Alibaba Cloud
Smart Access Gateway

User Guide

Issue: 20190128

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⊖	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⊖ Danger: Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	ⓘ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

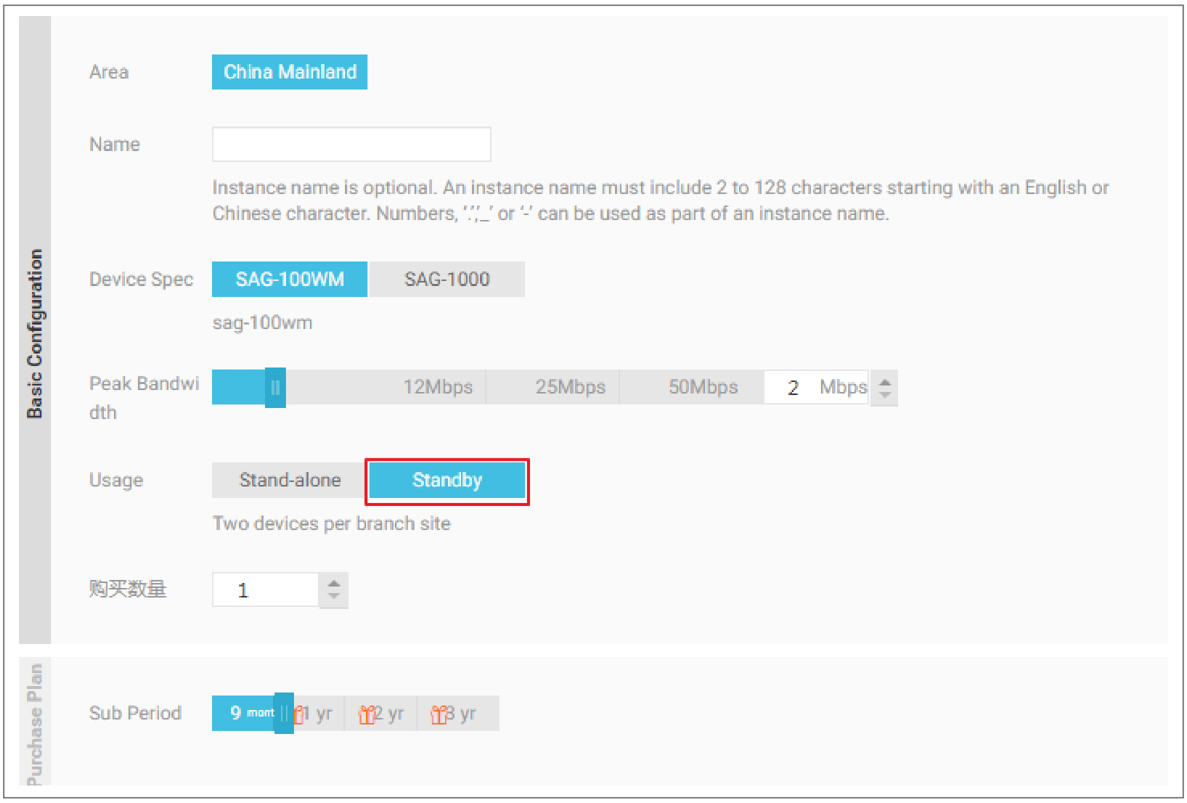
1 Manage a Smart Access Gateway instance

1.1 Device-level configurations for high availability

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

Prerequisites

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



Basic Configuration

Area: China Mainland

Name:

Instance name is optional. An instance name must include 2 to 128 characters starting with an English or Chinese character. Numbers, '.','_' or '-' can be used as part of an instance name.

Device Spec: SAG-100WM | SAG-1000

sag-100wm

Peak Bandwidth: 12Mbps 25Mbps 50Mbps 2 Mbps

Usage: Stand-alone | Standby

Two devices per branch site

购买数量: 1

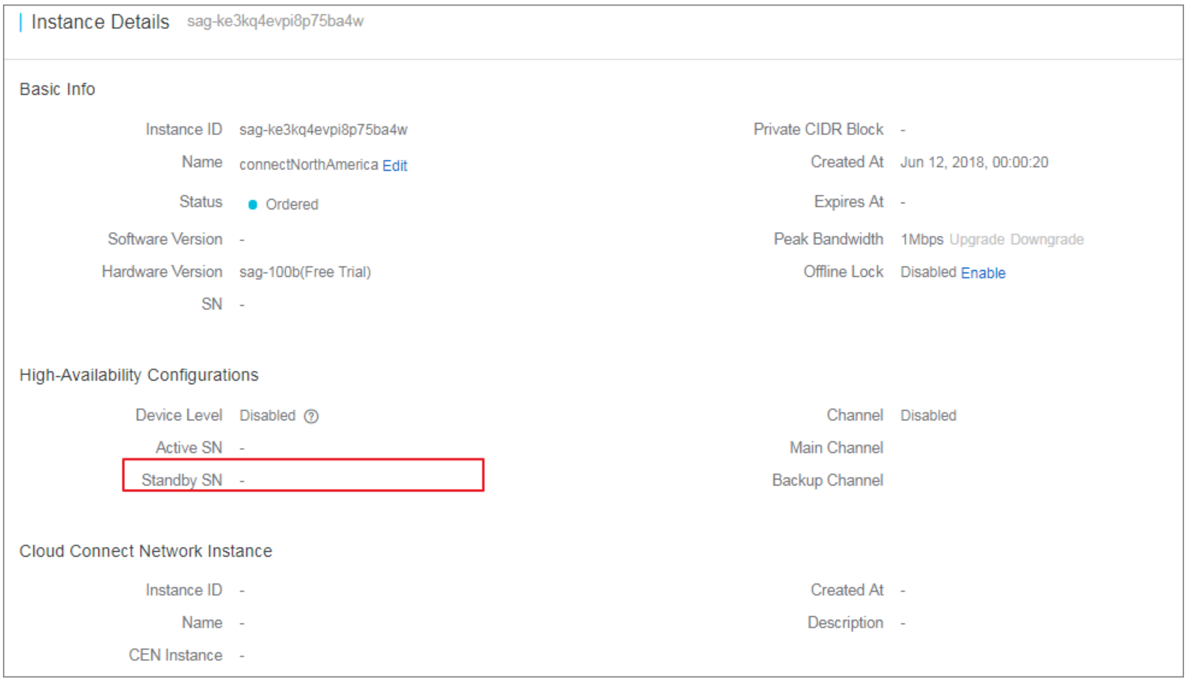
Purchase Plan

Sub Period: 9 mont | 1 yr | 2 yr | 3 yr

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

Procedure

1. Log on to the *Smart Access Gateway console*.
2. On the SAG page, find the target instance and click the ID of the instance.
3. In the High-Availability Configurations area, click Switch to switch to the other device.



Instance Details sag-ke3kq4evpi8p75ba4w

Basic Info

Instance ID sag-ke3kq4evpi8p75ba4w

Name connectNorthAmerica Edit

Status Ordered

Software Version -

Hardware Version sag-100b(Free Trial)

SN -

Private CIDR Block -

Created At Jun 12, 2018, 00:00:20

Expires At -

Peak Bandwidth 1Mbps Upgrade Downgrade

Offline Lock Disabled Enable

High-Availability Configurations

Device Level Disabled

Active SN -

Standby SN -

Channel Disabled

Main Channel

Backup Channel

Cloud Connect Network Instance

Instance ID -

Name -

CEN Instance -

Created At -

Description -

Note:

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

1.2 Device-level configurations for high availability

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

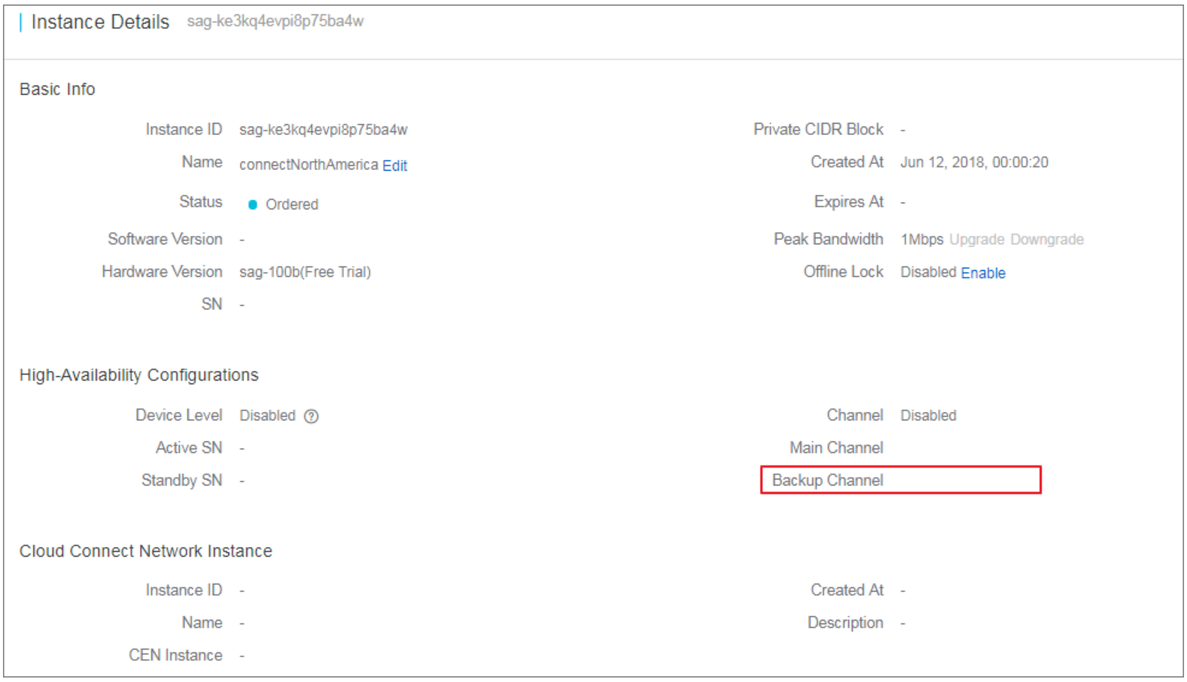
Context

Note:

Currently, active/standby links are only supported by SAG-100WM devices.

Procedure

1. Log on to the *Smart Access Gateway console*.
2. On the SAG page, find the target instance and click the ID of the instance.
3. In the High-Availability Configurations area, view the active/standby links.



Instance Details sag-ke3kq4evpi8p75ba4w

Basic Info

Instance ID	sag-ke3kq4evpi8p75ba4w	Private CIDR Block	-
Name	connectNorthAmerica Edit	Created At	Jun 12, 2018, 00:00:20
Status	● Ordered	Expires At	-
Software Version	-	Peak Bandwidth	1Mbps Upgrade Downgrade
Hardware Version	sag-100b(Free Trial)	Offline Lock	Disabled Enable
SN	-		

High-Availability Configurations

Device Level	Disabled ⓘ	Channel	Disabled
Active SN	-	Main Channel	
Standby SN	-	Backup Channel	

Cloud Connect Network Instance

Instance ID	-	Created At	-
Name	-	Description	-
CEN Instance	-		

2 Cloud Connect Network

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

CCN areas

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

A local branch can access the Alibaba Cloud without any other configurations if the CCN area and CEN area are the same. For example, to connect a local branch in Hangzhou to a VPC in Shanghai, you just need to bind the CCN instance to which the Smart Access Gateway is bound to the CEN instance where the VPC is located.

Note:

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

CCN area	CEN area	Regions in CEN area
Mainland China	Mainland China	China (Qingdao) China (Beijing) China (Zhangjiakou) China (Shenzhen) China (Hangzhou) China (Shanghai) China (Hohhot)
Hong Kong	Asia Pacific	Hong Kong
Singapore		Singapore
Malaysia (Kuala Lumpur)		Malaysia (Kuala Lumpur)
Japan (Tokyo)		Japan (Tokyo)

CCN area	CEN area	Regions in CEN area
India (Mumbai)		India (Mumbai)
North America	North America	US (Silicon Valley)
		US (Virginia)
Europe	Europe	Germany (Frankfurt)
Australia	Australia	Sydney

Create a CCN instance

To create a CCN instance, follow these steps:

1. Log on to the *Smart Access Gateway console*.
2. In the left-side navigation pane, click CCN.
3. Select the target area and click Create CCN Instance.
4. Enter the name and description of the CCN instance and click OK.

Bind a CCN instance to a CEN instance

After you bind a CCN instance to a CEN instance, local branches connected to the CCN instance can access Alibaba Cloud without any other configurations if the CCN areas and CEN areas are the same.

To bind a CCN instance to a CEN instance, follow these steps:

1. Log on to the *Smart Access Gateway console*.
2. In the left-side navigation pane, click CCN.
3. Select the area of the CCN instance, and click Bind CEN Instance in the Actions column of the target CCN instance.
4. Select the CEN instance where the VPC is located and click OK.

3 Manage a Smart Access Gateway instance

After purchasing a Smart Access Gateway device, you can use the corresponding Smart Access Gateway instance to activate or lock the device, or add it to CCN.

Activate the gateway device

After receiving the gateway device, you need to activate it on the console. Billing starts right after the device is activated. For more information, see 计费说明.

Note:

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

To activate the Smart Access Gateway device, complete these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the SmartAG page, find the target gateway instance.
3. Click Activate in the Actions column.

Attach to CCN

After activating the Smart Access Gateway device, you also need to attach it to CCN and then attach the CCN instance to a CEN instance, so that on-premises branches can be connected to Alibaba Cloud.

To configure the network, complete these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the SmartAG page, find the target gateway instance.
3. Click Configure Network in the Actions column.
4. Complete network configurations according to the following information.

Configuration	Description
Name/ID	Displays the name and ID of the Smart Access Gateway instance.

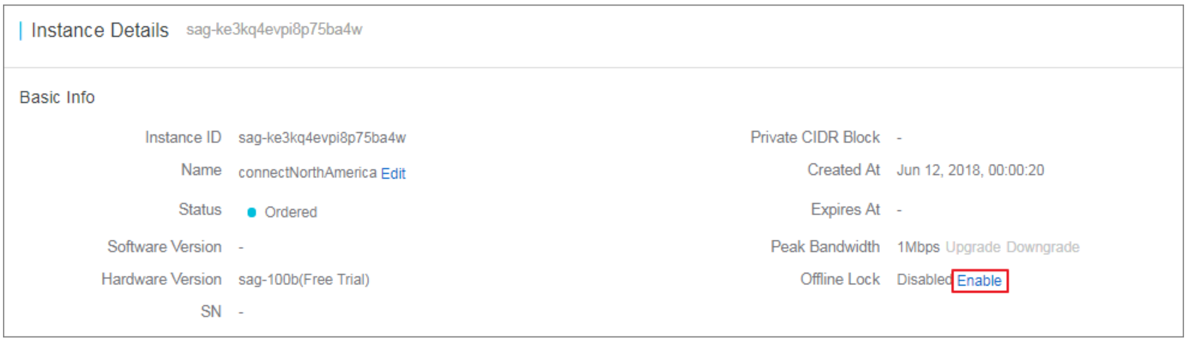
Configuration	Description
Private CIDR Block	Configure the private CIDR blocks used by the local clients to access Alibaba Cloud. Make sure all private CIDR blocks do not conflict with each other. Click Add Private CIDR Block to add more CIDR blocks. Up to five private CIDR blocks can be configured. The LAN port configuration of the local gateway device determines which private IP address is used: · If the LAN port of the Smart Access Gateway device uses the dynamic IP mode and DHCP is enabled on the client , the IP address that the local client uses for communication are allocated from the first specified private CIDR block. · If the LAN port of the Smart Access Gateway device is in static IP mode, the static IP must be in the specified private CIDR block.
CCN Instance ID/ Name	Select the CCN instance to attach. You can use the default CCN instance or a created CCN instance. CCN is a device access matrix composed of Alibaba Cloud distributed access gateways. After a Smart Access Gateway device is attached to a CCN instance, the gateway device can communicate with other gateway devices attached to the CCN instance. Note: Make sure that the CCN instance and Smart Access Gateway instances attached to it are in the same area.
Bind CEN Instance	Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, all networks (VPCs and VBRs) attached to the CEN instance can communicate with the CCN instance. Note: Make sure that the CCN instance and the CEN instance are in the same area. For more information, see 云连接网区域.

Enable locking

When the gateway device is offline, you can lock the gateway device and then the device cannot be used any more.

To lock a Smart Access Gateway instance, follow these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the SmartAG page, find the target gateway instance.
3. On the Instance Details page, click the Enable option for Offline Lock.



Instance Details sag-ke3kq4evpi8p75ba4w

Basic Info

Instance ID	sag-ke3kq4evpi8p75ba4w	Private CIDR Block	-
Name	connectNorthAmerica Edit	Created At	Jun 12, 2018, 00:00:20
Status	● Ordered	Expires At	-
Software Version	-	Peak Bandwidth	1Mbps Upgrade Downgrade
Hardware Version	sag-100b(Free Trial)	Offline Lock	Disabled Enable
SN	-		

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

   If, for example, 3600 is entered, the gateway device becomes locked after 60 minutes.

Disable locking

To disable the locked status of the gateway device, follow these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the SmartAG page, click the ID of the target gateway instance.
3. On the Instance Details page, click the Disable option for Offline Lock.

Modify the bandwidth

To disable the bandwidth of the gateway device, follow these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the SmartAG page, find the target gateway instance.
3. On the Instance Details page, click the Upgrade or Downgrade option for Peak Bandwidth.
4. On the Update page, adjust the bandwidth and complete the payment.

Renew an instance

To renew an instance and avoid service interruption, follow these steps:

1. Log on to the *Smart Access Gateway console*.
2. On the SmartAG page, find the target instance.
3. Click More > Renew.
4. Select the renewal duration and complete the payment.