# Alibaba Cloud
# 智能接入网关

# QoS

**Issue: 20191028**

# 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, consequent**

ial, 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 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 contact Alibaba Cloud directly if you discover any errors in this document.

# Document conventions

| Style | Description | Example |
| --- | --- | --- |
|  | A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. |  **Danger:**<br>Resetting will result in the loss of user configuration data. |
|  | A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. |  **Warning:**<br>Restarting will cause business interruption. About 10 minutes are required to restart an instance. |
|  | A caution notice indicates warning information, supplementary instructions, and other content that the user must understand. |  **Notice:**<br>If the weight is set to 0, the server no longer receives new requests. |
|  | A note indicates supplemental instructions, best practices, tips, and other content. |  **Note:**<br>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]` |

| Style | Description | Example |
| --- | --- | --- |
| **{} or {a\|b}** | **This format is used for a required value, where only one item can be selected.** | `switch {active\|stand}` |

# Contents

# 1 QoS policy overview

**This topic provides an overview of the Quality of Service (QoS) policy function of Smart Access Gateway (SAG). You can set QoS policies based on a quintuple (including protocol, source IP address, source port, destination IP address, and destination port) to differentiate traffic from different services and guarantee the bandwidth of important services.**

**QoS can improve the quality of a network by ensuring a sufficient bandwidth and reducing latency, packet loss, and jitter.**

**If you have multiple stores and each store has multiple service systems, such as ERP , order, and OA. All these systems and stores consume bandwidth. The bandwidth for important services cannot be guaranteed and packets may be lost.**

**To solve this issue, you can set QoS policies to allocate network resources based on the characteristics of different services and make better use of the network resources.**

## QoS policy configuration process

**The process for configuring a QoS policy is as follows:**

1. **Create a QoS policy, including setting a speed limiting rule for traffic of different priorities and specify the traffic to which the speed limiting rule applies. For more information, see** *Create a QoS policy*.
2. **Apply the QoS policy to an SAG instance. For more information, see** *Associate a QoS policy with an SAG instance*.

## Note

**Note the following before you configure a QoS policy:**

- **After a QoS policy is applied to an SAG instance, it only limits the speed of outbound traffic, not inbound traffic.**
- **The five parameters included in quintuples of different QoS policies cannot be the same.**
- **There is no limit on the maximum and minimum bandwidth.**

## Limits

**QoS policies have the following limits:**

- **By default, an account can create up to 10 QoS policies. To increase the quota,** *open a ticket*.
- **By default, up to 50 quintuples can be created for each QoS policy. To increase the quota,** *open a ticket*.
- **By default, up to three speed limiting rules can be created for each QoS policy. You can** *open a ticket* **to apply for a maximum of seven rules.**
- **By default, each SAG instance can be associated with one QoS policy. The quota cannot be adjusted.**

# 2 Create a QoS policy

**This topic describes how to create a Quality of Service (QoS) policy. When you create a QoS policy, you need to set one or more speed limiting rules, priorities of the rules, and quintuples (including the protocol type, source CIDR block, source port, destination CIDR block, and destination port).**

**Procedure**

1. **Log on to the** *Smart Access Gateway console*.
2. **In the left-side navigation pane, click QoS Policies.**
3. **On the QoS Policies page, click Create QoS Policy.**
4. **On the displayed Create QoS Policy page, set the name of the QoS policy and the speed limiting rule.**

   **Configure the QoS policy according to the following information:**

| Parameter | Description |
| --- | --- |
| **Basic information** | |
| **Name** | **Enter a name for the QoS policy. The name must be 2 to 100 characters in length and start with a letter. It can contain numbers,** `periods (.)`, `hyphens (-)`, **and** `underscores (_)`.<br><br>**Note:**<br>**Each account can create up to ten QoS policies. To increase the quota,** *open a ticket*. |
| **Description** | **Enter a description for the QoS policy.** |
| **Speed limiting rule** | |
| **Note:**<br>**You can create up to three speed limiting rules for each QoS policy. You can** *open a ticket* **to apply for a maximum of seven rules.** | |

| Parameter | Description |
| --- | --- |
| Priority | Set the priority of the speed limiting rule.<br>Value range: 1 to 3. A greater value indicates a higher priority. |
| Speed Limiting Method | Two speed limiting methods are provided:<br>· By percentage: The bandwidth of target packets is guaranteed to be in a specified percentage range of the total bandwidth. If you select this method, you must select the bandwidth type. This method applies to the scenario where many stores are involved and have different bandwidths.<br>For example, if the total outbound bandwidth of the WAN is 20 Mbit /s, you can set the maximum bandwidth percentage to 95% and the minimum bandwidth percentage to 20%.<br>· By bandwidth: The bandwidth of target packets is guaranteed to be in a specified bandwidth range.<br>If you select this method, you do not need to select the bandwidth type. |
| Stream Classification Rule: the rule used to divide the traffic of your service. The rule is a quintuple that includes five parameters: the transport layer protocol, source CIDR block, source port, destination CIDR block, and destination port. | |

| Parameter | Description |
| --- | --- |
| Name | Enter a name for the quintuple.<br>The name must be 2 to 100 characters in length and must start with a letter. It can contain numbers, `periods (.)`, `hyphens (-)`, and `underscores (_)`.<br>**Note:**<br>You can create up to 50 quintuples for each QoS policy. To increase the quota, *open a ticket*. |
| Description (optional) | The description of the quintuple. |
| Protocol Type | Select the transport layer protocol of the traffic whose bandwidth needs to be guaranteed. |
| Source CIDR Block | Enter the CIDR block that initiates the access. |
| Source Port | Enter the source port of the transport layer.<br>Value range: 1 to 65535.<br>Format: start port/end port, for example, `1/200` or `80/80`. |
| Destination CIDR Block | Enter the destination CIDR block to be accessed. |
| Destination Port | Enter the destination port of the transport layer.<br>Valid values: 1 to 65535.<br>Format: start port/end port, for example, `1/200` or `80/80`. |
| Validity Period | Set the start and end dates. The quintuple rule takes effect only during the period from the start data to the end date. |

5. Click OK.

# 3 Associate a QoS policy with an SAG instance

**This topic describes how to associate a QoS policy with an SAG instance. After you create a QoS policy, you must associate it with a Smart Access Gateway (SAG) instance.**

**Procedure**

1. **Log on to the** *Smart Access Gateway console*.
2. **In the left-side navigation pane, click QoS Policies. Find the target QoS policy and click Bind instance in the Actions column, or click the QoS policy ID. On the displayed page, click the Associated Instances tab, and then click Bind instance.**
3. **Select the SAG instance to be associated with the QoS policy.**
4. **Click Confirm.**

> **Note:**
> **Each SAG instance can be associated with only one QoS policy.**