ALIBABA CLOUD

Alibaba Cloud

CDN

Domain Management

Document Version: 20200828

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.Features

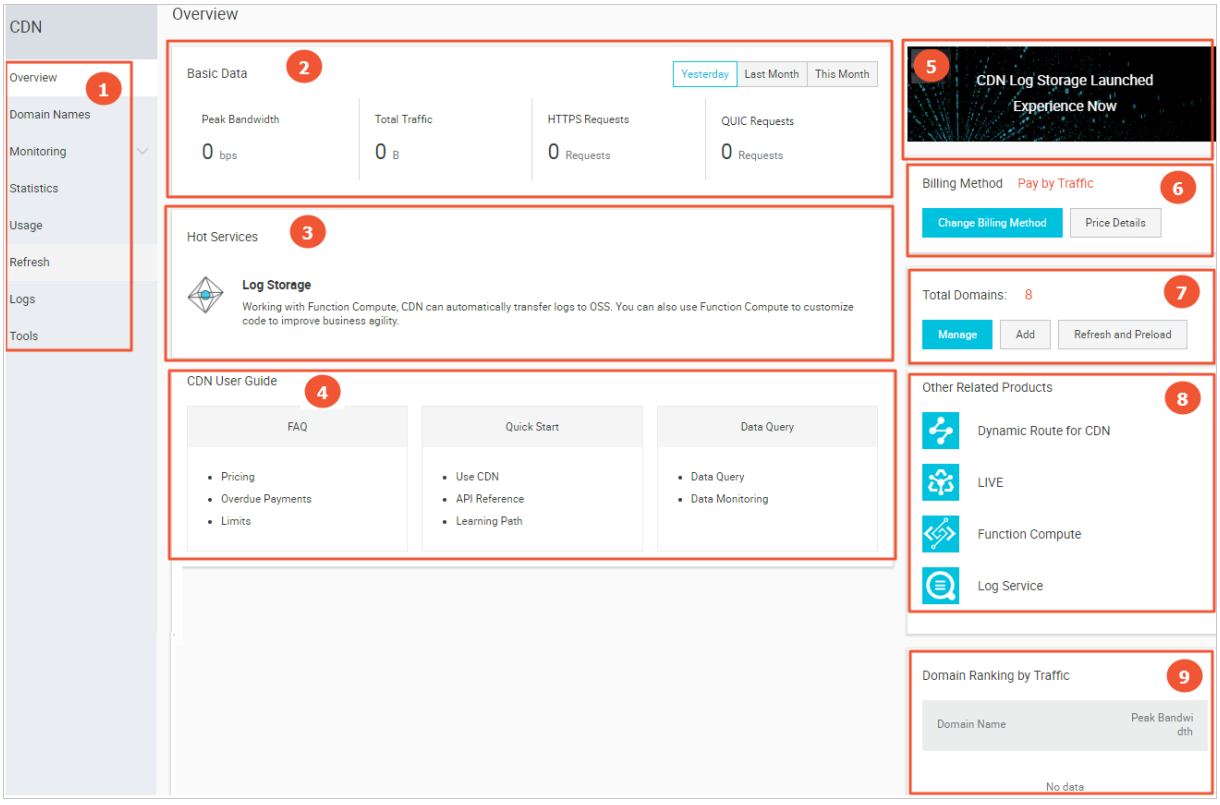
In the Alibaba Cloud Content Delivery Network (CDN) console, you can configure domain names and complete other basic operations. You can also view resource monitoring data and analyze data in real time. The CDN console provides your billing information and allows you to change the billing method at any time. This topic describes the CDN console and the domain management features.

Alibaba Cloud CDN libraryCDN listPage options provided by CDN

> **Note** To help you understand and obtain up-to-date information about CDN, this topic divides the features in the CDN console into domain management and service management according to your business needs.

Console guide

The following figure shows the CDN console interface.



The following table describes the CDN console interface.

No.	Element	Description
1	Left-side navigation pane	Displays the navigation pane for domain management. For more information, see Domain management features.
2	Basic Data	Displays the usage status of each billing item based on the billing method of your CDN service. For more information, see Basic service billing.

No.	Element	Description
3	Hot Services	Shows you how to access the frequently used CDN features.
4	CDN User Guide	Displays the links of the CDN help documents. For more information, see CDN Learning Path.
5	Billing Method	Displays the billing method you have selected. You can also modify the billing method as needed. For more information, see Basic service billing and Value-added service billing.
6	Resource Plans	Displays the resource plans you have purchased. For more information, see Resource plans.
7	Total Domains	Allows you to manage the existing domains, add domains, and perform the refresh or prefetch operation.
8	Other Related Products	Displays CDN-related products.
9	Domain Ranking by Traffic	Displays top five accelerated domains ranked by network traffic.

Domain management features

The following table lists the accelerated domain management features.

Feature	Reference	Description	Default value
Copy configurations	Copy configurations	Allows you to copy one or more configurations of an accelerated domain to another one or more accelerated domains.	None
Alert settings	Set an alert rule	Monitors accelerated domains by using the following metrics: peak bandwidth, proportions of HTTP status codes 4xx and 5xx, hit rate, Internet outbound traffic, and queries per second (QPS). This allows CloudMonitor to send an alert message through SMS or email based on the settings in the CDN console. This alert message is generated according to an alert rule.	None
Tag management	Attach tags to a domain name	Allows you to add tags to a domain name or group domain names by tags.	None
	Manage domain names by tag	Allows you to use tags to filter domain names for group management.	None
	Query domain names by tag	Allows you to use tags to filter domain names for data query.	None
Basic information	Modify basic information	Allows you to modify the accelerated region.	None

Feature	Reference	Description	Default value
Basic information settings	Configure an origin server	Allows you to modify the origin information.	None
Back-to-origin settings	Configure an origin host	Allows you to modify the domain name of the origin host.	Enabled
	Configure the origin protocol policy	Allows CDN to communicate with your origin according to the specified origin protocol policy. If you specify the Follow policy, CDN communicates with your origin over HTTP or HTTPS, depending on the protocol of the client request.	Disabled
	Enable private bucket back-to-origin authorization	Grants CDN permissions to access the specified private Object Storage Service (OSS) bucket that serves as the origin.	Disabled
	Configure an origin SNI	Allows you to set a Server Name Indication (SNI) value to specify the requested domain name in an HTTPS back-to-origin request. You must enable this feature when the IP address of the origin server is mapped to multiple domain names.	Disabled
	Customize an HTTP header	Allows you to add or remove HTTP headers when CDN communicates with the origin over HTTP.	Disabled
	Set the origin request timeout	Allows you to set the maximum amount of time that CDN waits for a response after it redirects a request to the origin. If CDN does not receive a response before the timeout period expires, the connection between the CDN node and the origin is terminated.	30 seconds
Cache settings	Create a cache expiration rule	Allows you to customize cache expiration rules for specified resources.	None
	Create a status code expiration rule	Allows you to customize the expiration rules for the status codes of the resources in the specified directories or with the specified file extensions.	None
	Create an HTTP header	Allows you to customize HTTP request headers. CDN provides 10 HTTP request header parameters for customization.	None
	Customize an error page	Allows you to customize a complete URL to redirect for an HTTP or HTTPS response code.	404
	Configure a rewrite rule	Allows you to modify a request URI and perform a 302 redirect to the specified target URI.	None

Feature	Reference	Description	Default value
HTTPS secure acceleration	Configure an SSL certificate	Provides an end-to-end HTTPS secure acceleration solution. You can enable the secure acceleration mode and upload the certificate and private key for an accelerated domain. This feature also allows you to view, disable, enable, or modify certificates.	Disabled
	Enable HTTP/2	Enables the binary protocol HTTP/2 to provide multiple benefits including scalability, security, multiplexing, and header compression.	Disabled
	Enable force redirect	Redirects requests from clients to L1 nodes as HTTP or HTTPS requests if HTTPS secure acceleration is enabled.	Disabled
	Configure TLS	Enables the TLS handshake for the accelerated domain after a TLS protocol version is enabled. Only TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 are supported.	Disabled
	Configure HSTS	HTTP Strict Transport Security (HSTS) is used to force clients such as browsers to use HTTPS to connect to the server.	Disabled
Access control	Configure hotlink protection	Allows you to configure a referer blacklist or whitelist to identify and filter visitors.	Disabled
	Configure URL signing	Allows you to configure URL signing to prevent unauthorized downloads of and access to the resources on the origin server.	Disabled
	Configure an IP address blacklist or whitelist	Allows you to configure an IP address blacklist or whitelist to identify and filter visitors.	Disabled
	UA blacklist and whitelist	Allows you to configure a User-Agent blacklist or whitelist to identify and filter visitors.	Disabled
Performance optimization	HTML optimization	Compresses and removes HTML redundant content, such as blank lines and carriage return characters, to reduce the file size.	Disabled
	Intelligent compression	Supports intelligent compression for content in multiple formats to reduce the size of transmitted content.	Disabled
	Configure Brotli compression	Compresses static text files. This reduces the size of transmitted content and accelerates content delivery.	Disabled

Feature	Reference	Description	Default value
	Parameter filtering	Specifies whether CDN retains parameters that follow a question mark (`?`) in the URL of a back-to-origin request. You can enable this feature when the URL includes a question mark and *parameters*.	Disabled
Advanced settings	Configure bandwidth cap	Allows you to specify a maximum bandwidth value. If the average bandwidth measured at five-minute intervals exceeds the maximum bandwidth, the accelerated domain is disabled automatically. This can protect the accelerated domain. In this case, all requests are redirected to the origin server.	Disabled
Video-related settings	Object chunking	Reduces the consumption of back-to-origin network traffic and shortens resource response time.	Disabled
	Video seeking	Allows you to drag and drop the playback progress of an audio or video file and ensures the playback quality.	Disabled
	Configure audio or video preview	Allows you to preview audio and video content.	Disabled
	Audio extraction	Allows you to request audio data from a video file. With this feature enabled, a CDN node extracts audio data from a video file and returns the audio data to the client. This reduces network traffic usage.	Disabled
IPv6	Configure IPv6 settings	Allows IPv6 clients to send requests to CDN over IPv6. CDN can also include the IPv6 information of the clients in back-to-origin requests.	Disabled

2.Copy configurations

This topic describes how to copy one or more configurations from a source domain to one or more target domains.

Copy Content Delivery Network (CDN) configurations

Prerequisites

Make sure that the source domain has been enabled and configured.

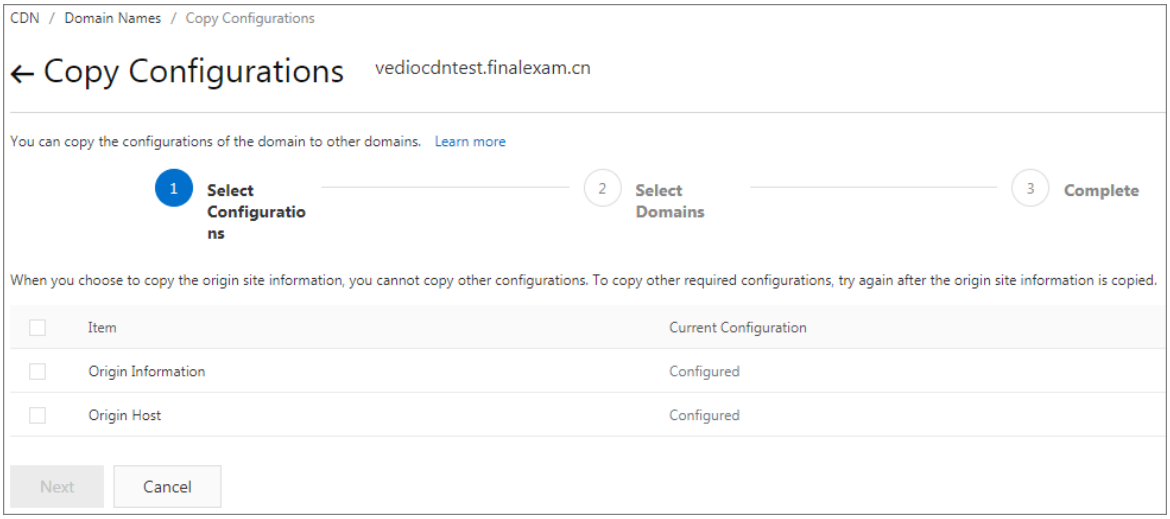
Context

Note the following points when you copy the configurations of the source domain:

- The copy operation cannot be undone. Make sure the configurations are correct before you copy them.
- Exercise caution when you copy the configurations of domain names that have high network traffic or bandwidth to avoid unexpected fees caused by high network traffic.
- Non-standard backend configurations that are implemented through the ticketing system cannot be copied.

Procedure

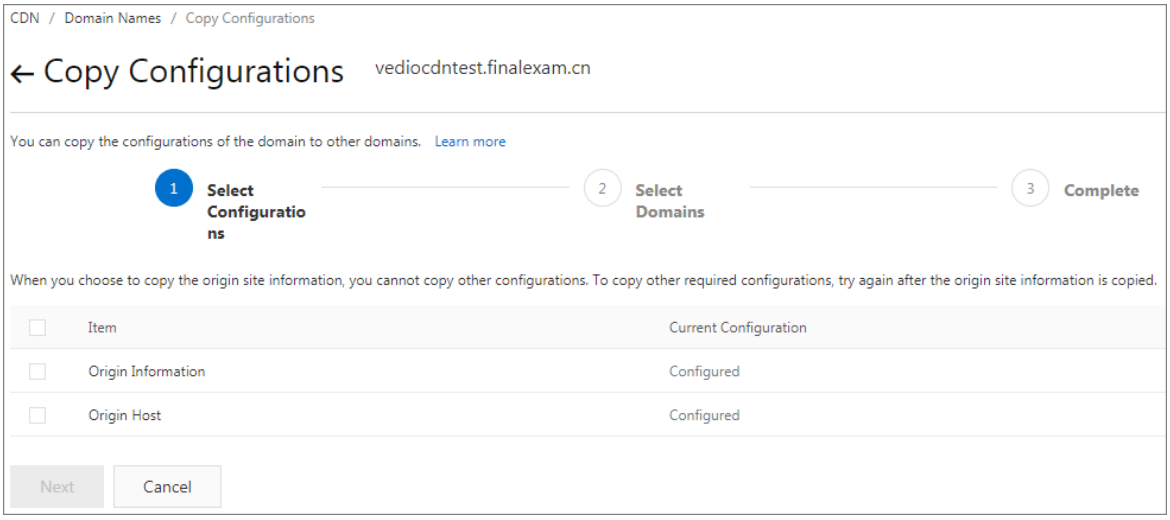
1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the source domain, and click **Copy Configurations**.



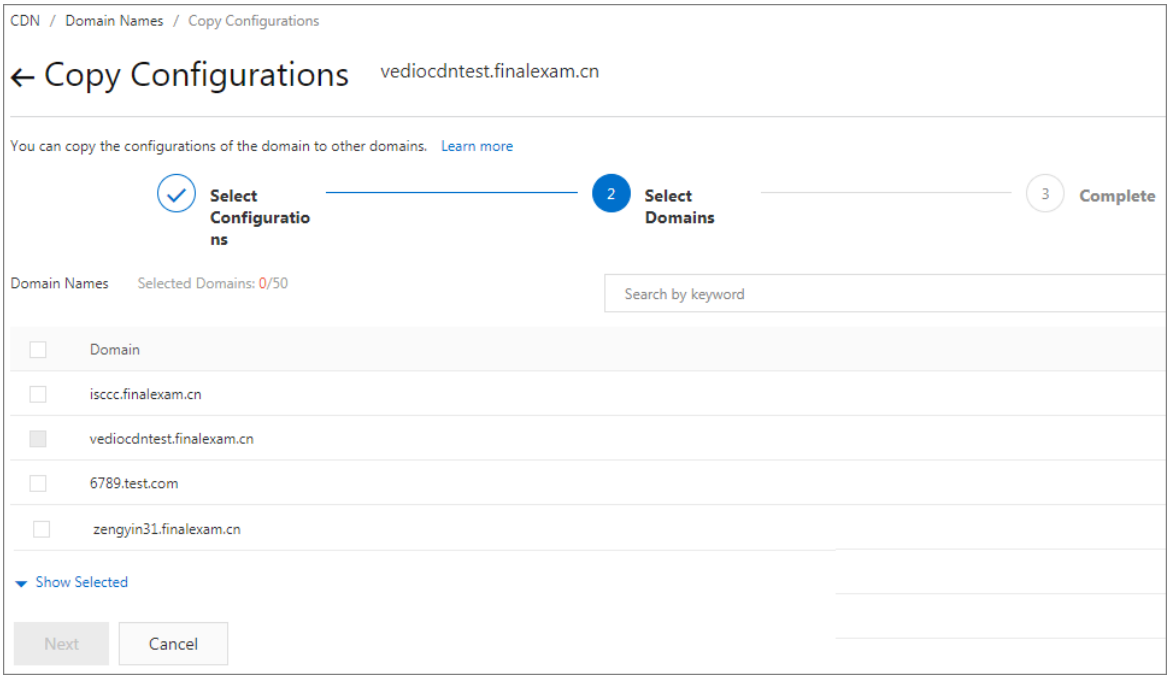
4. Select the configurations you want to copy, and click **Next**.

Note

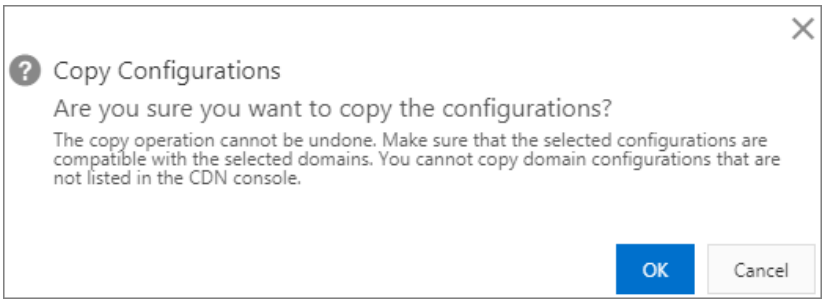
- The Origin Information item cannot be copied at the same time as the other items.
- HTTPS certificates cannot be copied.
- The rules of Custom HTTP Origin Header are copied from the source domain and added to the existing rules of the target domain. For example, if Domain A has two rules of Custom HTTP Origin Header and you copy another five rules of Custom HTTP Origin Header from Domain B to Domain A, Domain A will have a total of seven rules of Custom HTTP Origin Header.
- The rules of HTTP Header are copied from the source domain and overwrite the existing rules of the target domain. For example, if the cache_control HTTP header is set to private for Domain A and to public for Domain B and you copy the HTTP header configuration of Domain B to Domain A, the cache_control HTTP header of Domain A is set to public.
- If you copy switch-related configurations, the new configurations overwrite the existing configurations of the target domains.
- Copied blacklists or whitelists of referers or IP addresses also overwrite the existing configurations of the target domains.



5. **Select the target domains, and click Next. You can enter a keyword in the search bar to search for a domain.**



6. In the **Copy Configurations** dialog box, click **OK**.



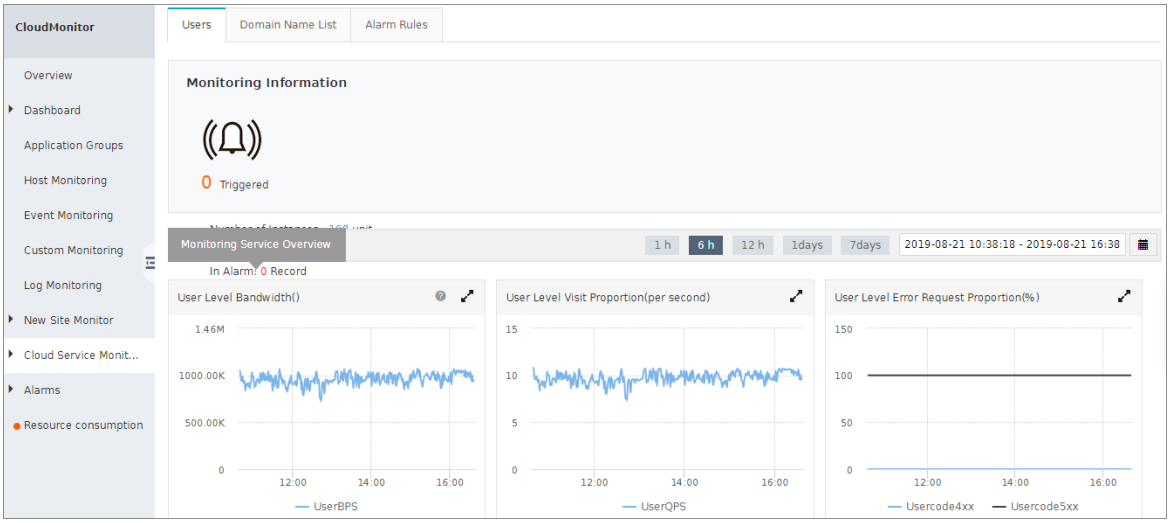
3.Set an alert rule

This topic describes how to create an alert rule in the Alibaba Cloud CDN console. You can use CloudMonitor to set alert rules specific to CDN domain metrics. When an alert rule is triggered, CloudMonitor sends an alert by using the specified notification method (for example, SMS or email).

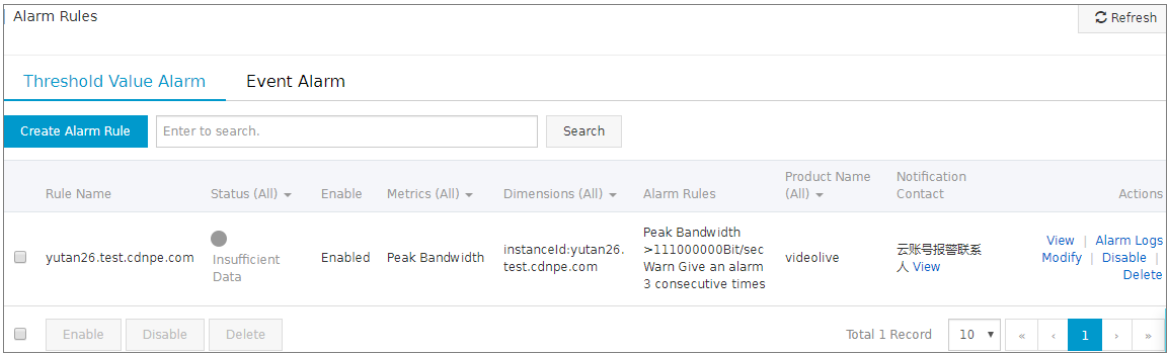
Alert rules CDN

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, click **Alert Settings** to go to the CloudMonitor console.



4. Choose **Cloud Service Monitoring > CDN**, and click the **Alert Rules** tab.
5. Click **Create Alert Rule**.



6. Create a CDN alert rule. For more information, see Create a threshold-triggered alert rule.

4.Tags

4.1. Tag overview

This topic provides an overview of domain name tags. Each tag is represented by a string of characters. In Alibaba Cloud CDN, you cannot define tags, but you can attach tags to domain names, detach tags from domain names, and use tags to group or filter domain names.

manage tags attach tags detach tags

Limits

- Each tag is a key-value pair (`Key:Value`), which consists of a key and a value.
- Up to 20 tags can be attached to a domain name.
- For the same domain name, the key for each tag must be unique. If two tags have the same key but different values, the current tag overwrites the previous tag. For example, if you configure the `Key1:Value1` tag and then the `Key1:Value2` tag for the `test.example.com` domain name, only the `Key1:Value2` tag is attached to the domain name.
- A key cannot start with *aliyun* or *acs*, contain `http://` or `https://` , or be left unspecified.
- A value cannot contain `http://` or `https://` , but can be left unspecified.
- A key can contain up to 64 Unicode characters.
- A value can contain up to 128 Unicode characters.
- Tags are case-sensitive.

Functions

You can use tags to perform the following operations:

- Attach tags to domain names to identify or group the domain names. For more information, see Attach tags.
- Detach tags from domain names. For more information, see Detach tags.
- Manage domain names based on their tags. For more information, see Manage domain names by tag.
- Query the domain names to which specific tags are attached. For more information, see Filter domain names by tag.

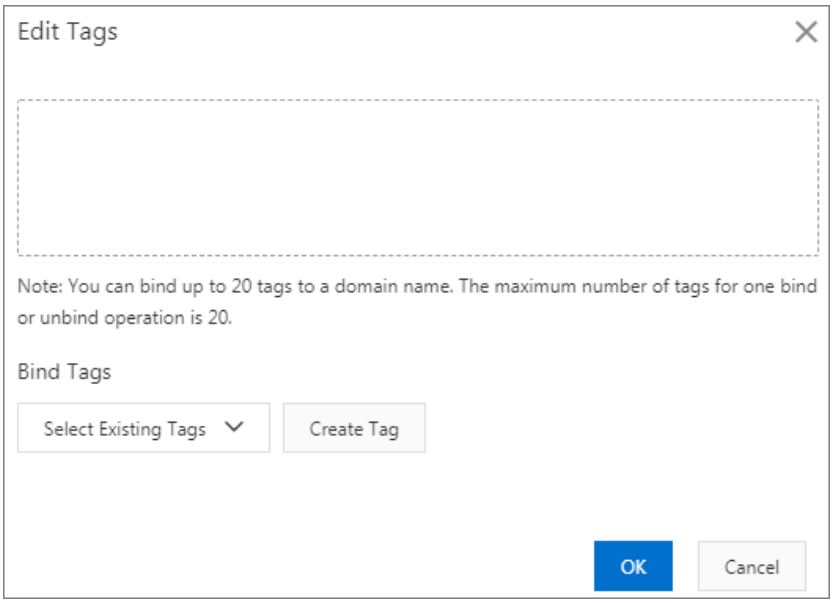
4.2. Attach tags to a domain name

If you want to identify and group domain names, you can attach tags to domain names.

Edit tags Domain names

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the domain name for which you want to set tags, and move the pointer over the corresponding icon in the Tags column.
4. Click **Edit**.



5. In the **Edit Tags** dialog box, click **Select Existing Tags** or **Create Tag** to attach tags to the domain name.
6. Click **OK**.

API

You can call API operations to attach tags to domain names. For more information, see TagResources.

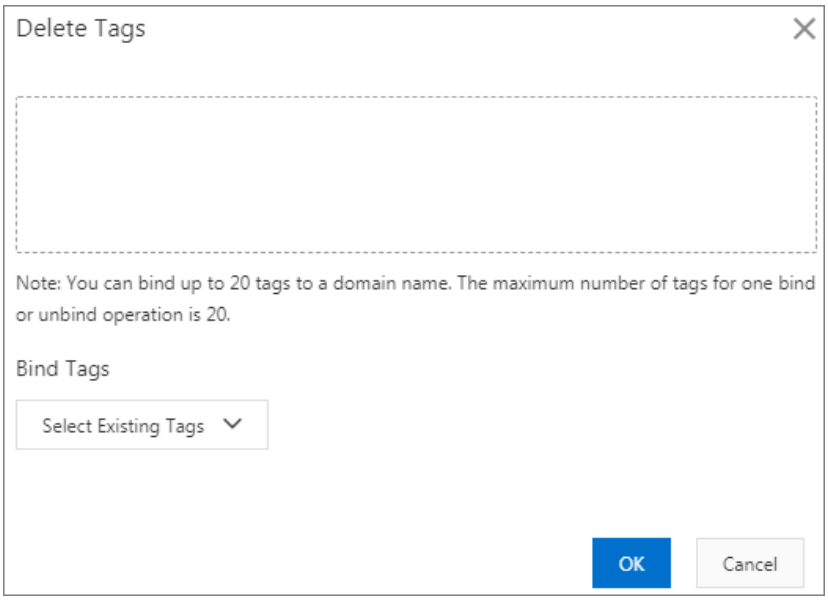
4.3. Detach tags from a domain name

If the tags no longer apply to one or more domain names, you can detach these tags from the corresponding domain names.

Detach tags from a domain name CDN

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the Domain Names page, find the domain name for which you want to delete tags, and choose **Manage Tags** > **Delete Tags**.
4. In the **Delete Tags** dialog box, select the tags to be deleted, and click **OK**.



API

You can call API operations to detach tags from domain names. For more information, see UntagResources.

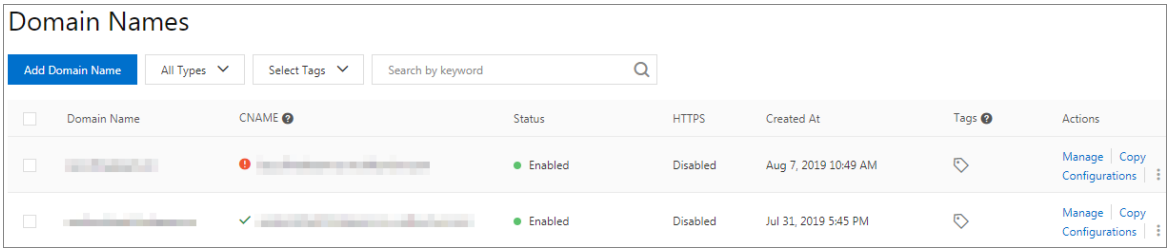
4.4. Manage domain names by tag

After attaching tags to domain names, you can use the tags to quickly filter the corresponding domain names and manage these domain names by group.

Tags

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, select tags from the **Select Tags** drop-down list.



API

You can call API operations to manage domain names by their tags. For more information, see DescribeTagResources.

4.5. Query domain names by tag

If you want to query the data of some domain names, you can use tags to quickly filter the corresponding domain name and query the data after attaching tags to domain names.

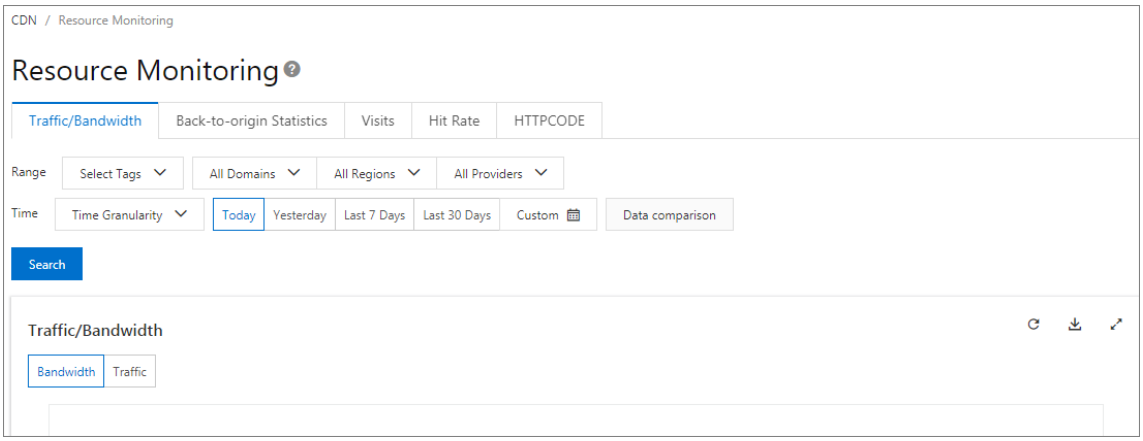
Query domain names Tags

Procedure

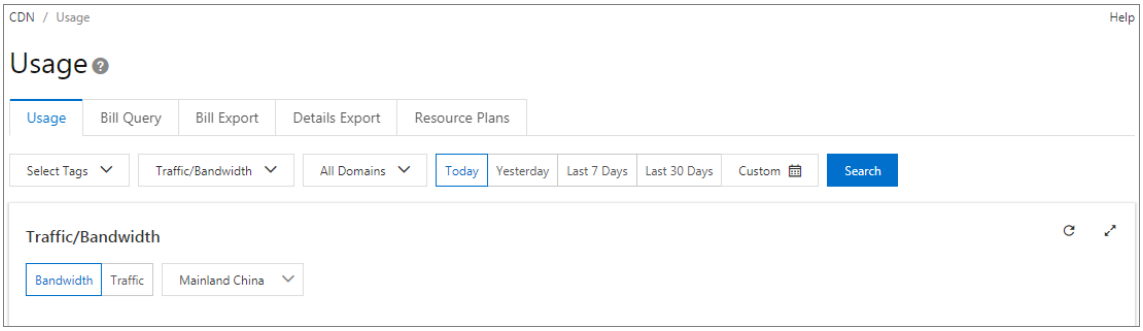
1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. You can use one of the following methods to query the domain names to which specific tags are attached:

   > **Note** If you select multiple tags, only the domain names that contain all the selected tags are returned by the system.

   - In the left-side navigation pane, choose **Monitoring > Resource Monitoring**. In the main workspace, select tags from the Select Tags drop-down list and click **Search**.



   - In the left-side navigation pane, click **Usage**. In the main workspace, select tags from the Select Tags drop-down list and click **Search**.



4.6. Tag use case

This topic describes how to group and manage domain names with tags by using the example of attaching tags to manage domain names.

attach tags manage domain names
Assume the following scenario as a use case for tags. A company has 100 domain names on Alibaba Cloud CDN. These domain names are used by three departments (E-commerce, Gaming, and Entertainment) to supply marketing, gaming (specially for example games A and B), and post-production services. Each department has an executive, whose names are Bob, John, and Tom, respectively.

Define tags

This company defines the following tags, each of which consists of a key and a value. These are used to make grouping and managing domain names easier.

Key	Value
Department	E-commerce, Gaming, and Entertainment
Services	Marketing, Gaming (Games A and B), and Post-production
Executive	Bob, John, and Tom

The company can attach the preceding keys and values to its corresponding domain names.

Use tags to query domain names

- If the company wants to query the domain names that are managed by Tom, it can select the **Executive: Tom** tag.
- If the company wants to query the domain names that are managed by John from the Gaming department, it can select the **Department: Gaming** and **Executive: John** tags.

5.Basic settings

5.1. Overview

On the Basics page of a CDN domain, you can view the corresponding basic information and origin information. You can also modify the region and origin information of the CDN domain.

Change region Origin configuration Content Delivery Network (CDN)

Billing

- If you set the origin type to **IP** or **Origin Domain**, you are charged according to the Internet traffic price.
- If you set the origin type to **OSS Domain**, CDN will redirect the requests to the specified OSS bucket. Therefore, you are charged according to the internal traffic price. For more information, see OSS pricing.
- If you set the origin type to **Origin Domain** and specify the domain name of an OSS bucket, you are still charged according to the Internet traffic price.

Features

You can perform the following basic configurations:

- Modify basic information to change the acceleration region of your CDN service.
- Configure an origin server to modify origin information, including origin type, origin address, and port.

5.2. Modify basic information

You can change the acceleration region of your CDN service.

Region CDN

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the **Basic Information** section, click **Modify**.
5. In the **Region** dialog box, select the region you want to switch to.

   When you select a region, note the following:

   - Mainland China

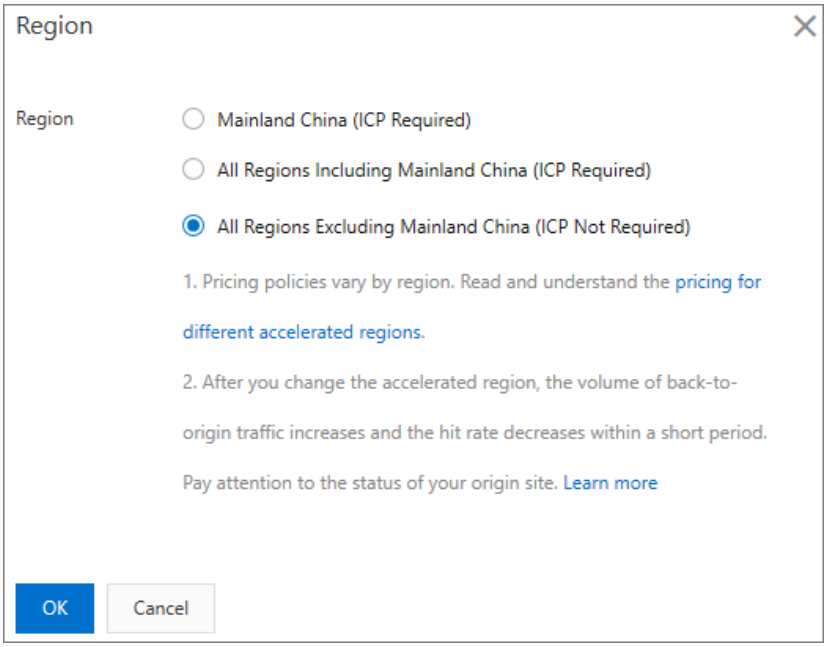
     If you select Mainland China, you must apply for an Internet content provider (ICP) filing with the Ministry of Industry and Information Technology (MIIT) of China. For more information, see Domain filing.

   - Global

     If you select Global, you must apply for an ICP filing with the MIIT of China. For more information, see Domain filing.

   - Outside Mainland China

     If you select Outside Mainland China, no ICP filing is required.



6. Click **OK**.

5.3. Configure an origin server

This topic describes how to modify the information about an origin server in the Alibaba Cloud Content Delivery Network (CDN) console.

origin domain nameCDN

Context

> **Notice** When you modify the information about an origin server, if you set **Origin Information** to **OSS Domain**, **IP**, or **Site Domain**, you can specify a custom port that redirects requests to the origin server. Alibaba Cloud CDN redirects only HTTP requests to origin servers over custom ports.

Alibaba Cloud CDN supports the following types of origin server: Object Storage Service (OSS) endpoints, IP addresses, domain names of origin servers, and Function Compute domain names. If you set Origin Info to IP or Site Domain, you can specify one or more IP addresses or domain names and set the priority for each IP address or domain name.

> **Note** Layer-4 health checks are performed on origin servers. Port 80, port 443, or custom ports of origin servers are probed. Probes are sent at an interval of 2.5 seconds. If an origin server fails three consecutive probes, the system marks the origin server as unavailable.

Alibaba Cloud CDN supports switchover between primary and secondary origin servers. If multiple origin servers are configured, Alibaba Cloud CDN redirects requests to the origin server whose **Priority** is **Primary**. If the primary origin server fails three consecutive probes, Alibaba Cloud CDN forwards requests to the origin server whose **Priority** is **Secondary**. If the primary origin server passes the health check, the system marks the origin server as available and restores the priority of this origin server to primary. If you set the same priority for all origin servers, Alibaba Cloud CDN automatically redirects requests to the origin servers based on the round robin scheme.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the **Origin Information** section, click **Modify**.
5. In the **Modify Origin Information** dialog box, set the origin type, origin address, and port.

   The following table lists the parameters that you must set.

   - Origin Info

Origin type	Description
IP	You can specify the public IP addresses of one or more servers. If your origin servers are Alibaba Cloud Elastic Compute Service (ECS) instances, review of the IP addresses is not required. For more information, see What is ECS?

Origin type	Description
Site Domain	You can specify the domain names of one or more origin servers. Note The origin domain name that you specified cannot be the same as the accelerated domain name. Otherwise, a DNS resolution loop occurs, and the requests cannot be redirected to the origin server correctly. For example, if the domain name of your origin server is img.yourdomain.com, you can set the accelerated domain name to cdn.yourdomain.com.
OSS Domain	You can enter the public endpoint of an OSS bucket, for example, xxx.oss-cn-hangzhou.aliyuncs.com. To view the public endpoint of an OSS bucket, go to the OSS console. You can also directly select an OSS bucket under the current account.
Function Compute Domain	If you choose to specify a Function Compute domain name, you must set the Region and Domain Name parameters. For more information, see Set a Function Compute domain name.

- **Port**

Port	Description
Port 80	Alibaba Cloud CDN retrieves resources from your origin server by using port 80 over HTTP or HTTPS.
Port 443	Alibaba Cloud CDN retrieves resources from your origin server by using port 443 over HTTP or HTTPS. If the IP address of your origin server is associated with multiple domain names, you must configure an origin Server Name Indication (SNI). For more information, see Configure an origin SNI.
Custom Port	Alibaba Cloud CDN redirects only HTTP requests to origin servers over custom ports. If you need to redirect HTTPS requests to origin servers over custom ports, submit a ticket. Notice If you specify a custom port, disable the origin protocol policy. Otherwise, the specified port cannot work as expected. For more information, see Configure the origin protocol policy. If the origin server is an OSS bucket, OSS determines whether you can specify a custom port.

6. Click **OK**.

6.Back-to-origin settings

6.1. Overview

When you send a resource access request from a client, if CDN cannot find the resource on the CDN node, it retrieves the resource from the origin and then loads the resource to the CDN node. You can configure back-to-origin functions to accelerate access to CDN resources.

CDN supports the following back-to-origin functions.

Function	Description
Configure an origin host	Allows you to specify the domain type of the origin host for CDN nodes retrieving resources from the origin.
Configure the origin protocol policy	Allows you to configure an origin protocol policy for retrieving resources from the origin to CDN nodes when CDN cannot find the resources on CDN nodes.
Enable private bucket back-to-origin authorization	Allows you to use private Object Storage Service (OSS) buckets as origins in order to prevent resource hotlinking.
Disable private bucket back-to-origin authorization	You can log on to the RAM console and remove authorization from a specified role to disable private bucket access.
Configure an origin SNI	If CDN nodes access your origin over HTTPS and your origin IP address is bound to multiple domain names, then you must select a domain name for CDN by specifying the Server Name Indication (SNI) of the domain name.
Customize an HTTP header	If you configure CDN to use HTTP to communicate with your origin, you can add or remove HTTP header fields.
Set the origin request timeout	The default timeout period for a resource request sent from a CDN node to an origin is 30 seconds. You can customize the timeout period. If the CDN node does not receive any response before the timeout period expires, the CDN node disconnects from the origin.

6.2. Configure an origin host

If you want to customize the domain of the server to which CDN initiates back-to-origin requests, you must configure the domain type of the origin host. The domain types available for an origin host are CDN domain, origin domain, and custom domain.

Origin host CDN node back-to-origin

Context

An origin host is the domain of the origin server to which CDN initiates back-to-origin requests.

> Note If your origin is bound to multiple domains or servers, you must specify the domain to which the back-to-origin requests are sent. Otherwise, the back-to-origin process fails.

Differences between an origin and an origin host:

- An origin determines the specific IP address to which CDN initiates back-to-origin requests.
- An origin host determines the requested domain associated with a specific IP address to which CDN initiates back-to-origin requests.

Default settings for the origin host:

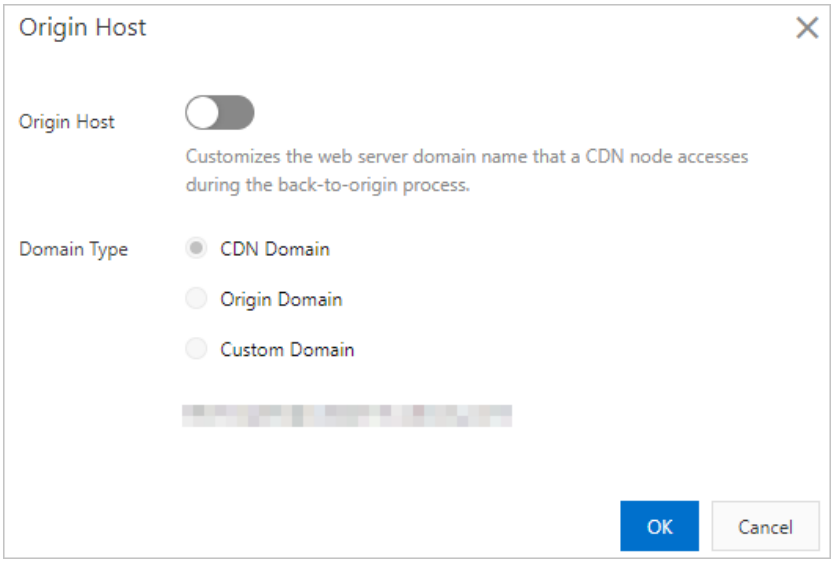
- If your origin type is **IP**, the default domain type of your origin host is **CDN Domain**.
- If your origin type is **OSS Domain**, the default domain type of your origin host is **Origin Domain**.

Examples:

- If your origin is `www.a.com` and your origin host is `www.b.com`, CDN initiates back-to-origin requests to the IP address obtained by resolving `www.a.com`, but the requested domain is `www.b.com`.
- If your origin is `1.1.1.1` and your origin host is `www.b.com`, CDN initiates back-to-origin requests to `1.1.1.1`, which maps the `www.b.com` origin server on the host.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. In the **Origin Host** section, click **Modify**.
6. Turn on **Origin Host**, and set **Domain Type**.



7. Click **OK**.

6.3. Configure the origin protocol policy

If a client requests for resources that are not cached on a CDN node, the node fetches these resources from the origin based on the origin protocol policy and caches these resources on the node. This topic describes how to configure the origin protocol policy.

CDN back-to-origin Static protocol Dynamic protocol

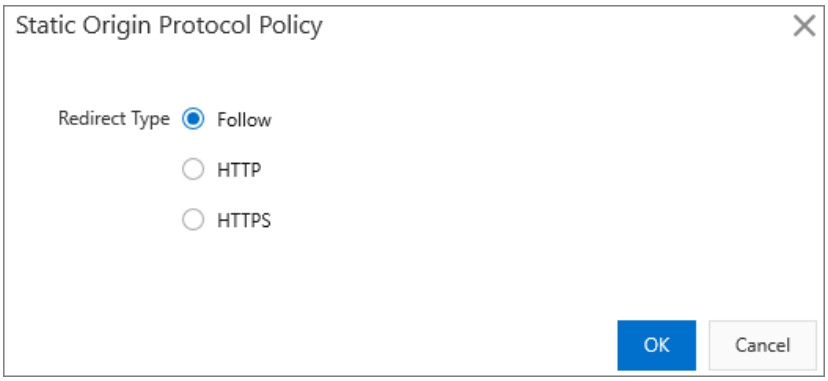
Context

When origin protocol policy is enabled, back-to-origin requests for resources use the same protocol that is used by the client to request resources. If the client sends an HTTPS request to access resources that are not cached on a CDN node, the node uses the same HTTPS protocol to request for resources from the origin. This origin protocol policy also applies to HTTP requests.

> **Note** The origin must support both port 80 and port 443. Otherwise, the back-to-origin process may fail.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. In the **Origin Protocol Policy** section, turn on **Origin Protocol Policy**.
6. Click **Modify**.



7. In the **Static Origin Protocol Policy** dialog box, set Redirect Type to **Follow**, **HTTP**, or **HTTPS** as needed.
   - Follow: If the client sends HTTP or HTTPS requests to access resources on CDN, CDN uses the same protocol to request for resources from the origin.
   - HTTP: CDN initiates back-to-origin requests only over HTTP.
   - HTTPS: CDN initiates back-to-origin requests only over HTTPS.
8. Click **OK**.

6.4. Enable private bucket back-to-origin authorization

If your origin is Alibaba Cloud OSS, you can grant permissions to CDN domains to access the private OSS bucket to prevent resource hotlinking. This topic describes how to enable private bucket back-to-origin authorization.

OSS domain Private bucket CDN back-to-origin

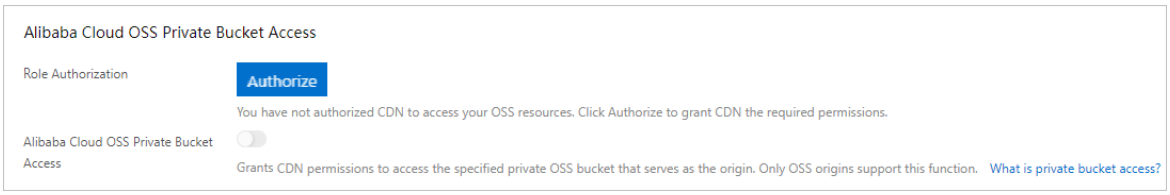
Context

You can use functions such as the referer hotlink protection and authentication provided by Alibaba Cloud CDN to protect resource security. For more information, see Configure hotlink protection and Configure URL signing.

> **Notice**
>
> - Only CDN domains that use OSS as the origin are allowed to enable private bucket back-to-origin authorization.
> - Once back-to-origin authorization is performed, CDN is granted the read-only permissions to access all your buckets.
> - After back-to-origin authorization is performed and enabled for a specific CDN domain, the domain can access the resource content in your private bucket. Use caution when you decide whether to enable this function. If the content in the private bucket to be authorized is not suitable to function as the back-to-origin content of the CDN domain, do not perform authorization or enable the function.
> - If your website is at risk of attacks, note the following precautions:
>   - Make sure that you purchase Anti-DDoS Pro.
>   - Make sure that you do not perform or enable private bucket back-to-origin authorization.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. In the **Alibaba Cloud OSS Private Bucket Access** section, click **Authorize**.



6. Click **Confirm**.
7. In the **Alibaba Cloud OSS Private Bucket Access** section, turn on **Alibaba Cloud OSS Private Bucket Access**. For more information, see Disable private bucket back-to-origin authorization.

6.5. Disable private bucket back-to-origin authorization

This topic describes how to revoke access permissions on your private bucket from an origin domain. You can revoke permissions for the corresponding roles to disable private bucket back-to-origin authorization in the Resource Access Management (RAM) console.

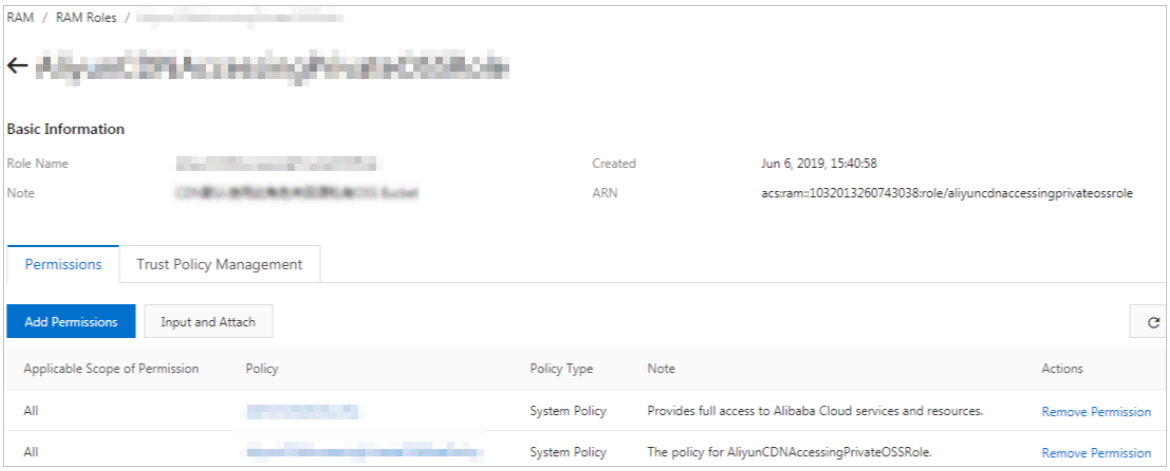
Back-to-origin authorization Private bucket

Context

> **Note** If your CDN domain uses your private bucket as its origin, do not disable or delete this authorization method.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click RAM role name **AliyunCDNAccessingPrivateOSSRole**.



4. Click **Remove Permission** in the Actions column corresponding to the RAM role to be deleted. In the Remove Permission dialog box, click **OK**.
5. Return to the **RAM Roles** page, click **Delete** in the Actions column corresponding to the RAM role to be deleted.

   In the **Delete RAM Role** dialog box, click **OK**.

6.6. Configure an origin SNI

If your origin IP address is bound to multiple domains, you must set a Server Name Indication (SNI) value to ensure that the CDN node can access your origin server over HTTPS.

Origin SNI CDN Origin

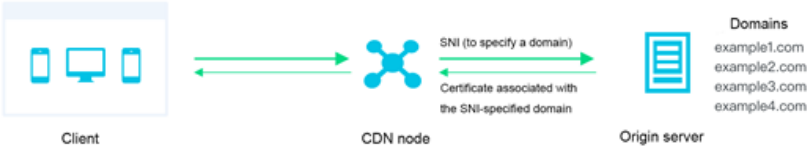
Context

SNI is an extension of Transport Layer Security (TLS) by which a client determines which hostname it is attempting to connect to at the beginning of the handshake process. This allows a server to present multiple certificates on the same IP address and TCP port. In this way, multiple HTTPS websites (or any other service over TLS) that have different certificates can be served by the same IP address.

If your origin server uses one IP address to provide HTTPS service for multiple domains and you have specified port 443 for CDN to communicate with the origin server, you must set an SNI value to specify the requested domain. In this way, when a CDN node wants to access your origin server over HTTPS, the server can return the correct certificate of the requested domain.

> **Note** If your origin is in Alibaba Cloud Object Storage Service (OSS), you do not need to set an SNI value.

The following figure shows how SNI works.



1. The CDN node wants to access the origin server over HTTPS. The requested domain is included in SNI.
2. After the origin server receives the request, it sends the certificate of the requested domain to the CDN node.
3. After the CDN node receives the certificate, it establishes a secure connection to the origin server.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. In the **Origin SNI** section, click **Modify**.
6. Turn on **Origin SNI**, and enter the name of the domain to be requested.

   In Alibaba Cloud CDN, SNI specifies a domain name of your origin server. If your origin server uses one IP address to provide HTTPS services for multiple domains, you must set an SNI value to specify the requested domain name.

7. Click **OK**.

6.7. Customize an HTTP header

HTTP header fields are components of the header section of request and response messages transmitted over Hypertext Transfer Protocol (HTTP). HTTP header fields define the resources being requested, the behavior of the client or server, and the operating parameters of an HTTP transaction. If you configure CDN to communicate with the origin over HTTP, you can add or remove HTTP header fields.

HTTP header Back-to-origin

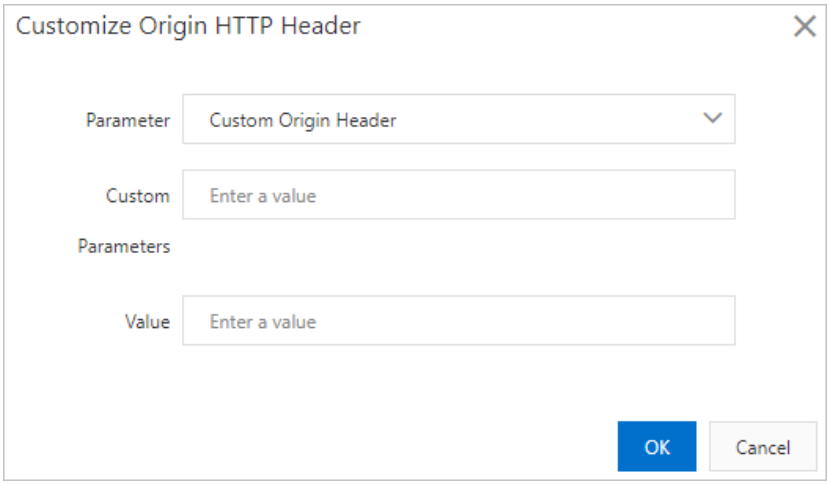
Context

HTTP header fields include general fields, request fields, and response fields.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. Click the **Custom HTTP Origin Header** tab.
6. Click **Customize**.
7. In the **Customize Origin HTTP Header** dialog box, select a field from the Parameter drop-down list and set its value.

> **Notice** When you customize an **HTTP header**, we recommend that you select **Custom Origin Header** from the **Parameter** drop-down list and add a custom field based on your needs. Do not select a system-defined field from the **Parameter** drop-down list.



8. Click **OK**.

What to do next

After you select **Custom Origin Header** from the **Parameter** drop-down list to add a **custom field**, the following error message may be returned. This means that the specified field is a reserved field for internal use.

6.8. Set the origin request timeout

This topic describes how to set the origin request timeout. The origin request timeout specifies the amount of time that Alibaba Cloud CDN waits for a response after forwarding a request to an origin. The default origin request timeout period is 30 seconds. If Alibaba Cloud CDN does not receive any response before the origin request timeout period expires, Alibaba Cloud CDN terminates the connection to the origin.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. In the **Back-to-origin Request Timeout** section, click **Modify**.
6. In the **Back-to-origin Request Timeout** dialog box, enter a value in the Timeout Value field. The maximum timeout period is 900 seconds. When Alibaba Cloud CDN communicates with the origin correctly, the origin request timeout period is no more than 100 seconds.

7. Click **OK**.

6.9. Configure URI rewrite

If you need to change the URI of the access requests sent to the origin, you can create rules to rewrite URIs. This topic describes how to create URI rewrite rules in the CDN console.

Context

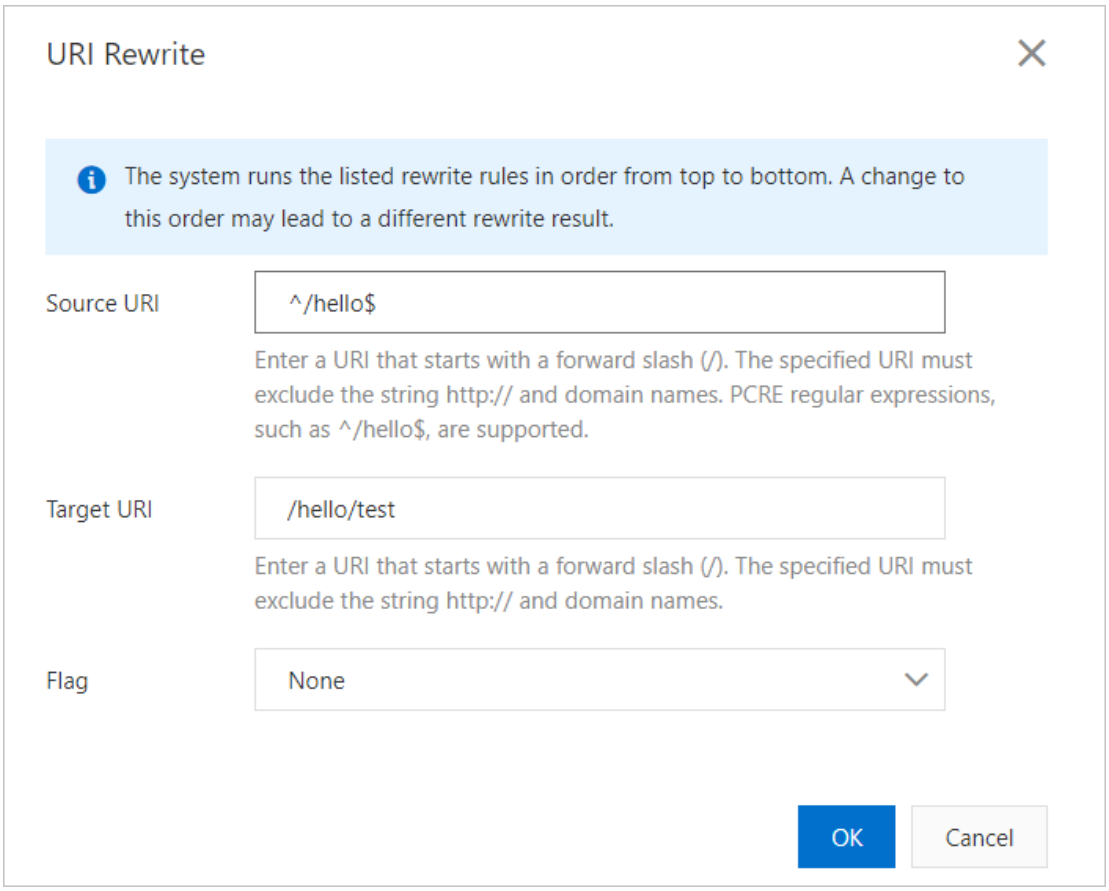
When a request URI does not match the URI of the requested resource on the origin server, you must change the request URI. You can create multiple rewrite rules as needed.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain name, click **Back-to-origin**.
5. Click the **URI Rewrite** tab.
6. On the **URI Rewrite** tab, click **Add**.
7. In the URI Rewrite dialog box that appears, specify the source URI, the target URI, and the flag.

Flag	Description
None	If multiple rules are created, the system continues to match rules after this rule is matched.

Flag	Description
break	If multiple rules are created, the system stops matching rules after this rule is matched. In addition, only the request URI is rewritten. The parameters following the question mark (?) are not rewritten.
enhance_break	If multiple rules are created, the system stops matching rules after this rule is matched. In addition, both the URI and the parameters following the question mark (?) are rewritten.



Notice

- If you set the flag of a **URI Rewrite** rule to break, the query parameters in the request URL will not be rewritten. However, the **Parameter Rewrite** feature still takes effect.
- If you set the flag of a **URI Rewrite** rule to enhance_break, the parameter rewrite settings may conflict with the settings of the **Parameter Rewrite** feature. If you configure both features at the same time, make sure that no conflicts exist.
- If you set the flag of a **URI Rewrite** rule to enhance_break, the parameter rewrite settings may conflict with the settings of the **Retain Parameters** or **Ignore Parameters** feature on the **Domain Names > Optimization** page. If you configure these three features at the same time, make sure that no conflicts exist.

8. Click **OK** to apply and run the rewrite rule.

   To modify or delete a rewrite rule, find the rule on the **URI Rewrite** tab, and click **Modify** or **Delete** in the Actions column.

   > **Notice**
   >
   > - A domain supports up to 50 URI rewrite rules.
   > - The system runs the listed rewrite rules on the URI Rewrite tab in order from top to bottom. A change to this order may lead to a different rewrite result.
   > - The **URI Rewrite** feature is different from the **Rewrite** feature on the Cache page. The **Rewrite** feature functions at the CDN edge nodes, which affects the internal links of CDN and rewrites the Cache Key. The **URI Rewrite** feature functions at the CDN nodes that communicate with the origin, which does not affect the internal links of CDN or rewrite the Cache Key.

Example 1

Source URI	^/hello$
Target URI	/index.html
Flag	None
Description	Original request: http://domain.com/hello Rewritten request: http://domain.com/index.html The system will continue to match this request against the subsequent URI rewrite rules in the list.

Example 2

Source URL	^/hello.jpg$
Target URI	/image/hello.jpg
Flag	break
Description	Original request: http://domain.com/hello.jpg Rewritten request: http://domain.com/image/hello.jpg The system will stop matching this request against the subsequent URI rewrite rules in the list.

Example 3

Source URI	^/hello.jpg\?code=123$
Target URI	/image/hello.jpg?code=321
Flag	enhance_break
Description	Original request: http://domain.com/hello.jpg?code=123 Rewritten request: http://domain.com/image/hello.jpg?code=321 The system will stop matching this request against the subsequent URI rewrite rules in the list.

6.10. Configure parameter rewrite

If you need to modify the parameters in URLs of the access requests sent to the origin, you can create rules to rewrite parameters. This topic describes how to create parameter rewrite rules in the CDN console.

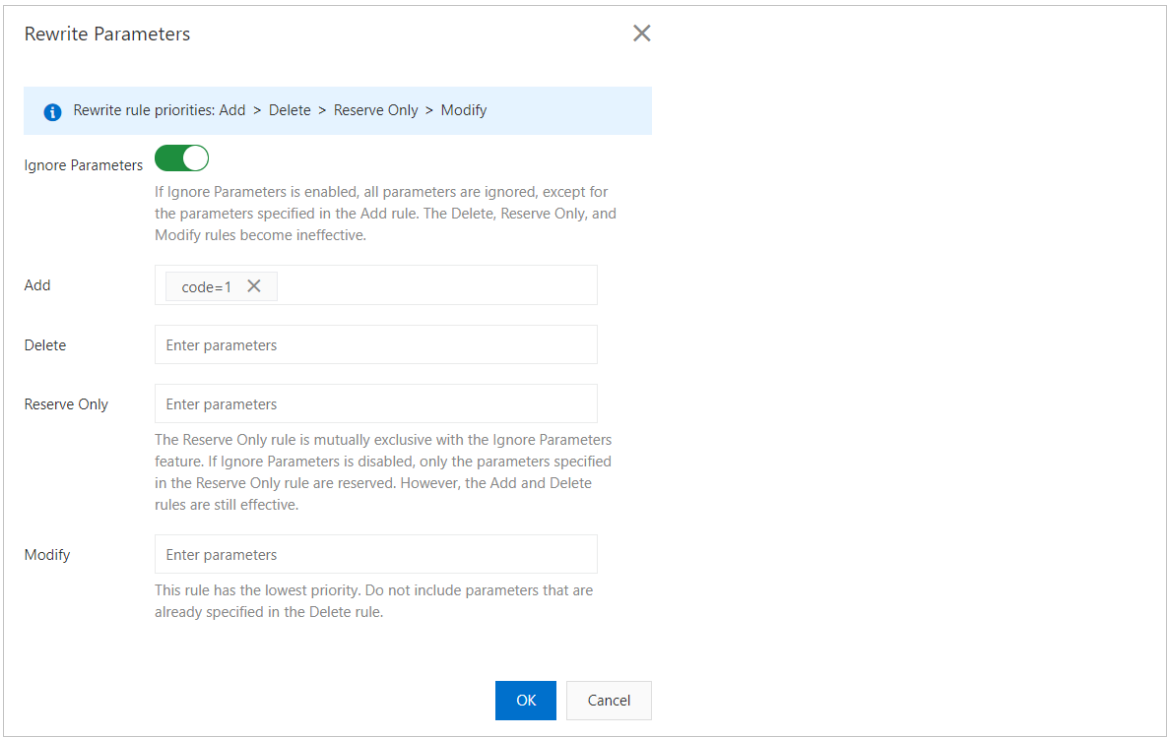
Context

When the parameters in a request URL are inconsistent with the parameters that you want to send to the origin, you can create parameter rewrite rules. These rules allow you to ignore, add, delete, retain, and modify the parameters.

Procedure

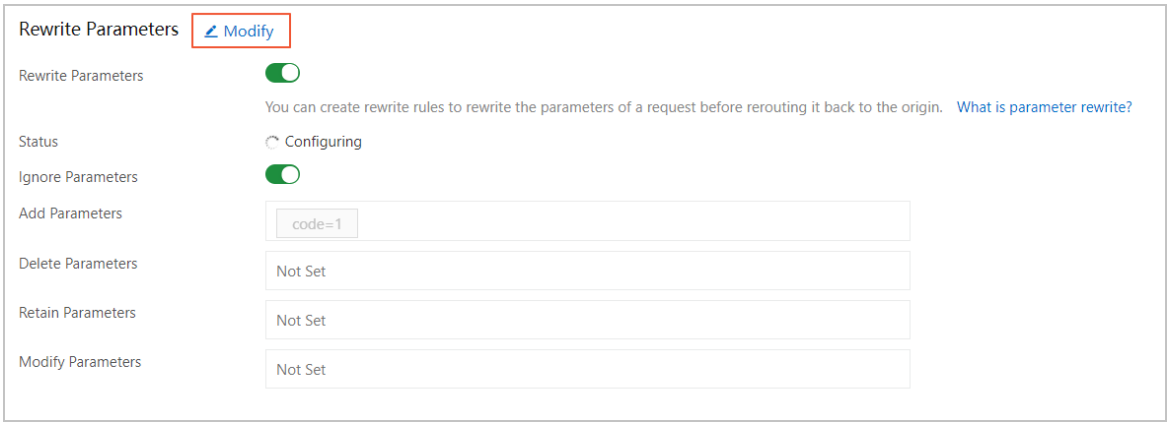
1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain name, click **Back-to-origin**.
5. Click the **Parameter Rewrite** tab.
6. On the **Parameter Rewrite** tab, turn on **Rewrite Parameters**.

7. You can configure different types of rewrite rules or press Enter to specify multiple parameters for a rewrite rule based on your business needs.



8. Click **OK** to apply and run the rewrite rules.

   To modify the existing rewrite rules, click **Modify** on the **Parameter Rewrite** tab.



Notice

When you configure parameter rewrite rules, note the following:

- The priorities of the following rewrite rules are in descending order: the **Add** rule, the **Delete** rule, the **Reserve Only** rule, and the **Modify** rule.
- The **Ignore Parameters** feature and the **Reserve Only** rule are mutually exclusive. Do not configure them at the same time to avoid feature conflicts.
- If you turn on **Ignore Parameters** and leave the **Reserve Only** field empty, all parameters included in the original request URLs will be ignored. However, the Add rule and the Delete rule still take effect because they have higher priorities.
- If you enter parameters in the **Reserve Only** field and turn off **Ignore Parameters**, only the specified parameters are retained in the original request URLs. However, the Add rule and the Delete rule still take effect because they have higher priorities.

Note

The parameter rewrite feature conflicts with other features as follows:

- The **Parameter Rewrite** feature rewrites the parameters in request URLs, which may conflict with a **URI Rewrite** rule whose flag is set to enhance_break. If you configure both features, make sure that no conflicts exist.
- The **Parameter Rewrite** feature rewrites parameters in request URLs, which may conflict with the settings of the **Retain Parameters** or **Ignore Parameters** feature on the **Domain Names** > **Optimization** page. If you configure the three features at the same time, make sure that no conflicts exist.
- The **Parameter Rewrite** feature functions at the CDN nodes that communicate with the origin, which does not affect the internal links of CDN or rewrite the Cache Key. The **Retain Parameters** or **Ignore Parameters** feature functions at the CDN edge nodes, which affects the internal links of CDN and rewrites the Cache Key.

Example 1

Ignore Parameters	Enabled
Add	None

Delete	None
Reserve Only	None
Modify	None
Description	Original request: `http://domain.com/index.html?code1=1&code2=2&code3=3` Rewritten request: `http://domain.com/index.html`

Example 2

Ignore Parameters	Disabled
Add	None
Delete	None
Reserve Only	code2
Modify	None
Description	Original request: `http://domain.com/index.html?code1=1&code2=2&code3=3` Rewritten request: `http://domain.com/index.html?code2=2`

Example 3

Ignore Parameters	Disabled
Add	code4=4
Delete	code2
Reserve Only	None
Modify	code3=0
Description	Original request: `http://domain.com/index.html?code1=1&code2=2&code3=3` Rewritten request: `http://domain.com/index.html?code1=1&code3=0&code4=4`

6.11. Customize an HTTP request header

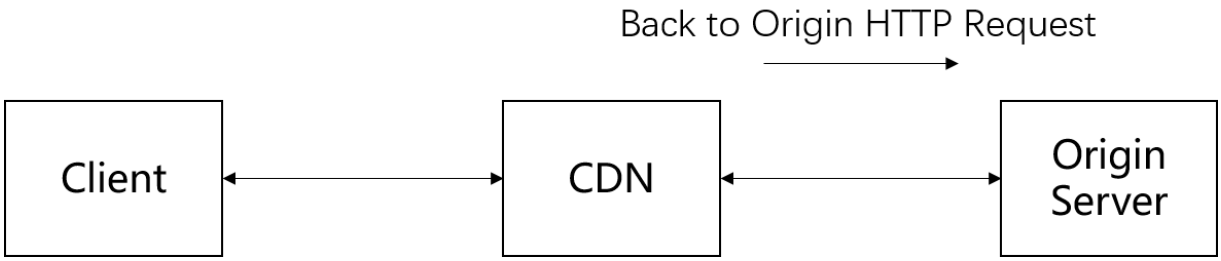
If you want to rewrite the HTTP header in a request URL, you can customize HTTP request headers in a back-to-origin HTTP request. This topic describes how to customize an HTTP request header.

HTTP request headers CDN Cross-region requests

Context

HTTP headers are components of the header section of request and response messages transmitted over Hypertext Transfer Protocol (HTTP).

HTTP headers include general headers, request headers, and response headers.



Note

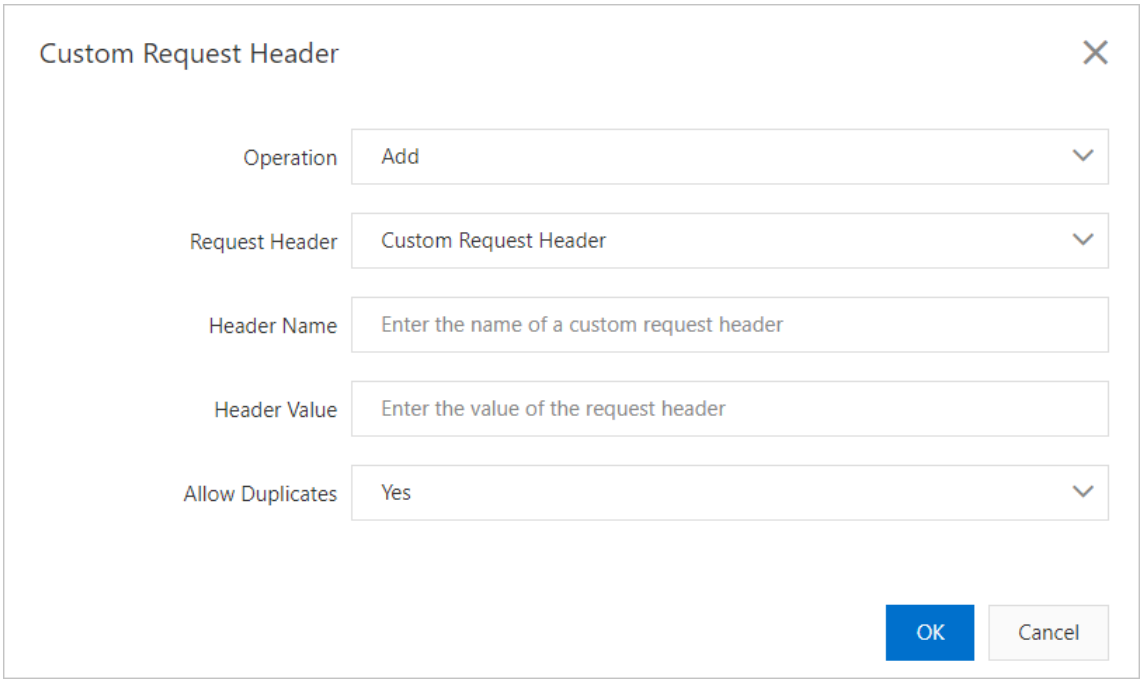
- A back-to-origin request is an HTTP message that is transmitted to the origin of a specific accelerated domain through CDN.
- Custom HTTP requests headers are only used in the HTTP responses from the origin. The back-to-origin settings do not change the HTTP responses from CDN to end users.
- Custom HTTP request headers do not support wildcard domains.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. Click **Custom Request Headers (New)**.
6. On the **Custom Request Headers (New)** tab, click **Customize**.
7. Set the parameters in the Custom Request Header dialog box that appears.

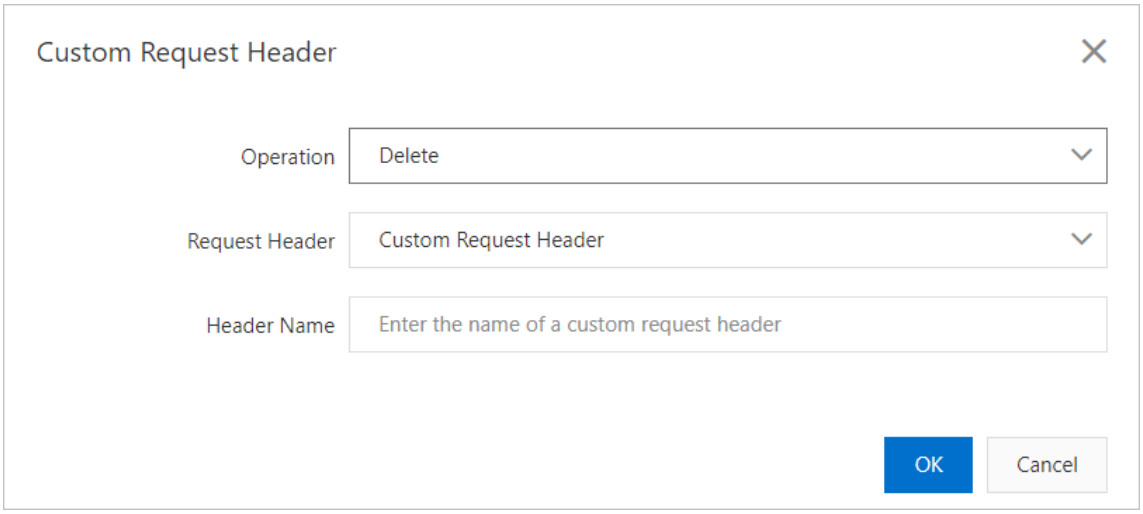
   Notice If different operations are performed on the same request header at the same time, these operations have different priorities. The priorities of the operations are as follows: **Replace** > **Add** > **Change**/**Delete**. For example, if you perform the Add and Delete operations on the same request header at the same time, the request header is added and then deleted.

   - Parameters of the Add operation



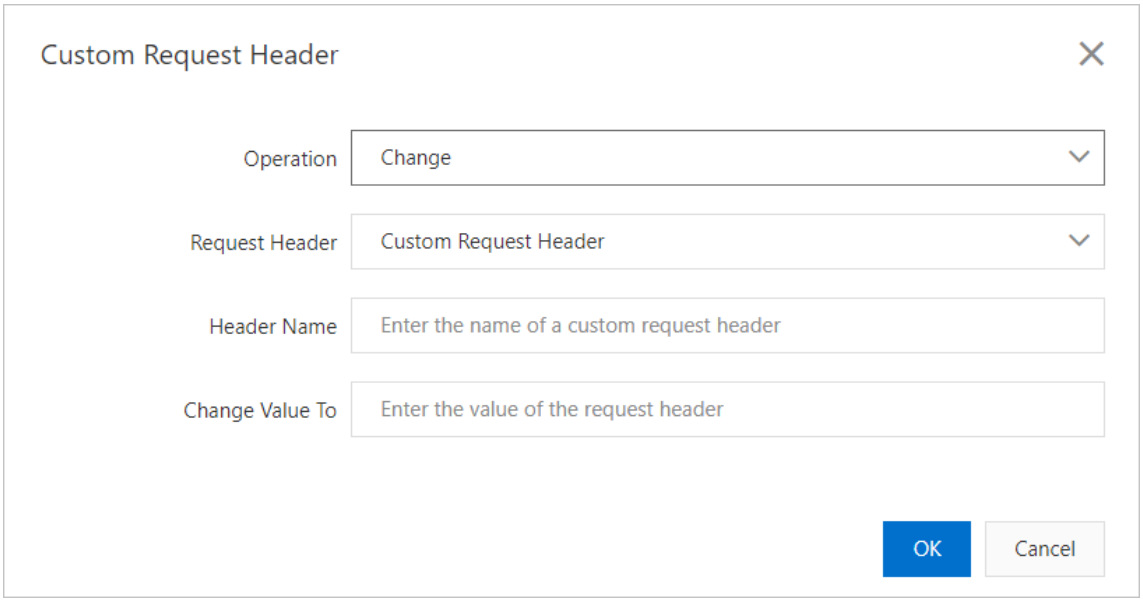
Parameter	Example	Description
Operation	Add	Adds a specific request header to the back-to-origin HTTP request.
Request Header	Custom Request Header	You can use the default value, or select **Custom Request Header** from the drop-down list to add a custom request header.
Header Name	x-code	Adds a custom request header named x-code.
Header Value	key1	You can specify multiple values for a request header. Separate multiple values with commas (,).
	key1, key2	
Allow Duplicates	Yes	When **Allow Duplicates** is set to **Yes**, you can add duplicate request headers. For example, `x-code:key1` and `x-code:key2` can coexist.
	No	When **Allow Duplicates** is set to **No**, the new header value overwrites the existing one with the same header name. For example, if you add `x-code:key1`, and then add `x-code:key2`, the final header name-value pair is `x-code:key2`

- **Parameters of the Delete operation**



Parameter	Example	Description
Operation	Delete	Deletes all request headers that match the value of the Header Name parameter. Duplicate request headers are also deleted.
Request Header	Custom Request Header	You can use the default value, or select **Custom Request Header** from the drop-down list to delete custom request headers.
Header Name	x-code	Deletes custom request headers named x-code.

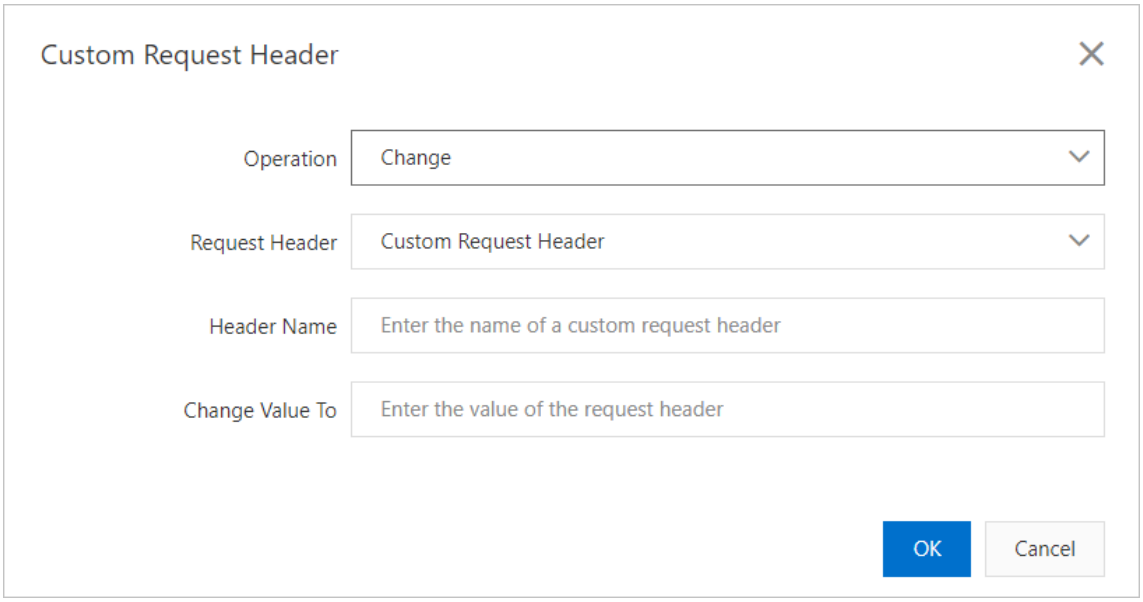
- **Parameters of the Change operation**



Parameter	Example	Description
Operation	Change	You can perform the Change operation only if no duplicate request header exists.

Parameter	Example	Description
Request Header	Custom Request Header	You can use the default value, or select **Custom Request Header** from the drop-down list to change a custom request header.
Header Name	x-code	Changes the custom request header named x-code.
Change Value To	key1, key3	You can specify multiple values for a request header. Separate multiple values with commas (,).

- **Parameters of the Replace operation**



Parameter	Example	Description
Operation	Replace	You can perform the Replace operation only if no duplicate request header exists.
Request Header	Custom Request Header	You can use the default value, or select **Custom Request Header** from the drop-down list to replace a custom request header.
Header Name	x-code	Replaces the custom request header named x-code.
Find	key	Allows you to use regular expressions to search for the value that you want to replace.
Replace With	abc	Allows you to use regular expressions to replace matching values.
	Match All	When **Match** is set to **Match All**, all matching values will be replaced. For example, if you use a regular expression to replace all the "key" in `x-code:key1,key2,key3` with "abc", the name-value pair is changed to `x-code:abc1,abc2,abc3`.

Parameter	Example	Description
Match	Match the First Only	When **Match** is set to **Match the First Only**, only the first matching value will be replaced. For example, if you use a regular expression to replace the first "key" in `x-code:key1,key2,key3` with "abc", the name-value pair is changed to `x-code:abc1,key2,key3`.

8. Click **OK**.

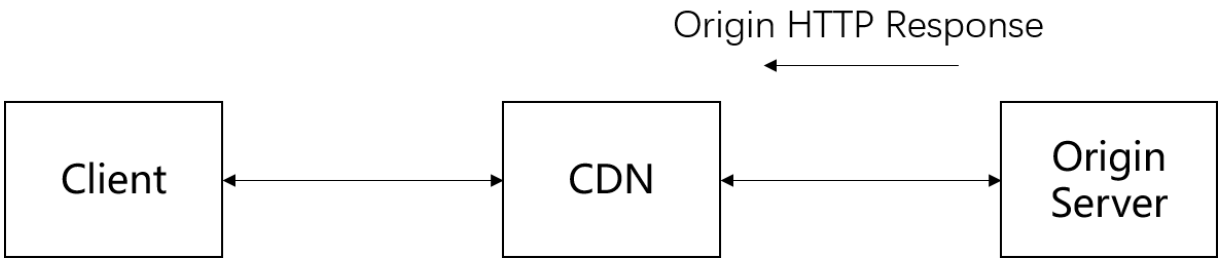
6.12. Customize an HTTP response header

The Alibaba Cloud CDN (CDN) console provides a **Custom Response Headers (New)** tab where you can customize HTTP response headers. This topic describes how to customize an HTTP response header on the **Custom Response Headers (New)** tab.

Context

HTTP headers are components of the header section of request and response messages transmitted over Hypertext Transfer Protocol (HTTP).

HTTP headers include general headers, request headers, and response headers.



Note

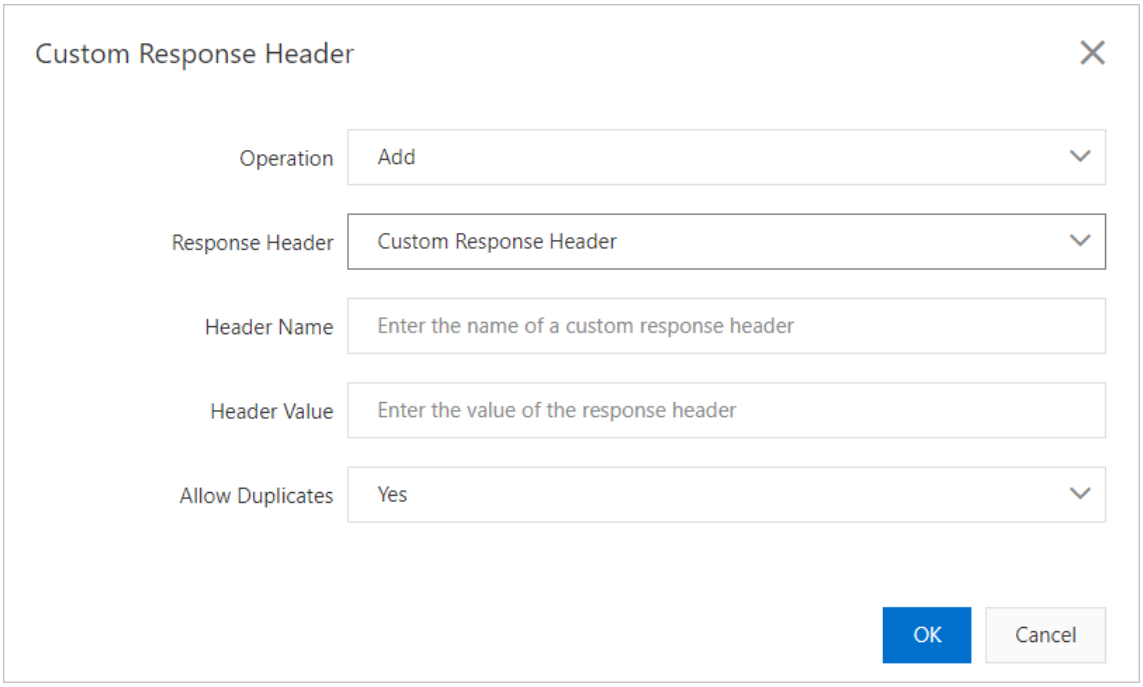
- A back-to-origin request is an HTTP message that is transmitted to the origin of a specific accelerated domain through CDN.
- Custom HTTP response headers are only used in the HTTP responses from the origin. The back-to-origin settings do not change the HTTP responses from CDN to end users.
- Custom HTTP response headers do not support wildcard domains.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Back-to-origin**.
5. Click **Custom Response Headers (New)**.
6. On the **Custom Response Headers (New)** tab, click **Customize**.
7. Set the parameters in the Custom Response Header dialog box that appears.

Notice If different operations are performed on the same response header at the same time, these operations have different priorities. The priorities of the operations are as follows: **Replace > Add > Change/Delete**. For example, if you perform the Add and Delete operations on the same response header at the same time, the response header is added and then deleted.

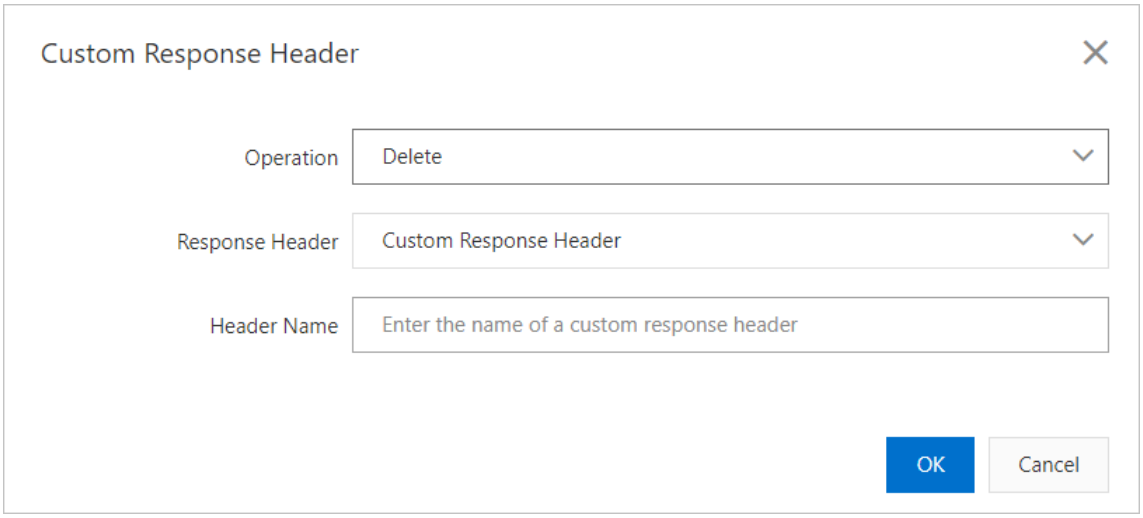
- **Parameters of the Add operation**



Parameter	Example	Description
Operation	Add	Adds a response header to a back-to-origin HTTP request.
Response Header	Custom Response Header	You can use the default value, or select **Response Header** from the drop-down list to add a custom response header.
Header Name	x-code	Adds a custom response header named x-code.
Header Value	key1	You can specify multiple values for a response header. Separate multiple values with commas (,).
	key1, key2	
Allow Duplicates	Yes	When **Allow Duplicates** is set to **Yes**, you can add duplicate response headers. For example, `x-code:key1` and `x-code:key2` can coexist.

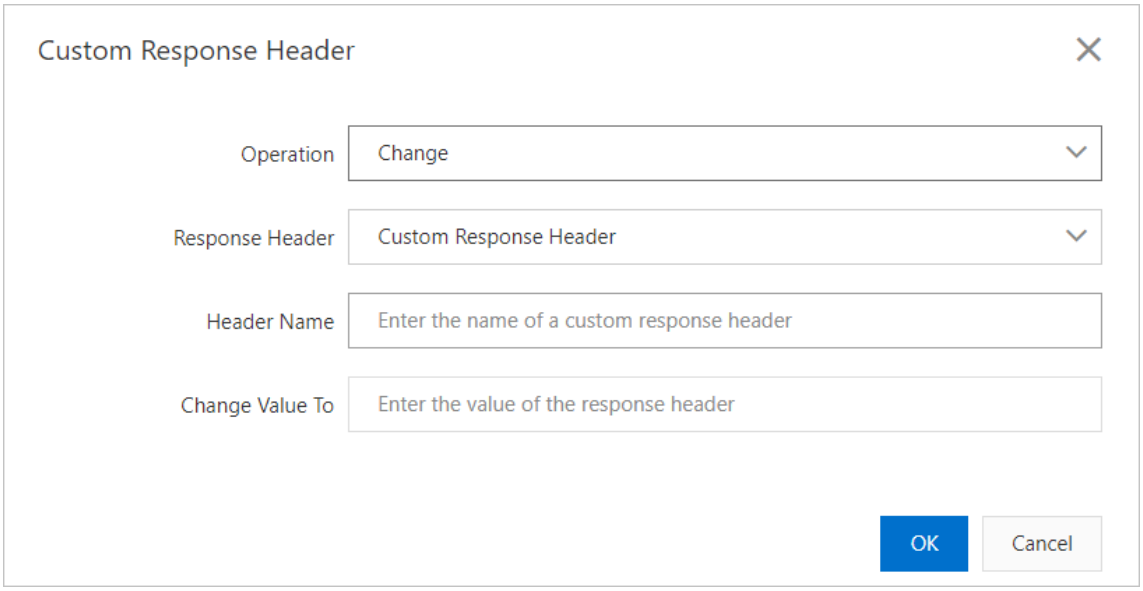
Parameter	Example	Description
	No	When **Allow Duplicates** is set to **No**, the new header value overwrites the existing one with the same header name. For example, if you add `x-code:key1` and then add `x-code:key2`, the final header name-value pair is `x-code:key2`.

- **Parameters of the Delete operation**



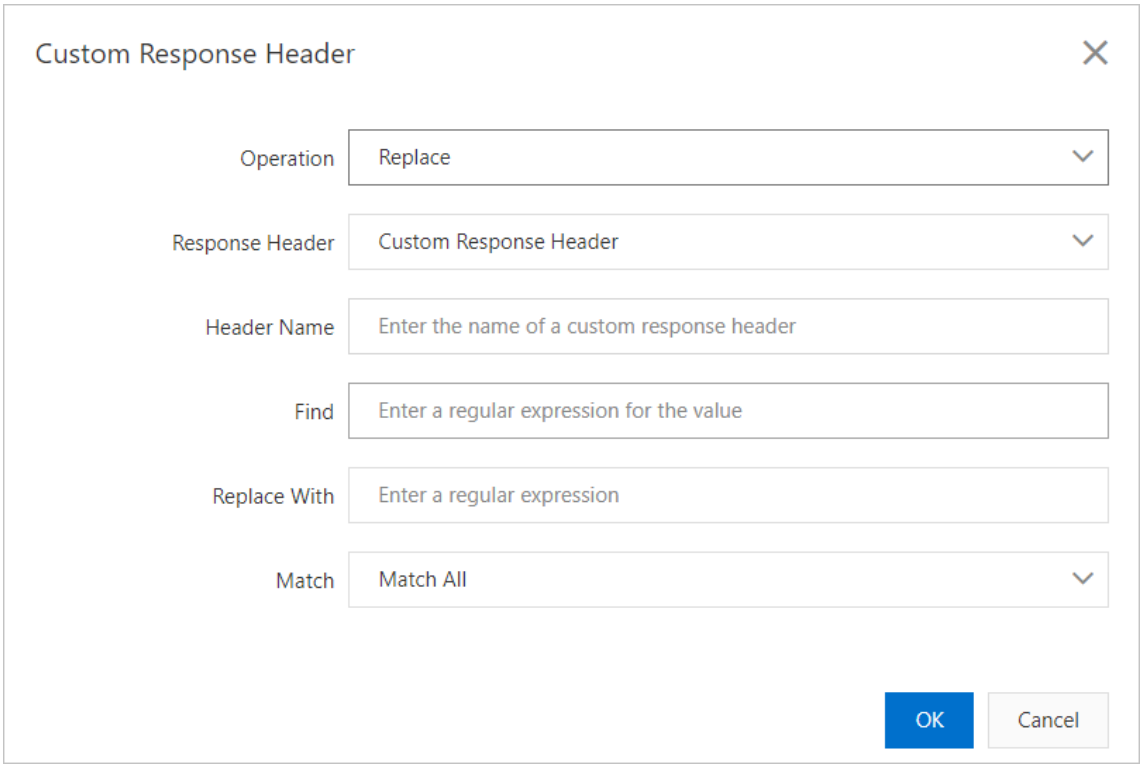
Parameter	Example	Description
Operation	Delete	Deletes all response headers that match the value of the Response Header parameter. Duplicate response headers are also deleted.
Response Header	Custom Response Header	You can use the default value, or select **Response Header** from the drop-down list to delete a custom response header.
Header Name	x-code	Deletes custom response headers named x-code.

- **Parameters of the Change operation**



Parameter	Example	Description
Operation	Change	You can perform the Change operation only if no duplicate response header exists.
Response Header	Custom Response Header	You can use the default value, or select **Response Header** from the drop-down list to change a custom response header.
Header Name	x-code	Changes the custom response header named x-code.
Change Value To	key1, key3	You can specify multiple values for a response header. Separate multiple values with commas (,).

- **Parameters of the Replace operation**



Parameter	Example	Description
Operation	Replace	You can perform the Replace operation only if no duplicate response header exists.
Response Header	Custom Response Header	You can use the default value, or select **Response Header** from the drop-down list to replace a custom response header.
Header Name	x-code	Replaces the custom response header named x-code.
Find	key	Allows you to use regular expressions to search for the value that you want to replace.
Replace With	abc	Allows you to use regular expressions to replace matching values.
Match	Match All	When **Match** is set to **Match All**, all matching values will be replaced. For example, if you use a regular expression to replace all the "key" in `x-code:key1,key2,key3` with "abc", the name-value pair is changed to `x-code:abc1,abc2,abc3`.

Parameter	Example	Description
	Match the First Only	When **Match** is set to **Match the First Only**, only the first matching value will be replaced. For example, if you use a regular expression to replace the first "key" in `x-code:key1,key2,key3` with "abc", the name-value pair is changed to `x-code:abc1,key2,key3`.

8. Click **OK**.

7.Cache settings

7.1. Overview

When Alibaba Cloud Content Delivery Network (CDN) accelerates static resource delivery, it loads resources from an origin server to the CDN node that is closest to the visitor. When the visitor accesses the static resources, CDN retrieves the resources from the CDN node instead of the origin server. This reduces the resource delivery time because retrieving resources from the origin server is time-consuming.

How to calculate the TTL for a cached object

- t = (Current time - Last-Modified) × 0.1
- t = max(10, t)
- t = min(t, 3600)

The time-to-live (TTL) is represented by t and measured in seconds.

Default caching rules

- If the `Last-Modified` value of an object is `20140801 00:00:00` and the current time is `20140801 00:01:00`, t = (Current time - Last-Modified) × 0.1 = 6 seconds. According to the calculation rules, the TTL is 10 seconds because the minimum value is 10 seconds.
- If the `Last-Modified` value of an object is `20140801 00:00:00` and the current time is `20140802 00:00:00`, t = (Current time - Last-Modified) × 0.1 = 8,640 seconds. According to the calculation rules, the TTL is 3,600 seconds because the maximum value is 3,600 seconds.
- If the `Last-Modified` value of an object is `20140801 00:00:00` and the current time is `20140801 00:10:00`, t = (Current time - Last-Modified) × 0.1 = 60 seconds. According to the calculation rules, the TTL is 60 seconds.
- If the response from the origin server does not contain the `Last-Modified` header but contains the `ETag` header, the accessed object is more likely a static resource. The default TTL for this object is set to the minimum value that is configured by using the `dft_expires` directive.
- If the response from the origin server does not contain the `Last-Modified` or the `ETag` header, the accessed object is a dynamic resource. The default TTL for this object is set to zero. The object will be retrieved from the origin server each time when it is requested.

> **Note**
>
> Website developers and related IT engineers are more familiar with the business logic of, and the static and dynamic content on their websites. We recommend that you set the TTL values in the console based on the file type and directory. For more information, see Create a cache expiration rule.

References

CDN supports the following cache functions.

Function	Description
Create a cache expiration rule	Allows you to configure cache expiration rules for static resources in a specified directory or with specified file extensions. In each cache expiration rule, you can set the TTL of the cached static resources and the priority. Based on these cache expiration rules, CDN caches the specified static resources on CDN nodes.
Create a status code expiration rule	Allows you to configure expiration rules for HTTP status codes that are returned for resources in a specified directory or with specified file extensions.
Create an HTTP header	Allows you to customize HTTP response headers.
Customize an error page	Allows you to customize an error page for a specific HTTP or HTTPS status code.
Configure a rewrite rule	Allows you to redirect request URIs to specified URIs by using 302 redirects.

7.2. Create a cache expiration rule

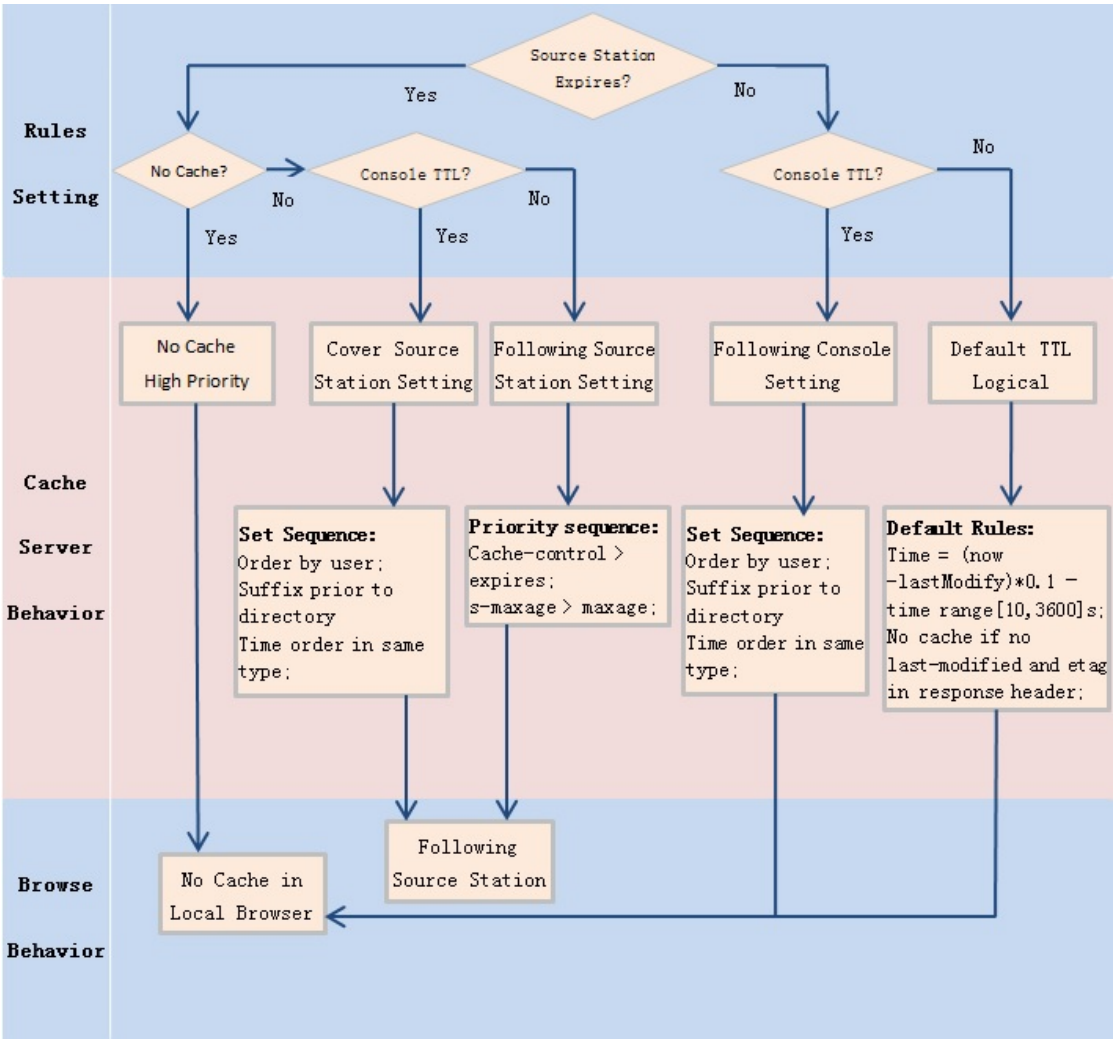
Alibaba Cloud Content Delivery Network (CDN) allows you to create cache expiration rules to expire static resources of specified file types or in specified directories. You can also specify a priority for each cache expiration rule. When a static resource expires, the resource is automatically deleted from the corresponding CDN node. This topic describes the rules of expiring cached resources on a CDN node and how to create a cache expiration rule.

Cache policy Time To Live (TTL) values of cached resources CDN

Context

When you update a resource file on the origin, we recommend that you include the version number in the name of the update file instead of using the same name as the existing resource file. For example, you can name two update files as *img-v1.0.jpg* and *img-v2.1.jpg*. Afterward, you can set a cache expiration rule for the resource file.

The following figure shows the cache expiration policy of resources on CDN nodes.

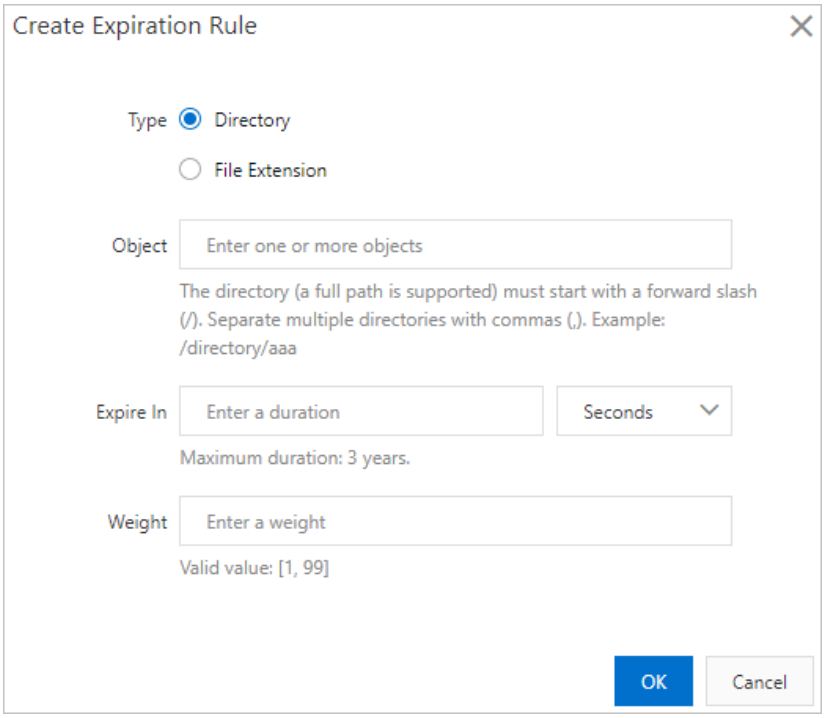


> **Note**
>
> - If an origin server has a caching rule configured, the cache expiration rule on the CDN node has a higher priority than the caching rule configured on the origin server. If an origin server has no caching rule configured, you can set a cache expiration rule by directory or by file extension. You can set a full-path cache expiration rule.
> - A CDN node may remove the cached files that are not updated frequently on the node before they expire.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Cache**.
5. On the **Cache Expiration** tab, click **Create Rule**.
6. In the Create Expiration Rule dialog box that appears, set Type to Directory or File Extension.

Item	Description
Type	○ Directory: specifies resources cached in a specified directory. ○ File Extension: specifies resources cached in files with specified file extensions.
Object	○ After you set Type to Directory, enter a directory name in the Object field. The directory name must start with a forward slash (/), for example, */directory/aaa*. ○ After you set Type to File Extension, enter one or more file extensions in the Object field. Separate multiple file extensions with commas (,), for example, `JPG,txt` .
Expire In	Specifies a TTL value of the cached resources. A CDN node can cache resources for up to three years. We recommend that you set this parameter according to the following rules: ○ Specify a TTL value of one month or longer for static files such as images and applications that are not frequently updated. ○ Specify a TTL value as needed for static files such as JavaScript and CSS files that are frequently updated. ○ Specify a TTL value of 0 second for dynamic files such as PHP, JSP, and ASP files. As a result, the CDN node will not cache these files.
Weight	Specifies the priority of the rule. Note ○ Set this parameter to an integer from 1 to 99. A higher value indicates a higher priority and a rule with a higher priority prevails over rules with lower priorities. ○ We recommend that you do not set the same priority for different rules. If different rules have the same priority value, one of these rules is applied at random. For example, if you set the following rules for the `example.aliyun.com` domain, Rule 1 takes effect preferentially over the other two rules: ○ Rule 1: Type is set to File Extension, Object is set to jpg,png, Expire In is set to 1 Months, and Weight is set to 90. ○ Rule 2: Type is set to Directory, Object is set to */www/dir/aaa*, Expire In is set to 1 Hours, and Weight is set to 70. ○ Rule 3: Type is set to Directory, Object is set to */www/dir/aaa/example.php*, Expire In is set to 0 Seconds, and Weight is set to 80.



7. Click **OK**.

   You can click **Modify** or **Delete** in the Actions column for the cache expiration rule to modify or delete the rule.

7.3. Create a status code expiration rule

Content Delivery Network (CDN) allows you to create status code expiration rules to expire static resources of specified file types or in specified directories. When a status code expires, the relevant static resource is deleted from the edge node. This topic describes how to create a status code expiration rule.

Status code expiration rule CDN

Context

When you create a status code expiration rule, note the following limits:

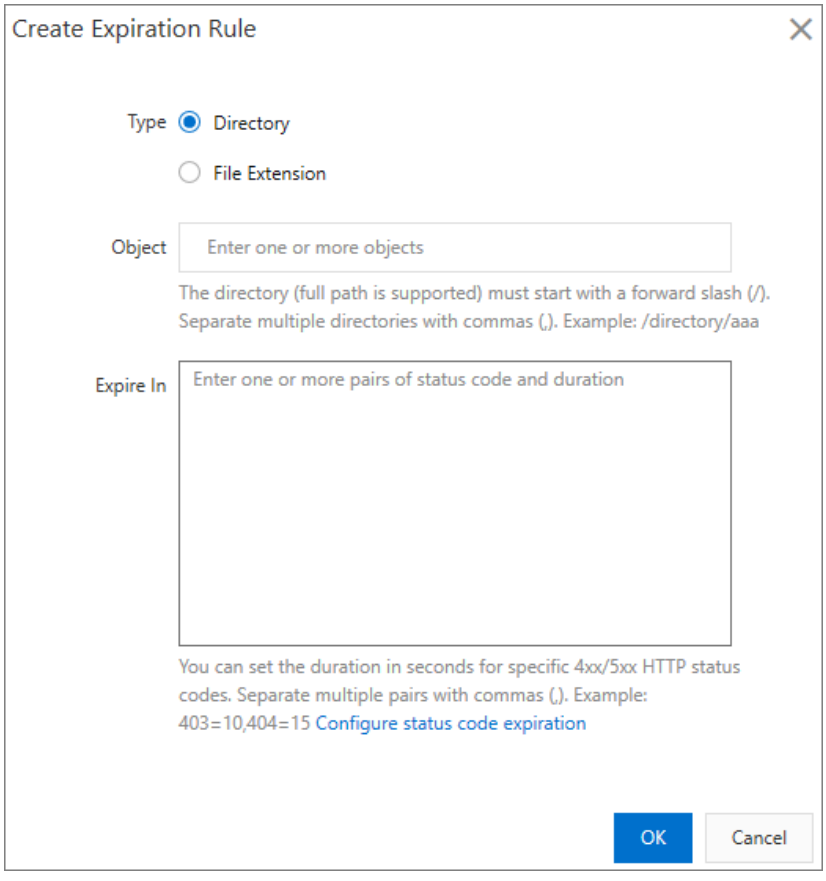
- The system does not cache status codes 303, 304, 401, 407, 600, and 601.
- If the origin returns a Cache-Control header, status codes 204, 305, 400, 403, 404, 405, 414, 500, 501, 502, 503, and 504 are cached according to the amount of time specified by the Cache-Control header. If no status code expiration rule is created, these status codes are cached according to the amount of time specified by negative_ttl (1 second by default).
- If you have created two status code expiration rules for static resources of specified file types and in specified directories, whichever created first takes effect.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Cache**.

5. Click **Status Code Expiration**.
6. In the **Create Expiration Rule** dialog box, select Directory or File Extension, enter directories or file extensions, and enter status code and caching time pairs.
   - Create a status code expiration rule for static resources of specified file types or in specified directories.
     a. Click **Create Rule**.
     b. Select a static resource type: Directory or File Extension.

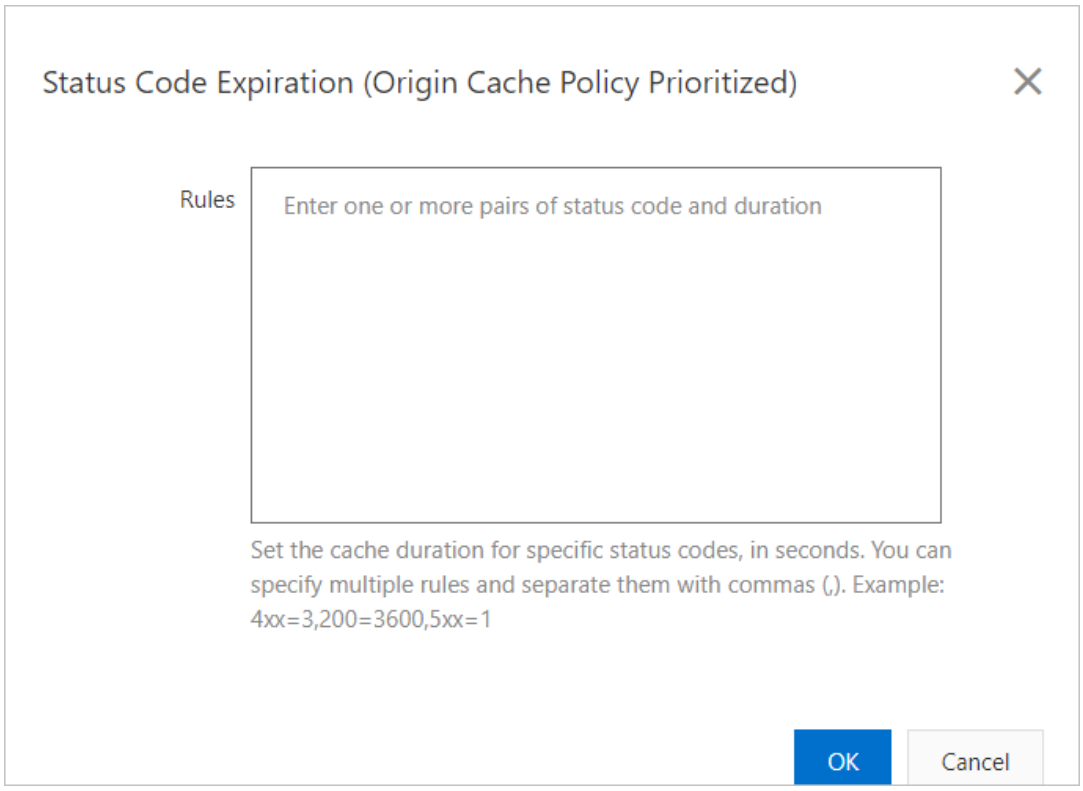
Resource type	Description
Directory	■ Enter a directory, which can be a full path. The directory must start with a forward slash (/), such as */directory/aaa*. ■ Status codes 2xx and 3xx are not cached.
File Extension	■ Enter one or more file extensions. Separate multiple file extensions with commas (,), for example, txt,jpg. ■ Asterisks (`*`) cannot be used as wildcard characters to match all file types. ■ Status codes 2xx and 3xx are not cached.



c. Click **OK** to add the expiration rule.

You can click **Modify** or **Delete** in the Actions column to modify or delete a rule.

- Create a status code expiration rule that prioritizes the origin cache policy.
  a. Click **Create Rule**.
  b. Enter status code and caching time pairs.



c. Click **OK**.

You can click **Modify** or **Delete** in the Actions column to modify or delete a rule.

7.4. Create an HTTP header

HTTP headers define the resources being requested, the behavior of the client or server, and the operation parameters of an HTTP transaction. This topic describes how to create an HTTP response header.

HTTP response header CDN Cross-region requests

Context

HTTP headers are components of the header section of request and response messages transmitted over Hypertext Transfer Protocol (HTTP).

HTTP header fields include the General-header, Client Request-header, and Server Response-header fields.

> Notice
>
> - The configurations of the HTTP response header of an accelerated domain name affect the response behavior of all client programs such as browsers in this domain. However, the configurations do not affect the behavior of the cache server.
> - Alibaba Cloud CDN does not allow you to configure response headers for wildcard domain names.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Cache**.
5. Click the **HTTP Header** tab.
6. On the **HTTP Header** tab, click **Customize**.
7. In the Cache Response Headers dialog box, set the parameters to create an HTTP response header.

   Alibaba Cloud CDN provides 10 types of HTTP response header. You can also create a custom HTTP response header. The following table lists different types of HTTP response header. If you want to create other types of HTTP response header, submit a ticket.

Parameter	Description	Example
Content-Type	Specifies the MIME type of the content returned to the client program.	image
Cache-Control	Specifies the cache policy that requests and responses follow.	no-cache
Content-Disposition	Specifies the default file name when the requested content is saved as a file on the client program.	123.txt
Content-Language	Specifies the language of the returned content for the intended audience.	zh-CN
Expires	Specifies the date and time after which the response is considered stale.	Wed, 21 Oct 2015 07:28:00 GMT

Parameter	Description	Example
Access-Control-Allow-Origin	Specifies the origins from which cross-origin requests are allowed.	* Note You can enter an asterisk (*) in the Header Value field to specify all domain names. You can also enter a complete domain name, for example, www.aliyun.com .
Access-Control-Allow-Headers	Specifies the fields that are allowed in cross-origin requests.	X-Custom-Header
Access-Control-Allow-Methods	Specifies the request methods that are allowed for cross-origin requests.	POST and GET
Access-Control-Max-Age	Specifies the time-to-live (TTL) value during which the response can be cached on the client program for a request that prefetches a particular resource.	600
Access-Control-Expose-Headers	Specifies the headers that can be exposed as part of the response.	Content-Length

8. Click **OK**.

   In the **HTTP Header** list, you can click **Modify** or **Delete** in the Actions column to modify or delete HTTP response headers.

7.5. Customize an error page

When a client requests a Web service through a browser, the website hosting server returns the default 404 Not Found page if the requested URL does not exist. However, you may dislike the way the default 404 Not Found page looks. To improve user experience, you can associate full URLs with error codes that are carried in HTTP or HTTPS responses. When an error occurs, the server returns the associated custom page. This topic describes how to customize an error page.

Custom pages Set the status code page CDN

Context

Alibaba Cloud Content Delivery Network (CDN) provides two types of error pages: default page and custom page. Status code 404 is used as an example to describe the differences between the default page and custom page.

- Default page: When the HTTP response carries a 404 error code, the server returns the default 404 Not Found page.
- Custom page: When the HTTP response carries a 404 error code, the server returns the custom page. You must specify a full URL for the custom page.

> Note
> - Default pages are considered Alibaba Cloud public resources and are free of charge.
> - Custom pages are considered personal resources and are charged.

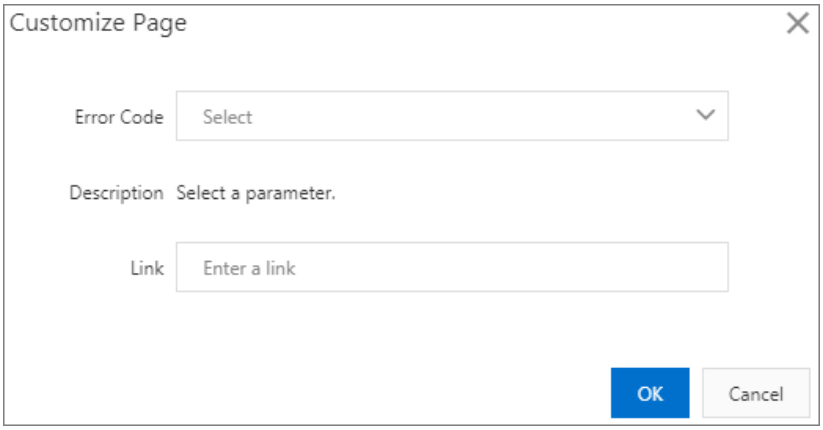
When the Web server returns an HTTP 404 status code, the Web page is automatically redirected to the 404 Not Found page. Visitors may fail to access a URL if the URL generation rules of the Web page change, the file on the Web page is renamed or relocated, or a spelling error exists in the URL. When the Web server receives such a request, it returns a 404 status code to inform the visitor that the requested resource does not exist. Possible causes for a 404 error:

- The website cannot be accessed through the requested port.
- The Web service extension lockdown policy blocks this request.
- The MIME map policy blocks this request.

> Note When only one resource is requested and the resource is not found on the origin server, a 404 status code is returned and a 404 error page is displayed. When multiple resources are requested and only some of the resources are not found on the origin server, the 404 error page is not displayed.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Cache**.
5. Click **Custom Pages**.
6. On the **Custom Pages** tab, click **Customize**.



7. In the Customize Page dialog box, set the parameters. For example, you want to store the `error404.html` page for the 404 error together with other static files to the origin and return this error page to requests addressed to the CDN domain `exp.aliyun.com`. Then, you only need to select **404** from the Error Code drop-down list and enter the full URL `http://exp.aliyun.com/error404.html` into the Link field.
8. Click **OK**.

   After the custom page is created, you can click **Modify** or **Delete** in the Actions column to modify or delete the custom page.

7.6. Configure a rewrite rule

The rewrite function allows you to modify the requested Uniform Resource Identifier (URI) and configure destination URIs for 302 redirects. You can configure multiple rewrite rules as needed. This topic describes how to configure rewrite rules in the CDN console.

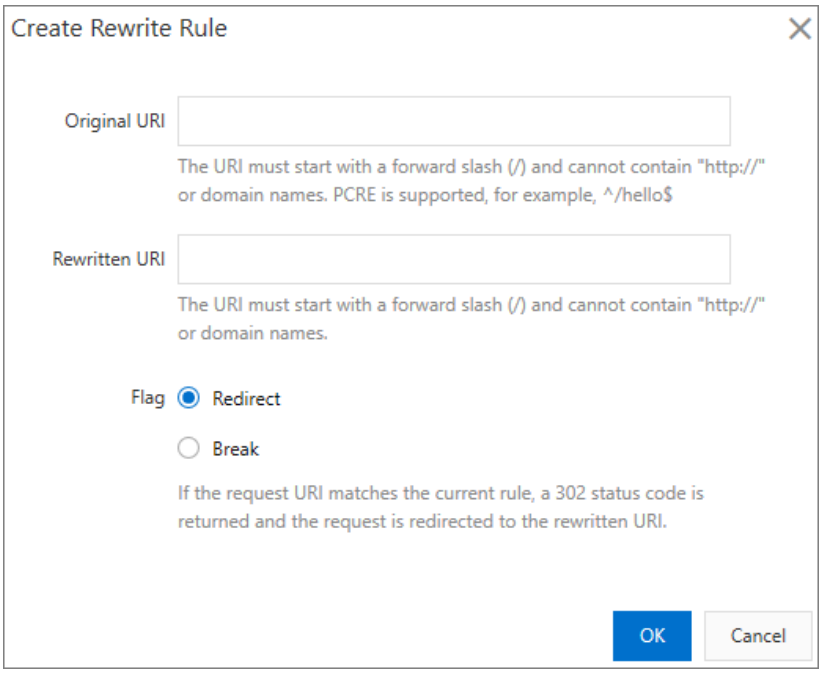
Rewrite Cache

Context

If you need to modify the requested URI, create a rewrite rule. For example, if a client requests to visit http://example.com through HTTP, you can create a rewrite rule to redirect the request to https://example.com.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Cache**.
5. On the **Rewrite** tab, click **Create**.
6. Click **Rewrite**.
7. On the **Rewrite** tab, click **Create**.



8. Set the Original URI, Rewritten URI and Flag as needed.

   A CDN node uses one of the following methods to run rewrite rules:

   - Redirect: If the requested URI matches the current rule, the CDN node returns a 302 status code and redirects the request to the destination URI.
   - Break: If the requested URI matches the current rule, the CDN node returns the content of the requested URI, but does not check whether the requested URI matches the remaining rules.

9. Click **OK**.

   After a rewrite rule is configured, you can click **Modify** or **Delete** in the Actions column to modify or delete the rewrite rule.

Example No.	Requested URI	Destination URI	Rewrite flag	Description
1	/hello	/index.html	Redirect	When a client requests the content of `http://domain.com/hello`, the CDN node returns a 302 status code and redirects the client to `http://domain.com/index.html`.
2	^/hello$	/index.html	Break	When a client requests the content of `http://domain.com/hello`, the CDN node returns the content of `http://domain.com/index.html`, but does not check whether the requested URI matches the remaining rewrite rules.
3	^/$	/index.html	Redirect	When a client requests the content of `http://domain.com`, the CDN node returns a 302 status code and redirects the client to `http://domain.com/index.html`.

8.HTTPS

8.1. HTTPS secure acceleration overview

This topic provides an overview of Hypertext Transfer Protocol Secure (HTTPS) secure acceleration, including its working principles, benefits, and notes. HTTPS secure acceleration allows HTTPS-based encryption between clients and Content Delivery Network (CDN) nodes to ensure data security during transmission.

HTTPS secure acceleration CDN

HTTPS

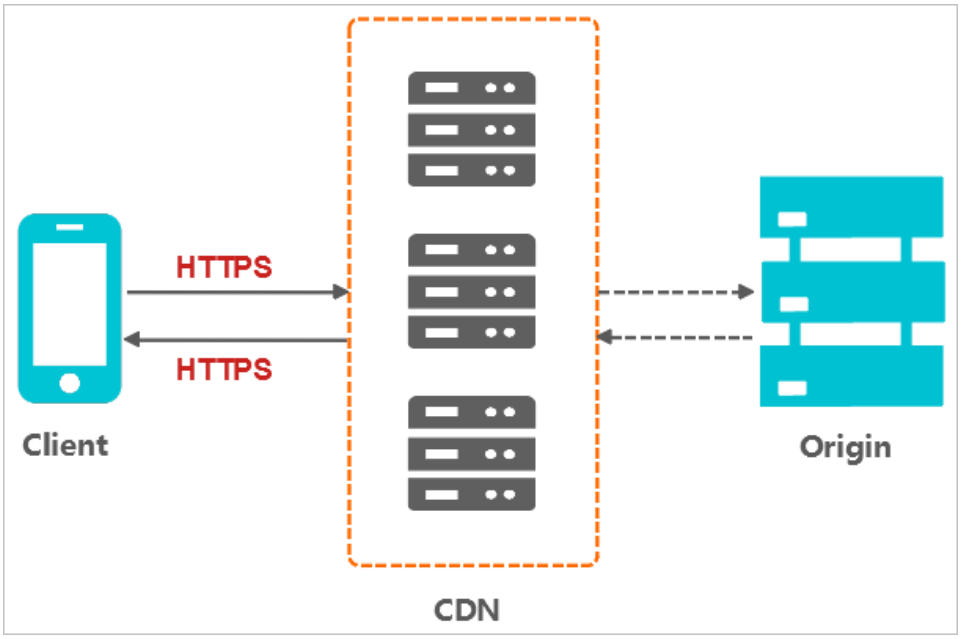
Hypertext Transfer Protocol (HTTP) transmits content in plaintext and does not encrypt data in any form. As an extension of HTTP, HTTPS is an HTTP channel designed to enhance security. Secure Sockets Layer (SSL) or Transport Layer Security (TLS) is used as a sublayer under the regular HTTP application to authenticate users and encrypt data. HTTPS is widely used to protect sensitive user data for services such as payment transactions.

According to a report released by Electronic Frontier Foundation (EFF) in 2017, more than 50% of web traffic worldwide is transmitted over HTTPS.

Working principles

After you enable HTTPS in the Alibaba Cloud CDN console, the requests from clients to Alibaba Cloud CDN nodes are encrypted over HTTPS. A CDN node retrieves the requested resources from the origin and then returns them to a client based on the origin configuration. We recommend that you enable HTTPS on the origin to implement end-to-end HTTPS encryption.

The following figure shows the HTTPS encryption process.



1. The client sends a request over HTTPS.
2. The server prepares a public key and a private key in advance.

> Note You can prepare the keys on your own or request them from a professional organization. You can also request a free HTTPS certificate in the Alibaba Cloud CDN console.

3. The server sends the public key to the client.
4. The client authenticates the certificate.
   - If the certificate is valid, the client generates a random number as a key. The client uses the public key to encrypt the random number and transmits the random number to the server.
   - If the certificate is invalid, the SSL handshake fails.

   > Note A valid certificate must meet the following requirements:
   > - The certificate has not expired.
   > - The certificate is issued by a trusted certificate authority (CA).
   > - The digital signature of the issuer in the certificate can be decrypted with the public key of the issuer.
   > - The domain name in the certificate is the same as that of the server.
5. The server decrypts the random number by using the private key.
6. The server uses the random number to encrypt data and transmits the data to the client.
7. The client uses the random number to decrypt the received data.

Benefits

- HTTPS provides protection against the following HTTP security threats:
  - Eavesdropping, where third parties may intercept your data during transmission.
  - Tampering, where third parties alter your data during transmission.
  - Spoofing, where third parties impersonate the identity of a user.
  - Hijacking, where your data is rerouted to third-party servers.
- Benefits of HTTPS transmission:
  - HTTPS encrypts sensitive information such as session IDs and cookies before transmission. This prevents security threats caused by sensitive information leakage.
  - HTTPS checks data integrity during transmission to protect your Domain Name System (DNS) or content against man-in-the-middle (MITM) attacks such as hijacking and tampering.
  - HTTPS is the new norm. An increasing number of major browsers such as Google Chrome and Mozilla Firefox have labelled HTTP websites as insecure since 2018. If you choose to use HTTP, your website may be exposed to security risks. Users who visit your website by using these browsers are prompted that this website is insecure. This compromises user experience and may reduce visits to the website.
  - Google and Baidu prioritize HTTPS websites in the search results. Additionally, major browsers must support HTTPS to support HTTP/2. HTTPS is a more reliable choice in terms of security, market presence, and user experience. Therefore, we recommend that you upgrade your communication protocol to HTTPS.

Scenarios

The following table describes the scenarios of HTTPS.

Scenario	Description
Enterprise application	HTTPS protects confidential information on enterprise websites from being hijacked or intercepted. The confidential information includes customer relationship management (CRM) data and enterprise resource planning (ERP) data.
Government website	HTTPS protects authoritative information on government websites against vulnerabilities such as phishing and hijacking. Leakage of such information may compromise the public trust.
Payment system	HTTPS protects sensitive data such as the customer names and phone numbers used in payment transactions against hijacking and spoofing. If sensitive data is leaked, attackers can use such data to trick customers into making duplicate payments. This causes losses to both the customer and the enterprise.
API operations	API operations use HTTPS to encrypt important information such as sensitive data and crucial instructions. This protects the information against hijacking.
Enterprise website	HTTPS makes users feel more secure. Web browsers display a green lock icon in the address bar for websites with domain validated (DV) and organization validated (OV) certificates. The enterprise name is displayed together with the green lock for websites that include extended validated (EV) certificates.

Notes

The following table describes the rules of using HTTPS secure acceleration.

Type	Note

Type	Note

Configurations	• The following business scenarios support HTTPS secure acceleration:
	  ○ Image and small file distribution
	  Web portals, e-commerce websites, news websites and applications, government or enterprise official websites, and entertainment or gaming websites and applications.
	  ○ Large file downloading
	  Video or audio applications and websites that provide content for users to download.
	  ○ VOD
	  Websites and applications that provide audio and video content such as movies, online education, news, and social networking.
	• You can enable HTTPS for wildcard domains.
	• You can enable or disable HTTPS secure acceleration as needed.
	  ○ When HTTPS secure acceleration is enabled: You can modify certificates. The system supports HTTP and HTTPS requests by default. In addition, you can Enable force redirect to customize request methods.
	  ○ When HTTPS secure acceleration is disabled: The system no longer supports HTTPS requests and no longer keeps certificate or private key information. To enable certificates again, you must re-upload the certificates or private keys. For more information, see Configure an SSL certificate.
	• You can view certificates but not private keys. Keep certificate-related information confidential.
	• You can update certificates. However, proceed with caution. HTTPS certificates take effect within one minute after they are updated.

Billing	HTTPS secure acceleration is a value-added service. After you enable HTTPS, you will be billed based on HTTPS requests. For more information about the billing standards, see Number of static HTTPS requests. Note The billing for HTTPS requests is calculated separately and is not covered by the CDN data transfer plan. Before you enable HTTPS secure acceleration, make sure that your account balance is sufficient. CDN services may be suspended when your balance is insufficient.

Type	Note
Certificates	• You must upload certificate and private key files in the `PEM` format for domains for which HTTPS secure acceleration is enabled. **Note** The Tengine web server used by CDN is designed based on the NGINX web server architecture. Therefore, the web server supports only certificate files in the NGINX-compatible `PEM` format. For more information, see Overview of certificate formats. • The uploaded certificate file must match the private key. Otherwise, the certificate authentication fails. • A private key cannot have a password configured. • Only SSL and TLS handshakes that include Server Name Indication (SNIs) are supported.

Related features

You can enable the following features as needed to enhance data security.

Feature	Description
Configure an SSL certificate	Enables HTTPS secure acceleration.
Enable HTTP/2	Enables the latest HTTP protocol HTTP/2. Major browsers such as Google Chrome, Internet Explorer 11, Safari, and Mozilla Firefox support HTTP/2.
Enable force redirect	Forcibly redirects end users' requests as HTTP or HTTPS requests.
Configure TLS	Ensures communication security and data integrity.
Configure HSTS	Forces clients such as browsers to communicate with servers over HTTPS. This reduces the risk where requests are hijacked.

8.2. Overview of certificate formats

This topic provides an overview of the certificates supported by Alibaba Cloud CDN and how to convert various certificates into PEM formats. To access resources through HTTPS secure acceleration, you must configure an HTTPS certificate.

certificate format HTTPS secure acceleration PEM format

Root CA certificates

Root CA certificates are issued by root CAs including Apache, IIS, Nginx, and Tomcat. Each root CA certificate is unique. Alibaba Cloud CDN uses root CA certificates issued by Nginx. A .crt file contains certificate information and a .key file contains private key information.

A root CA certificate must conform to the following rules:

- It starts from `-----BEGIN CERTIFICATE-----` and ends with `-----END CERTIFICATE-----`.
- All lines except the last line must contain 64 characters.
- The last line contains 1 to 64 characters.

The following figure shows an example certificate in PEM format when your system runs a Linux operating system.

Intermediate CA certificates

A certificate file issued by an intermediate CA includes multiple certificates. You must copy and paste them at the end of the server certificate file.

> **Note** In most cases, the rules for combining the server certificate with the intermediate certificates are specified when the intermediate CA issues the certificates. Read the rules before you combine the certificates.

The chain of certificates issued by an intermediate CA is as follows:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

The certificates in the chain must conform to the following rules:

- Blank lines are not allowed between certificates.
- Each certificate must be in the specified format.

RSA private keys

An RSA private key must conform to the following rules:

- In the private key `openssl genrsa -out privateKey.pem 2048` generated on your computer, `privateKey.pem` is your private key file.
- The private key starts with `-----BEGIN RSA PRIVATE KEY-----` and ends with `-----END RSA PRIVATE KEY-----`.
- All lines except the last line must contain 64 characters.
- The last line contains 1 to 64 characters.

If your private key does not comply with the preceding rules, for example, `-----BEGIN PRIVATE KEY-----` or `-----END PRIVATE KEY-----`), you can convert it as follows:

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

Then, upload the `new_server_key.pem` private key file together with the certificate file.

Convert certificate formats

HTTPS only supports certificates in PEM format. If your certificates are not in PEM format, you must convert them into PEM formats. We recommend that you use OpenSSL to convert certificate formats. The following are methods for converting various certificates into PEM formats:

- Certificates in DER format

  These certificates are typically used for Java.

  - Convert a certificate from DER to PEM formats as follows:

    ```
    openssl x509 -inform der -in certificate.cer -out certificate.pem
    ```

  - Convert a private key from DER into PEM formats as follows:

    ```
    openssl rsa -inform DER -outform pem -in privatekey.der -out privatekey.pem
    ```

- Certificates in P7B format

  These certificates are typically used for Windows Server and Tomcat.

  - Convert a certificate from P7B to PEM formats as follows:

    ```
    openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
    ```

    You must copy the part starting from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----` in the `outcertificat.cer` certificate to the certificate file.

  - A certificate in P7B format does not have a private key. When you configure an HTTPS certificate on the Alibaba Cloud console, you only need to enter the certificate information.

- Certificates in PFX format

  These certificates are typically used for Windows Server.

  - Convert a certificate from PFX to PEM formats as follows:

    ```
    openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
    ```

  - Convert a private key from PFX to PEM formats as follows:

    ```
    openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
    ```

8.3. Configure an SSL certificate

Hypertext Transfer Protocol Secure (HTTPS) is used for secure communication over networks. It provides reinforced protection for content accelerated by Alibaba Cloud Content Delivery Network (CDN). Secure Sockets Layer (SSL) secures the data transmitted between clients and servers while Alibaba Cloud CDN accelerates content delivery. This topic describes how different types of SSL certificate are validated and configured.

HTTPS secure acceleration accelerated domain name CDN

Context

Alibaba Cloud CDN supports only SSL certificates in the `PEM` format. If your certificate is not in the `PEM` format, convert it to the PEM format first. For more information, see Convert certificate formats.

HTTPS secure acceleration is a value-added service. After you enable HTTPS, you are charged based on the number of HTTPS requests. You cannot use CDN data transfer plans to offset the fees. For more information about the pricing of HTTPS secure acceleration, see Value-added service billing.

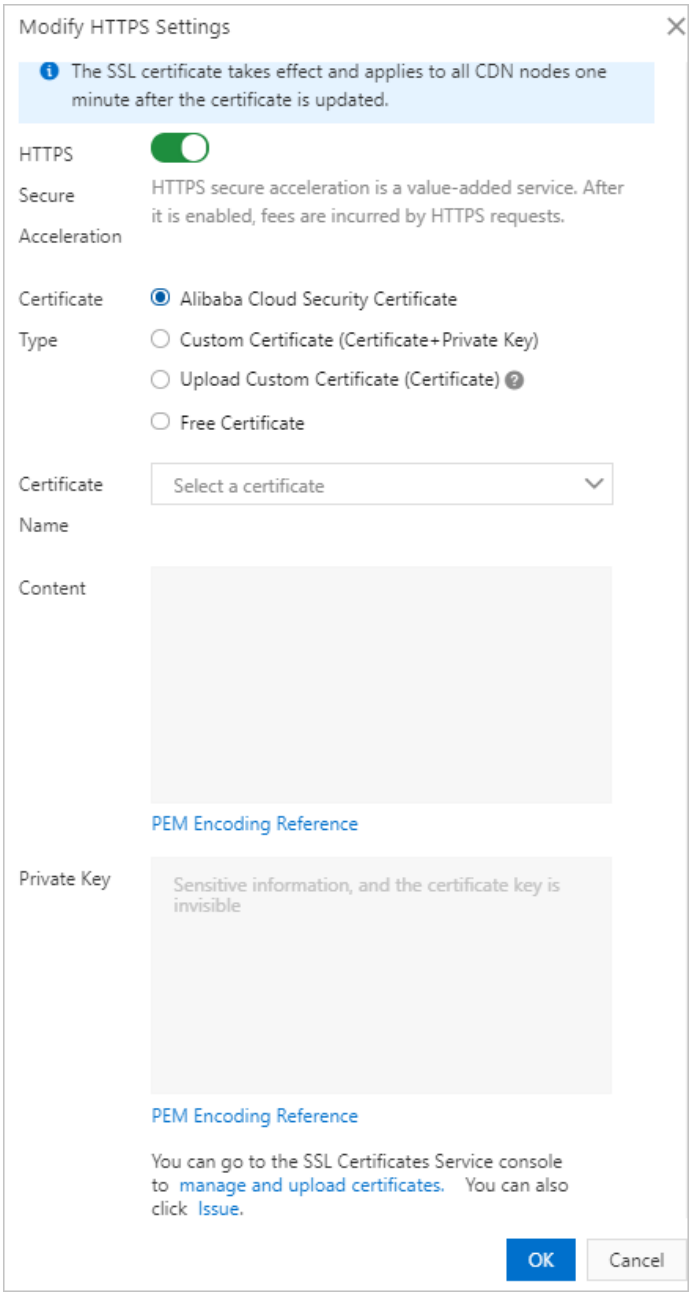
Certificates are classified into the following types based on the validation level:

- A domain validated (DV) certificate has a safety lock. It only verifies the ownership of a domain. A DV certificate verifies the ownership of a domain name by verifying the specified file of the domain name or the TXT record of the domain name.
- An organization validated (OV) certificate is a standard SSL certificate that verifies the identity of an organization. An OV certificate provides more trust than a DV certificate, but the validation process is stricter and longer. OV certificates are typically used in the e-commerce, education, and gaming sectors.
- An extended validation (EV) certificate follows the guidelines maintained by the Certification Authority Browser Forum, also known as the CA/Browser Forum. EV certificates are SSL certificates of the highest security level. Each EV certificate is identified by an object identifier (OID), which is a complete enterprise name. EV certificates are widely used in sectors such as financial transactions and online banking.

> **Note** SSL certificates for Alibaba Cloud CDN do not support the 3DES algorithm.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4.
5. In the **HTTPS Certificate** section, click **Modify**.
6. In the **Modify HTTPS Settings** dialog box, turn on the **HTTPS Secure Acceleration** switch and set the required parameters.



After you enable HTTPS secure acceleration, the system displays a message, stating that HTTPS secure acceleration is charged independently. Confirm whether to enable this feature based on your actual needs. For more information about the pricing of HTTPS secure acceleration, see Value-added service billing.

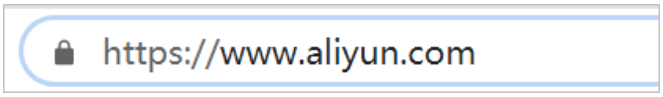
Parameter	Description

Parameter	Description
Certificate Type	◦ Alibaba Cloud Security Certificate You can apply for certificates of various providers and types in the SSL Certificates Service console. ◦ Custom Certificate (Certificate+Private Key) If you cannot find a suitable certificate, upload a custom certificate. To upload a custom certificate, you need to enter a certificate name and upload the certificate content and private key. The uploaded certificate will be saved to SSL Certificates Service. You can check the certificate on the SSL Certificates page. ◦ Free Certificate Free certificates are used only for HTTPS secure acceleration. You cannot manage free certificates or view their public or private keys in the SSL Certificates Service console. ■ Free certificates are typically issued within one to two business days. During this period of time, you can choose to upload a custom certificate or select a certificate from Alibaba Cloud SSL Certificates Service. Note After you submit the application, the certificate may be issued within several hours or two business days. The time it takes depends on the verification process required by the certificate authority. ■ Free certificates are valid for one year and are automatically renewed upon expiration. ■ You do not need to apply for a new certificate each time you enable HTTPS secure acceleration. You must apply for a new certificate only if the current one has expired. You can switch between an Alibaba Cloud certificate, a custom certificate, and a free certificate as needed.
Certificate Name	When you set **Certificate Type** to **Alibaba Cloud Security Certificate** or **Custom Certificate (Certificate+Private Key)**, you must specify the certificate name.
Content	When you set **Certificate Type** to **Custom Certificate (Certificate+Private Key)**, this parameter is required. For more information, see the **Content** below the **PEM Encoding Reference** field.
Private Key	When you set **Certificate Type** to **Custom Certificate (Certificate+Private Key)**, this parameter is required. For more information, see the **Private Key** below the **PEM Encoding Reference** field.

7. Click **OK**.

What's next

After a certificate is uploaded, it takes effect within one minute. To verify that the HTTPS certificate takes effect, send HTTPS requests to access resources. If the URL is displayed with a lock icon in the address bar of the browser, HTTPS secure acceleration is working as expected.



8.4. Enable HTTP/2

HTTP/2 is the latest version of HTTP, which has improved resource access efficiency and security. This topic describes the concept and benefits of HTTP/2, and how to enable it.

HTTP/2 Configure certificate CDN HTTP 2.0

Prerequisites

Make sure an HTTPS certificate is configured. For more information, see Configure an SSL certificate.

Note

- If this is the first time that you configure an HTTPS certificate, you must wait for the certificate to take effect before enabling HTTP/2.
- If you disable HTTPS acceleration after enabling HTTP/2, HTTP/2 is automatically disabled.

Context

HTTP/2, originally named HTTP 2.0, is the latest version of HTTP. It is supported by all major browsers such as Google Chrome, Internet Explorer 11, Safari, and Mozilla Firefox. HTTP/2 provides optimized performance and is compatible with HTTP/1.1 semantics. HTTP/2 is similar to SPDY but differs greatly from HTTP/1.1.

Benefits of HTTP/2:

- Binary encoding: Unlike HTTP 1.x that parses data into texts, HTTP/2 splits the data to be transmitted into messages and frames and encodes them into binary formats. Binary encoding makes HTTP/2 more scalable. For example, frames can be introduced to transmit data and instructions.
- Content security: HTTP/2 is designed based on HTTPS, protecting content security while maintaining network performance.
- Multiplexing: HTTP/2 allows multiplexing of multiple concurrent streams on a single connection. Specifically, you can initiate countless requests at the same time over one connection by using a browser, and the server returns the responses to these requests at the same time. In addition, you can set stream dependencies, which the client uses to inform the server of the importance of a given stream relative to other streams on the same connection, so that resources can be allocated appropriately.
- Header compression: HTTP headers carry large volumes of information, which is transmitted repeatedly. HTTP/2 compresses HTTP headers into the HPACK format, allowing both ends of the communications to each cache a copy of the HTTP header indexes and hence transmit only index numbers for duplicate HTTP headers. This increases transmission speed and efficiency.
- Server push: Like SPDY, HTTP/2 can push messages to clients. HTTP/2 is widely adopted by many websites, such as Google.com, Amazon.com, and Taobao.com. You can use Google Chrome to log on to the Alibaba Cloud CDN console and check whether HTTP/2 is enabled.

> **Note** SPDY is an application layer protocol developed by Google based on TCP. SPDY minimizes network latency to accelerate network access and improve user experience. SPDY is not a replacement for HTTP but serves as an enhancement to HTTP. Similar to HTTP/2, SPDY also provides multiplexing, request prioritization, and HTTP header compression.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4.
5. On the **HTTP/2** tab, turn on **HTTP/2**.

8.5. Enable force redirect

You can enable the Force Redirect function to redirect the original requests from a client to L1 as HTTP or HTTPS requests. This topic describes how to enable the Force Redirect function.

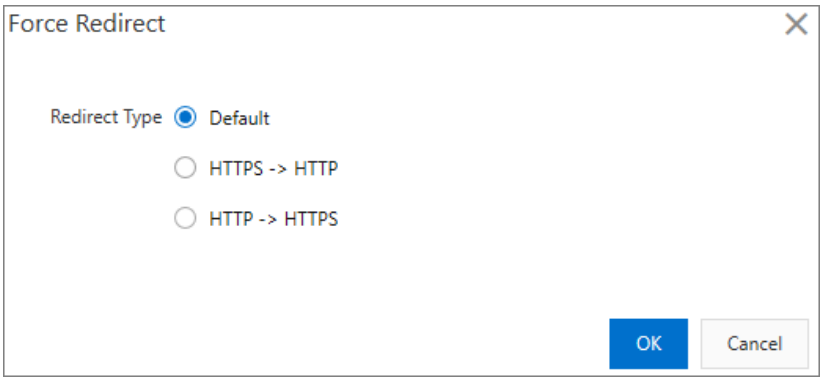
Force redirect CDN HTTPS acceleration

Prerequisites

Make sure an HTTPS certificate is configured. For more information, see Configure an SSL certificate.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **HTTPS**.
5. In the **Force Redirect** section, click **Modify**.

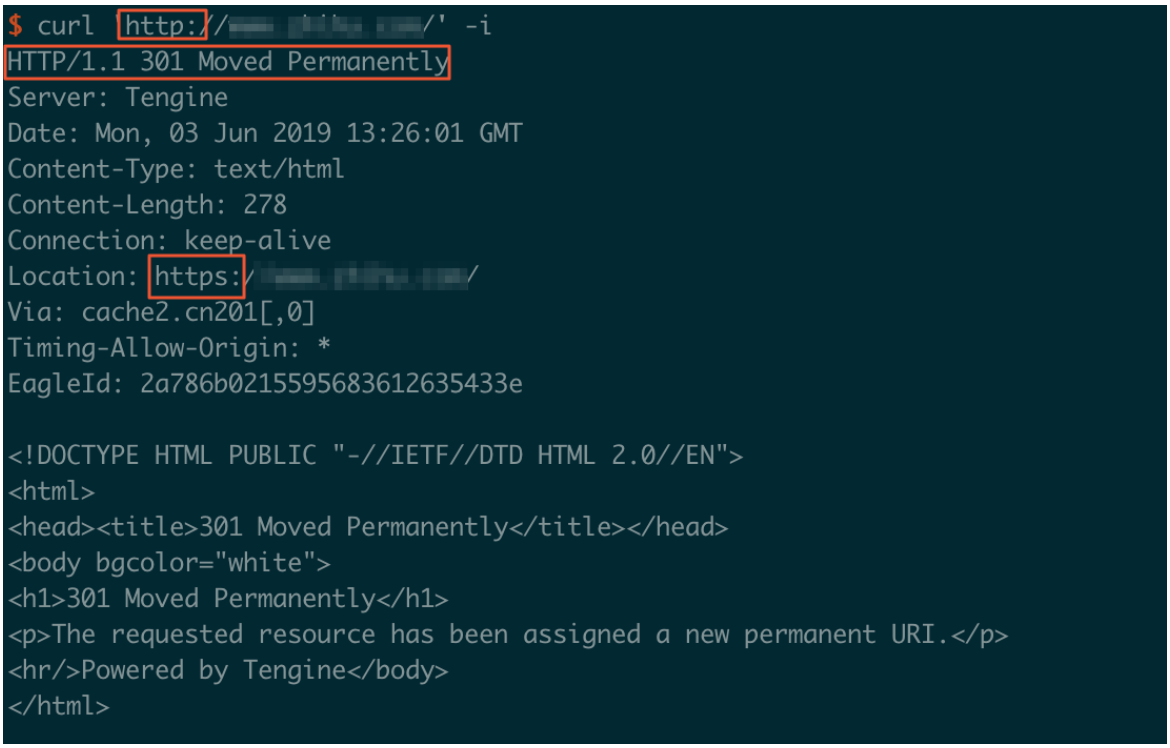


6. In the **Force Redirect** dialog box that appears, set **Redirect Type**.

Redirect Type	Description
Default	CDN supports both HTTP and HTTPS requests.
HTTPS -> HTTP	CDN redirects the requests from a client to L1 as HTTP requests.
HTTP -> HTTPS	CDN redirects the requests from a client to L1 as HTTPS requests.

Assume that you set Redirect Type to HTTP -> HTTPS.

When your client initiates an HTTP request, the server returns a 301 redirect response to redirect the HTTP request as an HTTPS request, as shown in the following figure.



7. Click **OK**.

8.6. Configure TLS

You can use the TLS Version Control function of Alibaba Cloud CDN to ensure the data security and integrity of all Internet services and communications. You can configure TLS versions based on domain names. This topic describes how to configure TLS for a domain.

TLS HTTPS certificate

Prerequisites

Make sure an HTTPS certificate is configured. For more information, see Configure an SSL certificate.

Context

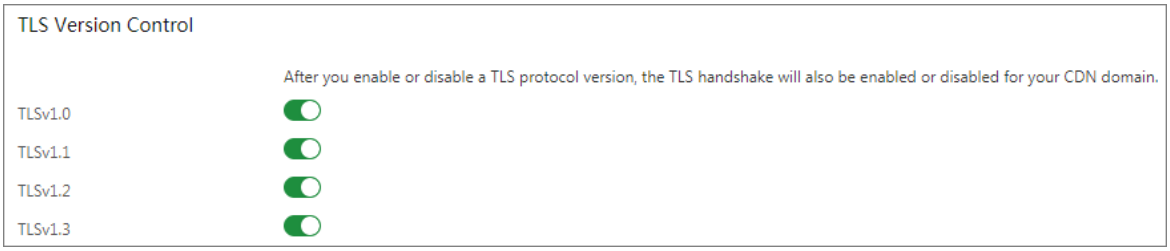
Transport Layer Security (TLS) is designed to ensure the security and integrity of data transmitted between two applications. HTTPS is a typical application of TLS. HTTPS, also known as HTTP over TLS, is a secure version of HTTP. HTTPS runs below the top application layer (HTTP) and above the transport layer (TCP), providing data encryption and decryption services.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4.
5. In the **TLS Version Control** section, you can enable or disable specific TLS versions as needed.

The following table describes TLS versions.

TLS version	Description	Supported browser
TLS 1.0	TLS 1.0 was defined in RFC 2246 in 1999 as an upgrade of SSL 3.0. This version is vulnerable to various attacks such as BEAST and POODLE attacks. It is not strong enough to protect today's network connections and does not comply with Payment Card Industry Data Security Standard (PCI DSS).	○ Internet Explorer 6 and later ○ Google Chrome 1 and later ○ Mozilla Firefox 2 and later
TLS 1.1	TLS 1.1 was defined in RFC 4346 in 2006 as an update for TLS 1.0. This version fixed some vulnerabilities of TLS 1.0.	○ Internet Explorer 11 and later ○ Google Chrome 22 and later ○ Mozilla Firefox 24 and later ○ Safari 7 and later
TLS 1.2	TLS 1.2 was defined in RFC 5246 in 2008 and has become the most widely used TLS version.	○ Internet Explorer 11 and later ○ Google Chrome 30 and later ○ Mozilla Firefox 27 and later ○ Safari 7 and later
TLS 1.3	TLS 1.3 was defined in RFC 8446 in 2018. TLS 1.3 is faster because it supports the 0-RTT mode. Also, this version is more secure as it only supports perfect forward secrecy key exchange algorithms.	○ Google Chrome 70 and later ○ Mozilla Firefox 63 and later



Note TLS 1.0, TLS 1.1, and TLS 1.2 are enabled by default.

8.7. Configure HSTS

This topic describes how to configure HTTP Strict Transport Security (HSTS). After HSTS is configured, a client can only establish HTTPS connections.

HSTS CDN HTTPS connection

Prerequisites

An HTTPS certificate is configured. For more information, see Configure an SSL certificate.

Context

When HTTPS is enabled for your website, all HTTP requests destined for the website are redirected to HTTPS through 301 and 302 errors regardless whether you enter an HTTP URL in the address bar of the browser or directly click an HTTP URL. During the redirection process, the request and response messages may be hijacked and consequently the redirected requests cannot be sent to the server. HSTS is introduced to resolve this issue.

HSTS is a response header, `Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]`. The following table describes the parameters in the header.

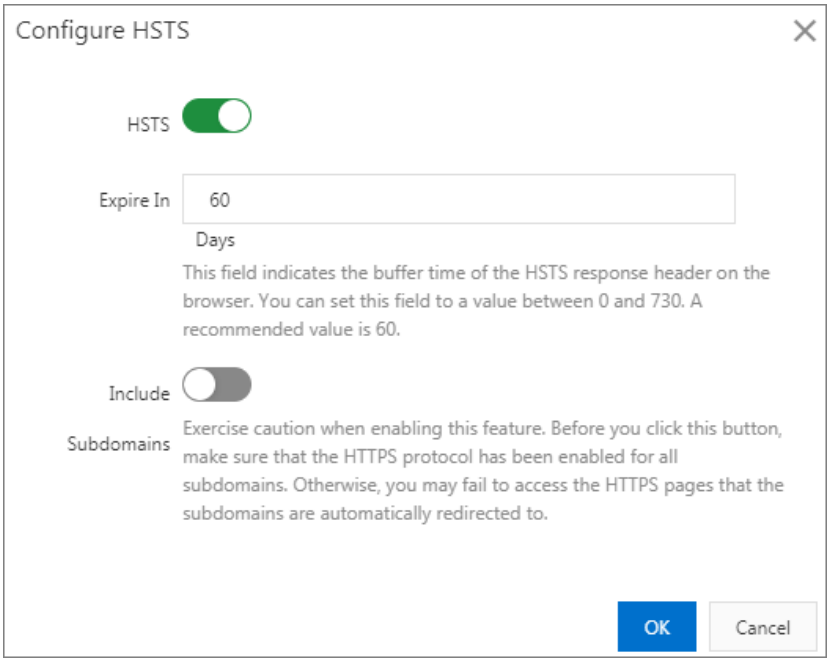
Parameter	Description
max-age	The maximum time period during which the requested resource is cached. Unit: second.
Strict-Transport-Security	Within the time period specified by the max-age parameter, if the Strict-Transport-Security parameter in the HTTP request from the domain has not expired, the browser redirects the HTTP request to HTTPS through a 307 error. This helps to prevent hijacking risks that may arise when the HTTP request is redirected between the server and browser through a 310 or 302 error.
includeSubDomains	Optional. If this parameter is set, the preceding parameters take effect on all subdomains of the domain.
preload	Optional. This parameter enables you to preload a list.

Note

- Before HSTS takes effect, the first HTTP request is redirected to HTTPS through a 301 or 302 error.
- The HSTS response header takes effect on the responses to HTTPS requests but not on the responses to HTTP requests.
- HSTS takes effect only on Port 443 and on domains instead of IP addresses.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4.
5. In the **HSTS** section, click **Modify**.



6. In the displayed **Configure HSTS** dialog box, turn on the **HSTS** switch, and set Expire In and Include.
7. Click **OK**.

8.8. Configure OCSP stapling

OCSP stapling is an alternative approach to the Online Certificate Status Protocol (OCSP) that you can use to validate digital certificates. OCSP stapling allows Alibaba Cloud CDN servers to retrieve OCSP details. This reduces the latency that occurs when clients send requests to validate digital certificates. OCSP stapling also reduces the time that is required by clients to receive the validation responses. This topic describes the application scenarios of OCSP stapling. It also provides details about how to enable this feature in the Alibaba Cloud CDN console.

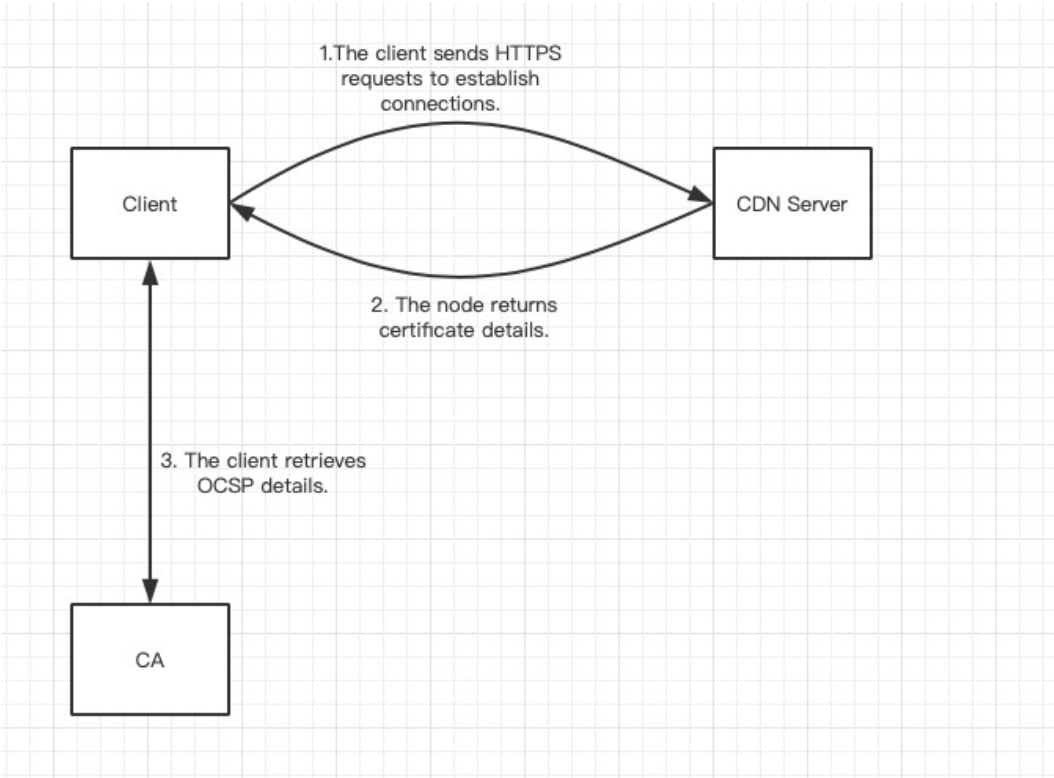
Prerequisites

OCSP extension fields are supported by clients. Otherwise, the OCSP stapling feature fails to take effect.

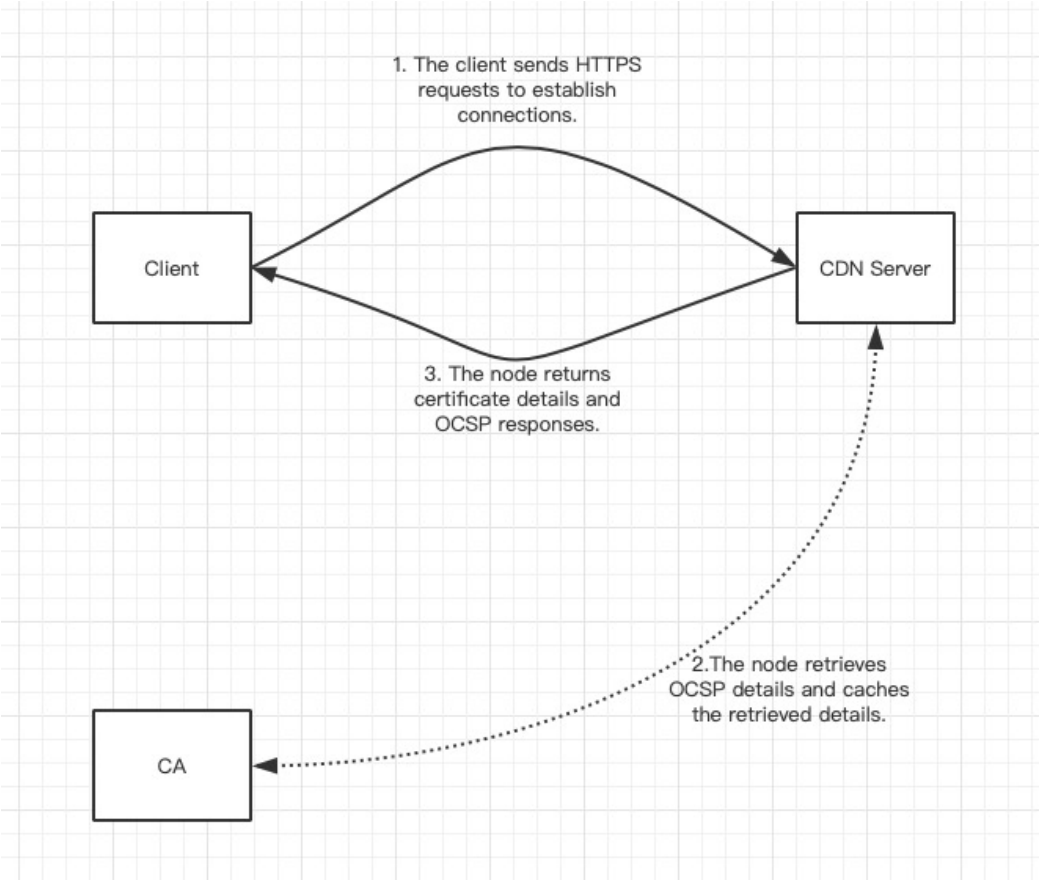
Context

OCSP details are provided by the certification authority (CA) that issues the digital certificates. Based on the OCSP details, you can check the digital certificates online in real time to determine whether they are valid.

Issue description: Clients such as web browsers send certificate validation requests to the OCSP responders that are provided by CAs. If network connections are intermittent or interrupted, clients have to wait for the validation responses for a long time. During this period, blank pages appear and your users cannot perform subsequent operations as expected.



Solution: Alibaba Cloud CDN provides the OCSP stapling feature. If this feature is enabled, Alibaba Cloud CDN servers send requests to retrieve OCSP details at a low frequency, and cache the retrieved OCSP details. When clients initiate Transport Layer Security (TLS) handshakes, Alibaba Cloud CDN servers return the OCSP details and certificate chains to clients. OCSP stapling provides a quick method for the clients to receive the validation responses. This allows your users to perform subsequent operations as expected. Another benefit is that the OCSP stapling process does not introduce additional security risks. This is because the OCSP details of digital certificates cannot be forged.



Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4.
5. In the **OCSP Stapling** section, turn on the **switch**.

8.9. FAQ

- Does HTTPS secure acceleration incur additional fees?
- Will my access speed drop and resource usage increase after I enable HTTPS secure acceleration?
- Should I enable HTTPS only for when I log on to a website?
- What are common HTTP attacks?

Does HTTPS secure acceleration incur additional fees?

Yes. HTTPS secure acceleration takes effect on the link from the client to the serving edge node. The SSL handshakes and content encryption and decryption all require computation, which makes the CDN server consume more CPU resources. However, the number of resources consumed on the origin server remains unchanged because the link from the serving edge node to the client still uses HTTP.

- If you purchase a certificate, you are charged for additional fees.

  > **Note** You can apply for free certificates on the Alibaba Cloud CDN console. Free certificates provided by Alibaba Cloud CDN are of the DV certification level. You can apply for one free certificate for each accelerating domain. The validity period of a free certificate is one year. When a free certificate is about to expire, the system automatically renews it.

- After you configure an HTTPS certificate for an accelerating domain, you are charged 0.008 USD for every 10,000 static HTTPS requests destined for CDN nodes in this domain.

Will my access speed drop and resource usage increase after I enable HTTPS secure acceleration?

No, overall your access speed will remain the same, and the number of resources used will not increase as a result of enabling HTTPS secure acceleration. However, note that your access speed may drop by 10% the first time you access a website after you enable HTTPS because an initial Secure Sockets Layer (SSL) connection takes more time. After an HTTPS connection has been established, the access speed will return to normal.

Should I enable HTTPS only for when I log on to a website?

We do not recommend that you enable HTTPS only for when you log on to a website because this will negatively affect overall your website security and network performance. Specially, in terms of website security, if HTTPS is enabled for only some web pages, then there is the possibility that resources may be leaked while you are using HTTPS or an unsecure CDN service. Next, in terms of network performance, enabling HTTPS for only some web pages will cause the server to need to continually switch from HTTPS and HTTP, which can result in access speed decreases.

What are common HTTP attacks?

HTTPS is only one of the many ways to guarantee secure access. To ensure the overall network security, you need to deploy web application firewalls (WAFs) and defend against threats such as distributed denial-of-service (DDoS) attacks. Common HTTPS attacks are as follows:

- SQL injection

  SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into entry fields for execution in an SQL database. As a result, SQL statements are not executed as what developers have expected.

- Cross-site scripting (XSS)

  Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages. When other users surf on these web pages, their identities and permissions are exploited to execute the injected scripts, which are intended to tamper with or even steal the user information.

- Cross-site request forgery (CSRF)

  Cross-site request forgery (CSRF) enables attackers to forge a request, in which a user submits a form, thereby tampering with the user data or executing a specific task. To spoof a user's identity, CSRF is often launched with XSS or by using means such as tricking the user into clicking a link into which CSRF is embedded.

- HTTP header injection

  When you use a browser to visit a website, HTTP is used no matter what technology and framework were used to design this website. According to HTTP, a blank line lies between the header and content of a response message. This blank line, which is equivalent to two sets of CRLF (0x0D 0A), marks the end of the header and the start of the content. Attackers can exploit this vulnerability to inject any characters into the header.

- Open redirect

  Open redirect is typically launched by using a phishing attack. Attackers masquerade as a trusted entity to send a user a link. When the user clicks this link, they are redirected to a malicious website, where the user data is stolen. We recommend that all redirection operations must be authenticated, so that users will not be redirected to malicious websites. One solution to this vulnerability is to add trusted URLs to a whitelist. Any redirections to domains that are not included in the whitelist will be denied. The other solution is to add redirection tokens to trusted URLs, which will be verified based on the tokens when users are to be redirected to these URLs.

9.Access control

9.1. Overview

You can configure referer, IP, and User-Agent blacklists or whitelists and URL signing to authenticate and authorize visitors. With these features, you can control access to CDN resources and improve the security of your CDN service.

You can use the following features to implement access control.

Feature	Description
Configure hotlink protection	Allows you to configure a referer blacklist or whitelist to authenticate and authorize visitors, so that you can control access to CDN resources.
Configure URL signing	Allows you to configure URL signing to prevent unauthorized downloads and use of resources on origin servers. URL signing is more secure than referer-based hotlink protection.
Configure an IP address blacklist or whitelist	Allows you to configure an IP address blacklist or whitelist to authenticate and authorize visitors, so that you can control access to CDN resources.
UA blacklist and whitelist	Allows you to configure a User-Agent blacklist or whitelist to authenticate and authorize visitors, so that you can control access to CDN resources.

9.2. Configure hotlink protection

You can configure a referer blacklist or whitelist to authenticate and authorize visitors. This can restrict access to CDN resources and improve CDN security. This topic describes how the hotlink protection feature of Alibaba Cloud CDN works and how to configure the feature.

Hotlink protection CDN

Context

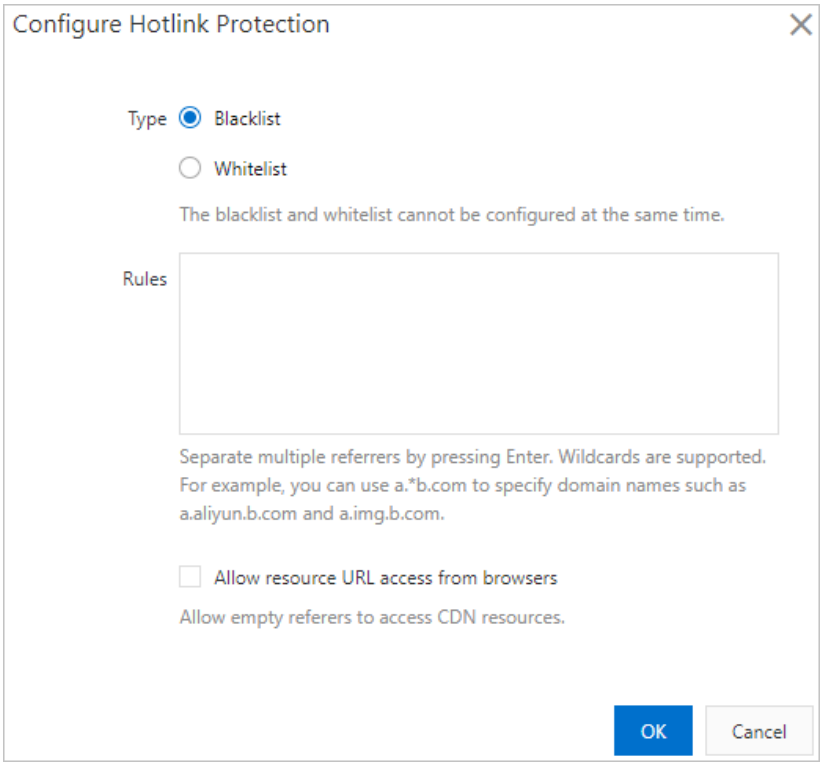
- Hotlink protection is implemented by the HTTP referer mechanism. Referer is used to track and identify where requests come from.
- Hotlink protection supports blacklist or whitelist configuration. When a CDN node receives resource requests from users, it will filter requests based on the configured blacklist or whitelist. A request with the domain name in the whitelist will be allowed. A request with the domain name in the blacklist will be rejected and status code 403 will be returned.

> Notice
>
> - Hotlink protection is optional. By default, hotlink protection is disabled.
> - The blacklist and whitelist are mutually exclusive, and whichever configured last takes effect.
> - When a domain name is added to the whitelist or blacklist, a wildcard (*) is automatically prepended to the domain name. For example, if you enter a.com, the domain name that actually takes effect is *.a.com. Hotlink protection takes effect on all the subdomains of a.com.
> - You can select the check box to specify whether to allow requests with an empty referer header to access CDN resources. If the check box is selected, you can directly access CDN resources by entering a URL in the address bar of your browser.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Access Control**.
5. On the **Hotlink Protection** tab, click **Modify**.
6. Configure **Blacklist** or **Whitelist** as prompted.

Parameter	Description
Type	The following two types are supported: ○ Blacklist Blacklisted domain names cannot be used to access the current CDN resources. ○ Whitelist Only whitelisted domain names can be used to access the current CDN resources. The blacklist and whitelist are mutually exclusive, and whichever configured last takes effect.
Rules	Separate multiple domain names with carriage return characters. You can use wildcards (*) to perform a fuzzy match. For example, `a.*b.com` can match `a.aliyun.b.com` or `a.img.b.com`.



7. Click **OK**.

9.3. Business type

9.3.1. Configure URL signing

The URL signing feature protects origin server resources from unauthorized download and access. With the hotlink protection feature, you can configure a referer blacklist or whitelist to prevent some hotlinking issues. However, hotlink protection cannot completely protect resources on the origin server because referer content can be forged. To resolve this issue, URL signing is provided to protect resources on the origin server, which is more secure and effective.

Signing Content Delivery Network (CDN) Access control

Context

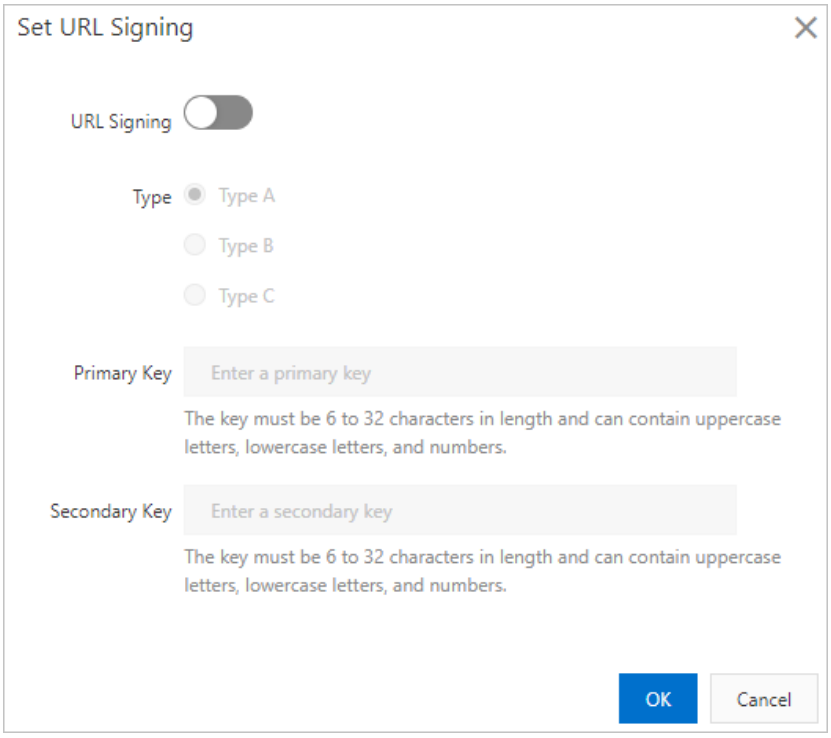
By working with the origin server, a CDN node implements URL signing to protect resources on the origin server in a more secure and reliable manner.

- The CDN node provides encrypted URLs that contain permission verification information.
- You can send a request to a CDN node by using an encrypted URL.
- The CDN node authenticates the permission information in the encrypted URL to determine whether the request is valid. If the request is valid, the CDN node returns a successful response. If the request is invalid, the CDN node rejects the request.

For more information about sample Python authentication code, see Sample authentication code.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Access Control**.
5. Click the **URL Signing** tab.
6. In the **URL Signing** section, click **Modify**.



7. Turn on **URL Signing** and configure the required parameters.

Parameter	Description
Type	Alibaba Cloud CDN supports three signing types. You can select a signing type based on your needs to protect resources on the origin server. The following URL signing types are supported: ○ Authentication type A ○ Authentication Type B ○ Authentication type C **Note** If a URL signing error occurs, a 403 error is returned. ○ MD5 calculation errors Example: `X-Tengine-Error:denied by req auth: invalid md5hash=de7bfdc915ced05e17380a149bd760be` ○ Time-related errors Example: `X-Tengine-Error:denied by req auth: expired timestamp=1439469547`
Primary Key	The primary key corresponding to the selected signing type.
Secondary Key	The secondary key corresponding to the selected signing type.

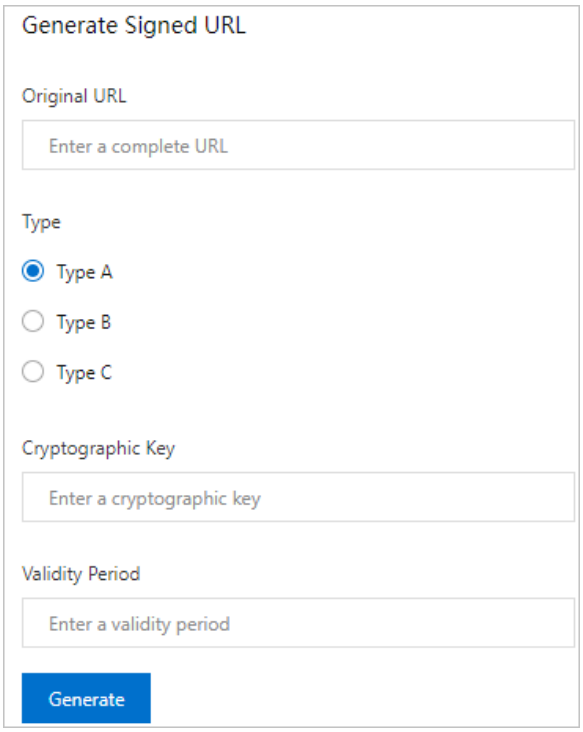
8. Click **OK**.

What's next

To generate a signed URL, follow these steps:

1. In the **Generate Signed URL** section, configure **Original URL** and signing information.

Parameter	Description
Original URL	Enter a complete original URL, for example, `https://www.aliyun.com`.
Type	Select a signing type based on your needs. ○ Authentication type A ○ Authentication Type B ○ Authentication type C
Cryptographic Key	Set the signing key. Cryptographic Key can be Primary Key or Secondary Key configured in the **Set URL Signing** dialog box.
Validity Period	Set the validity period for URL signing. Unit: seconds. Example: 1800.



2. Click **Generate**.

You can obtain **Signed URL** and **Timestamp**.

9.3.2. Authentication type A

The URL authentication feature can help you protect resources on your origin server from unauthorized downloads and access. CDN supports three types of URL authentication. This topic describes the principle of URL authentication type A and provides an example.

Alibaba Cloud CDN authentication CDN authentication

How it works

A URL is signed in the following format:

```
http://DomainName/Filename?auth_key=timestamp-rand-uid-md5hash
```

The following table describes the fields in a signed URL.

Parameter	Description
DomainName	The domain name of the CDN node.
Filename	The actual URL that points to the requested resource on the origin server. The FileName field must start with a forward slash (`/`).
auth_key	The cryptographic key that you have set.
timestamp	The expiration date of the cryptographic key. The value is a 10-digit positive integer. It specifies the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970 plus the time-to-live (TTL) value of the cryptographic key. The TTL of the cryptographic key is set on the client. If it is set to 1,800 seconds, the cryptographic key expires 1,800 seconds after you connect to the CDN node. For example, if you set the connection time to 2020-08-15 15:00:00, the cryptographic key expires at 2020-08-15 15:30:00.
rand	The random number. The number must not contain hyphens `(-)` . Example: 477b3bbc253f467b8def6711128c7bec. We recommend that you use a UUID.
uid	The user ID. Set this field to 0.
md5hash	The string calculated by using the MD5 algorithm. It must be 32 characters in length and can contain digits and lowercase letters.

When a CDN node receives a request, it determines whether the sum of the `timestamp` plus the *TTL of the cryptographic key* in the request is earlier than the current time.

- If the sum of the `timestamp` plus the *TTL of the cryptographic key* is earlier than the current time, the CDN node determines that the cryptographic key expires and returns a 403 error.
- If the sum of the `timestamp` plus the *validity period of the cryptographic key* is later than the current time, the CDN node generates a string in the same format as the `sstring` string. It then uses the MD5 algorithm to calculate the `HashValue`, and compares it with the `md5hash` in the request.
  - If they are the same, the authentication succeeds. The CDN node returns the requested resource.
  - If they are different, the authentication fails. The CDN node returns a 403 error.

  The `HashValue` is calculated based on the following string:

  ```
  sstring = "URI-Timestamp-rand-uid-PrivateKey". The URI specifies the address that points to the reque
  sted resource. It does not contain parameters such as /Filename.
  HashValue = md5sum(sstring)
  ```

Example

The following example shows how to implement type-A authentication.

1. Request the resource through `req_auth`.

   ```
   http:// cdn.example.com/video/standard/1K.html
   ```

2. Set the cryptographic key to aliyuncdnexp1234.
3. Set the expiration date of the authentication configuration file to 2015-10-10 00:00:00. Then, the validity period is 1,444,435,200 seconds.
4. The CDN node generates a signature string to calculate the `HashValue`.

   ```
   /video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234
   ```

5. The CDN node calculates the `HashValue` based on the signature string.

   ```
   HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") = 80cd3862d699
   b7118eed99103f2a3a4f
   ```

6. Sign the request URL.

   ```
   http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-80cd3862d699b7118eed9
   9103f2a3a4f
   ```

If the `HashValue` calculated by the CDN node is the same as the `md5hash` contained in the request (both are *80cd3862d699b7118eed99103f2a3a4f*), the request passes the authentication. Otherwise, the authentication fails.

9.3.3. Authentication Type B

The URL authentication feature protects origin server resources from unauthorized download and access. CDN provides you with three authentication types. This topic describes the principle of authentication type B and illustrates it with examples.

Alibaba Cloud CDN authentication CDN authentication

Principle

Encrypted URLs can have the following format:

```
http://DomainName/timestamp/md5hash/FileName
```

If authentication is passed, actual back-to-origin URLs can have the following format:

```
http://DomainName/FileName
```

The following table describes authentication fields.

Parameter	Description
DomainName	The domain name of the CDN node.
timestamp	The time when resources expire. The time is included in the URL and is used to calculate `md5hash`. It is in the YYYYMMDDHHMM format. The validity period is 1,800 seconds. For example, if you set the access time to 2020-08-15 15:00:00, the request URL will expire at 2020-08-15 15:30:00.
md5hash	The string calculated by using the MD5 algorithm. It must be 32 characters in length, and can contain digits and lowercase letters.
Filename	The actual back-to-origin access URL. During authentication, the Filename field must start with a forward slash `(/)`.

Example

The following example shows you how to implement authentication type B.

1. Retrieve the resource from the origin server.

   ```
   http://cdn.example.com/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
   ```

2. Set the key to aliyuncdnexp123.
3. Set the time when origin server is accessed to 201508150800.
4. The CDN node constructs a signature string to calculate `Hashvalue`.

   ```
   aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
   ```

5. The CDN node calculates `md5hash` based on the signature string .

   ```
   md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3")
   = 9044548ef1527deadafa49a890a377f0
   ```

6. Encrypt the request URL.

   ```
   http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0/4/44/44c0909bcfc20a01
   afaf256ca99a8b8b.mp3
   ```

If the `md5hash` calculated by the CDN node is the same as the `md5hash` contained in the request (both are *9044548ef1527deadafa49a890a377f0*), URL authentication succeeds. Otherwise, URL authentication fails.

9.3.4. Authentication type C

The URL authentication feature protects origin server resources from unauthorized download and access. CDN provides you with three authentication types. This topic describes the principle of authentication type C and illustrates it with examples.

Alibaba Cloud CDN authentication CDN authentication

Principle

Encrypted URLs can have the following formats:

- Format 1

```
http://DomainName/{<md5hash>/<timestamp>}/FileName
```

- Format 2

```
http://DomainName/FileName{&KEY1=<md5hash>&KEY2=<timestamp>}
```

> **Note** The content enclosed by braces ({}) indicates the encrypted information that is added based on the standard URL.

The following table describes authentication fields.

Parameter	Description
DomainName	The domain name of the CDN node.
FileName	The actual back-to-origin access URL. During authentication, the Filename field must start with a forward slash (/).
timestamp	The time when the origin server is accessed. The time must be in the UNIX format. It is an unencrypted plain text string that is 10 digits in length. It indicates the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970, expressed in hexadecimal format.
md5hash	The string calculated by using the MD5 algorithm. It must be 32 characters in length, and can contain digits and lowercase letters.

Example

The following example shows you how to implement authentication type C.

- The value of the PrivateKey field: `aliyuncdnexp1234`.
- The value of the FileName field: `/test.flv`.
- The value of the timestamp field: `55CE8100`.
- The MD5 hash value is calculated as follows:

  ```
  md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5fb8f71214b1e7c95ec7a1bd
  ```

- The following encrypted URLs are generated:
  - Format 1:

    ```
    http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/test.flv
    ```

  - Format 2:

    ```
    http://cdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1e7c95ec7a1bd&KEY2=55CE8100
    ```

When you use an encrypted URL to access a CDN node, the CDN node extracts encrypted string 1 and obtains `FileName` and access time of the original URL. The CDN node performs the following steps to validate the request based on the defined business logic:

1. The CDN node uses `Filename`, access time, and `PrivateKey` of the original URL to perform MD5 encryption. The encrypted string 2 is generated.
2. The CDN node compares string 1 and string 2. If the two strings are different, the request is rejected.
3. The CDN node checks whether the difference between its current time and time in the original URL has exceeds the time limit t. The default value of t is 1,800 seconds.
   - If the time difference is less than the time limit, the CDN node returns a successful response.
   - If the time difference is greater than the time limit, the CDN node rejects the request and returns a 403 error.

   > **Note** A validity period of 1,800 seconds indicates that authentication fails when the difference between the time you access the origin server and the preset access time is greater than 1,800 seconds. For example, if you set the access time to 2020-08-15 15:00:00, the request URL will expire at 2020-08-15 15:30:00.

9.3.5. Sample authentication code

Using this demo, you can perform URL authentication based on your business needs. For URL authentication rules, see Configure URL signing.

Authentication

Python version

The following Python Demo contains three authentication methods: Authentication type A, Authentication Type B, and Authentication type C. Each method describes the composition of requested URLs and hash strings.

> Note If the URL contains Chinese characters, you must perform URL encoding.

```
import re
import time
import hashlib
import datetime
def md5sum(src):
m = hashlib.md5()
m.update(src)
return m.hexdigest()
# Authentication method A
def a_auth(uri, key, exp):
p = re.compile("^(http://|https://)?([ ^/?] +) (/[^?] *)? ( \\?. *)? $ ")
if not p:
return None
m = p.match(uri)
scheme, host, path, args = m.groups()
if not scheme: scheme = "http://"
if not path: path = "/"
if not args: args = ""
rand = "0" # "0" by default, other value is ok
uid = "0" # "0" by default, other value is ok
sstring = "%s-%s-%s-%s-%s" %(path, exp, rand, uid, key)
hashvalue = md5sum(sstring)
auth_key = "%s-%s-%s-%s" %(exp, rand, uid, hashvalue)
if args:
return "%s%s%s%s&auth_key=%s" %(scheme, host, path, args, auth_key)
else:
return "%s%s%s%s? auth_key=%s" %(scheme, host, path, args, auth_key)
# Authentication method B
def b_auth(uri, key, exp):
p = re.compile("^(http://|https://)?([ ^/?] +) (/[^?] *)? ( \\?. *)? $ ")
if not p:
return None
m = p.match(uri)
scheme, host, path, args = m.groups()
if not scheme: scheme = "http://"
if not path: path = "/"
```

```
if not args: args = ""
# convert unix timestamp to "YYmmDDHHMM" format
nexp = datetime.datetime.fromtimestamp(exp).strftime('%Y%m%d%H%M')
sstring = key + nexp + path
hashvalue = md5sum(sstring)
return "%s%s/%s/%s%s%s" %(scheme, host, nexp, hashvalue, path, args)
# Authentication method C
def c_auth(uri, key, exp):
p = re.compile("^(http://|https://)?([ ^/?] +) (/[^?] *)? ( \\?. *)? $ ")
if not p:
return None
m = p.match(uri)
scheme, host, path, args = m.groups()
if not scheme: scheme = "http://"
if not path: path = "/"
if not args: args = ""
hexexp = "%x" %exp
sstring = key + path + hexexp
hashvalue = md5sum(sstring)
return "%s%s/%s/%s%s%s" %(scheme, host, hashvalue, hexexp, path, args)
def main(_):
uri = "http://xc.cdnpe.com/ping?foo=bar" # original uri
key = "<input private key>" # private key of authorization
exp = int(time.time()) + 1 * 3600 # expiration time: 1 hour after current itme
authuri = a_auth(uri, key, exp) # auth type: a_auth / b_auth / c_auth
print("URL : %s\nAUTH: %s" %(uri, authuri))
if __name__ == '__main__':
main()
```

9.4. Configure an IP address blacklist or whitelist

You can configure an IP address blacklist or whitelist to identify and filter users. This can restrict access to CDN resources and improve CDN security. This topic describes how to configure an IP address blacklist or whitelist.

CDN whitelist IP address blacklist IP address whitelist

Context

- IP address blacklist: Blacklisted IP addresses are not allowed to access CDN resources.

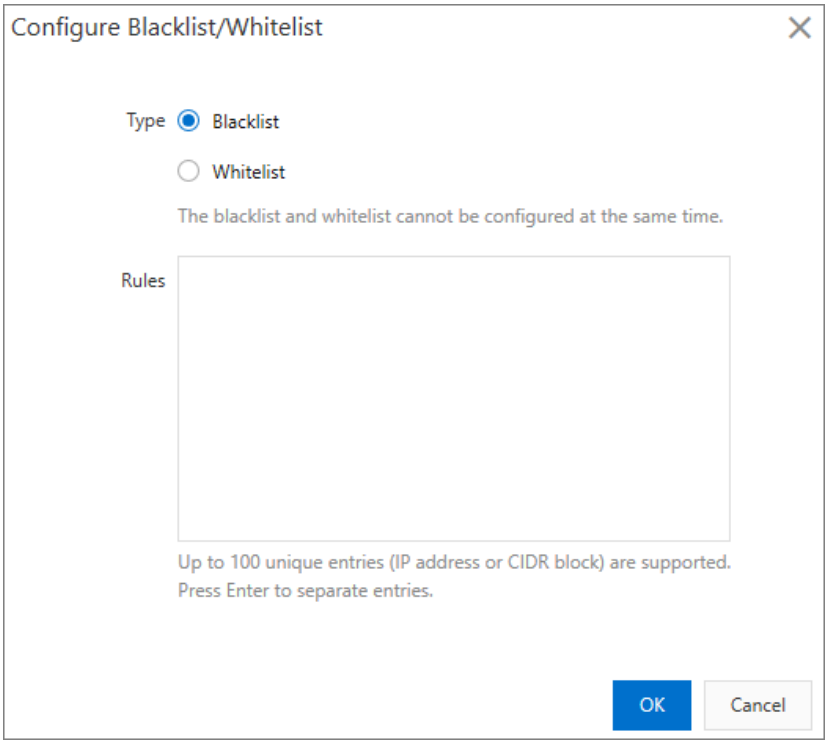
  If your IP address is added to the blacklist, a request from your IP address can still be sent to a CDN node. However, the CDN node will reject the request and return a 403 error. The requests from blacklisted IP addresses are recorded in CDN logs.

- IP address whitelist: Only whitelisted IP addresses are allowed to access CDN resources.

> Note
>
> - Both the IP address blacklist and whitelist support IPv6 addresses.
> - Both the IP address blacklist and whitelist support CIDR notations. For example, in the CIDR block 192.168.0.0/24, /24 indicates that the first 24 bits are network bits. The remaining 8 bits are host bits. The subnet can accommodate 254 hosts. 192.168.0.0/24 indicates the IP addresses from 192.168.0.1 to 192.168.0.254.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Access Control**.
5. Click the **IP Blacklist/Whitelist** tab.
6. Click **Modify** next to **IP Blacklist/Whitelist**.



7. Configure **Blacklist** or **Whitelist** as prompted.

Parameter	Description
Type	The following two types of IP address lists are supported: ○ Blacklist The blacklisted IP addresses are not allowed to access CDN resources. ○ Whitelist Only the whitelisted IP addresses are allowed to access CDN resources. The blacklist and whitelist are mutually exclusive, and whichever configured last takes effect.
Rules	You can add a maximum of 100 IP addresses or CIDR blocks and separate them with carriage return characters. Do not add the same IP address or CIDR block repeatedly. For example, if the CIDR block 192.168.0.1/24 already exists, it cannot be added again.

8. Click **OK**.

9.5. UA blacklist and whitelist

This topic describes UA blacklists and whitelists and how to configure them in the CDN console.

blacklist and whitelist Usage Agent

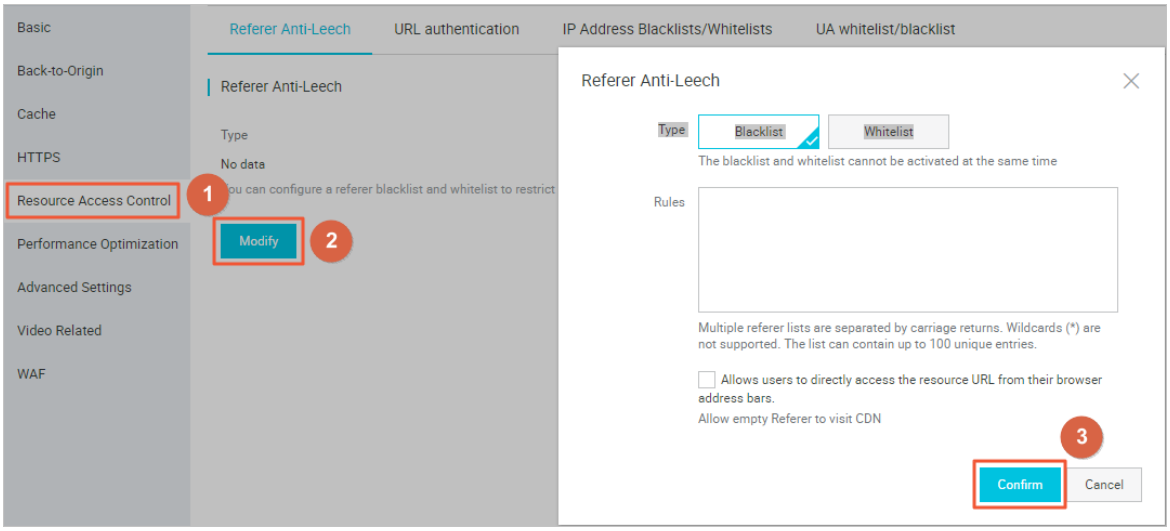
Context

Both UA blacklists and whitelists contain `Usage-Agent` information elements (IEs), which are carried in request messages. After you configure UA blacklists or whitelists for a CDN node, the CDN node filters request messages and permits only the access requests from specific clients.

> **Note**
>
> - `Usage-Agent` IEs are not case-sensitive and can contain wildcard characters (*). The multiple options in a `Usage-Agent` IE are separated by using vertical bars (|). An example `Usage-Agent` IE is as follows: `*curl*|*IE*|*chrome*|*firefox*` .
> - Only the UA blacklist or whitelist can be enabled at a specific time point.

Procedure

1. Log on to the CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. Find the domain name you want to set, and click **Manage** in the **Actions** column.
4. In the left-side navigation pane, click **Resource Access Control**.
5. On the **UA whitelist/blacklist** tab, click **Modify**.
6. Configure the blacklist or whitelist as needed, and click **Confirm**.



9.6. Basic security protection

This topic describes basic security protection features provided by Content Delivery Network (CDN).

Compared with the basic security protection features provided by CDN, Alibaba Cloud Security provides more comprehensive security features. CDN provides the following basic security protection features:

- Hotlink protection

  As an HTTP header field, Referer indicates a URL that can be used to track and identify where an HTTP request comes from. You can configure hotlink protection based on the Referer field to filter requests. In the CDN console, you can configure a whitelist or blacklist of the Referer field values, and specify whether to allow any request with an empty Referer field to retrieve CDN resources. A request with a domain name in the whitelist is allowed. A request with a domain name in the blacklist is rejected. The blacklist and whitelist are mutually exclusive, and whichever is configured last takes effect. In this way, hotlink protection can block malicious requests and secure your business. For more information about the configuration, see Configure hotlink protection.

- IP address blacklist or whitelist

  You can configure an IP address blacklist to restrict requests from the specified IP addresses. For more information about the configuration, see Configure an IP address blacklist or whitelist.

- URL signing

  The URL signing feature prevents unauthorized requests for confidential resources from your origin server. You can configure the rule of signing a specified URL with the key information provided in a specific signing type. This feature can be used to authenticate requests for classified files. A client has to calculate a temporary signature for each request. We recommend that you do not enable this feature for retrieval of common files. Otherwise, compared with the use of a common URL, it takes more time to retrieve common resources based on URL signing. For more information about the configuration, see Configure URL signing.

10.Performance optimization

10.1. Overview

CDN provides multiple optimization functions for you to reduce the size of the content that you want to access, accelerate content delivery, and improve the readability of the requested Web pages.

CDN supports the following optimization functions.

Function	Description
Configure HTML optimization	Removes comments and whitespaces in HTML pages to reduce the payload size and improve the readability.
Configure intelligent compression	Automatically compresses static content with gzip. This significantly reduces the size of the transmitted content and accelerates content delivery.
Configure Brotli compression	Enable Brotli compression if you want to compress static text files. It can reduce the size of the transmitted content and accelerate content delivery.
Configure parameter filtering	If a CDN node receives a URL request with a question mark (`?`) followed by *request parameters*, it determines whether the URL request needs to be rerouted to the origin with the parameters.

10.2. Configure HTML optimization

When you enable the HTML optimization feature, CDN automatically removes redundant comments and duplicate spaces from all HTML pages. This helps reduce file size and improve page readability. This topic describes how to enable the HTML optimization feature.

HTML optimization Performance optimization

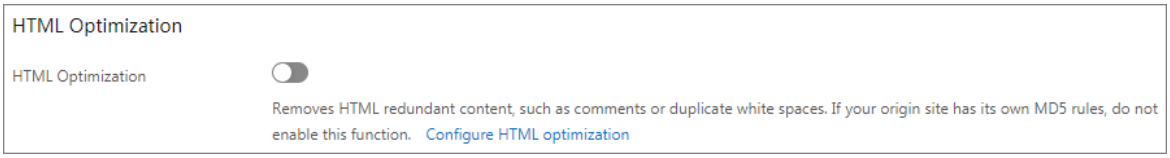
Context

When you enable the HTML optimization feature, CDN automatically removes redundant comments and duplicate spaces from all HTML pages. This helps reduce file size and improve the efficiency of content delivery.

If MD5 validation is configured for a file in the origin server, do not enable this feature. When pages are optimized, the MD5 value of the optimized file is different from that of the file in the origin server, which causes MD5 validation to fail.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Optimization**.
5. In the **HTML Optimization** section, turn on HTML Optimization.



10.3. Configure intelligent compression

When you enable the intelligent compression feature, static files will be automatically GZIP compressed. GZIP compression reduces the size of the transmitted files and accelerates content delivery. This topic describes how to enable the intelligent compression feature.

Accelerated content delivery Intelligent compression GZIP Performance optimization

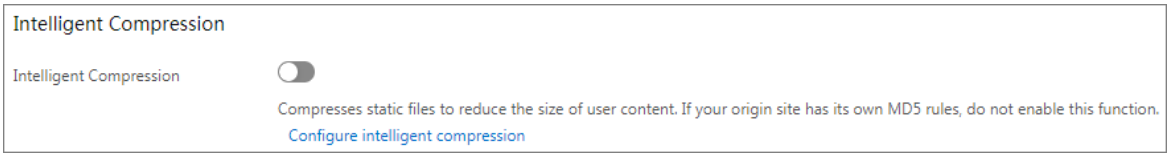
Context

- Intelligent compression supports the following formats: text/html, text/xml, text/plain, text/css, application/javascript, application/x-javascript, application/rss+xml, text/javascript、image/tiff, image/svg+xml, application/json, and application/xmltext.
- If a request from the client includes the `Accept-Encoding: gzip` request header, the client expects the requested resource to be GZIP compressed.
- If a response from a CDN node includes the `Content-Encoding: gzip` response header, the requested resource is GZIP compressed.

> **Notice**
>
> - If MD5 validation is configured for a file in the origin server, do not enable this feature. When a static file is compressed, the MD5 value of the compressed file is different from that of the file in the origin server, which will cause MD5 validation to fail.
> - Files in the origin server will be GZIP compressed only when the file size exceeds 1,024 B.
> - Internet Explorer 6 is not fully compatible with GZIP. If your customers expect to use Internet Explorer 6, we recommend you disable the intelligent compression feature.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Optimization**.
5. In the **Intelligent Compression** section, turn on Intelligent Compression.



10.4. Configure parameter filtering

A CDN node may receive a request of which the URL contains a question mark `(?)` and *parameters*, for example, `http://alibaba.com/content?a=10`. In this case, the CDN node will determine whether to ignore these parameters when it retrieves the requested resource from the cache or the origin server. This topic describes how to filter parameters in URLs of requests that Alibaba Cloud CDN receives.

Filter parameters Parameter filtering

Context

- Parameter filtering is enabled.

  When a CDN node receives a request, the CDN node ignores the parameters following the question mark (?) in the URL. The CDN node caches only one version of the requested resource.

  - Most HTTP requests contain parameters. Content can still be retrieved from the origin when parameters with low priorities are ignored. After you enable parameter filtering, the cache hit ratio and delivery efficiency are improved.
  - If a parameter contains important information such as the file version, we recommend that you specify the parameter as a retained parameter. You can set up to 10 retained parameters. If the requested URL contains a retained parameter, the CDN node will retrieve content from the origin server based on the URL with the retained parameter.
  - Configure the parameter filtering feature to ignore parameters following the question mark (`?`) in the requested URLs. This feature can increase the CDN cache hit ratio. For example, when `http://www. ****.com/1.jpg` is accessed for the first time, Alibaba Cloud CDN cannot retrieve the requested resource from the cache. It needs to request the resource from the origin server. When `http://www. ****.com/1.jpg? test1` is accessed, the parameters following the question mark (`?`) are ignored because parameter filtering is enabled. As a result, the requested resource can be directly retrieved from the cache of `http://www. ****.com/1.jpg`.

- Parameter filtering is disabled.

  A CDN node caches a unique version of a requested resource for each URL that includes different parameters.

After the parameter filtering feature is disabled, the requested resource can be retrieved from the cache only if the parameters following the question mark (?) in the URL are an exact match with the previously cached one. Exact matches can increase request accuracy. For example, when http://www. ****.com/1.jpg is accessed for the first time, Alibaba Cloud CDN cannot retrieve the requested resource from the cache. It needs to request the resource from the origin server. When http://www. ****.com/1.jpg? test1 is accessed, the parameters following the question mark (?) in the URL must be an exact match because parameter filtering is disabled. As a result, the CDN node cannot respond with the cached resource of http://www. ****.com/1.jpg . Instead, the CDN node needs to retrieve the requested resource of http://www. ****.com/1.jpg?test1 from the origin server.

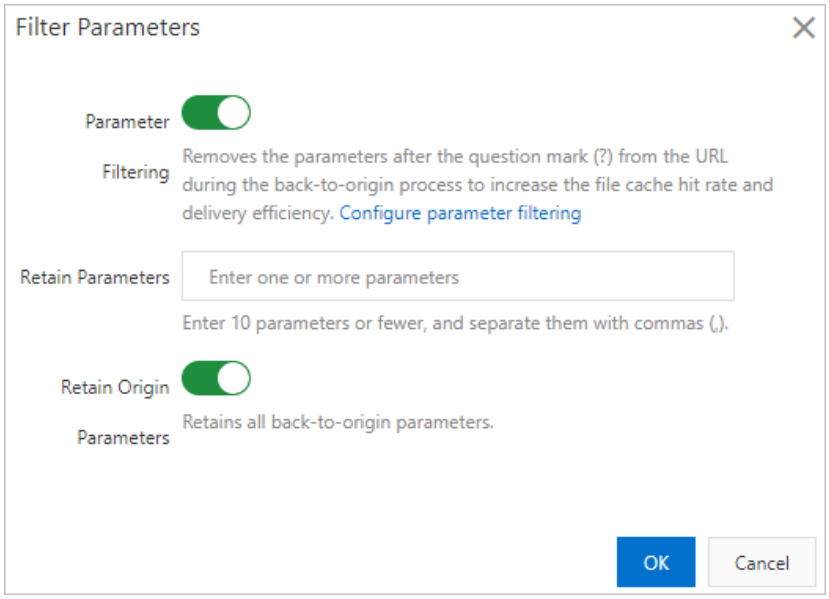
The parameter filtering feature allows you to configure retained parameters or ignored parameters.

- Retained parameters: You can specify one or more parameters to be retained. You must separate multiple parameters with commas (,). Unspecified parameters are not retained.
- Ignored parameters: You can specify one or more parameters to be ignored. You must separate multiple parameters with space characters. Unspecified parameters are not ignored.

> **Note** The URL signing feature takes priority over the parameter filtering feature. The signing information in type A contains the parameters of an HTTP request. Therefore, a CDN node must verify the signed URL of the request before it caches a version of the requested resource. For more information about how to configure URL signing, see Configure URL signing.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Optimization**.
5. On the **Optimization** page, specify the retained parameters or ignored parameters.
   - Retain parameters
     a. On the **Retain Parameters** section, click **Modify**.
     b. You can specify the retained parameters as needed.



Parameter	Description
Parameter Filtering	Enable or disable the parameter filtering feature. After this feature is enabled, the parameters following the question mark (?) in the URL are ignored when the CDN node serves the requested resource from the cache or the origin server. This helps to increase the cache hit ratio.
Retain Parameters	Specify the parameters to be retained. Up to 10 parameters can be specified. Separate multiple parameters with commas (,). Unspecified parameters are not retained. Example: Enter `x=1` in the **Retain Parameters** field for the URL `http://www.abc.com/a.jpg?x=1` .
Retain Origin Parameters	Specify whether to retain all parameters in a URL of a request when Alibaba Cloud CDN retrieves the requested resource from the origin server. After the Retain Origin Parameters switch is turned on, all parameters are retained during the back-to-origin process.

Example description:

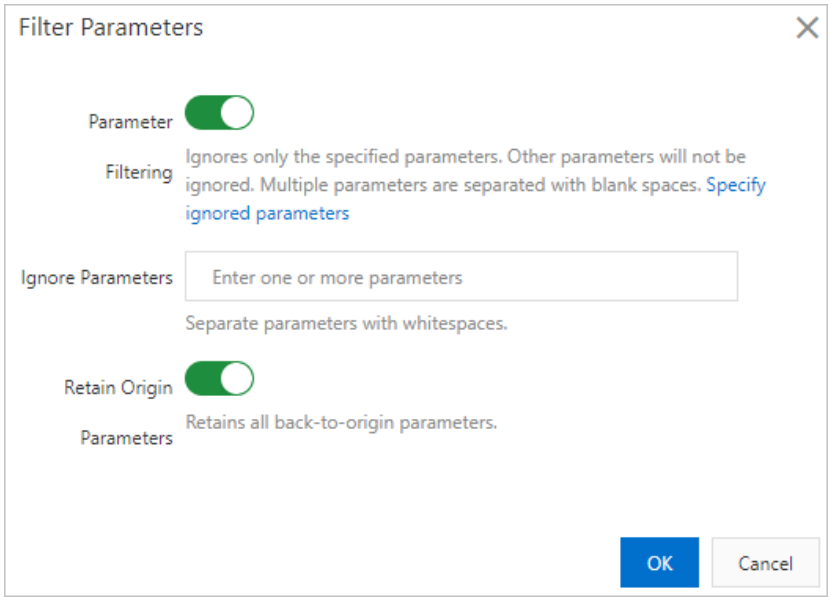
The CDN node sends a request for `http://www.abc.com/a.jpg? x=1` to the origin server with the parameter x=1. The CDN node then retrieves the resource and caches a version of the requested resource. When the CDN node receives a request of which the URL contains the `x=1` parameter, it always returns the version of the resource that was previously cached for `http://www.abc.com/a.jpg?x=1` .

c. Click **OK**.

- Ignore parameters

a. On the **Ignore Parameters** section, click **Modify**.

b. You can specify the ignored parameters as needed.



Parameter	Description
Parameter Filtering	Enable or disable the parameter filtering feature. After parameter filtering is enabled, the parameters following a question mark (?) in a requested URL are ignored when the CDN node serves the requested resource from the cache or the origin server.
Ignore Parameters	Specify the parameters to be ignored. Up to 10 parameters can be ignored. Separate multiple parameters with space characters. Unspecified parameters are not ignored. For example, enter `x=1` in the **Ignore Parameters** field for the URL `http://www.abc.com/a.jpg?x=1`.
Retain Origin Parameters	Specify whether to retain all parameters in a URL when Alibaba Cloud CDN retrieves the requested resource from the origin server. After the Retain Origin Parameters switch is turned on, all parameters are retained during the back-to-origin process.

Example description:

When `http://www.abc.com/a.jpg? x=1` is accessed for the first time, the x=1 parameter is ignored when the CDN node requests the resource from the origin server. Therefore, the CDN node caches the retrieved resource for `http://www.abc.com/a.jpg`. When `http://www.abc.com/a.jpg?x=2` is accessed for the first time, the x=2 parameter is not ignored. Therefore, the CDN node cannot return the requested resource from the cache and needs to request the resource from the origin server. Then, the CDN node caches the retrieved resource for URL http://www.abc.com/a.jpg?x=2.

c. Click **OK**.

10.5. Configure Brotli compression

When you want to compress static text files, you can enable the Brotli compression feature to reduce the size of the transmitted content and accelerate content delivery. This topic describes how to enable the Brotli compression feature.

Brotli compression Performance optimization

Context

Brotli is a new open-source compression algorithm. With Brotli compression enabled, CDN nodes can compress the text files such as HTML, JavaScript, and CSS when it returns the requested resource. The efficiency of Brotli compression is 15 to 25% higher than that of intelligent compression.

- If a request includes the `Accept-Encoding: br` request header, the client expects the requested resource to be Brotli compressed.
- If a response from a CDN node includes the `Content-Encoding: br` response header, the requested resource is Brotli compressed.

> **Notice** If both Brotli compression and GZIP compression are enabled, and the `Accept-Encoding` request header includes `br` and `gzip`, Brotli compression takes priority.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Optimization**.
5. In the **Brotli Compression** section, turn on Brotli Compression.

10.6. Customize images

Alibaba Cloud Content Delivery Network (CDN) allows you to customize images. This topic describes how to customize images.

Feature description

You can specify conditions to customize images.

Image customization is in public preview. To enable this feature, submit a ticket.

Basic settings

Alibaba Cloud CDN allows you to customize images on CDN nodes. You can pass parameters to the `image_process` object to specify how you want to customize the images.

You can pass multiple parameters to the object. Separate multiple parameters with forward slashes (/).

Format: `image_process=action1,param_value1/action2,param_value2` .

Example: `image_process=resize,l_200/quality,q_90/format,webp` .

The following settings are supported:

- image_transform_enable: Specify whether to enable image customization. Valid values: *on*|*off*.
- image_transform_filetype: Specify the image formats. Both the original format and desired format must be supported by image customization. Valid values: *jpg*|*png*|*webp*.

Resize images

Set the action to `resize` .

- Specify the longer side to resize images based on a specific aspect ratio. Example: `image_process=resize,l_200` .
- Specify the shorter side to resize images based on a specific aspect ratio. Example: `image_process=resize,s_200` .
- Specify the width to resize images based on a specific aspect ratio. Example: `image_process=resize,w_200` .
- Specify the height to resize images based on a specific aspect ratio. Example: `image_process=resize,h_200` .
- Specify both the width and height to resize images. Example: `image_process=resize,fw_200,fh_200`

If the value is set to a negative number, images remain at their original sizes.

Crop images

Set the action to `crop` .

- You can specify the *x* coordinate, *y* coordinate, *width*, and *height* to crop an image. The *x* and *y* coordinates specify the lower-left corner of an image. The *width* and *height* specify the size to which you want to crop the image. Example: `image_process=crop,x_10,y_10,w_400,h_200` .
- You can specify the *width* and *height* to crop equally on all four sides at a time. Example: `image_process=crop,mid,w_400,h_200` .

If the value is set to a negative number, images remain at their original sizes.

Adjust image quality

Set the action to `quality`.

- Image quality can be represented by an absolute value. You cannot adjust the image quality to a higher value. For example, if you set `image_process=quality,Q_90`, the attempt to adjust the image quality from *80* to 90 fails and the image quality remains at *80*.
- Image quality can be adjusted based on the original quality and a quality coefficient. For example, if you set `image_process=quality,q_90` to adjust an image whose quality is *80*, the image quality is adjusted to *72*.

Valid range of the quality coefficient: *0* < quality < *100*. The coefficient must be a positive multiple of 5 (quality % 5 == 0). Other values are not supported.

Sharpen images

Set the action to `sharpen`.

Images sharpening increases the apparent sharpness of an image. Valid values are *50*, *100*, *150*, *200*, *250*, and *300*. Example: `image_process=sharpen,100`.

Rotate images

Set the action to `rotate`.

Images can be rotated to a specific angle clockwise. Supported angles are *90*, *180*, and *270*. Example: `image_process=rotate,180`.

Automatically orient images

Set the action to `auto-orient`.

Images taken by some cameras may be displayed in specific orientation. You can specify whether to automatically rotate these images to proper orientation. Example: `image_process=auto-orient`.

Convert image formats

Set the action to `format`.

You can convert images to a specific format. Example: `image_process=format,webp`.

Compress images

This feature is enabled after your application for the image customization feature is approved. This feature reduces the size of all images under a domain name without changing the resolution, format, or quality of the images.

Automatically convert images to WebP

This feature is enabled after your application for the image customization feature is approved. Alibaba Cloud CDN determines whether to convert images in the response to the WebP format based on the Accept parameter in the request header. If `image/webp` is included in the request header, images in the response are converted to the WebP format. Example: `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`.

11.Video Service Configuration

11.1. Overview

The object chunking and video seeking functions of CDN can help you reduce data transfer usage and improve the quality of video and audio playback.

With these functions, you can perform the following tasks.

Function	Description
Configure object chunking	Reduces the amount of data forwarded back to the origin and the data delivery time.
Video seeking	Allows you to seek to a specified position when playing video or audio, without affecting the playback effects.

11.2. Configure object chunking

Object chunking allows the client to notify the origin server to return partial content within a specified range. It helps accelerate delivery of large files. This feature also helps reduce the consumption of back-to-origin traffic and improve resource response speed. This topic describes how to enable object chunking and related precautions.

Range Back-to-origin

Context

When you configure object chunking, take note of the following points:

- Ensure that the origin server supports range requests. If the HTTP request header contains the range field, the origin server must be able to return 206 Partial Content.
- Object chunking is optional and is disabled by default.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Video**.
5. In the **Object Chunking** section, click **Modify**.

6. Object Chunking can be set to On, Off, or Force.

Object chunking	Description	Example
On	Requests with the Range parameter can be sent to the origin server. The origin server returns a file that has the number of bytes within the range specified by the Range parameter. CDN nodes return the file to the client.	When a request sent from the client to a CDN node contains `range: 0-100`, the request received by the origin server also contains `range: 0-100`. The origin server returns a file with 101 bytes in the range of 0 to 100 to the CDN node. Then, the CDN node returns this file to the client.
Off	A CDN node redirects a request for the entire file on the origin server. The client automatically disconnects the HTTP connection to the CDN node after receiving a file that has the number of bytes within the range specified by the Range parameter. The requested file is not cached on the CDN node. This results in a low cache hit rate and large back-to-origin traffic.	When a request sent from the client to a CDN node contains `range: 0-100`, the request received by the origin server does not contain the Range parameter. The origin server returns a complete file to the CDN node. However, the CDN node returns a file with the first 101 bytes to the client. Because the HTTP connection is disconnected, this file is not cached on the CDN node.
Force	The requests with the range parameter are forcibly sent to the origin server.	When you set Object Chunking to Force, make sure that the origin server supports the Range parameter.

> **Note**
>
> When you set Object Chunking to Force, all chunked requests are forcibly sent to the origin server.

7. Click OK.

11.3. Video seeking

With video seeking enabled, you can seek to a specified position when you play video and audio. This topic describes how to configure video seeking.

Video seeking Video seeking

Context

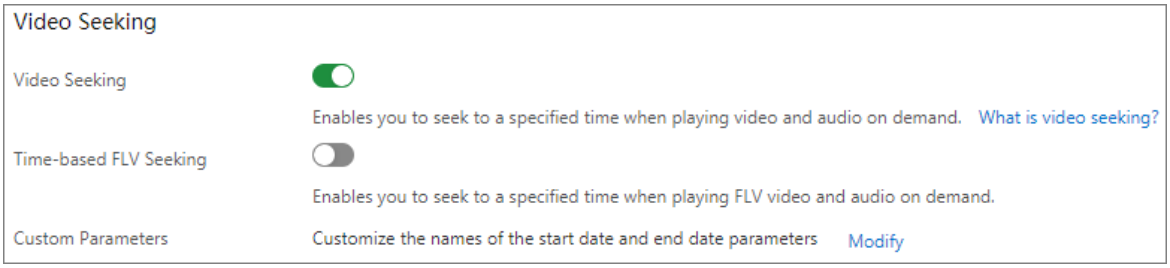
With video seeking enabled, if you seek to a specified position when you play video or audio on demand, the client sends a request to the server. The request contains the URL of the video or audio file, for example, `http://www.aliyun.com/test.flv?start=10`. The start parameter specifies the position that you want to seek to. After the server receives the request, it seeks to the keyframe at the specified position and then returns the content starting from this keyframe. If no keyframe can be found at the specified position, the server seeks to the last keyframe before the specified position.

- Before you configure video seeking, make sure that the origin site supports HTTP range requests. If an HTTP request contains the Range field in its header, then an origin site must return a 206 partial content status message.
- The file formats supported by video seeking and the sample URLs are as follows:

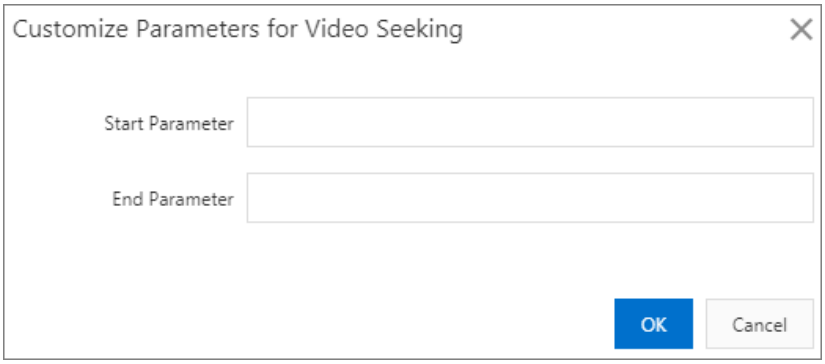
File format	Metadata	Start parameter	Example
MP4	Only MP4 video files with the metadata contained in their header support video seeking. MP4 video files with the metadata contained in their footer do not support video seeking.	The start parameter specifies the time that you want to seek to, in seconds. Milliseconds are expressed with decimals. For example, start=1.01 represents 1.01 second. If CDN cannot find the keyframe at the time specified by start, it seeks to the last keyframe before the specified time.	The request URL `http: //domain/video.mp4? start=10` is to seek forward by 9 seconds.
FLV	FLV video files must contain metadata.	The start parameter specifies the byte that you want to seek to. If CDN cannot find the keyframe at the byte specified by the start parameter, it seeks to the last keyframe before the specified byte.	For video file `http: //domain/video.flv`, the request URL `http:// domain/video.flv? start=10` is to seek to the tenth byte. If no keyframe can be found at the tenth byte, then CDN seeks to the last keyframe before the tenth byte.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Video**.
5. Click the Video Seeking switch under **Video Seeking** to enable the function.



6. Click the Time-based FLV Seeking switch to enable the function.
7. Click **Modify**.



8. Set the Start Parameter and End Parameter for video seeking.
9. Click **OK**.

11.4. Audio extraction

Audio extraction allows you to request the audio data in a video file. With audio extraction enabled, a CDN node extracts audio data from a video file and then returns only the audio data to the client. This reduces network traffic usage. This topic describes how to enable audio extraction.

Context

When a client requests a video file, it sends a request to the CDN server. The request contains the URL of the video file, for example, `http://www.aliyun.com/test.flv?ali_audio_only=1`. After the CDN server receives the request, it returns the audio data in the video file to the client.

The client must support this transmission method: `Transfer-Encoding:chunked`.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Video**.
5. Click the **Audio Extraction** switch to enable audio extraction.

   After audio extraction is enabled, add the `ali_audio_only` parameter to the video file URL in a request to perform audio extraction. Audio extraction supports the following file formats:

Format	Metadata	ali_audio_only parameter	Example
MP4	Only MP4 video files with the metadata contained in their header support audio extraction. MP4 video files with the metadata contained in their footer do not support audio extraction.	Set the `ali_audio_only` parameter to 1 to require the CDN server to return only the metadata and audio data of the requested video. The video data is not returned. If you do not specify this parameter or set the parameter to other values, audio extraction is not performed.	`http: //domain/video.mp4? ali_audio_only=1` .
FLV	No requirements.	Set the `ali_audio_only` parameter to 1 to require the CDN server to return only the metadata and audio data of the requested video. The video data is not returned. If you do not specify this parameter or set the parameter to other values, audio extraction is not performed.	`http:// domain/video.flv? ali_audio_only=1` .

11.5. Configure audio or video preview

Alibaba Cloud CDN provides the preview feature. After you set the preview duration, non-registered users can only watch a video clip for preview instead of the whole video. This topic describes the functionality and specific console operations of this feature.

Audio/video preview Video CDN

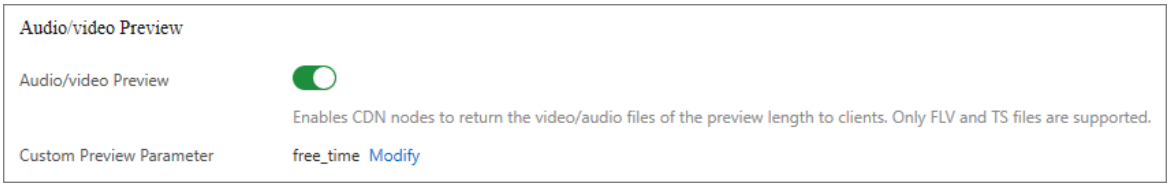
Context

The audio/video preview feature allows a CDN node to only return audio/video files of a specific length to the client.

Only FLV, MP4, and TS files support the preview feature.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Video**.
5. In the **Audio/video Preview** section, turn on **Audio/video Preview**.



6. Enter a parameter name in the **Custom Preview Parameter** field.

   This parameter is used to specify the length of the file to be returned in seconds. For example, if the parameter is set to free_time, the request from a client will include the "free_time=15" field, which indicates that the CDN node only needs to return the first 15 seconds of an audio or video file.

   > **Note** The actual effective length may not be exactly the same as the length that you have set on your client. We recommend that you set a value slightly larger than the expected length. For example, if a 13-second preview is expected on the client, you can set the preview duration to 15 seconds.

11.6. Configure M3U8 encryption and rewriting

This topic describes how to configure M3U8 encryption and rewriting.

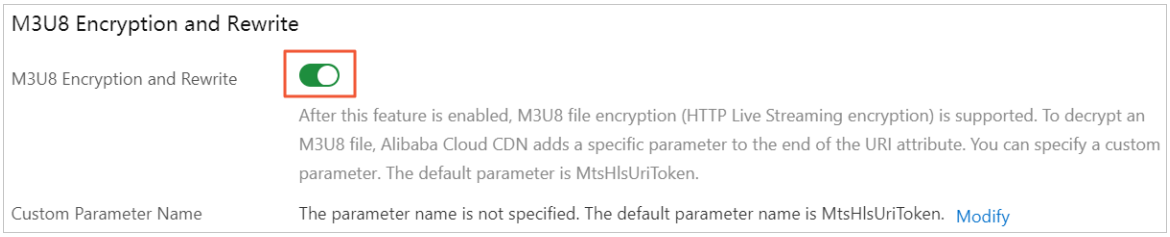
Overview

To accelerate the delivery of HTTP Live Streaming (HLS) content, Alibaba Cloud Content Delivery Network (CDN) rewrites an `#EXT-X-KEY` tag in an M3U8 file for HLS content. After the `#EXT-X-KEY` tag is rewritten, the specified parameter name and value are added to the end of the URI attribute in the tag to decrypt the M3U8 file. Client requests include the parameter name and value that are required for rewriting.

The **M3U8 encryption and rewriting** feature allows you to enable M3U8 encryption and rewrite M3U8 files for HLS content. You can specify a custom parameter name to rewrite an M3U8 file. The custom parameter name must be the same as that included in the client requests. If you do not use a custom parameter name, the parameter name `MtsHlsUriToken` is used by default.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Video**.
5. In the **M3U8 Encryption and Rewrite** section, turn on **M3U8 Encryption and Rewrite**.



> **Note** After you turn on **M3U8 Encryption and Rewrite**, the parameter name `MtsHlsUriToken` is used by default.

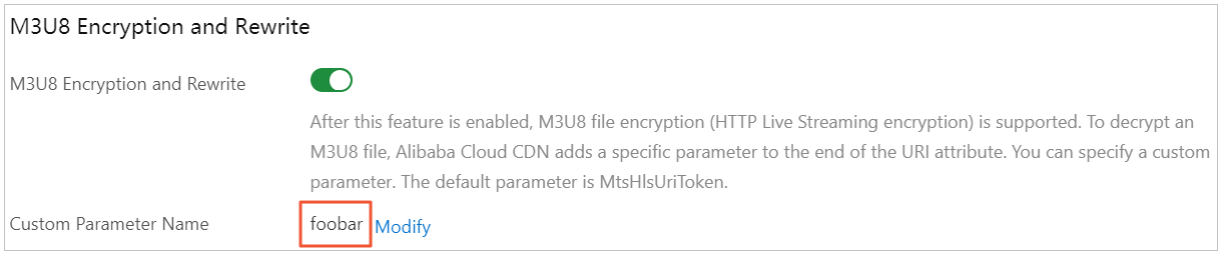
6. If you want to use a custom parameter name that is the same as that included in the client requests, perform the following steps:
   i. Click **Modify** next to the **Custom Parameter Name** field.
   ii. In the **Custom Parameter Name** dialog box, set the **Parameter Name** parameter.

> **Note** The parameter names are case-sensitive. Make sure that the specified parameter name is the same as that included in the client requests. For example, if the client requests include the `foobar` parameter name, the specified custom parameter name `FooBar` cannot be used to retrieve HLS content.

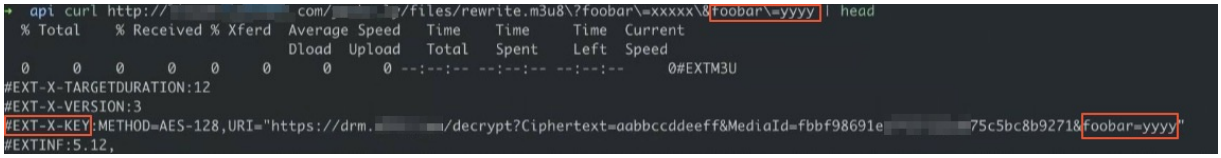
   iii. Click **OK** to complete the configuration.

Example

Log on to the Alibaba Cloud CDN console, turn on **M3U8 Encryption and Rewrite**, and then set the custom parameter name to `foobar`. The following figure shows this custom parameter name.



A client request includes the `foobar` parameter. The parameter value is `yyyy`. To decrypt the M3U8 file and accelerate the delivery of the requested HLS content, Alibaba Cloud CDN adds `foobar=yyyy` to the end of the URI attribute in the `#EXT-X-KEY` tag.



12.Security configuration

12.1. Configure CDN WAF

CDN integrates Web Application Firewall (WAF) capabilities to filter out malicious requests and reroute secure requests to servers. CDN WAF can help protect Web servers against intrusions, secure core data, and prevent server performance exceptions caused by attacks. This topic describes WAF protection, scenarios, billing methods, and setting methods.

Prerequisites

WAF is applicable only to CDN nodes in mainland China. Before enabling WAF protection, you must confirm the region of the domain name. For more information about how to change the region of a domain name, see Modify basic information.

Context

CDN WAF is the integration of WAF capabilities into CDN to protect CDN nodes. For more information about WAF protection, see What is Alibaba Cloud WAF?.

CDN WAF is applicable to industries such as finance, e-commerce, O2O, Internet Plus, games, government, and insurance. It protects your website against unexpected loss caused by attacks when you use CDN to accelerate your website.

CDN WAF can provide the following capabilities:

- Prevents leaks of core data on your website caused by injection attacks.
- Prevents trojans from being uploaded, which may tamper with your Web pages and safeguards the credibility of your website.
- Provides virtual patches that enable quick fix for newly discovered vulnerabilities.

When you enable CDN WAF for a domain name, CDN WAF will detect all requests for the domain name, count the number of requests by account, and then charge fees. The following table describes CDN WAF billing rules.

Requests per hour	Fees
1 to 20,000	CNY 0.4 (a fixed fee)
20,001 to 500,000	CNY 0.2 per 10,000 requests
500,001 to 5,000,000	CNY 0.18 per 10,000 requests
Over 5,000,000	CNY 0.15 per 10,000 requests

For example, user A enabled the CDN WAF feature for a domain name and user B enabled the CDN WAF feature for another domain name at 10:20, February 28, 2019. The following table describes all the fees incurred.

User	Requests between 10:20 and 11:20	Bill (CNY) received at 11:21
A	15,000	0.4
B	350,000	7 (350,000/10,000 × 0.2)

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain name, click **Security Settings**.
5. On the **WAF** page, turn on **WAF Configuration**.
6. Click **Modify**.
7. Configure **Web Application Protection** and **HTTP ACL Policy** as prompted.

Project	Parameter	Description
Web Application Protection	Status	The Web Application Protection switch.
	Mode	The following two Web application protection modes are supported: ○ Block An attack is blocked after it is detected. ○ Report An alert is sent after an attack is detected. However, the attack is not blocked.
	Mode of Protection Policy	The following Web application protection policies are used: ○ Loose Rule Group If many normal requests are blocked when you set Mode of Protection Policy to Medium Rule Group, we recommend you select Loose Rule Group. The loose rule group has the least false positives but the most false negatives. ○ Medium Rule Group The medium rule group is used by default. ○ Strict Rule Group If you require stricter protection against path traversal, SQL injections, and command execution attacks, we recommend that you select Strict Rule Group. When a protection rule is found to block normal requests, you can adjust the mode of protection policy. The loose rule group has the least false positives but the most false negatives.
HTTP ACL Policy	Status	The HTTP ACL Policy switch.
	Rules	A default rule is provided. You can click **Settings** to add a rule, and modify the default rule. Up to three conditions are allowed in each custom rule. The conditions are in the logical AND relationship. A rule is matched only when all the three conditions are satisfied.

12.2. Configure rate limiting

When your website responds slowly, you can use the rate limiting feature to block requests from specific IP addresses within seconds. This helps to improve website security. This topic describes how to configure rate limiting.

Security Rate limiting

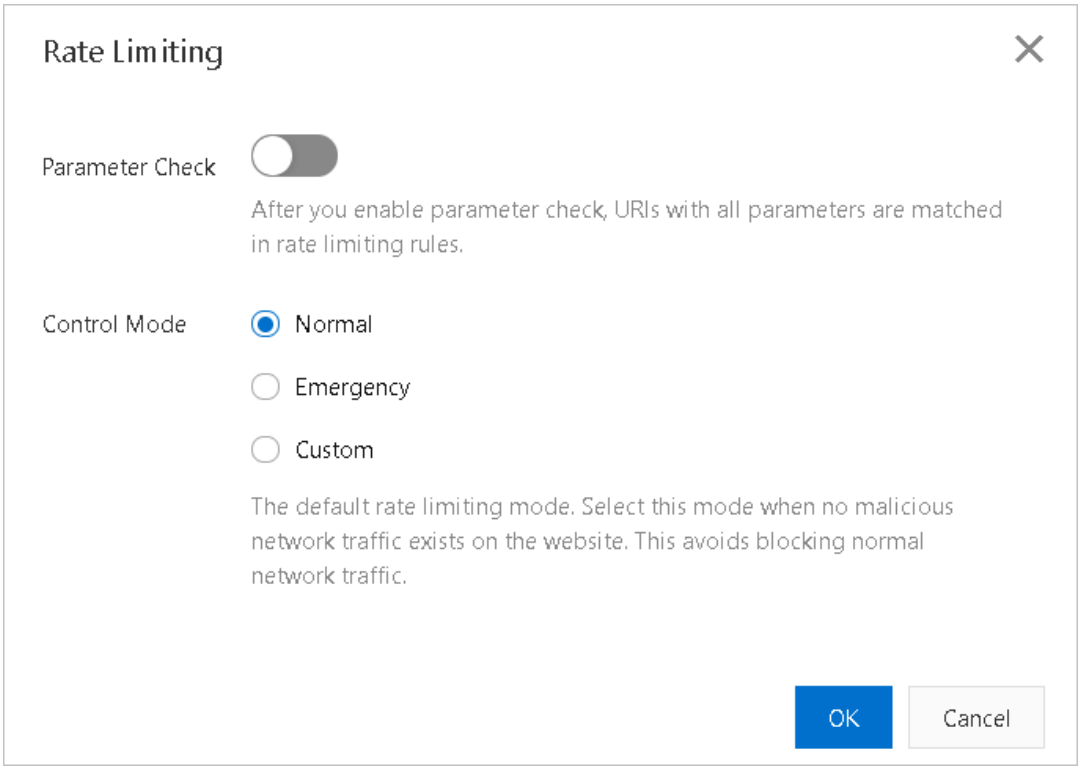
Context

Rate limiting is supported only in the CDN console V1.0.22.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain name, click **Security Settings**.
5. On the **Rate Limiting** page, click the **Set Rate Limiting** switch.
6. Click **Modify**.
7. In the **Rate Limiting** dialog box, enable parameter check, and select a control mode.

Parameter	Description
Parameter Check	After parameter check is enabled, the rate limiting feature will use the specified URIs with all parameters to match requests.
Control Mode	You can select one of the following control modes: ○ **Normal** The default rate limiting mode. Select this mode to prevent false positives when your website traffic is normal. ○ **Emergency** Select this mode when your website responds slowly and exceptions are detected in network traffic, CPU usage, memory usage, and other performance indicators. ○ **Custom** Select this mode when you want to customize rate limiting rules based on your actual needs. For more information about how to set a custom rule, see step 8.



8. If you set the control mode to **Custom**, you need to create custom rate limiting rules.
   i. Click **Create Rule** on the right side of **Custom Rules**.

   > **Note** You can create up to five custom rules in the CDN console.

   ii. Create a custom rule as follows.

Parameter	Description
URI	Enter the URI to be protected, for example, `/register`. You can include parameters in the URI, for example, `/user?action=login`.
Match Criteria	Select one of the following match modes: ■ **Exact Match** In this mode, requests from an address are counted only if the requested URI exactly matches the specified URI. ■ **Prefix Match** In this mode, requests from an address are counted if the requested URI starts with the specified URI. For example, if the URI is set to `/register`, requests sent to `/register.html` are counted. ■ **Regex Match** In this mode, requests from an address are counted if the requested URI matches the specified regular expression.

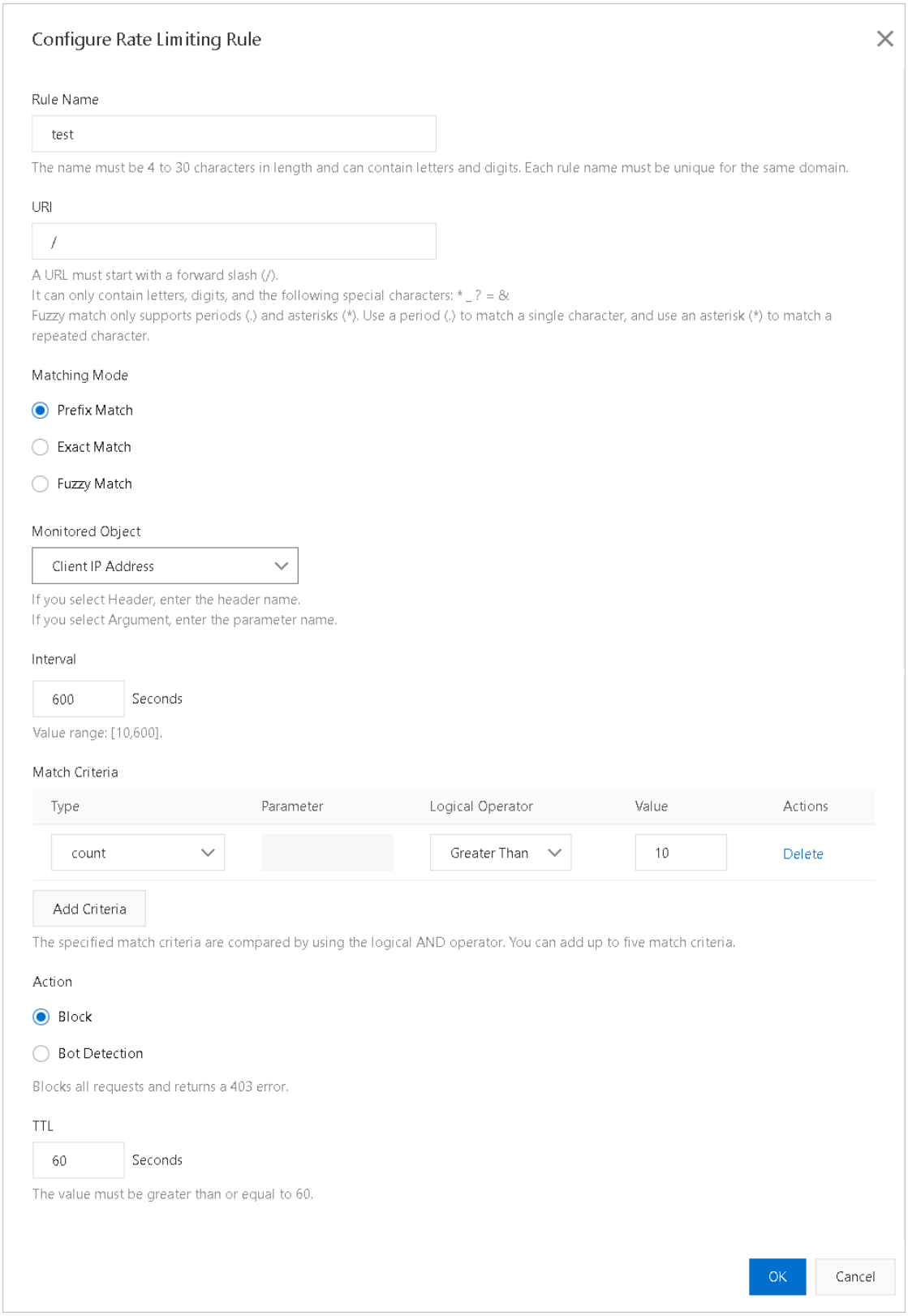
Parameter	Description
Interval	Set a period during which request statistics are collected. This interval must be used together with the number of visits from an individual IP address. The interval must be at least 10 seconds.
Monitored Object	Select one of the following objects for monitoring: ■ IP ■ Header ■ Domain ■ Parameter
Match Criteria	Click **Add Criterion** and configure the following parameters: **Type**, **Option**, **Operator**, and **Value**.
Action	Specify an action to be performed after the criteria are matched, and specify how long the IP address is blocked for. ■ **Block** When the criteria are matched, the connection is disconnected. ■ **Human-machine Identification** When the criteria are matched, CDN returns status code 200 and redirects the request for client verification. If the client passes the verification, requests are allowed to pass through. For example, if an IP address initiates requests more than five times within 20 seconds, a human-machine identification is performed. All requests from the IP address within 10 minutes must pass the human-machine identification. Requests from this IP address are allowed to pass through only when the IP address is verified.
Block Duration	Specify how long the IP address is blocked for. The minimum value is 60 seconds.

The following table lists some sample custom rules.

Scenario	Monitored object	Interval	Match criteria	Action	Block duration
A 4xx or 5xx error has occurred.	IP	10 seconds	`status_ratio|404>60% && count>50`	Block	10 minutes
A QPS spike has occurred.	Domain	10 seconds	`count>N`	Human-machine identification	10 minutes

Scenario	Monitored object	Interval	Match criteria	Action	Block duration
A large number of requests are sent to a URL in a short period of time.	IP	1 minute	`uri_num<2 && count>N`	Block	10 minutes
An arbitrary user-agent header is included in access requests.	IP	10 seconds	`header_num|user-agent>10`	Block	10 minutes

Note Assign a value to *N* based on your actual workloads.



iii. Click OK.

12.3. Integrate CDN with Anti-DDoS

Alibaba Cloud Content Delivery Network (CDN) integrates with Anti-DDoS to mitigate DDoS attacks for accelerated domain names. This topic describes how to set parameters in the Alibaba Cloud CDN console to integrate Alibaba Cloud CDN with Anti-DDoS.

Prerequisites

An Anti-DDoS instance is created. You can purchase Anti-DDoS instances in the Anti-DDoS console.

Context

You can use this feature if you require content delivery acceleration and DDoS mitigation at the same time. After this feature is activated, when attacks are detected, traffic of your workloads is automatically redirected from Alibaba Cloud CDN to Anti-DDoS.

This feature is available in public preview and primarily targeted at users in the finance, retail, transportation, media, and government sectors. You can join the DingTalk group 32615821 to request support.

This feature can be applied in scenarios including but not limited to the following:

- Finance

  Ensures the high availability (HA) of services and improves the experience of users across countries. Protects user information, transactions, and data assets to minimize the risk of great loss caused by attacks.

- Retail

  Accelerates the delivery of website content and services of e-commerce and ticketing platforms and collaborative software. Mitigates attacks to ensure the availability of services.

- Media

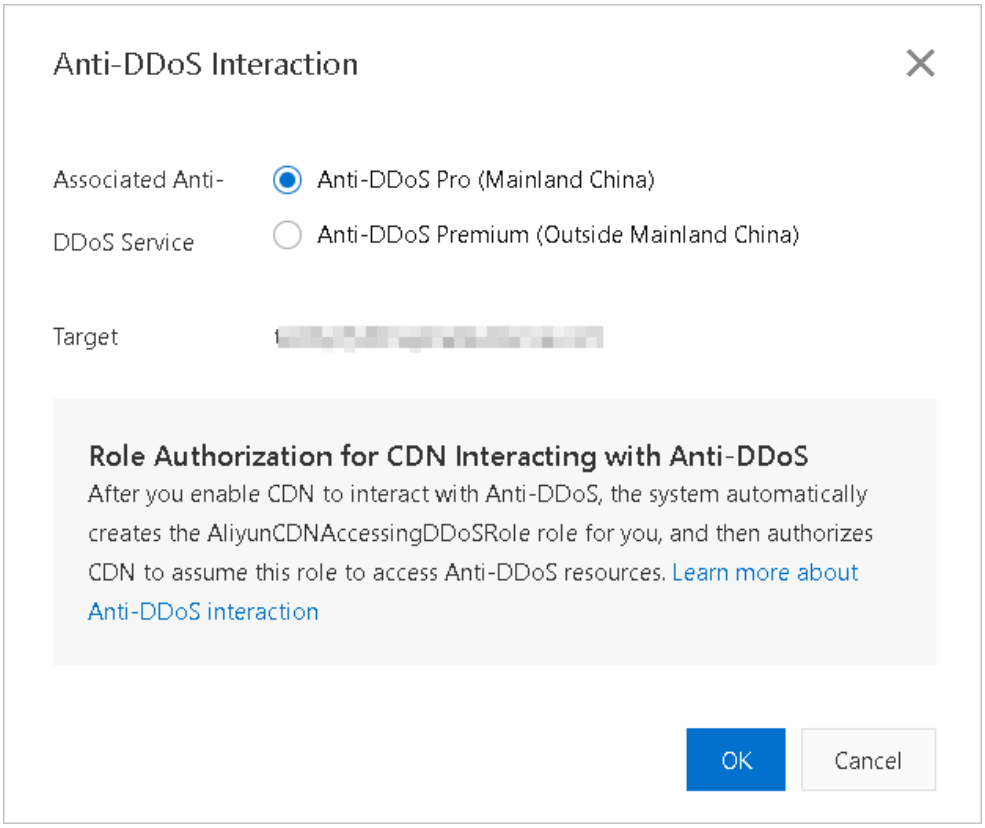
  Accelerates the delivery of media content. Provides protection to avoid service disruptions caused by workload spikes or attacks.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. Choose **Security Settings** > **DDoS Interaction**.

   If this feature is not activated under your account, click **Activate Now** to join the DingTalk group to request support.

5. Turn on the **Anti-DDoS Interaction** switch.
6. Set the **Associated Anti-DDoS Service**, **Association Type**, and **Target** parameters.



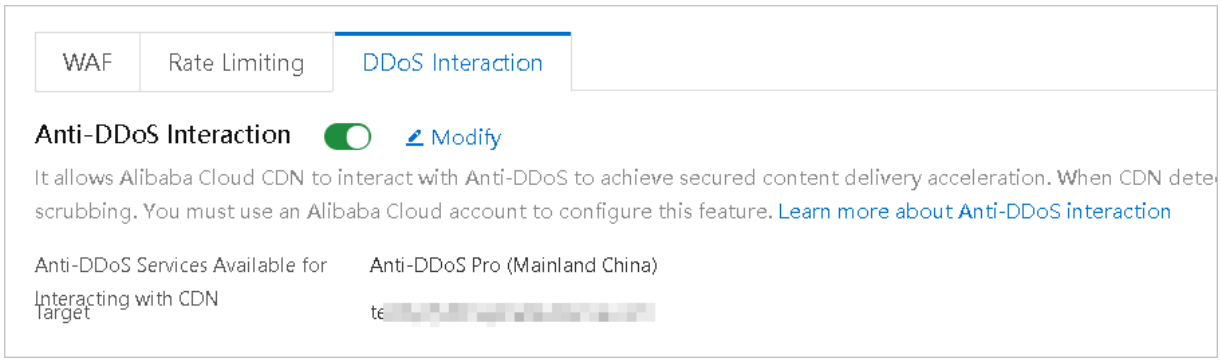
Note This message may appear: No Anti-DDoS Pro/Premium settings are found for the specified domain name.

- If you have not purchased any Anti-DDoS instance, you must purchase an Anti-DDoS instance in the Anti-DDoS console.
- If you have already purchased an Anti-DDoS instance, you must configure the Anti-DDoS instance in the Anti-DDoS console to have your domain name protected.

7. Click **OK**.

Result

On the DDoS Interaction tab, check whether the settings are effective.



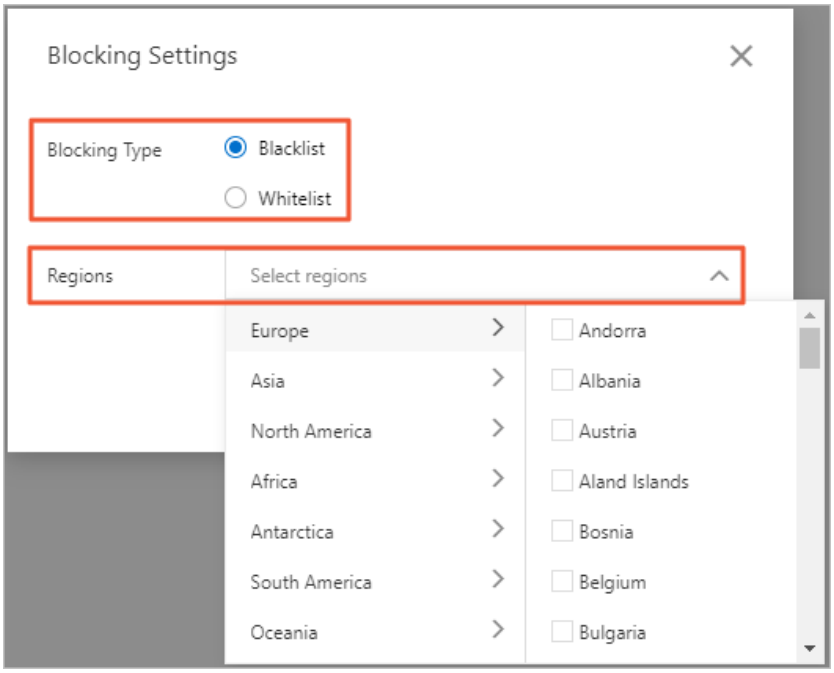
12.4. Block regions

Alibaba Cloud Content Delivery Network (CDN) allows you to block requests from specific regions. This feature blocks malicious requests that are frequently initiated from specific regions.

Context

To enable this feature, join the following DingTalk group and submit an application: 31327650.

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage** in the Actions column.
4. In the left-side navigation pane, click **Security Settings**.
5. On the **Blocked Regions** tab, click **Modify**.
6. In the **Blocking Settings** dialog box, set **Blocking Type** and **Regions**.



Parameter	Description
Blocking Type	○ Blacklist IP addresses in regions added to the blacklist are not allowed to access the accelerated domain name. ○ Whitelist Only IP addresses in regions added to the whitelist are allowed to access the accelerated domain name. The blacklist and whitelist are mutually exclusive. You can choose only one of them.
Regions	Add regions to the blacklist or whitelist.

7. Click **OK**.

8. If you need to clear the blacklist or whitelist, click **Clear**.

13.Advanced settings

13.1. Overview

You can configure bandwidth cap to guarantee the security of data transmission and CDN domain names.

CDN advanced configuration supports the following functions:

Function	Description
Configure bandwidth cap	If the specified bandwidth threshold is reached, the system automatically disables your CDN domain name to protect the domain name. All requests are rerouted to the origin. The CDN service is temporarily suspended.

13.2. Configure bandwidth cap

The bandwidth cap feature specifies the maximum bandwidth for a domain name. When the average bandwidth measured during each statistical cycle (five minutes) exceeds the specified maximum bandwidth, your domain name will automatically go offline to protect itself. All requests will be redirected to the origin server, and CDN will stop acceleration services to avoid excessive fees produced by abnormal traffic. After your domain name goes offline, you can re-enable it in the console. This topic describes how to enable the bandwidth cap feature and related precautions.

Alibaba Cloud CDN bandwidth Bandwidth cap

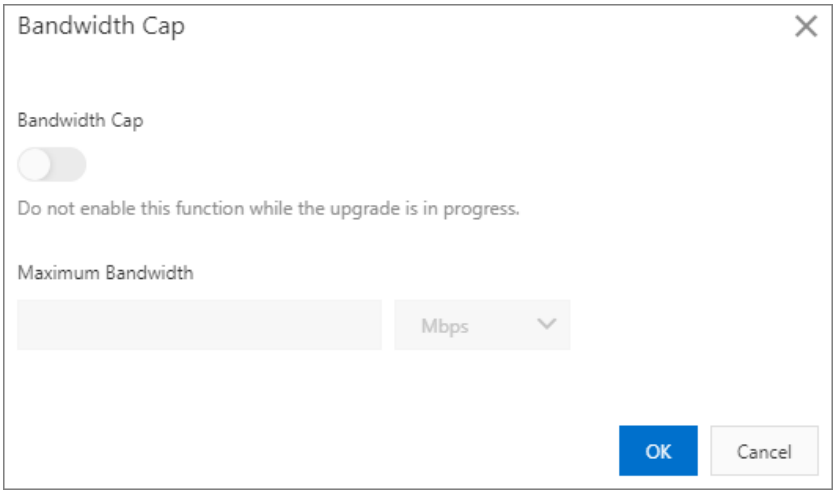
Context

When you configure the bandwidth cap feature, take note of the following points:

- If you intend to enable this feature by using a RAM user account, you must log on to the RAM console to create the AliyunCDNFullAccess policy. This policy grants the RAM user account permission to manage CDN.
- This feature is not applicable to wildcard domain names. Even if you set this feature for a wildcard domain name, this feature does not take effect.
- After you enable this feature, your services may go offline due to the bandwidth cap. To ensure that your domain name can provide normal services, we recommend you set the maximum bandwidth based on a reasonable estimation.
- If your CDN service goes offline due to the bandwidth cap, you can go to the **Domain Names** page in the CDN console, select the check box corresponding to the domain name, and then click **Enable**.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **Advanced**.
5. In the **Bandwidth Cap** section, click **Modify**.
6. Turn on **Bandwidth Cap** to set the maximum bandwidth.



> **Note**
>
> - You can only specify units at intervals of 1000. For example, 1 Tbit/s is equal to 1000 Gbit/s, and 1 Gbit/s is equal to 1000 Mbit/s.
> - You can choose to enable or disable this feature based on the actual usage of your domain name.
> - If this feature is being upgraded, you cannot enable it.

7. Click **OK**.

14.Configure IPv6 settings

This topic describes how to configure IPv6 settings for Alibaba Cloud CDN in the console. After you enable IPv6, an IPv6 client can access CDN by sending IPv6 requests. Requests that are forwarded back to the origin will also carry the IPv6 information of the client.

Context

Most Alibaba Cloud CDN nodes support IPv6. You can enable the IPv6 feature for a CDN domain on the domain configuration page.

After you enable this feature, clients can send IPv6 requests to the nearest CDN node if they are deployed in an IPv6 network and the nearest CDN node supports IPv6. If the nearest CDN node does not support IPv6, the client can still access the CDN node by sending IPv4 requests.

> **Note** Currently, nodes deployed in regions outside Mainland China, including China (Hong Kong), China (Macau), and China (Taiwan), do not support IPv6.

Procedure

1. Log on to the Alibaba Cloud CDN console.
2. In the left-side navigation pane, click **Domain Names**.
3. On the **Domain Names** page, find the target domain name and click **Manage**.
4. In the left-side navigation pane of the specified domain, click **IPv6 Settings**.
5. Click the **IPv6** switch to enable IPv6.

   After you enable IPv6, a client can access CDN through IPv6. Requests that are forwarded back to the origin will also carry the IPv6 information of the client.

15.FAQ

This topic describes some issues about domain name management in Alibaba Cloud Content Delivery Network (CDN) and their solutions.

- Terms
  - What are static content and dynamic content?
  - What is DNS resolution?
- Issues
  - Does CDN support wildcard domains for acceleration?
  - How can I query IP addresses of L2 nodes for a CDN domain?
  - How does CDN process 302 redirects from an origin server?
  - How do I handle domain names without any ICP licenses?
  - What is the difference between a CDN node and a mirror?
  - What is the health check mechanism of Alibaba Cloud CDN?
  - What is the impact if I switch the region where my CDN service is deployed?
  - What HTTP methods does CDN support?
  - How can I check whether a CNAME record is correctly resolved?
  - Why does the 404 Not Found page appear?