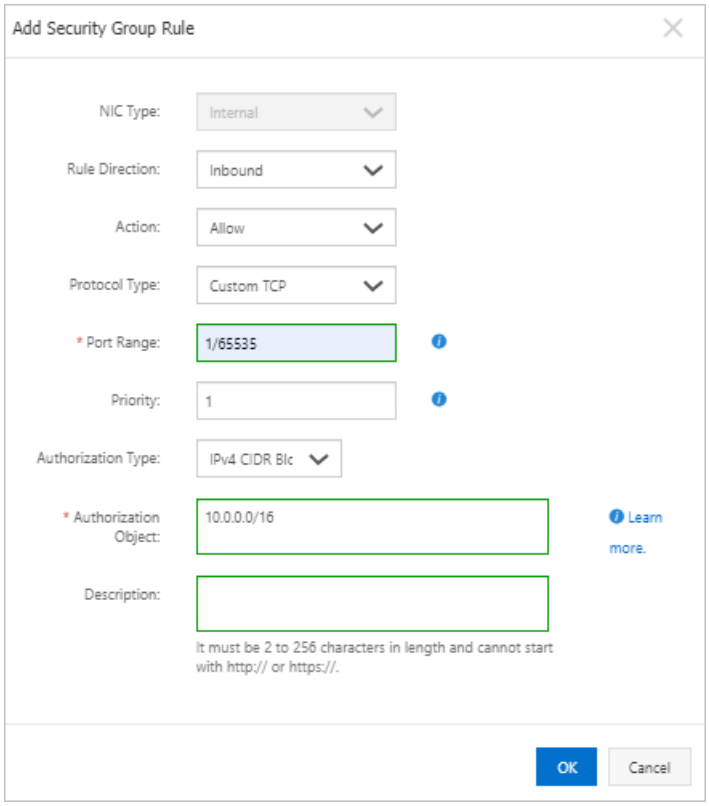
iv. In the **Bind CEN Instance** pane that appears, select the CEN instance and click **OK**.

After the CCN instance is associated with the CEN instance, SAG devices in the CCN can communicate with VPCs associated with the CEN.



4. Configure a security group rule.
   i. Log on to the ECS console.
   ii. In the left-side navigation pane, click **Instance**.
   iii. Find the ECS instance deployed in the VPC and choose **More > Network and Security Group > Configure Security Group**.
   iv. Click **Add Rules** and then click **Add Security Group Rule**.
   v. Create a security group rule that allows access from the private network to the VPC.

   The following figure shows how to configure a security group rule. Set Authorization Object to the CIDR block of the private network.



Step 8: Test the connectivity

After you complete the configurations in the preceding steps, access cloud resources deployed in the VPC from a client in your private network to test the connectivity.

9.Use SAG to set up standby network connections (leased line connected to SAG)

This topic describes how to deploy a Smart Access Gateway (SAG) device to set up standby network connections between an on-premises network and Alibaba Cloud. In this scenario, a leased line provides the active connection. This helps you build a high availability (HA) hybrid cloud.

Prerequisites

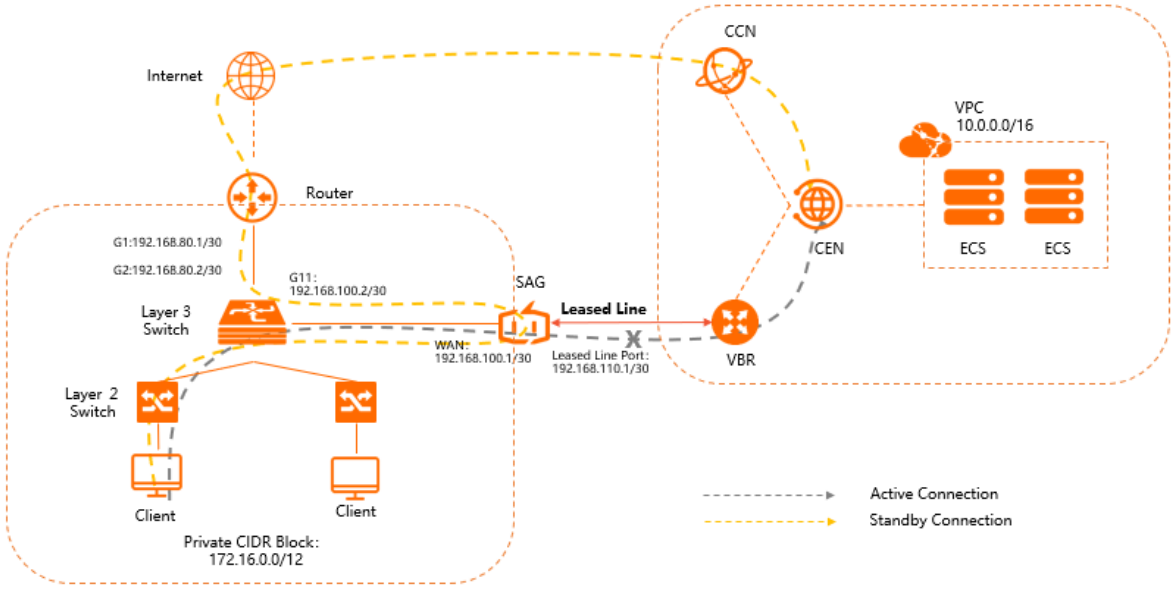
- A virtual private cloud (VPC) is created in the China (Beijing) region. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC in the China (Beijing) region. For more information, see Create a CEN instance.
- A leased line is connected to the on-premises network in the China (Beijing) region and a virtual border router (VBR) is created. For more information, see Create a dedicated connection over an Express Connect circuit or Overview.

Context

The following figure shows the network topology used in this topic. For example, an enterprise has created a VPC in the China (Beijing) region and deployed services in the VPC. To establish HA connections between the on-premises network and cloud resources, the enterprise plans to use an SAG device to provide standby connections, while a leased line provides active connections.

- To avoid changes in the network topology, an SAG-1000 device is deployed in one-arm mode to connect the on-premises network to Alibaba Cloud. Only the SAG-1000 device model supports leased lines.
- The leased line is connected to the leased line port of the SAG device. The SAG device uses the leased line and CCN to connect the on-premises network to Alibaba Cloud. In this scenario, the CCN connection is established over the Internet. When either the leased line connection or the CCN connection is malfunctioning, the other connection takes over.
- The SAG device and VBR use BGP to learn and advertise routes. This facilitates network management and operations and maintenance (O&M).
- The SAG instance is associated with a CCN instance and the VBR. The VBR and CCN instance are associated with the same CEN instance. The SAG device is connected to the VPC through the CEN instance.
- In this example, network traffic is transmitted in the following directions:

  When the SAG device is associated with the CCN instance and VBR, CEN chooses the leased line by default. By default, the CEN instance learns and advertises routes through the leased line. When the leased line is malfunctioning, the CCN instance takes over. Specifically, outbound and inbound traffic are transmitted through the leased line by default. When the leased line is malfunctioning, outbound and inbound traffic are transmitted through the CCN instance.



Configuration procedure

Subnetting

The following table describes the subnetting in this example. We recommend that you plan the subnetting based on your business requirements and ensure that the CIDR blocks do not overlap with each other.

Item	Subnetting
On-premises network	Private CIDR block: 172.16.0.0/12.
	• Port G11 of the Layer 3 switch: 192.168.100.2/30. • Port G2 of the Layer 3 switch: 192.168.80.2/30.
	Port G1 of the Internet-facing router: 192.168.80.1/30.
SAG device	• WAN port (port 5): 192.168.100.1/30. IP address of the gateway: 192.168.100.2. • Leased line port (port 1): 192.168.110.1/30. VLAN ID: 0.
	BGP: • Autonomous system (AS) number: 65435 • Router ID: 192.168.2.2 • Keepalive time: 60 seconds • Hold Time: 180 seconds • BGP-enabled port: leased line port

Item	Subnetting
VBR	• Alibaba Cloud-side IP address: 192.168.110.2/30 • Client-side IP address (Layer 3 switch-side in this example): 192.168.110.1/30 • VLAN: 0
VPC in the China (Beijing) region	VPC CIDR block: 10.0.0.0/16

Step 1: Purchase an SAG device

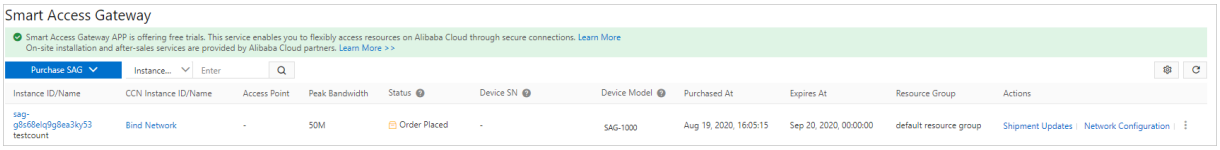
After you place an order in the SAG console, Alibaba Cloud delivers the SAG device to the specified address and creates an SAG instance to facilitate the management of the device.

> **Note** If the area where the SAG device is used is outside mainland China, you must purchase the device from a third-party vendor that is authorized by Alibaba Cloud. For more information, see Purchase SAG devices.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Purchase SAG**.
3. Select **Create SAG (CPE)**.
4. Set the following parameters and click **Buy Now**:
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the model of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have an SAG device. **No** is selected in this example.
   - **Edition**: Select the edition of the SAG device. **Standard** is selected in this example by default.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **1** is selected in this example.
   - **Area**: Select the area where the bandwidth will be used. The area is the same as that of the SAG device and cannot be changed.
   - **Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
   - **Peak Bandwidth**: Specify the maximum bandwidth value. **50 Mbps** is specified in this example.
   - **Subscription Duration**: Specify the subscription duration of the bandwidth resources.
5. Confirm the order information and click **Confirm Purchase**.
6. In the **Shipping Address** dialog box, enter the recipient address and click **Buy Now**.
7. On the **Pay** page, select a payment method and complete the payment.

You can check whether the order has been placed on the Smart Access Gateway page. After the order is placed, it will be shipped within two business days. If your order is not shipped as expected, you can submit a ticket to query the shipping status.



Step 2: Activate the SAG device

After you receive the SAG package, check whether you have received all the items. For more information, see Descriptions of SAG-1000.

1. Log on to the SAG console.
2. In the top menu bar, select the region.
3. On the **Smart Access Gateway** page, find the SAG instance.
4. In the **Actions** column, click **Activate**.
5. In the **Activate** dialog box, click **OK**.
6. After you activate the SAG device, connect it to the on-premises network based on the preceding network topology.
   - Use a network cable to connect the WAN port (port 5) of the SAG device to port G11 of the Layer 3 switch.
   - Connect the Express Connect leased line to the leased line port (port 1) of the SAG device.
7. (Optional)If the SAG device is purchased from a third-party vendor, you must manually associate the SAG device with the SAG instance. For more information, see Add a device.

Step 3: Configure the SAG device

After the SAG devices are connected to your on-premises network, you can configure the device ports in the SAG console.

Before you begin, make sure that the SAG device is started, the 4G network works as expected, and the SAG device is connected to Alibaba Cloud.

1. Log on to the SAG console.
2. Assign port roles.

   By default, port 5 functions as the WAN port. You must assign a leased line port to the SAG device. For more information, see Assign a role to a port. In this example, port 1 is assigned as the leased line port.
3. Configure the WAN port.
   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.
   v. In the left-side navigation tree, click **Manage WAN Ports**.
   vi. In the **WAN (Port 5)** section, click **Edit**.

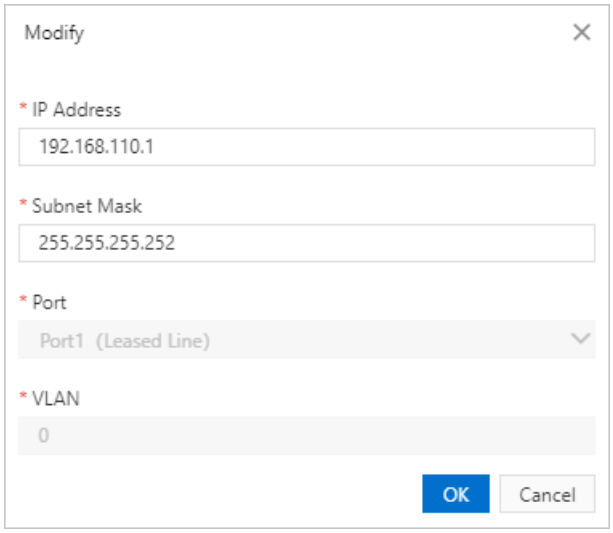
vii. In the **Configure WAN (Port 5)** dialog box, set the following parameters and click **OK**.

- **Link Type**: Select **Static**.
- **IP**: The IP address of the WAN port. 192.168.100.1 is used in this example.
- **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
- **Gateway**: Enter the IP address of the gateway. 192.168.100.2 is used in this example.

> **Note** After the parameter is set, a default route is added to the SAG device.

4. Configure the leased line port
   i. In the left-side navigation tree, click **Manage WAN Ports**.
   ii. On the **Manage Leased Lines** page. Click **Port1 (Leased Line)**.
   iii. On the page that appears, click **Edit**.

iv. In the **Modify** dialog box, set the following parameters and click **OK**. For more information about leased lines, see Configure a leased line port.



- **IP**: Enter the IP address of the leased line port. 192.168.110.1 is used in this example.
- **Subnet Mask**: Enter the subnet mask of the IP address of the leased line port. 255.255.255.252 is used in this example.
- **Port**: **Port1 (Leased Line)** is selected by default.
- **VLAN**: Specify the VLAN number of the leased line port. 0 is used in this example. 0 indicates that the leased line port functions as a physical port instead of a virtual port.

> **Note**
>
> The leased line port can work in one of the following modes:
>
> - Physical mode: The leased line port functions as an independent port and the VLAN number is 0.
> - Virtual mode: The leased line port functions as multiple sub ports. Each VLAN number indicates a sub port. If the VLAN number is not 0, the virtual mode is enabled. Valid values of the VLAN number: 1 to 4094.
>
> The VLAN number of the leased line port must be the same as that of the leased line peer.

5. Configure BGP.
   i. In the left-side navigation tree, click **Manage WAN Ports**.
   ii. In the **BGP Protocol Settings** section, click **Edit**.
   iii. In the **Configure BGP Route Protocol** dialog box, set the following parameters and click **OK**.
   - **Local AS**: 65435 is used in this example.
   - **Router ID**: 192.168.2.2 is used in this example.
   - **Hold Time**: 180 is used in this example.
   - **Keep Alive**: 60 is used in this example.
6. Enable BGP for the WAN port.

> **Note** You can enable BGP for the leased line port of an SAG device and configure BGP only in the SAG console, instead of the web console.

i. In the **Dynamic Routing Settings** section, select **Enable BGP Protocol**.

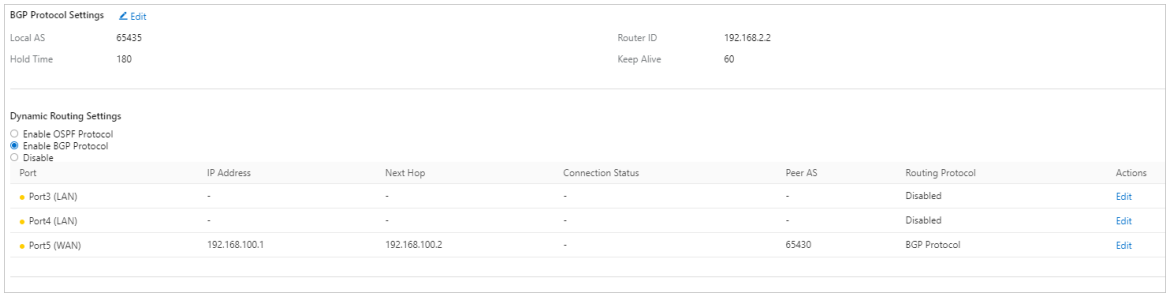
ii. In the **Change Routing Protocol** message, click **OK**.

iii. Find Port1 (Leased Line) in the **Leased Line Dynamic Routing Settings** section, and click **Edit** in the **Actions** column.

iv. In the **Modify BGP Dynamic Routing Settings** dialog box, select **Enable BGP**, set the Peer IP and Peer AS, and then click **OK**.

Set the Peer IP and Peer AS to the IP address of port G11 and the BGP AS number of the peer switch.

- **Peer AS**: 45104 is used in this example.
- **Peer IP**: 192.168.110.2 is used in this example.



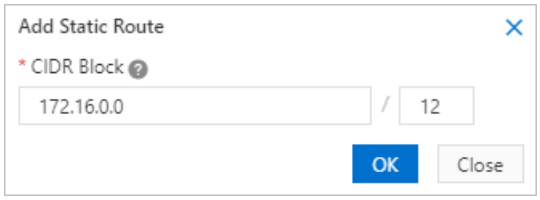
7. Advertise routes to Alibaba Cloud

i. On the SAG instance details page, click the **Network Configuration** tab.

ii. In the left-side navigation tree, click **Methods to Synchronize with On-premises Routes**.

iii. Select **Static Routing**, click **Add Static Route**, and then click **OK**.

Enter the CIDR block used to route network traffic from Alibaba Cloud to the on-premises network. 172.16.0.0/12 is used in this example.



Step 4: Configure the VBR

You must configure the VBR in the Express Connect console to establish the BGP peer relationship between the VBR and the SAG device.

1. Create a BGP group.

i. Log on to the Express Connect console.

ii. In the top menu bar, select the region.

iii. In the left-side navigation pane, choose **Virtual Border Routers (VBRs) > Virtual Border Routers (VBRs)**.

iv. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR.

v. On the details page, click the **BGP Groups** tab.

vi. On the **BGP Groups** tab, click **Create BGP Group** and set the following parameters:

- **Name**: Enter a name for the BGP group. test is used in this example.
- **Peer ASN**: Enter the AS number of the SAG device. 65435 is used in this example.
- **BGP Key**: Enter the key of the BGP group. This parameter is not set in this example.
- **Description**: Enter the description of the BGP group. SAGtest is used in this example.

vii. Click **OK**.

2. Configure the BGP neighbor.

i. On the VBR details page, click the **BGP Peers** tab.

ii. On the **BGP Peers** tab, click **Create BGP Peer**.

iii. In the **Create BGP Peer** dialog box, set the following parameters and click **OK**.

- **BGP Group**: Specify the BGP group to which you want to add the VBR and SAG device. The BGP group test is used in this example.
- **BGP peer IP address**: Enter the IP address of the BGP peer. The IP address of the leased line port of the SAG device. 192.168.110.1 is used in this example.

Step 5: Configure the switch and router

In this step, you must configure the peer switch and Internet-facing router for the SAG device. Switches and routers used in this example may be different from yours. For more information, see the manuals issued by your providers.

1. Configure routes for the Layer 3 switch.

```
interface GigabitEthernet 0/11
no switchport
ip address 192.168.100.2 255.255.255.252      #The IP address of the peer switch of the SAG device
ip route 10.0.0.0 255.255.0.0 192.168.100.1  #The route to the VPC in the China (Beijing) region
ip route 0.0.0.0 0.0.0.0 192.168.80.1        #The route to the Internet
```

2. Configure routes for the Internet-facing router.

```
ip route 192.168.100.0 255.255.255.252 192.168.80.2 #The route to the SAG device
```

Step 6: Set up network connections

After you configure the SAG device, you must set up network connections to connect the on-premises network to Alibaba Cloud.

1. Create a CCN instance.

i. Log on to the SAG console.

ii. In the top menu bar, select **Mainland China**.

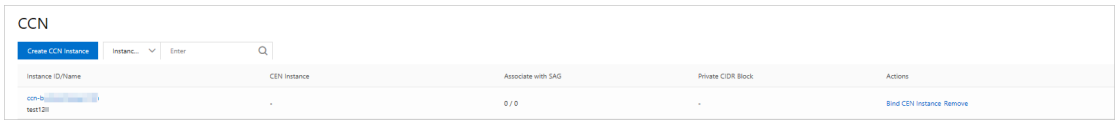
The CCN instance and SAG instance must be deployed in the same region.

iii. In the left-side navigation pane, click **CCN**.

iv. On the **CCN** page, click **Create CCN Instance**.

v. In the **Create CCN Instance** pane, specify a name for the CCN instance and click **OK**.

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



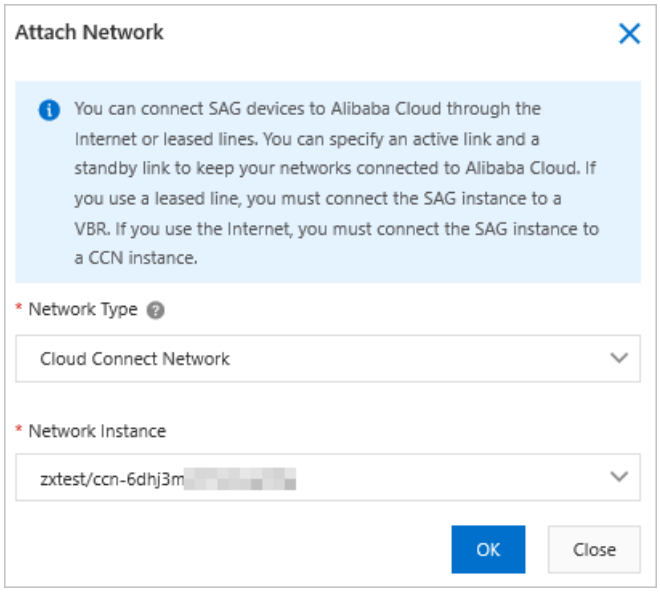
2. Associate the SAG instance with a CCN instance.

i. In the left-side navigation pane, click **Smart Access Gateway**.

ii. On the **Smart Access Gateway** page, find the SAG instance and click **Network Configuration** in the **Actions** column.

iii. In the left-side navigation tree, click **Network Instance Details**.

iv. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance you created, and then click **OK**.



v. Repeat the preceding steps to associate the VBR with the SAG instance. For more information, see Attach a network instance.

If the SAG instance is associated with the CCN instance and the VBR, the on-premises network is connected to the Alibaba Cloud through the leased line by default. When the leased line is malfunctioning, the on-premises network is connected to Alibaba Cloud through CCN. In this case, the connection is encrypted and established over the Internet.

3. Attach the CCN instance and VBR to the CEN instance. For more information, see Attach a network instance.

Then, the on-premises network that is connected to the SAG device can communicate with the VPC that is attached to the CEN instance.

> **Note** If the on-premises network, VBR, and VPC are not in the same region, you must purchase a bandwidth plan for the CEN instance and set cross-region bandwidth. This way, the on-premises network, VBR, and VPC can communicate with each other. For more information, see Use a bandwidth plan and Manage bandwidth for cross-region connections.

4. Create a security group rule.

   You must create a security group rule for the ECS instance in the VPC to allow the private CIDR block 172.16.0.0/12 to access resources deployed on the ECS instance. For more information, see Add a security group rule.

Step 7: Test the connectivity

1. After you complete the preceding steps, you can log on to the CEN console and view the route to the on-premises network from the VPC. For more information, see View CEN routes in the CEN console.
2. You can use the on-premises client to access the cloud resources in the connected VPC to test the connectivity.

10.Use SAG to set up standby network connections (leased line connected to Layer 3 switch)

This topic describes how to deploy a Smart Access Gateway (SAG) device to set up standby network connections between an on-premises network and Alibaba Cloud. In this scenario, a leased line provides the active connection. This helps you build a high availability (HA) hybrid cloud.

Prerequisites

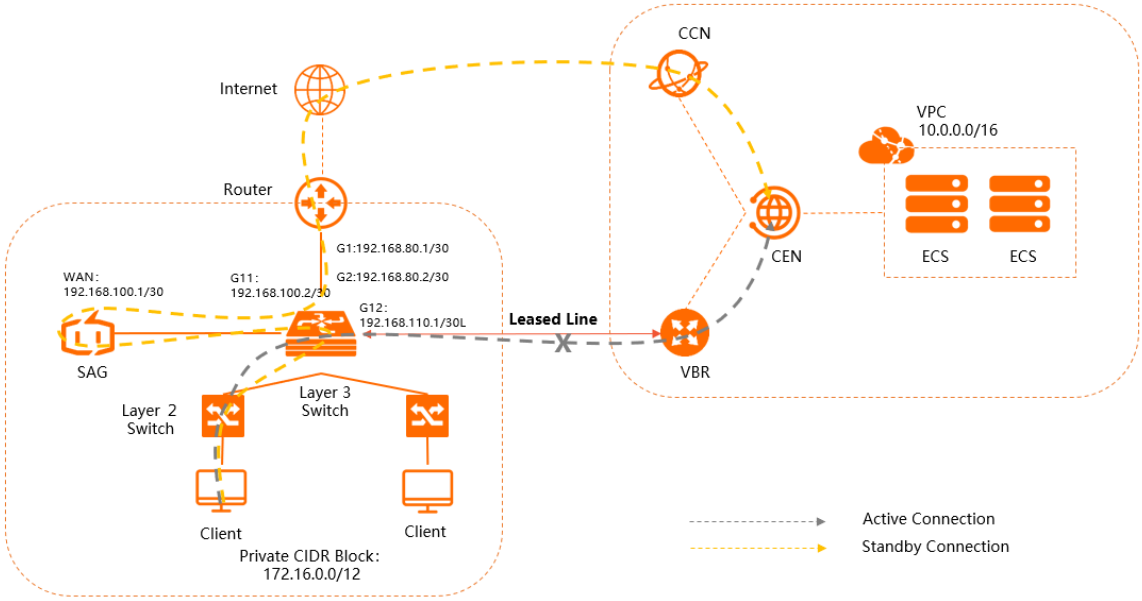
- A virtual private cloud (VPC) is created in the China (Beijing) region. For more information, see Create and manage a VPC.
- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC in the China (Beijing) region. For more information, see Create a CEN instance.
- A leased line is connected to the on-premises network in the China (Beijing) region and a virtual border router (VBR) is created. For more information, see Create a dedicated connection over an Express Connect circuit or Overview.

Context

The following figure shows the network topology used in this topic. For example, an enterprise has deployed services in the VPC in the China (Beijing) region and a leased line is connected to the on-premises network. To establish HA connections between the on-premises network and cloud resources, the enterprise plans to use an SAG device to provide standby connections, while a leased line provides active connections.

- To avoid changes in network topology, an SAG-1000 device is deployed in one-arm mode to connect the on-premises network to Alibaba Cloud.
- The on-premises network, SAG-1000 device, and VBR use BGP to learn routes. This facilitates network management and operations and maintenance (O&M).
- The SAG instance is associated with a Cloud Connect Network (CCN) instance and the VBR. The VBR and CCN instance are associated with the same CEN instance. The SAG device is connected to the VPC through the CEN instance.
- In this example, network traffic is transmitted in the following directions:

  When the SAG device is associated with the CCN instance and VBR, CEN chooses the leased line by default. By default, the CEN instance learns and advertises routes through the leased line. When the leased line is malfunctioning, the CCN instance takes over. Specifically, outbound and inbound traffic are transmitted through the leased line by default. When the leased line is malfunctioning, outbound and inbound traffic are transmitted through the CCN instance.



Subnetting

The following table describes the subnetting in this example. We recommend that you plan the subnetting based on your business requirements and ensure that the CIDR blocks do not overlap with each other.

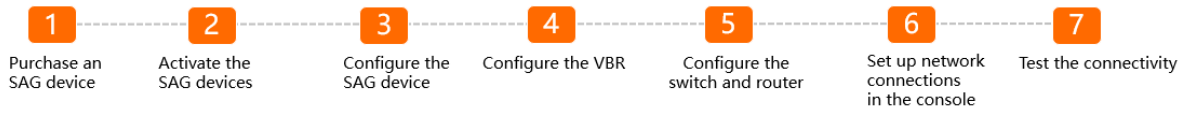
Item	Subnetting
On-premises network	Private CIDR block: 172.16.0.0/12

	• Port G11 of the Layer 3 switch: 192.168.100.2/30
	• Port G12 of the Layer 3 switch: 192.168.110.1/30
	• Port G2 of the Layer 3 switch: 192.168.80.2/30
	• BGP for the Layer 3 switch:
	  ○ Autonomous system (AS) number: 65430
	  ○ Router ID: 192.168.1.1

	Port G1 of the Internet-facing router: 192.168.80.1/30.
SAG device	WAN port (port 5): 192.168.100.1/30. IP address of the gateway: 192.168.100.2.
	BGP: • AS number: 65435 • Router ID: 192.168.2.2 • Keep Alive: 60 seconds • Hold Time: 180 seconds • BGP-enabled port: WAN port

Item	Subnetting
VBR	• Alibaba Cloud-side IP address: 192.168.110.2/30 • Client-side IP address (Layer 3 switch-side in this example): 192.168.110.1/30 • VLAN: 0
VPC in the China (Beijing) region	VPC CIDR block: 10.0.0.0/16

Configuration procedure



Step 1: Purchase an SAG device

After you place an order in the SAG console, Alibaba Cloud delivers the SAG device to the specified address and creates an SAG instance to facilitate the management of the device.

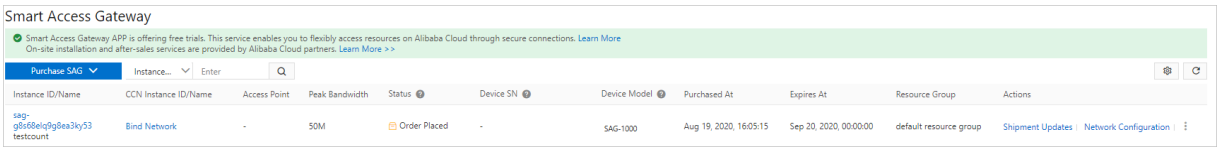
> **Note** If the area where the SAG device is used is outside mainland China, you must purchase the device from a third-party vendor that is authorized by Alibaba Cloud. For more information, see Purchase SAG devices.

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click **Purchase SAG**.
3. Select **Create SAG (CPE)**.
4. Set the following parameters and click **Buy Now**:
   - **Area**: Select the area where the SAG devices will be deployed. **Mainland China** is selected in this example.
   - **Device Spec**: Select the model of the SAG device. **SAG-1000** is selected in this example.
   - **Have SAG Devices Already**: Select whether you already have an SAG device. **No** is selected in this example.
   - **Edition**: Select the edition of the SAG device. **Standard** is selected in this example by default.
   - **Quantity**: Select the number of SAG devices that you want to purchase. **1** is selected in this example.
   - **Area**: Select the area where the bandwidth will be used. The area is the same as that of the SAG device and cannot be changed.
   - **Name**: Specify a name for the SAG instance.

     The name must be 2 to 128 characters in length, and can contain digits, periods (.), hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
   - **Peak Bandwidth**: Specify the maximum bandwidth value. **50 Mbps** is specified in this example.
   - **Subscription Duration**: Specify the subscription duration of the bandwidth resources.
5. Confirm the order information and click **Confirm Purchase**.

6. In the **Shipping Address** dialog box, enter the recipient address and click **Buy Now**.
7. On the **Pay** page, select a payment method and complete the payment.

You can check whether the order has been placed on the Smart Access Gateway page. After the order is placed, it will be shipped within two business days. If your order is not shipped as expected, you can submit a ticket to query the shipping status.



Step 2: Activate the SAG devices

After you receive the SAG device, check whether you have received all the accessories. For more information, see Descriptions of SAG-1000.

1. Log on to the SAG console.
2. In the top navigation bar, select the area of the SAG device.
3. On the **Smart Access Gateway** page, find the SAG instance created for the SAG device.
4. In the **Actions** column, click **Activate**.
5. In the **Activate** dialog box, click **OK**.
6. After the SAG device is activated, connect it to the private network based on the preceding network topology.

   Use a network cable to connect the WAN port (port 5) of the SAG device to port G11 of the Layer 3 switch.
7. (Optional)If the SAG device was purchased from a third-party vendor, you must manually associate the SAG device with the SAG instance. For more information, see Add a device.

Step 3: Configure the SAG device

After the SAG device is connected to the on-premises network, you must configure the device in the SAG console.

Before you begin, make sure that the SAG device is started, the 4G network works as expected, and the SAG device is connected to Alibaba Cloud.

1. Log on to the SAG console.
2. Configure the WAN port.
   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.
   v. In the left-side navigation tree, click **Manage WAN Ports**.
   vi. In the **WAN (Port 5)** section, click **Edit**.

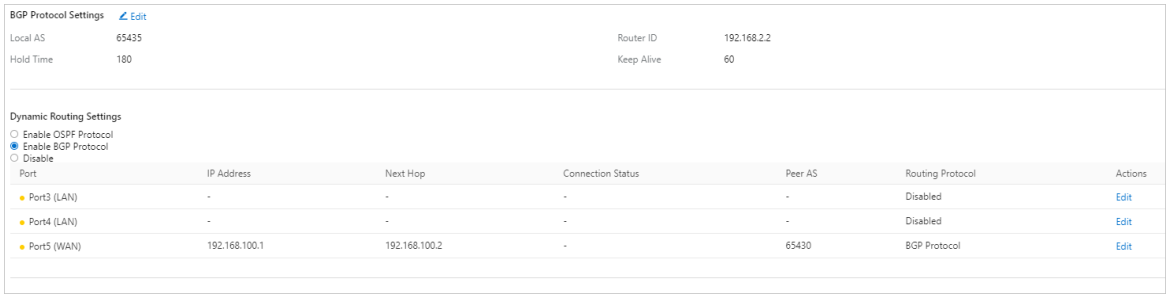
vii. In the **Configure WAN (Port 5)** dialog box, set the following parameters and click **OK**.

- **Link Type**: Select **Static**.
- **IP**: Enter the IP address of the WAN port. 192.168.100.1 is used in this example.
- **Subnet Mask**: Enter the subnet mask of the WAN port IP address. 255.255.255.252 is used in this example.
- **Gateway**: Enter the IP address of the gateway. 192.168.100.2 is used in this example.

> **Note** After the parameter is set, a default route is added to the SAG device.

3. Configure BGP.
   i. In the left-side navigation tree, click **Manage Routes**.
   ii. In the **BGP Protocol Settings** section, click **Edit**.
   iii. In the **Configure BGP Route Protocol** dialog box, set the following parameters and click **OK**.
   - **Local AS**: 65435 is used in this example.
   - **Router ID**: 192.168.2.2 is used in this example.
   - **Hold Time**: 180 is used in this example.
   - **Keep Alive**: 60 is used in this example.
4. Enable BGP for the WAN port.
   i. In the **Dynamic Routing Settings** section, select **Enable BGP Protocol**.
   ii. In the **Change Routing Protocol** message, click **OK**.
   iii. Find Port5 (WAN) in the Dynamic Routing Settings section, and click **Edit** in the **Actions** column.
   iv. In the **Modify BGP Dynamic Routing Settings** dialog box, select **Enable BGP**, set the Peer IP and Peer AS, and then click **OK**.

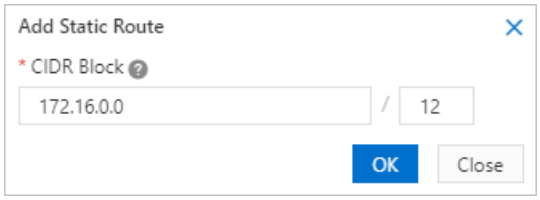
   Set the Peer IP and Peer AS to the IP address of port G11 and the BGP AS number of the peer switch.
   - **Peer AS**: 65430 is used in this example.
   - **Peer IP**: 192.168.100.2 is used in this example.



5. Advertise routes to Alibaba Cloud.
   i. On the instance details page, click the **Network Configuration** tab.
   ii. In the left-side navigation tree, click **Methods to Synchronize with On-premises Routes**.

iii. Select **Static Routing**, click **Add Static Route**, and then click **OK**.

Enter the CIDR block used to route network traffic from Alibaba Cloud to the on-premises network. 172.16.0.0/12 is used in this example.



Step 4: Configure the VBR

You must configure the VBR in the Express Connect console to establish the BGP peer relationship between the VBR and the Layer 3 switch.

1. Create a BGP group.
   i. Log on to the Express Connect console.
   ii. In the top menu bar, select the region.
   iii. In the left-side navigation pane, choose **Virtual Border Routers (VBRs) > Virtual Border Routers (VBRs)**.
   iv. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR.
   v. On the details page, click the **BGP Groups** tab.
   vi. On the **BGP Groups** tab, click **Create BGP Group** and set the following parameters:
      - **Name**: Enter a name for the BGP group. test is used in this example.
      - **Peer ASN**: Enter the AS number of the Layer 3 switch. 65430 is used in this example.
      - **BGP Key**: Enter the key of the BGP group. The parameter is not set in this example.
      - **Description**: Enter the description of the BGP group. SAGtest is used in this example.
   vii. Click **OK**.
2. Configure the BGP neighbor.
   i. On the VBR details page, click the **BGP Peers** tab.
   ii. On the **BGP Peers** tab, click **Create BGP Peer**.
   iii. In the **Create BGP Peer** dialog box, set the following parameters and click **OK**.
      - **BGP Group**: Specify the BGP group to which you want to add the VBR and Layer 3 switch. The newly created BGP group is used in this example.
      - **BGP peer IP address**: Enter the IP address of the BGP peer. 192.168.110.1 is used in this example, which is the IP address of port G12 of the Layer 3 switch.

Step 5: Configure the switch and router

You must configure the peer Layer 3 switch and Internet-facing router for the SAG device. The switch and router used in this example may be different from yours. For more information, see the manuals issued by your providers.

1. Configure routes for the Layer 3 switch.

```
interface GigabitEthernet 0/11
no switchport
ip address 192.168.100.2 255.255.255.252      #The IP address of the peer switch of the
SAG device
interface GigabitEthernet 0/12
no switchport
ip address 192.168.110.1 255.255.255.252     #The IP address of the peer switch of the
VBR
router bgp 65430
bgp router-id 192.168.1.1
network 172.16.0.0 mask 255.240.0.0          #Advertise the private CIDR block of the o
n-premises network
neighbor 192.168.100.1 remote-as 65435       #Establish the neighbor relationship with
the SAG device
neighbor 192.168.100.1 timers 60 180         #Set the keepalive time interval and hold
time for BGP
neighbor 192.168.110.2 remote-as 45104       #Establish the neighbor relationship with
the VBR
exit
```

Note In this example, the switch is configured as shown in the preceding content. Configure routes and advertise CIDR blocks based on your actual needs.

For example, if you have multiple Layer 3 switches in your on-premises network and the switches learn the on-premises CIDR blocks through OSPF, you must redistribute the OSPF and BGP routes in the Layer 3 switch that is connected to the SAG device. This way, all the Layer 3 switches in your on-premises network can learn the CIDR block of the VPC through OSPF, and the VBR can learn the private CIDR block of your on-premises network. For more information about the commands, see the manuals issued by your provider.

2. Configure routes for the Internet-facing router.

```
ip route 192.168.100.0 255.255.255.252 192.168.80.2 #The route to the SAG device
```

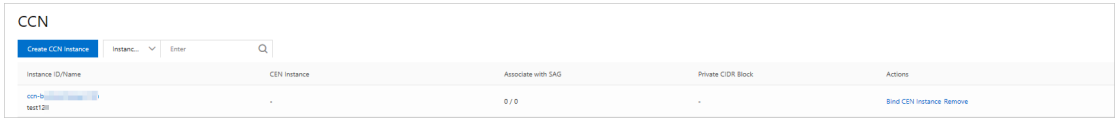
Step 6: Set up network connections in the console

After you configure the SAG device, you must set up network connections to connect the private network to Alibaba Cloud.

1. Create a Cloud Connect Network (CCN) instance.
   i. Log on to the SAG console.
   ii. In the top navigation bar, select **Mainland China**.
   The CCN instance and SAG instance must be deployed in the same region.
   iii. In the left-side navigation pane, click **CCN**.
   iv. On the **CCN** page, click **Create CCN Instance**.

v. In the **Create CCN Instance** pane, specify a name for the CCN instance and click **OK**.

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



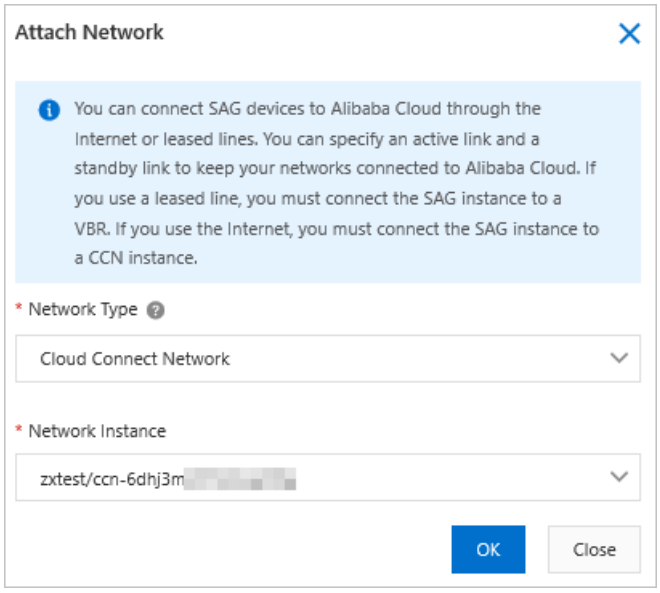
2. Associate the SAG instance with a CCN instance.

i. In the left-side navigation pane, click **Smart Access Gateway**.

ii. On the **Smart Access Gateway** page, find the SAG instance and click **Network Configuration** in the **Actions** column.

iii. In the left-side navigation tree, click **Network Instance Details**.

iv. On the **Network Instance Details** tab, click **Attach Network**, select the CCN instance you created, and then click **OK**.



v. Repeat the preceding steps to associate the VBR with the SAG instance. For more information, see Attach a network instance.

If the SAG instance is associated with the CCN instance and the VBR, the on-premises network is connected to the Alibaba Cloud through the leased line by default. When the leased line is malfunctioning, the on-premises network is connected to Alibaba Cloud through CCN. In this case, the connection is established over the Internet.

3. Attach the CCN instance and VBR to the CEN instance. For more information, see Attach a network instance.

Then, the on-premises network can communicate with the VPC that is attached to the CEN instance.

> **Note** If the on-premises network, VBR, and VPC are not in the same region, you must purchase a bandwidth plan for the CEN instance and set cross-region bandwidth. This way, the on-premises network, VBR, and VPC can communicate with each other. For more information, see Use a bandwidth plan and Manage bandwidth for cross-region connections.

4. Create a security group rule.

   You must create a security group rule for the ECS instance in the VPC to allow the private CIDR block 172.16.0.0/12 to access resources deployed on the ECS instance. For more information, see Add a security group rule.

Step 7: Test the connectivity

1. After you complete the preceding steps, you can disable the leased line port on your Layer 3 switch and check whether the routes destined for the VPC from the switch are changed. When the leased line is malfunctioning, the destination of the next hop changes from the VPC to the SAG device. For more information about commands used to view routes, see the manuals issued by your provider.
2. You can use the on-premises client to access the cloud resources in the connected VPC to test the connectivity.

11.Connect private networks outside the Chinese mainland to Alibaba Cloud

This topic describes how to use Smart Access Gateway (SAG) to connect an office outside the Chinese mainland to Alibaba Cloud.

Background information

A company has an office in Singapore and the company wants to connect the clients in the office to Alibaba Cloud, as shown in the following figure.

The framework in the Singapore region

The following table describes how network resources are allocated in this example.

Resources	Description	Capacity
SAG devices	SAG-100WM	1
SAG bandwidth	In the Singapore (Singapore) region	2 Mbps
Cloud Enterprise Network (CEN) instances	Default edition	1
Cloud Connect Network (CCN) instances	In the Singapore (Singapore) region	1
Virtual private clouds (VPCs)	In the Singapore (Singapore) region	1
Elastic Compute Service (ECS) instances	In the Singapore (Singapore) region	2

Prerequisites

- A VPC is deployed in the Singapore (Singapore) region. For more information, see Create and manage

a VPC.

- A Cloud Enterprise Network (CEN) instance is created and associated with the VPC. For more information, see Create a VPC connection.
- An SAG device is prepared.

  You cannot purchase SAG devices in the SAG console in areas outside the Chinese mainland. For more information, .

Procedure

Step 1: Purchase bandwidth for the SAG device

After you purchase an SAG device, you can purchase bandwidth for the SAG device in the SAG console. After you purchase bandwidth, Alibaba Cloud creates an SAG instance to facilitate device management.

1.
2.
3.
4. On the buy page, set the following parameters and click **Buy Now**.

Section	Description
SAG Device	
Area	Select the area where you want to use the SAG device. **Singapore (Singapore)** is selected in this example. **Note** If the area that you want to select is not listed on the buy page, we recommend that you select the nearest area. For example, if you want to use SAG devices in Thailand that is not listed on the buy page, you can select China (Hong Kong).
Device Spec	Select the model of the SAG device that you want to purchase. **SAG-100WM** is selected in this example.
Have SAG Devices Already	**Yes** is selected in this example.

Section	Description
Quantity	You do not need to set this parameter. The default value is used in this example.
Peak Bandwidth	
Area	Select the area where you want to use the bandwidth resources. This area must be the same as the **Area** that you specify for the SAG device.
Name	Specify a name for the SAG instance. *test123* is used in this example. The name must be 2 to 128 characters in length, and can contain letters, digits, periods (.), hyphens (-), and underscores (_). It must start with a letter.
Peak Bandwidth	Specify the maximum bandwidth that the SAG device can reach. The default value is used in this example.
Subscription Duration	Select a subscription duration. The default value is used in this example.

5. On the **Confirm Order** page, confirm the information and click **Confirm Purchase**.
6. In the **Shipping Address** dialog box, enter the recipient address and then click **Buy Now**.

   > **Note** You must provide the address of the recipient before you can complete the payment. The console does not record this information.

7. On the **Pay** page, select a payment method and complete the payment.

Step 2: Configure the SAG device

After you purchase an SAG device, you must configure the device and connect it to your private network.

1. Connect the SAG device to your private network.
   i. After you receive the SAG device, check whether you have received all the accessories in the purchase order.
   ii. After you start the SAG device, connect the wide area network (WAN) port to the modem and connect the local area network (LAN) port to the client.

   In this example, a client in the Singapore (Singapore) region is directly connected to the SAG device and the default CIDR block is used. For more information about how to configure WAN and LAN ports, see Configure SAG-100WM in the web console.
2.
3. In the top navigation bar, select the **Singapore (Singapore)** region. In the left-side navigation pane, click **Smart Access Gateway**.
4. Activate the SAG device.
   i. On the **Smart Access Gateway** page, find the SAG instance and choose > **Activate** in the **Actions** column.
   ii. In the **Activate** dialog box, click **OK**.

5. Associate the SAG device with the SAG instance.

   You can associate SAG devices with SAG instances to facilitate device management and configurations.

   i. Use one of the following methods to open the **Device Management** tab.

   - On the **Smart Access Gateway**, find and click the ID of the SAG instance that you want to manage. On the details page, click the **Device Management** tab.
   - On the **Smart Access Gateway** page, find the SAG instance and choose > **Device Management** in the **Actions** column.

   ii. On the **Device Management** tab, enter the serial number of the device and click **Add Device**.

6. Add routes.

   i. On the **Smart Access Gateway** page, find the SAG instance and click **Network Configuration** in the **Actions** column.

   ii. On the **Method to Synchronize with On-premises Routes** tab, select **Static Routing** and click **Add Static Route**.

   iii. Enter the CIDR block of the office and click **OK**.

   192.168.10.0/24 is used in this example. Therefore, the IP addresses of clients are allocated from 192.168.10.0/24.

Step 3: Enable network communication

After you configure the SAG device, you must create network connections to enable the clients in the office to communicate with the VPC.

1.
2. In the top navigation bar, select **Singapore (Singapore)**.
3. Attach the SAG instance to a CCN instance.

   > **Note** If you have already created a CCN instance in the area, proceed to the step .

   i. In the left-side navigation pane, click **CCN**.

   ii. On the **CCN** page, click **Create CCN Instance**.

   iii. In the **Create CCN Instance** panel, specify a name for the CCN instance and click **OK**.

   The name must be 2 to 100 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter. *test123* is used in this example.

   iv. In the left-side navigation pane, click **Smart Access Gateway**.

   v. On the **Smart Access Gateway** page, find the SAG instance and click **Network Configuration** in the **Actions** column.

   vi. Click the **Network Instance Details** tab and click **Attach Network**.

   vii. Set the parameters and click **OK**.

   - **Network Type**: **Cloud Connect Network** is selected in this example.
   - **Resource Group**: **Default Resource Group** is selected in this example.
   - **Network Instance**: The CCN instance created in the preceding step is selected in this example.

4. Attach the CCN instance to a CEN instance.
   i. In the left-side navigation pane, click **CCN**.
   ii. Find the CCN instance and click **Bind CEN Instance** in the **Actions** column.
   iii. In the **Bind CEN Instance** pane that appears, select the CEN instance that you want to attach and click **OK**.

   After the CCN instance is attached to the CEN instance, SAG devices associated with the CCN instance can communicate with VPCs that are attached to the CEN.
5. Configure an ECS security group.
   i. Log on to the ECS console.
   ii. In the top navigation bar, select the resource group and the **Singapore (Singapore)** region. In the left-side navigation pane, click **Instances**.
   iii. Find the ECS instance that you want to manage and choose **More > Network and Security Group > Configure Security Group** in the **Actions** column.
   iv. Find the security group that you want to manage and click **Add Rules** in the **Actions** column.

   > **Note** If you do not create a security group when you create an ECS instance, a default security group is created. If you want to add an ECS instance to a custom security group, you can create a custom security group. For more information, see Create a security group.

   v. Create a security group rule that allows access from the private network of the office to the VPC. For more information, see Add a security group rule.

   Set Authorization Object to the CIDR block of the private network. *192.168.10.0/24* is used in this example.

Step 4: Test network connectivity

After you complete the preceding steps, you can run the **ping** command to test the network connectivity between the office and the ECS instance. If an echo reply packet is returned, it indicates that the private network of the office is connected to Alibaba Cloud.

```
ping <IP address of the ECS instance>
```

12.Use SAG and CEN to access OSS

This topic describes how to use Smart Access Gateway (SAG) along with Cloud Enterprise Network (CEN) to connect on-premises clients to Alibaba Cloud. This way, the clients can access Object Storage Service (OSS) buckets through CEN.

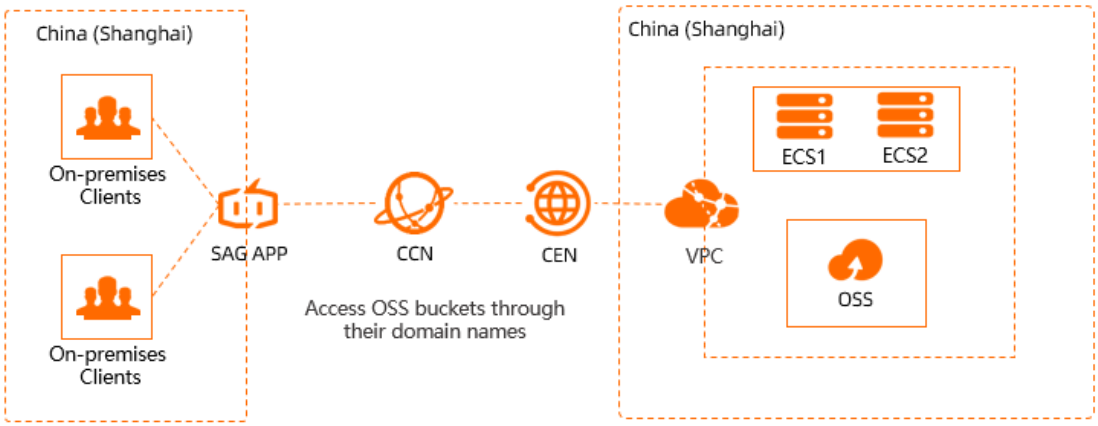
Prerequisites

- A Virtual Private Network (VPC) network is deployed in the China (Shanghai) region. For more information, see Create and manage a VPC.
- A CEN instance is created and associated with the VPC network in the China (Shanghai) region. For more information, see Create a CEN instance.

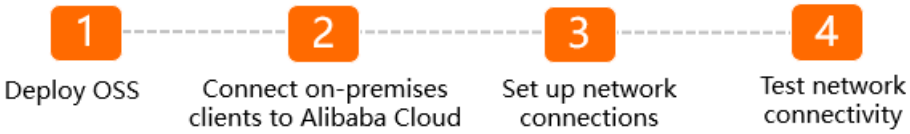
Context

Cloud services refer to Alibaba Cloud services, such as OSS, Log Service, and Data Transmission Service (DTS), that use the CIDR block 100.64.0.0/10 to provide services. You can use SAG to connect on-premises clients to Alibaba Cloud and then access cloud services through CEN.

OSS is a secure, cost-effective, and highly reliable cloud storage service provided by Alibaba Cloud. You can store large amounts of data in OSS buckets. OSS buckets are accessible through their endpoints. Endpoints refer to internal network connections between Alibaba Cloud services that are deployed in different regions. If you access an OSS bucket through its endpoint, no data transfer fees are incurred. The following figure shows how on-premises clients of a company are connected to Alibaba Cloud and access OSS buckets through their endpoints. The company has created a VPC network in the China (Shanghai) region and plans to activate OSS in this region. The company needs to store sensitive data in OSS buckets and allow employees to download the data through the endpoints of the OSS buckets. To meet the preceding requirements while minimizing expenses, the company plans to connect on-premises clients to Alibaba Cloud through the SAG app.



Configuration procedure



Step 1: Purchase OSS

You can deploy OSS through multiple methods. This procedure demonstrates how to deploy OSS in the OSS console. For more information, see What is OSS?

1. Activate OSS. For more information, see Activate OSS.
2. Create an OSS bucket.
   i. Log on to the OSS console.
   ii. In the left-side navigation pane, click **Buckets**. On the Buckets page, click **Create Bucket**.

iii. In the **Create Bucket** pane, set the parameters.

The following parameters are set in this example. You can set parameters based on your business requirements. For more information, see Create buckets.

- **Bucket Name**: Specify a name for the bucket. The name cannot be changed after the bucket is created. *shosstest* is used in this example.
- **Region**: Select the region where you want to create the bucket. The region cannot be changed after the bucket is created. **China (Shanghai)** is used in this example.
- **Storage Class**: Select a storage class for the bucket. **Standard** is used in this example.

  The standard storage class provides highly reliable, highly available, and high-performance object storage services that can handle frequent data access. Standard storage is suitable for scenarios such as image sharing, social media, audio and video applications, large-scale websites, and big data analytics. For more information, see Overview.
- **Zone-redundant Storage**: Select whether to enable zone-redundant storage. **Disable** is selected in this example.

  If you disable zone-redundant storage, replicas of files stored in the bucket are saved only in the current zone.
- **Versioning**: Select whether to enable versioning. **Enable** is selected in this example.

  If you enable versioning for the bucket, data that is overwritten or deleted is saved as a historical version. Versioning allows you to restore objects in a bucket to a specific version. It protects your data from accidental overwritten or deletion. For more information, see Overview.
- **Access Control List (ACL)**: Select the read and write permissions on the bucket. **Private** is selected in this example.

  Only the bucket owner can perform read and write operations on objects in the bucket. Other users do not have access to objects in the bucket.
- **Encryption Method**: Select whether to enable server-side encryption. **None** is selected in this example.
- **Real-time Log Query**: Select whether to enable real-time log query. **Disable** is selected in this example.
- **Scheduled Backup**: Select whether to enable scheduled backup to back up data in the OSS bucket by using Hybrid Backup Recovery (HBR). **Disable** is selected in this example.

iv. Click **OK**.

3. Upload an object to the OSS bucket.

i. In the left-side bucket management pane, click **Files**.

ii. Click **Upload**.

iii. In the **Upload** pane, set the parameters.

- **Upload To**: Specify the path to which you want to upload the object. The default path is used in this example.
- **File ACL**: Select the read and write permissions on the object. The default option is **Inherited from Bucket**. The default option is used in this example.
- **Upload**: Drag and drop one or more objects to this section, or click **Upload** to upload objects.

iv. In the **Upload Tasks** dialog box, wait until the objects are uploaded to the bucket and then close the dialog box.

4. Set permissions on the object.

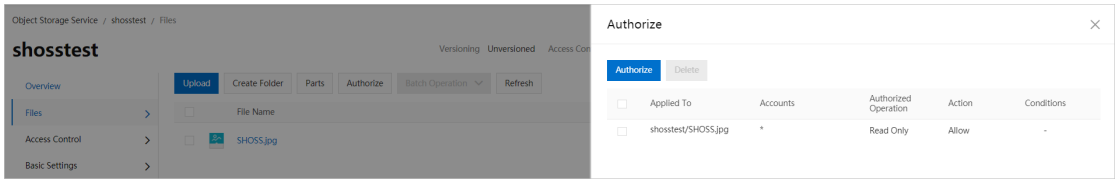
   For data security, the bucket is set to private in this example. Therefore, permissions on a specific object must be manually granted to users that need to access the object. The following example demonstrates how to grant read-only permissions on an image file to all users. You can set permissions on objects based on your business requirements. For more information, see Configure bucket policies to authorize other users to access OSS resources.

   i. On the **Files** tab, click **Authorize**.

   ii. In the **Authorize** pane, click **Authorize**.

   iii. In the Authorize pane to which you are redirected, set the following parameters and click **OK**.

   - **Applied To**: **Specified Resource** is selected in this example.
   - **Resource Paths**: *SHOSS.jpg* is specified in this example.
   - **Accounts**: **Anonymous Accounts** is selected in this example.
   - **Authorized Operation**: **Read Only** is selected in this example.



Step 2: Connect on-premises clients to Alibaba Cloud

In this step, you must purchase an SAG APP instance, set up network connections, and create client accounts in the SAG console. After the configurations are completed, on-premises clients can connect to Alibaba Cloud through the SAG app.

1. Purchase an SAG APP instance.

   i. Log on to the SAG console.

   ii. In the left-side navigation pane, click **Smart Access Gateway APP**.

iii. On the **Smart Access Gateway APP** page, click **Create SAG APP** and set the following parameters:

- **Region and Zone**: Select the area where you want to create the SAG APP instance. **Mainland China** is selected in this example.
- **Number of Client Accounts**: Specify the number of client accounts that can be added to the SAG APP instance. Typically, you need to create an account for each user that needs to log on to the SAG app. The default value 10 is used in this example.

> **Note** You can purchase 5 to 1,000 client accounts for each SAG APP instance. Pricing is tiered and based on the number of client accounts. For more information, see Billing and pricing of the SAG app.

- **Data Plan Per Account**: The amount of free data usage allocated to each client account per month. The data transfer plan cannot be shared among different accounts and remains effective only within the month. By default, 5 GB of data usage is offered to each client account per month.
- **Billing Method When Data Plan is Exhausted**: If the actual data usage of an account exceeds the data transfer plan, the excess data is charged based on the pay-as-you-go billing method.
- **Subscription Duration**: Select the subscription duration of the data transfer plan for each account. Monthly subscriptions and auto renewal are supported. One month is selected in this example.

iv. Click **Buy Now** to confirm the order and complete the payment.

2. Set up network connections.

After you purchase an SAG APP instance, you must set up network connections. In this step, you must associate the SAG APP instance with a Cloud Connect Network (CCN) instance and specify the CIDR blocks of the clients.

CCN is an important component of SAG. After an SAG APP instance is associated with a CCN instance, on-premises clients associated with the SAG APP instance can connect to Alibaba Cloud. For more information, see Introduction to CCN.

i. On the **Smart Access Gateway APP** page, find the SAG APP instance that you want to manage and click **Quick Configuration** in the **Actions** column.

ii. In the **Quick Configuration** wizard, set the required parameters.

- **CCN**: You can select one of the following options to associate the SAG APP instance with a CCN instance. **Create CCN** is selected in this example.
  - **Existing CCN**: If you have already created CCN instances, you can select an existing CCN instance from the drop-down list.
  - **Create CCN**: If you have not created a CCN instance, enter an instance name. The system then creates a CCN instance and automatically associates it with the SAG APP instance.

    The name must be 2 to 100 characters in length, and can contain digits, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
- (Optional)**Standby and Active DNS**: optional. The active and standby DNS servers that the clients use to connect to the private network through the SAG app. After you configure the DNS servers, the system automatically synchronizes the DNS settings to the clients. Ignore this parameter in this example.
- **Private CIDR Block**: Specify the private CIDR blocks that the clients use to connect to Alibaba Cloud. When a client connects to Alibaba Cloud, an IP address within the specified CIDR block is assigned to the client. Make sure that the private CIDR blocks do not overlap with each other. 192.168.10.0/24 is used in this example.

  You can click **Add Private CIDR Block** to add more private CIDR blocks. You can add a maximum of five private CIDR blocks.

3. Associate the CCN instance with a CEN instance.

   You must associate the CCN instance with a CEN instance. This way, on-premises clients associated with the SAG APP instance can access OSS through the CEN instance.

   i. Click **Associate with a CEN (Optional)** to associate the CCN instance with a CEN instance.

   ii. You can select one of the following options to associate the CCN instance with a CEN instance to enable communication between the clients and cloud resources. **Existing CEN** is selected in this example.
   - **Existing CEN**: If you have already created CEN instances, you can select a CEN instance from the drop-down list.
   - **Create CEN**: If you have not created a CEN instance, enter an instance name. The system then creates a CEN instance and automatically associates it with the CCN instance.

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

4. Create a client account.

   After you set up network connections, you must create client accounts to allow on-premises clients to log on to the SAG app and connect to the private network.

i. Click **Next: Create a client account** to create a client account.

- **Username**: optional. The username must be 7 to 33 characters in length, and can contain underscores (_), at signs (@), periods (.), and hyphens (-). It must start with a digit or a letter.

  > **Note**
  > - The usernames of client accounts added to the same SAG APP instance must be unique.
  > - When you create a client account, if you specify only the email address, the system automatically generates a username and password. The specified email address is used as the username.

- **Email Address**: required. The email address of the user. The username and password are sent to the specified email address.

  The email address must be 2 to 64 characters in length, and can contain letters, digits, underscores (_), periods (.), and hyphens (-). It must contain an at sign (@).

- **Static IP**:
  - If you enable this feature, you must configure the IP address of the client. The client account uses the specified IP address to connect to Alibaba Cloud.

    > **Note** The specified IP address must fall into the CIDR block of the private network.

  - If you disable this feature, an IP address within the CIDR block of the private network is assigned to the client. Each connection to Alibaba Cloud uses a different IP address.

- **Set Maximum Bandwidth**: Specify the maximum bandwidth for the client account. The default value is used in this example.

  You can set the maximum bandwidth to 1 to 2,000 Kbit/s. The maximum bandwidth is set to 2,000 Kbit/s by default.

- **Set Password**: optional. Set the password that is used to log on to the SAG app.

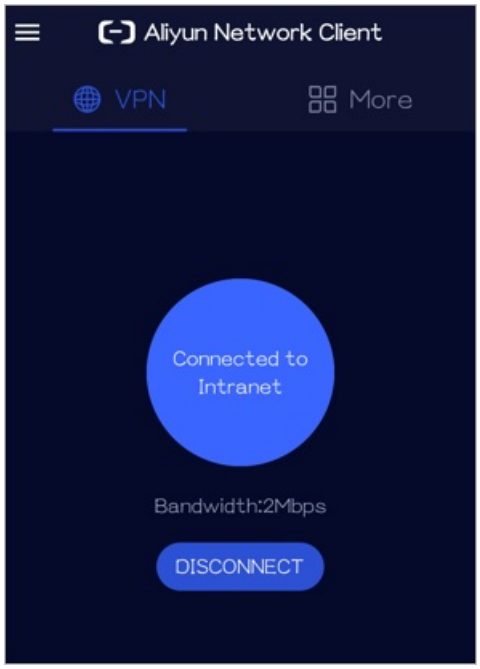
  The password must be 8 to 32 characters in length, and can contain underscores (_) and hyphens (-). It must start with a letter or a digit.

ii. Click **OK**.

5. Connect the client to Alibaba Cloud.

i. After you create a client account, click **Download Now** to go to the page that provides instructions on how to download and install the SAG app. For more information, see Install the SAG app.

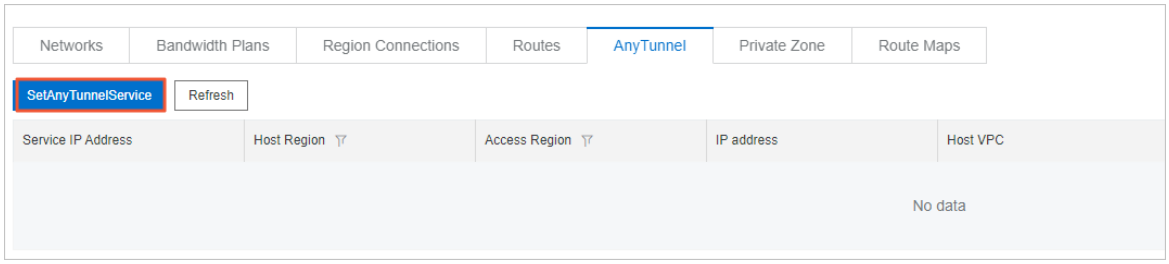
ii. After the SAG app is installed on a client, the client can log on to the SAG app with the client account and connect to Alibaba Cloud. For more information, see Connect to Alibaba Cloud.



Step 3: Configure routes to OSS

In this step, you must configure routes to OSS in the CEN console. After routes are configured, CEN establishes network communication between the network associated with the CCN and OSS. This way, on-premises clients can access OSS through CEN.

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 **AnnyTunnel** tab, click **SetAnyTunnelService**.



4. In the **SetAnyTunnelService** pane, set the following parameters:
   - **Service IP address**: Enter an IP address or CIDR block used by OSS. The IP address or CIDR block must fall into 100.64.0.0/10. In this example, 100.118.102.0/24 is used.

     Typically, a cloud service uses multiple IP addresses. Repeat the preceding steps to add routes to all the IP addresses of OSS. In the China (Shanghai) region, add the following CIDR blocks of OSS:

     - 100.98.35.0/24
     - 100.98.110.0/24
     - 100.98.169.0/24
     - 100.118.102.0/24

     For more information, see Internal endpoints of OSS buckets and VIP ranges.
   - **Host Region**: Select the region where OSS is deployed. **China (Shanghai)** is selected in this

example.

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

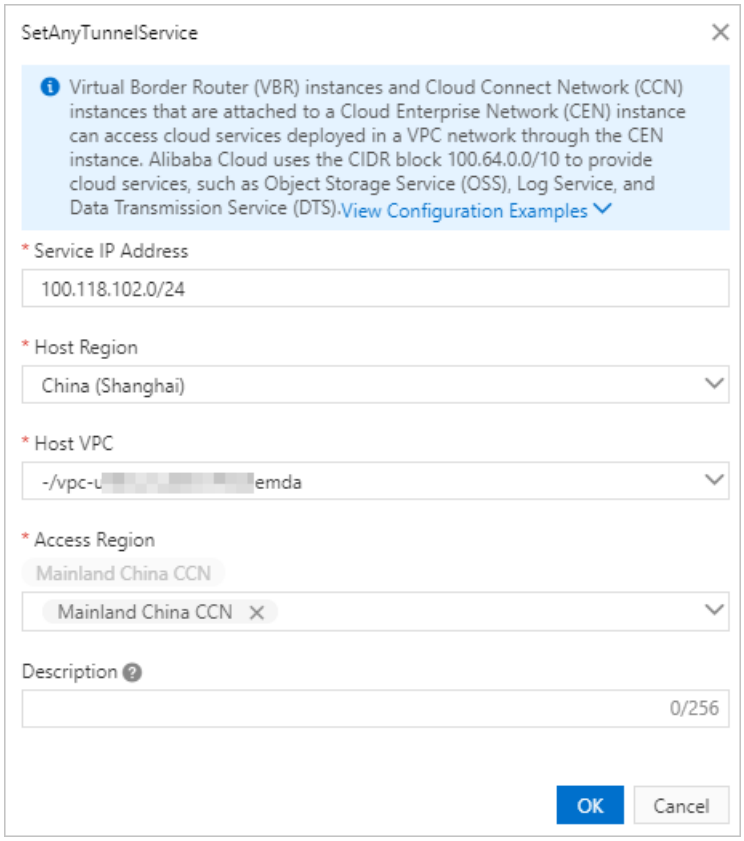
  After you select a VPC network, networks attached to the CCN instance can access OSS through the VPC network.

- **Access Region**: Select the CCN instance that is associated with the CEN instance. **Mainland China CCN** is selected in this example.

  > **Note** Make sure that the selected CCN instance is associated with the CEN instance. For more information, see Configure routes to OSS.

- **Description**: Enter a description for OSS. This parameter is optional.

  The description 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://`.



5. Click **OK**.

Step 4: Test network connectivity

After the preceding steps are completed, on-premises clients can connect to Alibaba Cloud through the SAG app and access OSS.

For example, you can visit `https://shosstest.oss-cn-shanghai-internal.aliyuncs.com/SHOSS.jpg` through the SAG app and download the image file `SHOSS.jpg`.

13.Use Log Service to query and analyze network traffic

This topic describes how to use Log Service to query and analyze the network traffic of a Smart Access Gateway (SAG) instance.

Prerequisites

- A project and a Logstore are created in Log Service. For more information, see Quick start.
- The SAG device is connected to Alibaba Cloud. For more information, see Deploy an SAG device in one-arm mode and enable static routing.
- The model of the SAG device is SAG-1000.

Context

SAG supports flow logs. You can use flow logs to capture network traffic that is distributed by SAG instances. Flow logs can be stored in Log Service or on a specified NetFlow collector. In this topic, Log Service is used as an example. This topic describes how to store the traffic information about an SAG instance, and query and analyze the collected information. This allows you to gain insights into the network traffic distribution of SAG instances.

Step 1: Add a data source

Before you can query or analyze network traffic, you must perform the following steps to collect and deliver the traffic information about the SAG instance to the specified Logstore in the Log Service project:

1. Create a flow log.

   In the SAG console, create a flow log for the SAG instance. Each flow log is associated with a Logstore in a Log Service project. Traffic information about the SAG instance is stored in the associated project and Logstore.

   i. Log on to the SAG console.

   ii. In the left-side navigation pane, click **Flow Log**.

   iii. On the **Flow Log** page, click **Create Flow Log**.

iv. In the **Create Flow Log** panel, set the parameters and click **OK**.

- **Name**: Enter a name for the flow log.
- **Output Interval Under Active Connections**: Enter a time interval at which log data of active network connections is collected. The default time interval is 300 seconds. You can set a time interval from 60 to 6,000 seconds.
- **Output Interval Under Inactive Connections**: Enter a time interval at which log data of inactive network connections is collected. The default time interval is 15 seconds. You can set a time interval from 10 to 600 seconds.
- **Deliver Flow Log Data To**: Select a service where you want to store the collected log data. **SLS** is selected in this example.
  - If you want to store the collected log data in Log Service, select **SLS**.
  - If you want to store the collected log data on a NetFlow collector, select **Netflow**.
  - To store log data both in Log Service and on a NetFlow collector, select **ALL**.
- **SLS Region**: Select the region where Log Service is deployed.
- **SLS Project**: Select the project to which the Logstore belongs.
- **SLS Logstore**: Select the Logstore where you want to store the collected log data.

For more information, see Create a flow log.

2. Associate the flow log with the SAG instance.

After you create a flow log, you must associate it with the SAG instance from which you want to collect traffic information. After the flow log is associated with the SAG instance, the information about the network traffic of the SAG instance is stored in the specified Log Service project and Logstore. You can query and analyze the collected log data in the Log Service console.

i. On the **Flow Log** page, find the flow log that you have created and click its ID.

ii. On the details page, click **Associate with Instance**.

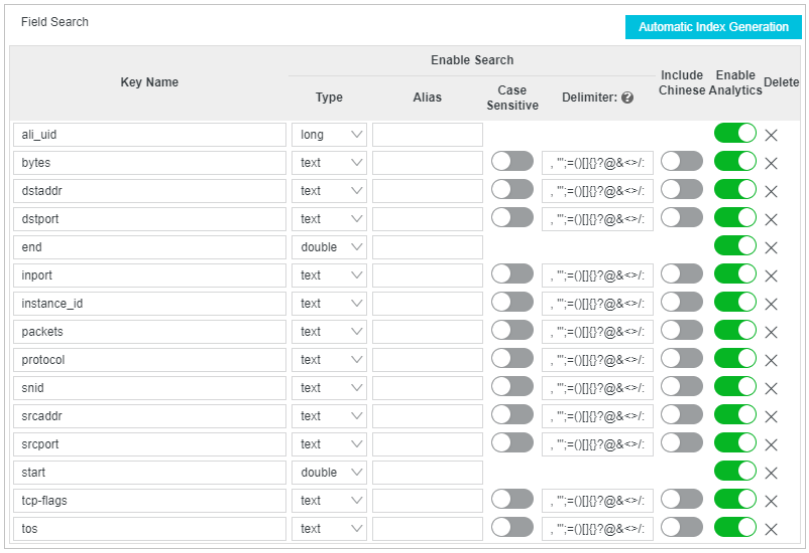
iii. In the **Associate with Instance** panel, select the SAG instance with which you want to associate the flow log and click **Save**.

Step 2: Query and analyze log data

After the flow log is associated with the SAG instance, you can query and analyze the collected log data in the Log Service console.

1.
2. In the Projects section, click the project in which you want to query and analyze logs.
3. On the **Log Storage > Logstores** tab, click the Logstore where logs are stored.
4. Enable the indexing feature for the Logstore. For more information, see Enable and configure the indexing feature for a Logstore.

   An index is a data structure that can be used to sort one or more columns of log data. You can query and analyze log data only after you add indexes. The query and analysis results vary based on the indexes. We recommend that you add indexes based on your business requirements. In this example, the field indexing and statistics features are enabled:



Note To facilitates data analytics, make sure that the bytes field is of the TEXT type when you configure field indexing.

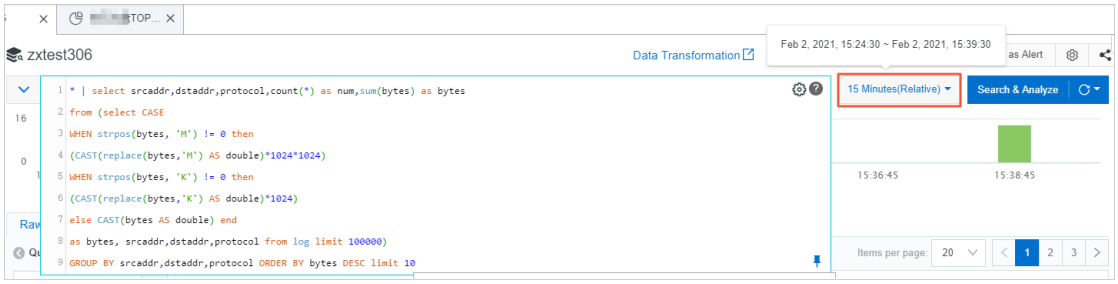
5. After you enable indexing, you can query and analyze log data. In the following example, the top ten 5-tuples that have generated the highest volume of network traffic are queried. The example shows how to query and analyze network traffic.

i. Enter a query statement in the search box.

In this example, the following fields are used to query the top ten 5-tuples that have generated the highest volume of network traffic: srcaddr, srcport, dstaddr, dstport, and protocol.

```
* | select srcaddr,srcport,dstaddr,dstport,protocol,count(*) as num,sum(bytes) as b
ytes
from (select CASE
WHEN strpos(bytes, 'M') != 0 then
(CAST(replace(bytes,'M') AS double)*1024*1024)
WHEN strpos(bytes, 'K') != 0 then
(CAST(replace(bytes,'K') AS double)*1024)
else CAST(bytes AS double) end
as bytes,srcaddr,srcport,dstaddr,dstport,protocol from log limit 100000)
GROUP BY srcaddr,dstaddr,srcport,dstport,protocol ORDER BY bytes DESC limit 10
```

By default, the system returns log data collected within the last 15 minutes. You can also specify a time range.



> **Note** Do not directly include the fields described in this topic in the query statements. These fields are for reference only. The fields in the collected log shall prevail. For more information, see Log search overview.

ii. Click **Search & Analyze**.

You are redirected to the **Graph** tab. The information about the top ten 5-tuples that have generated the highest volume of network traffic is displayed in a table. You can also choose to display the data in other types of graph. For more information, see Chart overview.

In this example, the data is displayed in a pie chart.

iii. On the **Graph** tab, you can modify the attributes of the pie chart.

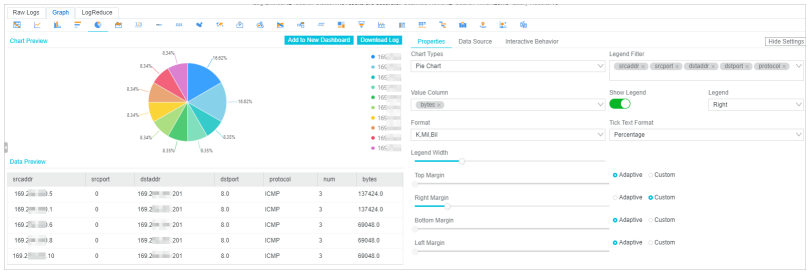
The following attributes are modified in this example. Other attributes use the default value. For more information, see View query results in a pie chart.

- **Category**: The category of the data.

  In this example, the data is classified based on the following fields: srcaddr, srcport, dstaddr, dstport, and protocol. The volume of network traffic is counted only if all the preceding fields match the specified conditions.

- **Value Column**: The value of the returned data entry.

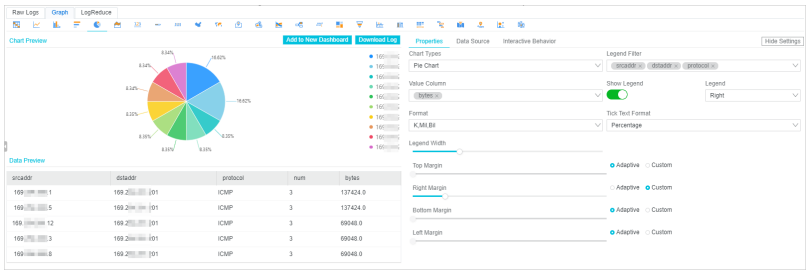
  In this example, the bytes field is used as the value column.



6. (Optional)You can perform the preceding steps to query the top ten 3-tuples that have generated the highest volume of network traffic or the top 10 source IP addresses that have generated the largest amount of network traffic.
   - Query the top ten 3-tuples that have generated the highest volume of network traffic
     - Fields that are queried: srcaddr, dstaddr, protocol.
     - Statements for querying data:

```
* | select srcaddr,dstaddr,protocol,count(*) as num,sum(bytes) as bytes
from (select CASE
WHEN strpos(bytes, 'M') != 0 then
(CAST(replace(bytes,'M') AS double)*1024*1024)
WHEN strpos(bytes, 'K') != 0 then
(CAST(replace(bytes,'K') AS double)*1024)
else CAST(bytes AS double) end
as bytes, srcaddr,dstaddr,protocol from log limit 100000)
GROUP BY srcaddr,dstaddr,protocol ORDER BY bytes DESC limit 10
```

     - Query results:

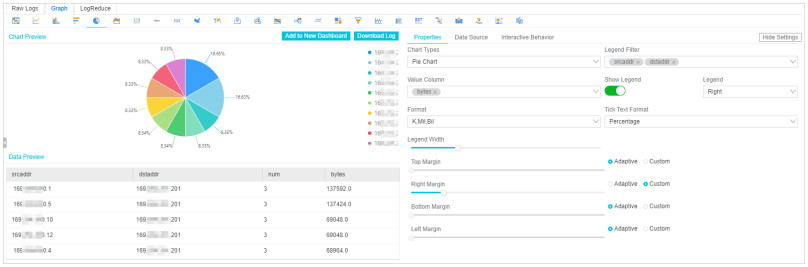


   - Query the top 10 source IP addresses that have generated the highest volume of network traffic
     - Fields that are queried: srcaddr and dstaddr.

- Statements for querying data:

```
* | select srcaddr,dstaddr,count(*) as num,sum(bytes) as bytes
from (select CASE
WHEN strpos(bytes, 'M') != 0 then
(CAST(replace(bytes,'M') AS double)*1024*1024)
WHEN strpos(bytes, 'K') != 0 then
(CAST(replace(bytes,'K') AS double)*1024)
else CAST(bytes AS double) end
as bytes, srcaddr,dstaddr from log limit 100000)
GROUP BY srcaddr,dstaddr ORDER BY bytes DESC limit 10
```

- Query results:



Step 3: (Optional) Add the graph to a dashboard

Log Service allows you to add graphs that contain query results to dashboards. This way, you can view the stored data as needed.

1. In the upper-right corner of the pie chart, click **Add to New Dashboard**.
2. In the **Add to New Dashboard** dialog box, set the parameters and click **OK**.
   - **Operation**: **Create Dashboard** is selected in this example.
   - **Dashboard Name**: Enter a name for the dashboard. *Statistics Based on 5-tuples* is used in this example.
   - **Chart Name**: Enter a name for the graph. *Pie Chart Based on 5-tuples* is used in this example.

   For more information, see Add charts to a dashboard.
3. In the left-side navigation pane, click the **Dashboard** icon.
4. Click the name of the dashboard that you have created to view the data.

   On the dashboard, you can click **Time Range** to specify a time range to filter analysis data. For more information, see Manage a dashboard in display mode.