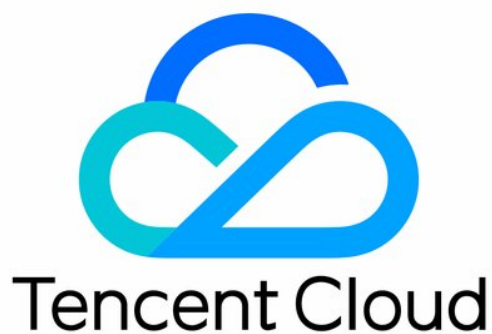


# **Tencent Cloud EdgeOne**

## **Domain Service&Origin**

### **Configuration**

#### **Product Documentation**



## Copyright Notice

©2013-2025 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Contents

## Domain Service&Origin Configuration

### Domain Service

#### Overview

#### Hosting DNS Records

##### Modifying DNS Servers

##### Configuring DNS Records

##### Batch Importing DNS Records

##### Advanced DNS Configuration

##### Enumeration of Resolution Lines and Corresponding Codes

### Domain Connection

#### Adding A Domain Name for Acceleration

#### Ownership Verification

#### Modifying CNAME Records

#### Verify Business Access

### Traffic Scheduling

#### Traffic Scheduling Management

## HTTPS Certificate

### Overview

#### Deploying/Updating SSL Certificate for A Domain Name

#### Configuring A Free Certificate for A Domain Name

#### Mutual Authentication

#### Using Keyless Certificate

### HTTPS Configuration

#### Forced HTTPS Access

#### Enabling HSTS

#### SSL/TLS Security Configuration

##### Configuring SSL/TLS Security

##### TLS Versions and Cipher Suites

#### Enabling OCSP Stapling

### Related References

#### Using OpenSSL to Generate Self-Signed Certificates

#### Certificate Format Requirements

## Origin Configuration

### Load Balancing

#### Overview

Quickly Create Load Balancers

Health Check Policies

Viewing the Health Status of Origin Server

Related References

Load Balancing-Related Concepts

Introduction to Request Retry Strategy

Origin Group Configuration

Origin-pull configuration

Origin-Pull Timeout

Configuring Origin-Pull HTTPS

Host Header Rewrite

Controlling Origin-pull Requests

Redirect Following During Origin-Pull

HTTP/2 Origin-Pull

Range GETs

Origin Protection

Related References

Id Version Origin Group Compatible Related Issues

# Domain Service&Origin Configuration

## Domain Service

### Overview

Last updated : 2024-11-27 11:29:58

Traffic scheduling management is a multi-CDN smart resolution and scheduling tool provided by Tencent Cloud EdgeOne. It supports custom traffic scheduling policies between the origin server and multiple service providers to implement smooth canary migration of traffic and flexible allocation of services, thereby ensuring a high service availability. Once your site is connected to EdgeOne, you can manage your connected domain name through the domain name service module. When your site is connected, EdgeOne provides you with three different connection modes, including connection via NS, connection via CNAME, and connection via DNSPod. Depending on the mode of site connection, different capabilities will be offered within the domain name service module.

### Description of Connection Modes

To allow users to flexibly connect to EdgeOne based on actual business needs, EdgeOne currently supports three connection modes: connection via NS, connection via CNAME, and connection via DNSPod. Below is a comparison of the three modes:

Mode	Connection via NS (Recommended)	Connection via CNAME	Connection via DNSPod
Use case	You can modify the DNS resolution service provider of your domain name and switch the domain name resolution service to EdgeOne.	If your current domain name is already managed by another DNS resolution service provider and you do not want to change the existing service provider, you can use the mode of connection via CNAME.	When the domain name is managed on Tencent Cloud DNSPod, it is recommended to use this connection mode.
DNS record management	After connection, DNS records of the current domain name are managed solely in EdgeOne.	After connection, DNS records are still managed by the existing DNS resolution service provider.	After connection, DNS records are still managed in the Tencent Cloud DNSPod console.
Advantage	You can manage DNS records of your domain name in EdgeOne in a one-	You can connect without changing the DNS resolution service provider for the	Through connection via DNSPod, you can skip domain name ownership

	stop manner. After domain name acceleration takes effect, it can support directly resolving A records by default to point to the nearest EdgeOne edge node, reducing the time taken for domain name resolution.	domain name, making the usage more flexible and allowing quick switching between multi-cloud vendors.	verification. It also supports one-click addition of domain name CNAME records for quick acceleration.
--	---	---	--

## Supported Capabilities

Depending on the connection mode, different capabilities will be provided for you in the domain name service menu:

Feature	Description	Applicable Connection Mode
<a href="#">DNS Records</a>	<p>This feature is used to manage DNS resolution records of the domain name. The capabilities differ, depending on the connection mode:</p> <p><b>Connection via NS:</b> After changing the DNS server to point to EdgeOne, you can manage all resolution records of the domain name in the DNS records. The addition, modification, and deletion of resolution records are supported.</p> <p><b>Connection via DNSPod:</b> Your current domain name's A/AAA/CNAME records configured in DNSPod will be automatically synchronized, and only viewing is allowed. To add, modify, or delete resolution records, you can go to the DNSPod console for management.</p>	Connection via NS Connection via DNSPod
<a href="#">DNS Configuration</a>	This feature is used to configure advanced DNS capabilities, including DNSSEC and custom NS server names.	Connection via NS
<a href="#">Domain Name Management</a>	This feature is used to perform centralized management of information on acceleration domain names connected to EdgeOne. On this page, you can configure the origin server and <a href="#">HTTPS Certificate</a> for these acceleration domain names.	All connection modes
<a href="#">Traffic Scheduling Management</a>	Traffic Scheduling Management is a smart resolution and scheduling tool provided by EdgeOne. It supports custom traffic scheduling policies between the origin server and multiple service providers to implement smooth canary migration of traffic and flexible allocation of services, thereby ensuring a high service availability.	Connection via CNAME Connection via DNSPod

# Hosting DNS Records

## Modifying DNS Servers

Last updated : 2025-06-23 14:49:13

This document describes how to modify the DNS server addresses when you select the NS access mode. EdgeOne provides integrated analysis, acceleration, and security services for your site only when you have completed the modification.

### Note:

DNS server modification is required only in the NS access mode.

## Directions

1. Log in to the administrator account at your domain registrar. You can query the domain registrar in [ICANN WHOIS](#).
2. Modify your DNS server addresses to the server address provided by EdgeOne.

Configuration guides for major domain registrars:

Tencent Cloud

Alibaba Cloud

Huawei Cloud

Godaddy

Google

Name

1. Log in to the [Domains console](#).
2. On **My Domains** page, locate the target domain, and click **Manage** on the right.

3. In the DNS resolution window, click **Modify DNS servers**.

4. In the window that appears, select **Custom DNS**, and enter the server addresses provided by EdgeOne.
5. Click **Submit**.

1. Log in to the [Alibaba Cloud Domains console](#).
2. Click **Domains List**, and locate the target domain. Click **Manage** on the right.

3. In the left sidebar, click **Modify DNS**.

4. On the DNS modification page, click **Modify DNS servers**.

5. Enter the DNS server addresses provided by EdgeOne, and then click **OK**.

1. Log in to the [Huawei Cloud Domains console](#).

2. Locate the target domain in the Domains List. Click **More > Manage** on the right.

3. On the basic information page, click **Modify**.

4. In the **Modify DNS servers** window, enter the server addresses provided by EdgeOne.

5. Click **OK**.

1. Log in to [GoDaddy](#).

2. Click **My Products**, and select **Manage All**.

3. Click the target **domain name**.

4. Click **Manage DNS** under **Additional Settings**.

5. Click **Change** under **Nameservers**.

6. Click **\*\*Enter my own nameservers (advanced)\*\***.

7. Enter the DNS server addresses provided by EdgeOne, and then click **Save**.

1. Log in to the [Google Domains console](#).

2. Select the target domain name.

3. Click **Menu > DNS** on the top-left corner.

4. Choose to use custom domain servers under **Domain Servers**.

5. Enter the server addresses provided by EdgeOne in the **Domain Servers** field.

6. Click **Save**.

1. Log in to the [Name console](#).

2. Click **My Domains**.

3. Select the target domain name.

4. In the **Nameservers column**, click **Manage Nameservers**.

5. Click **Delete All** to clear the current servers.

6. Enter the DNS server address provided by EdgeOne in the box labeled **Add Nameserver**, and then click **Add**.

Only one server address can be added at one time.

7. Click **Save Changes**.

3. After the modification is completed, the domain registrar needs some time to update the DNS servers.

**Note:**

If there are DNS records for the original DNS, please import all DNS records on the **DNS Records** page before modifying the DNS servers. For details, see [Configuring DNS Records](#).

# Configuring DNS Records

Last updated : 2024-11-27 11:18:05

This document describes how to configure the DNS record on EdgeOne.

## Note

This feature is only available for sites connected via the NS.

## Prerequisite

1. Connect your site to EdgeOne via NS.
2. Modify the DNS server of your domain to the DNS server provided by EdgeOne. For details, see [Modifying DNS Server](#).

## Adding one DNS Record

1. Log in to the [EdgeOne](#) console. Click the target site in the site list to display second-level menus for site management.
2. In the left sidebar, click **Domain Name Service > DNS Records**.
3. On the **DNS Record** page, click **Add record**, complete the parameters, and click **Save**. For a description of related parameters, refer to: [Description of DNS-related Concepts](#).

Record type	Host record	Record value	TTL	Operation
<input type="checkbox"/> A	Enter the host record	Enter the record value	Automatic	<a href="#">Save</a> <a href="#">Cancel</a> <a href="#">Collapse</a>

Use different record types for different purposes. "A record" is recommended. [Learn more](#)

<b>A</b>	Resolve host to an IPv4 address, such as 150.109.8.1	<b>AAAA</b>	Resolve host to an IPv6 address, such as 2012:da00:e0a1::a38f:1
<b>CNAME</b>	Resolve host to another domain name, such as www.example.com	<b>TXT</b>	Commonly used for domain verification, SPF check
<b>MX</b>	Used for mail servers. Params are provided by the mail registrar. The default priority (5) can be modified.	<b>NS</b>	Designate other DNS service provider to resolve the host

Total items: 0

10 / page 1 / 1 page

## Note:

After a DNS record is added, it only provides DNS resolution capabilities. If you want the domain name to be connected to EdgeOne for security acceleration, click **Add as Accelerated Domain Name** in the action column, and refer to the [Adding an Accelerated Domain Name](#) document to connect the domain name to EdgeOne.

## Description of DNS-related Concepts

## Host Record

The host record is equivalent to the subdomain name's prefix, and is used to map the domain name to a specific IP address or other related information. When you enter a URL in your browser, your device will query the DNS server to obtain the IP address corresponding to the URL. This process is completed by looking up the DNS record. For

example, if your current site is `example.com` and the domain name you want to connect is

`www.example.com` , `www` will be input as the host record.

## Description of Resolution Record Types

Record Type	Description	Example
A	It is used to resolve a domain name to an IPv4 address. The record value only allows the input of an address in the IPv4 format and does not permit the use of a private IP address.	For example, you have a domain name <code>example.com</code> , and its A record is <code>1.1.1.1</code> . When users visit <code>example.com</code> , the DNS will resolve it to the IP address.
AAAA	It is used to resolve a domain name to an IPv6 address. The record value only allows the input of an address in the IPv6 format and does not permit the use of a private IP address.	For example, you have a domain name <code>example.com</code> , and its AAAA record is <code>2001:0db8:85a3:0000:0000:8a2e:0370:7334</code> . When users visit <code>example.com</code> , the DNS will resolve it to the IP address, allowing users to access the website via IPv6.
CNAME	It is used to point a domain name alias to another domain name. The record value only allows the input of a domain name.	For example, you have a subdomain name <code>www.example.com</code> , and its CNAME record points to <code>example.com</code> . When users visit <code>www.example.com</code> , they will be redirected to <code>example.com</code> to obtain the corresponding resolution record result.
MX	It is used to specify a mail server for handling emails. The MX record must include the priority and the server address, where: Priority: The input range allowed is 0-50; Mail server address: Only a domain name is allowed.	If you want to forward emails sent to <code>example.com</code> to a mail server, you can set an MX record, such as <code>10 mail.example.com</code> , where 10 is the priority number, with a lower number indicating a higher priority.
TXT	It is used to store any text information, often for verification and security purposes. The record value must not exceed 256 bytes.	Common uses include sender policy framework (SPF) recording and domain name validation. For example, you can configure a TXT record <code>v=spf1 include:_spf.example.com ~all</code> to specify which

		servers are allowed to send emails on behalf of your domain name.
NS	It is used to specify the DNS server responsible for managing the domain name. The record value must be in the domain name format.	For example, you have a domain name <code>example.com</code> , and its NS record may be <code>ns1.example.com</code> and <code>ns2.example.com</code> , indicating that these DNS servers are responsible for authoritative DNS queries for the domain name.
SRV	It is used to define the hostname and port number of a specific service. The record value should include the corresponding host domain name and port number.	If you have a service (such as VoIP or instant messaging), you can use an SRV record to specify the service's hostname and port. For example: <code>_sip._tcp.example.com</code> may point to port 5060 of <code>sipserver.example.com</code> .
CAA	<p>It is used to specify which certificate authorities (CAs) are authorized to issue SSL/TLS certificates for domain names. The record value format needs to include three pieces of information: flag, tag, and value, separated by spaces:</p> <p>Flag: It must be set to 0, indicating that CAs are allowed to issue certificates for domain names even if they cannot recognize the CAA record attribute.</p> <p>Tag: It is usually "issue", "issuewild", or "iodef":</p> <p>issue: The specified CA is allowed to issue certificates for all subdomain names.</p> <p>issuewild: The specified CA is allowed to issue wildcard certificates for all subdomain names.</p> <p>iodef: A URL is provided, so that the CA can send a report to it when encountering a request that violates the CAA policy.</p> <p>Value: string type. It is usually the domain name of the CA allowed to issue certificates, and needs to be enclosed in double quotes.</p>	<p>You can set a CAA record so that only specific CAs can issue certificates for your domain name. For example: <code>0 issue "letsencrypt.org"</code> , indicating that only Let's Encrypt can issue certificates for the domain name.</p>

## Description of Resolution Record Conflicts

When recursive resolution queries are performed, there is priority among record types. For example, according to [RFC1034](#) and [RFC2181](#), CNAME has the highest priority. Therefore, the CNAME resolution record result will be returned first in the resolution requesting process. As a result, if a CNAME record is set, it is not allowed to configure MX and TXT records to prevent record conflicts.

✓: No conflict. Both types of resolution records can coexist under the same host record. For example, if an A record for `www.example.com` is set, an MX record for `www.example.com` can also be set.

✗: Conflict. Both types of resolution records cannot coexist under the same host record. For example, if an A record for `www.example.com` is set, a CNAME record for `www.example.com` cannot be set.

Record Type	A	AAAA	CNAME	MX	NS	TXT	SRV	CAA
A	✓	✓	✗	✓	✗	✓	✓	✓
AAAA	✓	✓	✗	✓	✗	✓	✓	✓
CNAME	✗	✗	✗	✗	✗	✗	✗	✗
MX	✓	✓	✗	✓	✗	✓	✓	✓
NS	✗	✗	✗	✗	✓	✗	✗	✗
TXT	✓	✓	✗	✓	✗	✓	✓	✓
SRV	✓	✓	✗	✓	✗	✓	✓	✓
CAA	✓	✓	✗	✓	✗	✓	✓	✓

### Note:

The above table shows conflicts when the host record is not @. When the host record is @, CNAME records do not conflict with MX and TXT records, and configuration is allowed. However, conflicts in resolution records may still occur. For conflict details and risks, refer to: [Description of Conflicts between CNAME and MX, TXT Records](#).

## Weight Description

The weight allows you to set different record values for the same host record, record type, and resolution route. During resolution, EdgeOne will randomly return the corresponding resolution result according to the weight ratio.

Only A/AAAA/CNAME records allow weight configuration. The default weight is empty, meaning no weight is configured. The input range is 0-100. When the weight is set to 0, it means no resolution, but it is not allowed to set all weights to 0. If there are multiple resolution records with the same name after the weight is configured, the resolution record result will be returned according to the weight. The calculation method for the weight is: **ultimately effective weight = weight of current record / sum of weights of all records with the same name**.

Below is an example:

Suppose there are currently 3 CNAME records with the same host record name: Record A, Record B, and Record C, with the weight set to 0, 60, and 40 respectively. The final weight effectiveness result is that Record A is not resolved, Record B's weight ratio is:  $60/(60 + 40) = 60\%$ , and Record C's weight ratio is:  $40/(60 + 40) = 40\%$ .

**Notes:**

Up to 15 A/AAAA/CNAME records for the same host record can be added simultaneously.

If there are multiple A/AAAA/CNAME records for the same host record name and the weights are configured, the weight switches for all records must be consistent, that is, the weights must be all configured or all disabled.

## Description of Resolution Route

By default, when DNS resolution is requested, the authoritative server will not determine the user's IP source to return the resolution record value. EdgeOne supports resolution route allocation, and can return the corresponding route's resolution record value based on the resolution route to which the user's request IP belongs during resolution. If you want to return different resolution records based on the user's IP region source, you can configure different record values according to the region. For example: for the current domain name `www.example.com`, if the A record for the Chinese mainland region route is configured to resolution to `1.1.1.1` and the A record for the default route is configured to resolution to `2.2.2.2`, then users from the Chinese mainland will have the domain name `www.example.com` resolved to `1.1.1.1`, whereas users from other regions will have it resolved to `2.2.2.2`.

**Notes:**

This feature is supported only by Standard and Enterprise plans.

Currently, only A/AAAA/CNAME records support the configuration of resolution routes, with a maximum of 15 resolution routes configurable for the same host record.

## TTL

TTL (Time To Live) indicates the caching duration (in seconds) of DNS records on DNS servers at all levels. When the TTL of a DNS record expires, the Local DNS server needs to request the authoritative DNS server to obtain the resolution of the record again to ensure the DNS record information is up to date. The shorter the set TTL, the more frequently you will need to request the authoritative server to resolve the record, which may slightly affect resolution performance. If the set TTL is long, it may affect the actual effective time of the record when there is a record update. The TTL of EdgeOne is set to 5 minutes by default, and you can modify it based on your actual business needs.

# Batch Importing DNS Records

Last updated : 2024-08-26 16:56:28

If your site needs to access EdgeOne using the NS mode, it is recommended to add the currently effective DNS records by batch importing before modifying the DNS server, to avoid interruptions in the current DNS resolution service.

## Note:

Up to 100 records can be imported at a time. If there are many records, it is recommended to import them in batches. The current import source supports Tencent Cloud DNSPod, Alibaba Cloud DNS, and CloudFlare. If your current DNS resolution is not hosted on these service providers or if the format has an error when EdgeOne resolves the DNS records of these providers (as the record formats of different providers may change at any time), it is recommended to use the template import method.

## Scenario 1: Batch Importing DNS Records During Site Access

### Sample Scenario

At present, `example.com` is added and needs to be accessed using NS. The current DNS resolution is hosted on Alibaba Cloud DNS, and the existing DNS records need to be batch imported to EdgeOne.

### Directions

1. Log in to the [EdgeOne console](#) and click **Add site** in the upper right corner on the service overview page.
2. Refer to [Quick Start](#) to complete Steps 1 and 2 of creating a site.
3. In Step 3, select the access mode as NS and click **Batch import**.
4. Select the import source, such as Alibaba Cloud DNS in this scenario. Then select the DNS record files exported from Alibaba Cloud DNS. For the export method, refer to the product documentation of the corresponding provider.

### Batch import DNS records

1

Select the imported DNS records

>

2

confirm import result

Select source: ☒ Template import ☐ Tencent Cloud DNSPod ☐ Alibaba Cloud DNS ☐ CloudFlare Domain Registration

1. Download the template: [csv table](#), [xlsx table](#), [txt file](#), [zone file](#), fill in the resolution records according to the template format, up to 100 records can be imported at a time;

2. Click to select file, select the filled DNS records template, or drag and drop the file into the area below, then click next step to Identify DNS records.

Select a file or drag it here

Next

Cancel

5. Click **Next** to identify the content of the imported file. If the file format is checked to be correct, you should further confirm the DNS record content to be imported. If the DNS record content has an error, you can modify it on this page.
6. After confirming no errors, click **Import** and wait for background import to complete.

## Scenario 2: Batch Importing DNS Records on the Domain Name Management Page

### Sample Scenario

At present, a site `example.com` exists and uses the NS access mode. Multiple DNS resolution records need to be batch added.

### Directions

1. Log in to the [EdgeOne console](#), click **Site List** in the left sidebar, and then click the **site** you want to configure in the site list.
2. On the site details page, click **Domain Name Service > DNS Records**.
3. Click **Batch import**, select the batch import source as **Template import**, and download the corresponding template. Four file formats are supported, including csv templates, xlsx spreadsheets, txt files, and zone files.
4. Fill in the DNS records according to the template format and save the file. You can select the completed import template by selecting a file or dragging it directly into the console.
5. Click **Next** to identify the template content. If the file format is checked to be correct, you should further confirm the DNS record content to be imported. If the DNS record content has an error, you can modify it on this page.

Batch import DNS records

- ✓

Select the imported DNS records
- >
- 2

confirm import result

Preview the results, confirm the correctness, and click confirm import to start importing records.

Record type	Host record	Record value	Weight	TTL	Operation	Import verification
CNAME			80	300	<a>Edit</a> <a>Delete</a>	<div><div>!</div>This record has enabled acceleration</div>
TXT			-	300	<a>Edit</a> <a>Delete</a>	pass
MX			-	300	<a>Edit</a> <a>Delete</a>	pass
NS			-	300	<a>Edit</a> <a>Delete</a>	pass
SRV			-	300	<a>Edit</a> <a>Delete</a>	pass
CAA			-	300	<a>Edit</a> <a>Delete</a>	pass

Import

Back

6. After confirming no errors, click **Import** and wait for background import to complete.

# Advanced DNS Configuration

Last updated : 2024-01-02 10:44:56

This document will introduce the advanced configuration principles and methods such as DNSSEC, custom NS, CNAME acceleration supported by EdgeOne.

## Note:

The following advanced DNS configuration features are only supported in NS access mode.

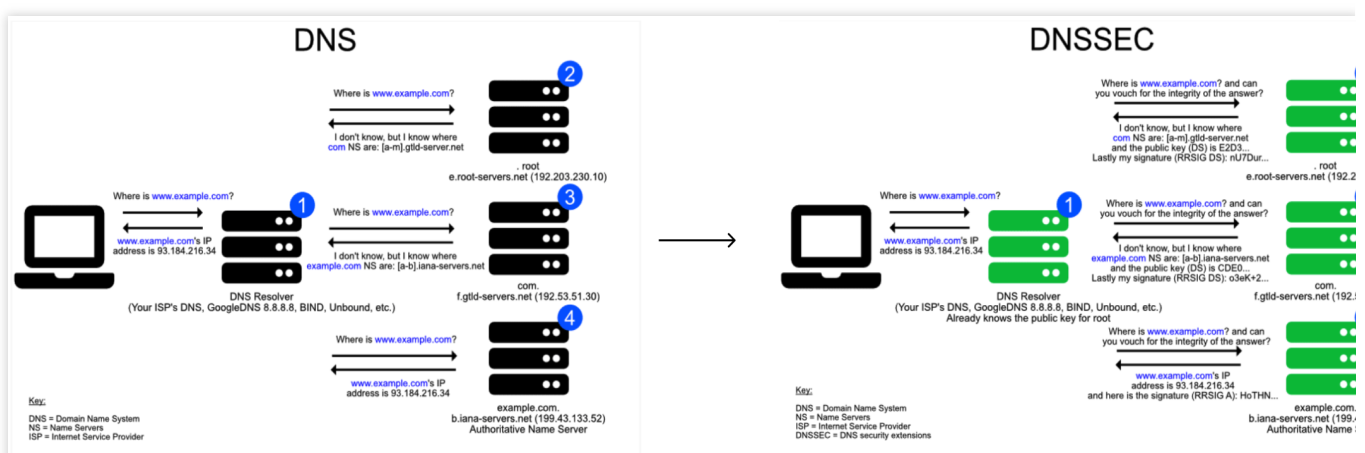
## DNSSEC

### Introduction

Domain Name System Security Extensions (DNSSEC) can effectively prevent attacks such as DNS spoofing and cache poisoning. By employing digital signatures, it guarantees the authenticity and integrity of DNS response messages, protecting users from being redirected to unintended addresses. This in turn fosters user trust in the internet while safeguarding your core business. If you wish to heighten the security of your site's resolution to prevent hijacking and tampering, activating this configuration is suggested.

### How It Works

Through the addition of encrypted signatures to existing DNS records, DNSSEC establishes a more secure DNS. These signatures are stored in the DNS name servers along with common record types such as AAAA and MX records. Thereafter, by simply checking the signature corresponding to the requested DNS record, one can confirm whether the record originates directly from an authoritative name server. This means that the DNS record will not be poisoned or otherwise altered during digital transmission, thus effectively preventing the introduction of forged records.



### Directions

1. Log in to the [TencentCloud EdgeOne Console](#), click on **Site List** in the left menu, and within the site list, click on the **Site** you need to configure to proceed to the site details page.

- On the Site Details page, click on **Domain Name Services** > **DNS configuration** to navigate to the DNS configuration page.
- On the DNS configuration page, click on



within the DNSSEC module. After double confirmation, enable the DNSSEC feature.

- EdgeOne will provide you with DS record information as shown in the picture below. For the corresponding relationship between the summary type and the algorithm, please refer to: [Summary Type](#) and [Algorithm](#).



- Next, you need to add a DS record at the Domain registration merchant based on the above information.
- Once the configuration is complete, wait for it to take effect at the Domain registration service provider's end.

## Custom NS

### Introduction

The custom NS feature allows you to create a name server (NS) dedicated to your own site to replace the default assigned name server. After creation, EdgeOne will automatically assign an IP to it.

### Overview

When you choose to connect your site via NS and you wish to customize the name of your site's DNS server, you can utilize this configuration.

#### Note

Custom NS has the following limits:

Only a subdomain (for example: ns.example.com) of the current site (for example: example.com) can be used as the custom NS server name.

Custom NS requires at least two domains to be added, and they must not conflict with the current existing DNS records.

## Directions

1. Log in to the [EdgeOne console](#), click on **Site List** in the left menu, and within the site list, click on the **Site** you need to configure to proceed to the site details page.
2. On the Site Details page, click on **Domain Name Services > DNS configuration** to navigate to the DNS configuration page.
3. On the DNS configuration page, within the Custom NS module, hit the



input field to add a custom NS server host record.

4. After clicking on **OK** to finalize the addition, you need to append the custom NS's glue record at your Domain Registration provider for the changes to fully become effective. If your domain is registered with Tencent Cloud, you may refer to [Custom DNS Host](#). For domains registered with other vendors, please consult the respective Domain Registration provider's guidance documentation to carry out the configuration.

### Note:

Upon enabling and adding your custom NS service, EdgeOne will automatically append the corresponding A records to your current domain name, with no requisite configuration on your part.

5. Once the configuration is complete, wait for it to take effect at the Domain registration service provider's end.

## CNAME Acceleration

### Introduction

The activation of this function effectively accelerates the resolution speed. If multi-level CNAME records for the domain are set in EdgeOne DNS, the system will directly provide the final IP resolution result, thus decreasing the number of resolutions. This feature is pre-set as enabled, typically needing no alterations. However, should you require offering the user a complete path of resolution, you can opt for deactivation. Example:

Assume your site is `example.com`, you have configured the following multi-level resolution records:

```
loopthree.example.com -> looptwo.example.com -> loopone.example.com -> 1.2.3.4 .
```

<input type="checkbox"/> Record type	Host record	Record value	TTL	Operation
<input type="checkbox"/> A	loopone	1.2.3.4	Automatic	<a href="#">Edit</a> <a href="#">Enable acceleration</a> <a href="#">Status</a> <a href="#">Delete</a>
<input type="checkbox"/> CNAME	looptwo	loopone.example.com	Automatic	<a href="#">Edit</a> <a href="#">Enable acceleration</a> <a href="#">Status</a> <a href="#">Delete</a>
<input type="checkbox"/> CNAME	loopthree	looptwo.example.com	Automatic	<a href="#">Edit</a> <a href="#">Enable acceleration</a> <a href="#">Status</a> <a href="#">Delete</a>

In the absence of **CNAME Acceleration**, the resolution results would be as follows:

```
;; ANSWER SECTION:
loopthree. 300 IN CNAME looptwo.
looptwo. 289 IN CNAME loopone.
loopone. 289 IN A 1.2.3.4
```

With **CNAME Acceleration** enabled, the resolution result will directly display as IP address:

```
;; ANSWER SECTION:
loopthree. 272 IN A 1.2.3.
```

# Enumeration of Resolution Lines and Corresponding Codes

Last updated : 2025-05-06 17:52:03

## Asia

Country/Region	Code	Country/Region	Code
Afghanistan	AF	Maldives	MV
Armenia	AM	Mongolia	MN
Azerbaijan	AZ	Myanmar	MM
Bahrain	BH	Nepal	NP
Bangladesh	BD	North Korea	KP
Bhutan	BT	Oman	OM
British Indian Ocean Territory	IO	Pakistan	PK
Cambodia	KH	Palestine	PS
Christmas Island	CX	Philippines	PH
Hong Kong (China)	HK	Qatar	QA
India	IN	Saudi Arabia	SA
Indonesia	ID	Singapore	SG
Iran	IR	South Korea	KR
Iraq	IQ	Sri Lanka	LK
Israel	IL	Syria	SY
Japan	JP	Taiwan (China)	TW
Jordan	JO	Tajikistan	TJ
Kazakhstan	KZ	Thailand	TH

Kuwait	KW	Turkmenistan	TM
Kyrgyzstan	KG	United Arab Emirates	AE
Laos	LA	Uzbekistan	UZ
Lebanon	LB	Vietnam	VN
Macao (China)	MO	Yemen	YE
Malaysia	MY		

Europe

Country/Region	Code	Country/Region	Code
Åland Islands	AX	Italy	IT
Albania	AL	Jersey Island	JE
Andorra	AD	Lithuania	LT
Austria	AT	Luxembourg	LU
Belarus	BY	Macedonia	MK
Belgium	BE	Malta	MT
Bosnia and Herzegovina	BA	Moldova	MD
Bulgaria	BG	Monaco	MC
Caribbean Netherlands	BQ	Montenegro	ME
Croatia	HR	Netherlands	NL
Czech	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Faroe Islands	FO	Romania	RO
Finland	FI	Russia	RU
France	FR	San Marino	SM

Germany	DE	Serbia	RS
Gibraltar	GI	Saint Martin (Dutch Part)	SX
Greece	GR	Slovakia	SK
Guernsey	GG	Spain	ES
Hungary	HU	Sweden	SE
Iceland	IS	Switzerland	CH
Ireland	IE	Ukraine	UA
Isle of Man	IM	United Kingdom	GB

Africa

Country/Region	Code	Country/Region	Code
Algeria	DZ	Mali	ML
Angola	AO	Mauritania	MR
Benin	BJ	Mauritius	MU
Botswana	BW	Mayotte	YT
Burkina Faso	BF	Morocco	MA
Burundi	BI	Mozambique	MZ
Cameroon	CM	Namibia	NA
Cape Verde	CV	Niger	NE
Central African Republic	CF	Nigeria	NG
Chad	TD	Rwanda	RW
Comoros	KM	Saint Helena	SH
Djibouti	DJ	São Tomé and Príncipe	ST
Egypt	EG	Senegal	SN

Equatorial Guinea	GQ	Seychelles	SC
Eritrea	ER	Sierra Leone	SL
Ethiopia	ET	Somalia	SO
Gabon	GA	South Africa	ZA
Gambia	GM	South Sudan	SS
Ghana	GH	Sudan	SD
Guinea	GN	Eswatini	SZ
Guinea-Bissau	GW	Tanzania	TZ
Kenya	KE	Togo	TG
Lesotho	LS	Tunisia	TN
Liberia	LR	Uganda	UG
Libya	LY	Western Sahara	EH
Madagascar	MG	Zambia	ZM
Malawi	MW	Zimbabwe	ZW

## Oceania

Country/Region	Code	Country/Region	Code
Australia	AU	Norfolk Island	NF
Cook Islands	CK	Northern Mariana Islands	MP
Timor-Leste	TL	Palau	PW
Guam	GU	Papua New Guinea	PG
Kiribati	KI	Solomon Islands	SB
Marshall Islands	MH	Tonga	TO
Nauru	NR	Tuvalu	TV

New Zealand	NZ		
-------------	----	--	--

North America

Country/Region	Code	Country/Region	Code
Anguilla	AI	Haiti	HT
Antigua and Barbuda	AG	Honduras	HN
Aruba	AW	Jamaica	JM
Bahamas	BS	Mexico	MX
Barbados	BB	Montserrat	MS
Bermuda	BM	Nicaragua	NI
Canada	CA	Panama	PA
Cayman Islands	KY	Puerto Rico	PR
Costa Rica	CR	Saint Kitts and Nevis	KN
Cuba	CU	Saint Lucia	LC
Curaçao	CW	Saint Martin (French Part)	MF
El Salvador	SV	Trinidad and Tobago	TT
Greenland	GL	Turks and Caicos Islands	TC
Grenada	GD	United States	US
Guatemala	GT		

South America

Country/Region	Code	Country/Region	Code
Argentina	AR	Guyana	GY

Bolivia	BO	Paraguay	PY
Brazil	BR	Peru	PE
Chile	CL	Suriname	SR
Colombia	CO	Uruguay	UY
Ecuador	EC	Venezuela	VE
French Guiana	GF		

Antarctica

Country/Region	Code
Antarctica	Antarctica

Provinces in Chinese Mainland

Province	Code	Province	Code
Chinese mainland	CN	Jiangsu	CN.JS
Anhui	CN.AH	Jiangxi	CN.JX
Beijing	CN.BJ	Jilin	CN.JL
Chongqing	CN.CQ	Liaoning	CN.LN
Fujian	CN.FJ	Ningxia	CN.NX
Gansu	CN.GS	Qinghai	CN.QH
Guangdong	CN.GD	Shaanxi	CN.SN
Guangxi	CN.GX	Shandong	CN.SD
Guizhou	CN.GZ	Shanghai	CN.SH
Hainan	CN.HI	Shanxi	CN.SX
Hebei	CN.HE	Sichuan	CN.SC

Heilongjiang	CN.HL	Tianjin	CN.TJ
Henan	CN.HA	Xizang	CN.XZ
Hubei	CN.HB	Xinjiang	CN.XJ
Hunan	CN.HN	Yunnan	CN.YN
Inner Mongolia	CN.NM	Zhejiang	CN.ZJ

## ISPs in Chinese Mainland

ISP	Code	ISP	Code
China Education Network	CN/CERNET	China Telecom	CN/CT
China Broadnet	CN/CBN	China Unicom	CN/CU
China Mobile	CN/CM	China Tietong	CN/CTT

## Provincial ISPs in Chinese Mainland

Provincial ISP	Code	Provincial ISP	Code
Anhui Mobile	CN.AH/CM	Jiangsu Unicom	CN.JS/CU
Anhui Telecom	CN.AH/CT	Jiangxi Mobile	CN.JX/CM
Anhui Unicom	CN.AH/CU	Jiangxi Telecom	CN.JX/CT
Beijing Mobile	CN.BJ/CM	Jiangxi Unicom	CN.JX/CU
Beijing Telecom	CN.BJ/CT	Jilin Mobile	CN.JL/CM
Beijing Unicom	CN.BJ/CU	Jilin Telecom	CN.JL/CT
Chongqing Mobile	CN.CQ/CM	Jilin Unicom	CN.JL/CU
Chongqing Telecom	CN.CQ/CT	Liaoning Mobile	CN.LN/CM
Chongqing Unicom	CN.CQ/CU	Liaoning Telecom	CN.LN/CT
Fujian Mobile	CN.FJ/CM	Liaoning Unicom	CN.LN/CU

Fujian Telecom	CN.FJ/CT	Ningxia Mobile	CN.NX/CM
Fujian Unicom	CN.FJ/CU	Ningxia Telecom	CN.NX/CT
Gansu Mobile	CN.GS/CM	Ningxia Unicom	CN.NX/CU
Gansu Telecom	CN.GS/CT	Qinghai Mobile	CN.QH/CM
Gansu Unicom	CN.GS/CU	Qinghai Telecom	CN.QH/CT
Guangdong Mobile	CN.GD/CM	Qinghai Unicom	CN.QH/CU
Guangdong Telecom	CN.GD/CT	Shaanxi Mobile	CN.SN/CM
Guangdong Unicom	CN.GD/CU	Shaanxi Telecom	CN.SN/CT
Guangxi Mobile	CN.GX/CM	Shaanxi Unicom	CN.SN/CU
Guangxi Telecom	CN.GX/CT	Shandong Mobile	CN.SD/CM
Guangxi Unicom	CN.GX/CU	Shandong Telecom	CN.SD/CT
Guizhou Mobile	CN.GZ/CM	Shandong Unicom	CN.SD/CU
Guizhou Telecom	CN.GZ/CT	Shanghai Mobile	CN.SH/CM
Guizhou Unicom	CN.GZ/CU	Shanghai Telecom	CN.SH/CT
Hainan Mobile	CN.HI/CM	Shanghai Unicom	CN.SH/CU
Hainan Telecom	CN.HI/CT	Shanxi Mobile	CN.SX/CM
Hainan Unicom	CN.HI/CU	Shanxi Telecom	CN.SX/CT
Hebei Mobile	CN.HE/CM	Shanxi Unicom	CN.SX/CU
Hebei Telecom	CN.HE/CT	Sichuan Mobile	CN.SC/CM
Hebei Unicom	CN.HE/CU	Sichuan Telecom	CN.SC/CT
Heilongjiang Mobile	CN.HL/CM	Sichuan Unicom	CN.SC/CU
Heilongjiang Telecom	CN.HL/CT	Tianjin Mobile	CN.TJ/CM
Heilongjiang Unicom	CN.HL/CU	Tianjin Telecom	CN.TJ/CT
Henan Mobile	CN.HA/CM	Tianjin Unicom	CN.TJ/CU
Henan Telecom	CN.HA/CT	Xizang Mobile	CN.XZ/CM

Henan Unicom	CN.HA/CU	Xizang Telecom	CN.XZ/CT
Hubei Mobile	CN.HB/CM	Xizang Unicom	CN.XZ/CU
Hubei Telecom	CN.HB/CT	Xinjiang Mobile	CN.XJ/CM
Hubei Unicom	CN.HB/CU	Xinjiang Telecom	CN.XJ/CT
Hunan Mobile	CN.HN/CM	Xinjiang Unicom	CN.XJ/CU
Hunan Telecom	CN.HN/CT	Yunnan Mobile	CN.YN/CM
Hunan Unicom	CN.HN/CU	Yunnan Telecom	CN.YN/CT
Inner Mongolia Mobile	CN.NM/CM	Yunnan Unicom	CN.YN/CU
Inner Mongolia Telecom	CN.NM/CT	Zhejiang Mobile	CN.ZJ/CM
Inner Mongolia Unicom	CN.NM/CU	Zhejiang Telecom	CN.ZJ/CT
Jiangsu Mobile	CN.JS/CM	Zhejiang Unicom	CN.ZJ/CU
Jiangsu Telecom	CN.JS/CT		

## States of the United States

State	Code	State	Code
Alabama	US.AL	Nebraska	US.NE
Alaska	US.AK	Nevada	US.NV
Arizona	US.AZ	New Hampshire	US.NH
Arkansas	US.AR	New Jersey	US.NJ
California	US.CA	New Mexico	US.NM
Colorado	US.CO	New York	US.NY
Connecticut	US.CT	North Carolina	US.NC
Delaware	US.DE	North Dakota	US.ND
Florida	US.FL	Ohio	US.OH
Georgia	US.GA	Oklahoma	US.OK

Hawaii	US.HI	Oregon	US.OR
Idaho	US.ID	Pennsylvania	US.PA
Illinois	US.IL	Rhode Island	US.RI
Indiana	US.IN	South Carolina	US.SC
Iowa	US.IA	South Dakota	US.SD
Kansas	US.KS	Tennessee	US.TN
Kentucky	US.KY	Texas	US.TX
Louisiana	US.LA	US Virgin Islands	US.VI
Maine	US.ME	Utah	US.UT
Maryland	US.MD	Vermont	US.VT
Massachusetts	US.MA	Virginia	US.VA
Michigan	US.MI	District of Columbia	US.DC
Minnesota	US.MN	Washington	US.WA
Mississippi	US.MS	West Virginia	US.WV
Missouri	US.MO	Wisconsin	US.WI
Montana	US.MT	Wyoming	US.WY

## States of India

State	Code	State	Code
Andaman and Nicobar Islands	IN.AN	Madhya Pradesh	IN.MP
Andhra Pradesh	IN.AP	Maharashtra	IN.MH
Arunachal Pradesh	IN.AR	Manipur	IN.MN
Assam	IN.AS	Meghalaya	IN.ML
Bihar	IN.BR	Mizoram	IN.MZ

Chandigarh	IN.CH	Nagaland	IN.NL
Chhattisgarh	IN.CG	Odisha	IN.OR
Dadra and Nagar Haveli	IN.DN	Puducherry	IN.PY
Daman and Diu	IN.DD	Punjab	IN.PB
Delhi	IN.DL	Rajasthan	IN.RJ
Goa	IN.GA	Sikkim	IN.SK
Gujarat	IN.GJ	Tamil Nadu	IN.TN
Haryana	IN.HR	Telangana	IN.TG
Himachal Pradesh	IN.HP	Tripura	IN.TR
Jammu and Kashmir	IN.JK	Uttarakhand	IN.UT
Jharkhand	IN.JH	Uttar Pradesh	IN.UP
Karnataka	IN.KA	West Bengal	IN.WB
Kerala	IN.KL		

# Domain Connection

## Adding A Domain Name for Acceleration

Last updated : 2025-06-14 12:58:24

This document describes how to connect your domain name to EdgeOne and enable domain acceleration.

### Note:

After a domain name is created, EdgeOne will assign a CNAME address to it. You need to complete the CNAME configuration to enable secure acceleration for the domain name. For configuration methods, refer to [Modifying CNAME Records](#).

## Prerequisites

1. You have connected the site (such as `example.com`) to EdgeOne. If you want to accelerate domain names in Chinese mainland AZs or global AZs, please complete ICP filing first.
2. Your site is hosted on an accessible service, such as Cloud Virtual Machine (CVM) or Cloud Object Storage (COS). For example, you have built a cross-border e-commerce site based on Tencent Cloud CVM, and the current server IP address is: `10.1.1.1`.
3. If the site is connected via CNAME, you must [verify ownership](#) of the domain name. If the site is connected via NS, you must [modify DNS server addresses](#) first.

## Scenario 1: Quickly Adding a Domain Name

If your domain name does not require complex configuration, you can click **Quick add** to add a domain name and quickly connect to EdgeOne.

1. Log in to the [EdgeOne console](#), select the **site** to configure from the site list and enter the site management submenu.
2. On the left navigation bar, click **Domain Name Service** > **Domain Management** to enter the domain name management page.
3. Click **Quick add** to add a new domain name. Fill in the domain name configuration information by referring to [Description of Domain Name Configuration Items](#), and then click **Save** to apply the domain name configuration.

## Scenario 2: Adding a Domain Name and Completing Basic Configuration

If you need to fully configure the domain name's basic information, such as the origin-pull protocol and origin-pull port, it is recommended to use Add domain name. The steps for adding a domain name will vary based on the connection mode you choose.

Connecting via NS

Connecting via CNAME

DNSPod Managed Access

1. Log in to the [EdgeOne console](#), select the **site** to configure from the site list and enter the site management submenu.
2. On the left navigation bar, click **Domain Name Service > Domain Management** to enter the domain name management page.
3. Click **Add domain name**. Fill in the domain name configuration information by referring to [Description of Domain Name Configuration Items](#).
4. (Optional) When a domain name is added, EdgeOne provides recommended configurations based on common business scenarios to ensure your business runs more securely and smoothly. You can choose the recommended configuration based on your business scenarios, and the corresponding configuration will be displayed as a rule in the rule engine module.
5. Then click **Next**. In the NS access mode, EdgeOne will automatically add a CNAME address directing to EdgeOne based on your domain name in the background. You can click One-click Add to immediately enable acceleration. If you need to complete other domain name configurations, you can also click Add Later and refer to [Modify CNAME Records](#) for the configuration.

1. Log in to the [EdgeOne console](#), select the **site** to configure from the site list and enter the site management submenu.
2. On the left navigation bar, click **Domain Name Service > Domain Management** to enter the domain name management page.
3. Click **Add domain name**. Fill in the domain name configuration information by referring to [Description of Domain Name Configuration Items](#).
4. (Optional) When a domain name is added, EdgeOne provides recommended configurations based on common business scenarios to ensure your business runs more securely and smoothly. You can choose the recommended configuration based on your business scenarios, and the corresponding configuration will be displayed as a rule in the rule engine module.
5. Then click **Next**. In CNAME access mode, EdgeOne will assign a CNAME address to the domain name. You need to complete the CNAME configuration to enable secure acceleration for the domain name. For configuration methods, refer to [Modifying CNAME Records](#). After completing the configuration, click **Finish**.

1. Log in to the [EdgeOne console](#), select the **site** to configure from the site list and enter the site management submenu.
2. On the left navigation bar, click **Domain Name Service > Domain Management** to enter the domain name management page.

3. Click **Add domain name** . Fill in the domain name configuration information by referring to [Domain Name Configuration Item Description](#).
4. (Optional)When a domain name is added, EdgeOne provides recommended configurations based on common business scenarios to ensure your business runs more securely and smoothly. You can choose the recommended configuration based on your business scenarios, and the corresponding configuration will be displayed as a rule in the rule engine module.
5. Then click **Next**.In DNSPod managed access mode, EdgeOne will assign a CNAME address to the domain name. You can use **One-click Add** to make EdgeOne automatically complete the CNAME configuration for the domain name. If you need to complete other domain name configurations, you can also click **Add Later** and refer to [Modifying CNAME Records](#) for configuration.

## References

### Description of Domain Name Configuration Items

Configuration Item	Description
Domain name	<p>A domain name provided for client access. Enter the host record value corresponding to the domain name. Wildcard domain name access is supported. If you need to access the primary domain name, enter @.</p> <p>For example: If you need to accelerate the website <code>www.example.com</code> , enter <code>www</code> here.</p>
Origin settings	<p>The origin server is the final resource address accessed when the client initiates a request. You can choose from IP/Domain name, COS origin server, and Origin Group:</p> <p><b>IP/Domain name:</b> Used to connect a single origin server. You can enter a single IP address or a single domain name as the origin server.</p> <p><b>COS origin server:</b> Used to add Tencent Cloud COS and an AWS S3-compatible COS bucket as the origin server. If the bucket has public read-write access, you can also access it directly using the IP/Domain name origin server type.</p> <p><b>Origin Group:</b> If the origin server has multiple IP addresses, you can add them by configuring an origin server group.</p> <p><b>Load balancing:</b> Origin server latency and health status are actively detected, and intelligent traffic scheduling policies are configured to provide more secure and efficient traffic distribution services.</p> <p><b>VOD:</b> For buckets authorized in VOD, the distribution scope can be set to all files within the application or files in a specific bucket.</p> <p>For example: There is a cross-border e-commerce website built using Tencent CVM. The server IP address is <code>10.1.1.1</code> . When configuring the origin server, select IP/Domain name for Origin settings and enter the server address.</p> <p><b>Note:</b></p>

	<p>1. We recommend that you configure your origin server in the same region as the acceleration region. For example, if the acceleration region is a Chinese mainland availability zone, set the origin server to be within the Chinese mainland for better origin-pull performance. If the origin server is in a global availability zone (excluding the Chinese mainland) and requires cross-border access, the origin-pull effect may not be guaranteed. To accelerate access for Chinese mainland users with the origin server in a global availability zone (excluding the Chinese mainland), refer to <a href="#">Cross-regional Secure Acceleration (Oversea Sites)</a>.</p> <p>2. If your acceleration region is a global availability zone, you can add corresponding rules in the rule engine. Set the matching condition to the client's geo location and choose to modify the origin server, directing requests to different origin servers based on the regions to ensure the origin-pull effect.</p> <p>3. If your origin server type is IP/Domain name, the default origin host is the accelerated domain name. If you need to specify a domain name for the origin host, refer to <a href="#">Host Header Rewrite</a>. If your origin server is a COS origin server, the default origin host is the COS origin server domain name.</p>
IPv6 access	Choose whether to enable IPv6 access. Refer to <a href="#">IPv6 Access</a> . The default is to follow site configuration.
Origin Protocol	<p>Select the protocol supported by your origin server. The default is to follow the protocol. Options:</p> <p><b>Follow protocol:</b> The origin-pull protocol is the same as the user request protocol.</p> <p><b>HTTP :</b> Use the HTTP protocol for origin-pull.</p> <p><b>HTTPS:</b> Use the HTTPS protocol for origin-pull.</p>
Origin Port	Specify the port used for origin-pull. Ensure that the port specified on your origin server is accessible. By default, HTTP origin-pull uses port 80, and HTTPS origin-pull uses port 443.
Origin HOST header	<p>If your origin server hosts multiple sites and you need to specify which site to access via the origin HOST header, you can select one of the following options when the origin type is IP/domain:</p> <p>Use acceleration domain name: Use the acceleration domain as the origin HOST header;</p> <p>Use origin domain name: Use the origin domain as the origin HOST header. If the origin address is an IP address, this option is not available;</p> <p>Custom: Customize the origin HOST header used when requesting resources from the origin server.</p>

## Verifying Domain Name Acceleration

The verification procedure varies based on the access mode you have selected.

NS Access

CNAME Access

DNSPod Managed Access

In NS access mode, when the client accesses the accelerated domain, EdgeOne automatically schedule the access to the nearest edge node. You can check whether the IP address of the assigned edge node is on EdgeOne to verify

whether the site has been added to EdgeOne.

You can obtain the IP address of the assigned edge node as instructed below.

Windows

Mac/Linux

1. Open the command prompt and run the `nslookup -qt=A www.example.com` command. Then, check the IP address of the domain obtained by the A record resolution.

2. On the [IP Location Query](#) page of the EdgeOne console, paste the IP address in the **IP** field and click **Search** to check whether the IP address is on EdgeOne. If yes, DNS of the accelerated domain has been switched to EdgeOne.

1. Open the terminal and run the `dig www.example.com` command. Then, check the IP address of the domain obtained by the A record resolution.

2. On the [IP Location Query](#) page of the EdgeOne console, paste the IP address in the **IP** field and click **Search** to check whether the IP address is on EdgeOne. If yes, DNS of the accelerated domain has been switched to EdgeOne.

After you complete the CNAME configuration, EdgeOne automatically detects whether the CNAME configuration has taken effect. In the domain list, if the **Status** of the accelerated domain is **Activated**, the domain is correctly configured and accelerated.

If you have correctly configured the CNAME record, but the status is not **Activated**, this may be caused by the CNAME resolution latency of the DNS provider. In this case, you can manually verify the connection as instructed below.

Windows

Mac/Linux

Open the command prompt and run the `nslookup -qt=cname www.example.com` command. Then, check the CNAME information of the domain. If the CNAME information is the same as that provided by EdgeOne, DNS of the accelerated domain has been switched to EdgeOne.

Open the terminal and run the `dig www.example.com` command. Then, check the CNAME information of the domain. If the CNAME information is the same as that provided by EdgeOne, DNS of the accelerated domain has been switched to EdgeOne.

After you complete the CNAME configuration, EdgeOne automatically detects whether the CNAME configuration has taken effect. In the domain list, if the **Status** of the accelerated domain is **Activated**, the domain is correctly configured and accelerated.

If you have correctly configured the CNAME record, but the status is not **Activated**, this may be caused by the CNAME resolution latency of the DNS provider. In this case, you can manually verify the connection as instructed below.

Windows

Mac/Linux

Open the command prompt and run the `nslookup -qt=cname www.example.com` command. Then, check the CNAME information of the domain. If the CNAME information is the same as that provided by EdgeOne, DNS of the accelerated domain has been switched to EdgeOne.

Open the terminal and run the `dig www.example.com` command. Then, check the CNAME information of the domain. If the CNAME information is the same as that provided by EdgeOne, DNS of the accelerated domain has been switched to EdgeOne.

# Ownership Verification

Last updated : 2025-06-14 13:12:41

## Applicable Scenarios

When your site/domain name is connected to EdgeOne for the first time, in order to ensure that you are the owner of the currently accessed site/domain name, we need you to verify the ownership of the site/domain name.

### Note :

This operation is only required in CNAME connection. If your site is accessed in NS mode, you can directly switch the DNS server to EdgeOne to complete the ownership verification.

## Differences Between Domain and Site Verification

Assume that you have domain names `a.example.com` , `b.example.com` , `c.example.com` and the site you connected is `example.com` .

Site verification: If you have permission to configure DNS root domain resolution or root name server, use this method to reduce operating costs.

Once your ownership of the site is verified by EdgeOne, you can directly add its subdomain names

`a.example.com` , `b.example.com` , `c.example.com` .

Domain verification: If your company is a multi-level business or provides domain operations and maintenance and you only have permission to configure DNS resolution and the origin server for the subdomain names, you can skip verification when connecting the site. However, all its subdomain names need to be verified before being added.

Using domain verification requires you to verify `a.example.com` , `b.example.com` and `c.example.com` before connection.

Once your ownership of these domain names is verified, you can directly add all their subdomain names. For instance, when `a.example.com` is verified, `test.a.example.com` can be directly added.

## Steps to Verify the Site or Domain Name Ownership

The verification steps of site ownership are the same as those of domain name ownership. The following example describes how to verify the site ownership.

DNS Verification

File Verification

1. On the **Verify your site** page, select **DNS verification** to obtain the host record, record type, and record value required for ownership verification.

2. Log in to the console of the DNS service provider of the domain name and add a TXT record for the verification of the site ownership. The following examples describe how to add the TXT record in the console of different DNS service providers.

Tencent Cloud DNSPod

Alibaba Cloud DNS

Godaddy

a. Log in to the [DNSPod console](#) and click **My Domains** in the left sidebar. On the page that appears, click the target domain name to enter its configuration page.

b. On the domain name configuration page, click **Add Record** to add a DNS record for the ownership verification of the domain name.

c. Enter the record type, host record, and record value obtained in Step 1 .

Parameter	Description
Record Type	TXT
Host	edgeonereclaim
Split Zone	Default
Text content	Enter the record value provided by EdgeOne
TTL	600

d. Click **OK**.

a. Log in to the [Alibaba Cloud DNS console](#).

b. On the **Manage DNS** page, find the target domain name, and click **Configure** in the **Actions** column to go to the **DNS Settings** page.

c. Click **Add Record** to add a DNS record for ownership verification of the domain name.

d. Enter the record type, host record, and record value obtained in Step 1 .

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

Type	TXT
Host	edgeonereclaim
ISP Line	Default
Value	Enter the record value provided by EdgeOne
TTL	10 minutes

d. Click **OK**.

a. Log in to the Godaddy Domain Portfolio console.

b. On the **Portfolio** page, click the target domain name to go to the **Domain Settings** page.

c. Click **Add** to add a DNS record for ownership verification of the domain name.

d. Enter the record type, host record, and record value obtained in Step 1.

Parameter	Description
Type	TXT
Name	edgeonereclaim
Value	Enter the record value provided by EdgeOne
TTL	Default

d. Click **Add Record**.

3. Verify whether the current TXT record is effective by the following methods :

Windows

Mac/Linux

Open the command prompt and run the `nslookup -qt=txt edgeonereclaim.example.com` command.

Then, check the TXT record information of the domain. If the TXT record is the same as that provided by Step 1, the TXT record is effective.

Open the terminal and run the `dig txt edgeonereclaim.example.com` command. Then, check the TXT record information of the domain. If the TXT record is the same as that provided by Step 1, the TXT record is effective.

4. After the TXT record takes effect, click **Verify**.

1. On the **Verify your site** page, select **File verification**.

2. The following examples describe how to perform file verification on Windows and Linux.

Windows

Linux

1. Go to the root directory of the server and create the verification directory `.well-known/teo-verification` .

2. Click the file URL in Step 2 to get the verification file and upload it to the verification directory.

3. Copy the URL in Step 3 to your browser and make sure that the resource is accessible.

4. Click **Verify**.

1. Open a command window and get to the web server's root directory.

2. Copy the code in Step 2 to the command window and run it.

3. Copy the URL in Step 3 to your browser and make sure that the resource is accessible.

4. Click **Verify**.

# Modifying CNAME Records

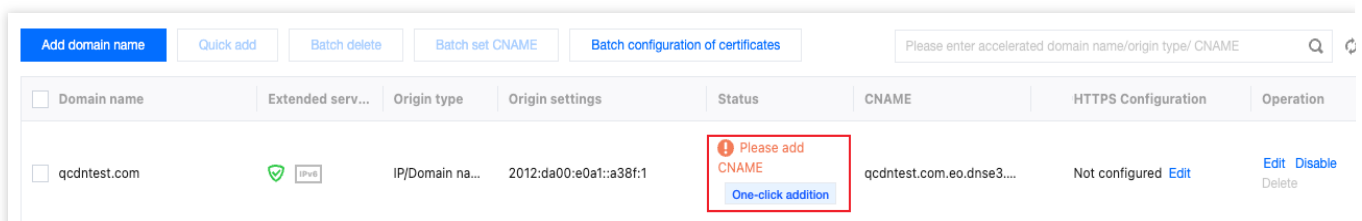
Last updated : 2024-11-12 17:36:02



After a domain name is created, EdgeOne will assign a CNAME address to it. You need to complete the CNAME configuration to enable secure acceleration for the domain name.

## Scenario 1: One-click CNAME Addition in NS Mode or DNSPod Managed Mode

In DNSPod managed access mode, domain names support one-click CNAME addition, helping you quickly complete the CNAME configuration.

1. Log in to the [EdgeOne console](#), select the **site** to configure from the site list and enter the site management submenu.
2. On the left navigation bar, click **Domain Name Service** > **Domain Management** to enter the domain name management page.
3. If the current domain name has not yet configured with a CNAME, click **One-click Add** in the status column.



Add domain name		Quick add	Batch delete	Batch set CNAME	Batch configuration of certificates		Please enter accelerated domain name/origin type/ CNAME		Q	↺
<input type="checkbox"/> Domain name	Extended serv...	Origin type	Origin settings	Status	CNAME	HTTPS Configuration	Operation			
<input type="checkbox"/> qcdntest.com	 IPv6	IP/Domain na...	2012:da00:e0a1::a38f:1	<div> Please add CNAME</div> <div>One-click addition</div>	qcdntest.com.eo.dnse3....	Not configured	<a href="#">Edit</a> <a href="#">Delete</a>			

4. In the pop-up window, after confirming the relevant CNAME information that EdgeOne will operate on, click **OK**. In the second pop-up window, click **OK** again to make EdgeOne automatically complete the CNAME configuration for you.

## Scenario 2: Manual CNAME Configuration

1. After a domain is added, EdgeOne provides you a CNAME pointed to the EdgeOne node.

Host record

Record type CNAME

CNAME

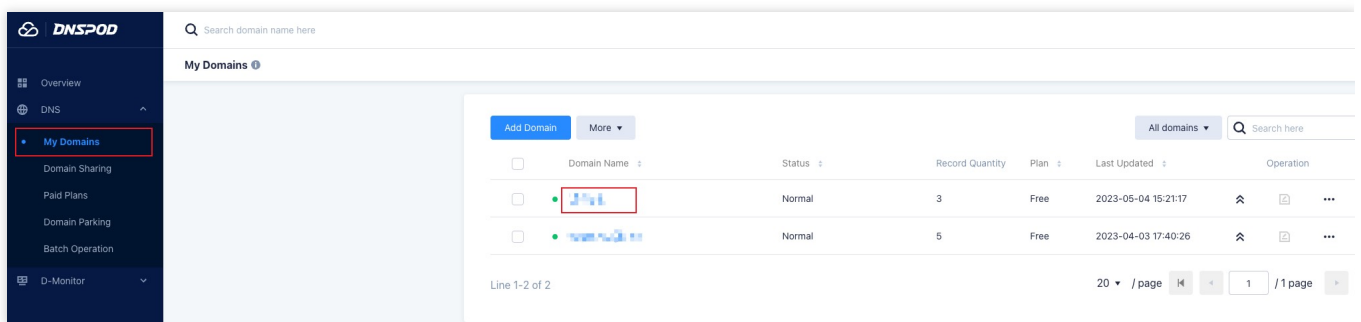
2. Go to the DNS service provider of the domain name and add a CNAME record. See below for examples for different DNS service providers.

Tencent Cloud DNSPod

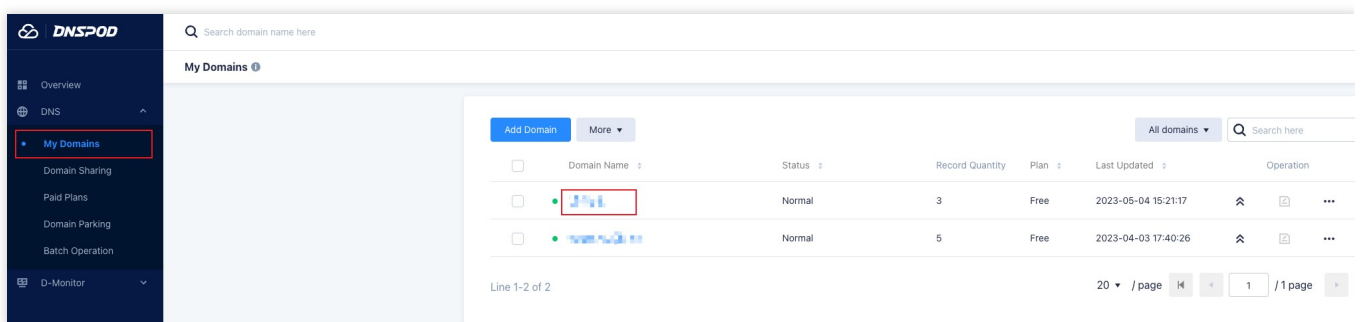
Alibaba Cloud DNS

Godaddy

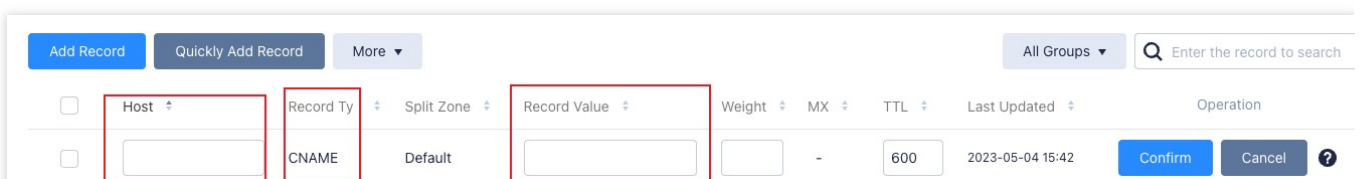
a. Log in to the [DNSPod console](#). Find the domain to verify in **My Domains**. Click the domain to enter the domain name configuration page.



b. On the domain name configuration page, click **Add Record** to add a DNS record for the domain name.



c. Enter the record type, host record, and record value obtained in Step 1.



Parameter name	Description
Record type	CNAME
Host	Enter the domain name
ISP Line	Default
Domain	Enter the CNAME provided by EdgeOne.
TTL	600

d. Click **OK**.

a. Log in to the [Alibaba Cloud DNS console](#).

b. On the **Manage DNS** page, find the target domain name, and click **Configure** in the **Actions** column to go to the **DNS Settings** page.

c. Click **Add Record** to add a CNAME record for the domain name.

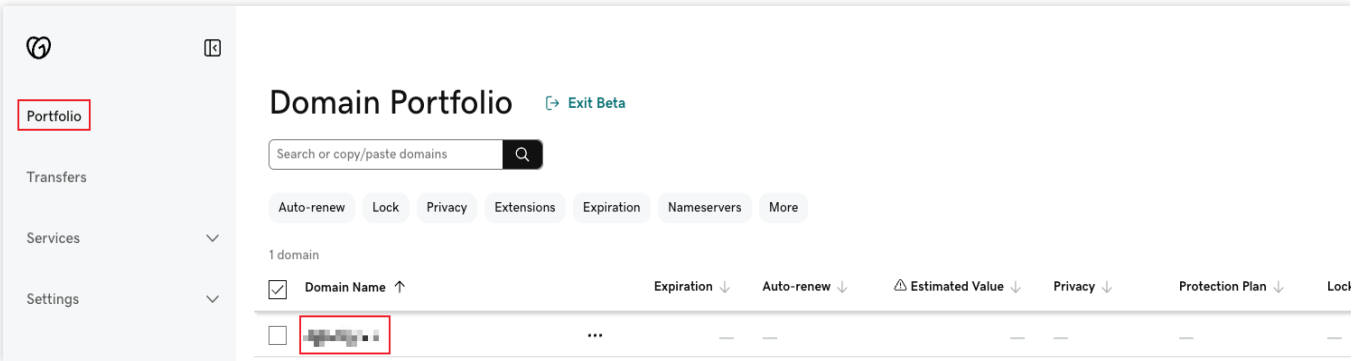
d. Enter the record type, host record, and record value obtained in Step 1.

Parameter name	Description
Record type	CNAME
Host	Enter the domain name
ISP Line	Default
Record value	Enter the CNAME provided by EdgeOne.
TTL	10 minute

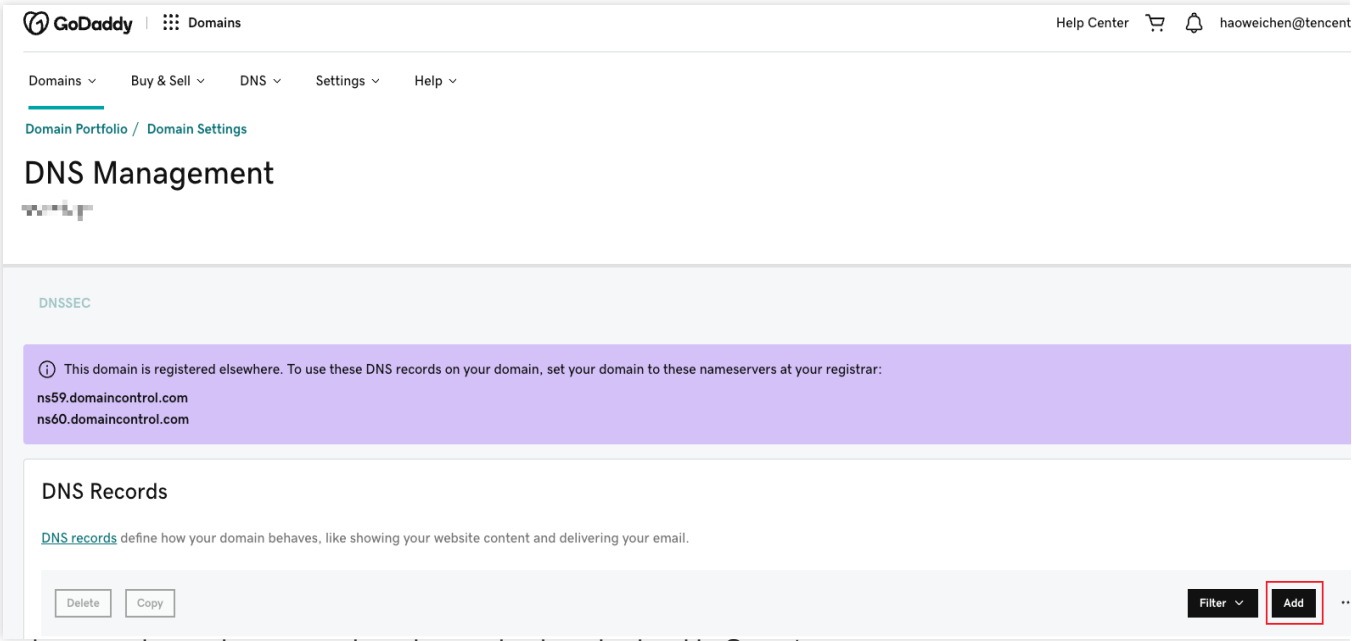
e. Click **OK**.

a. Log in to the [Godaddy Domain Portfolio console](#).

b. On the **Portfolio** page, click the target domain name to go to the **Domain Settings** page.



c. Click **Add** to add a DNS record for ownership verification of the domain name.



d. Enter the record type, host record, and record value obtained in Step 1.

CNAME records are a type of subdomain, or alias, that points to another domain name.

Type*	Name *	Value *	TTL
CNAME	blog or shop	coolexample.com	Default

Add record Clear

Parameter name	Description
Type	CNAME
Name	Enter the domain name
Value	Enter the CNAME provided by EdgeOne.
TTL	Default

e. Click **Add Record**.

3. Now, the **Status** of the domain should be **Validated**.

<input type="checkbox"/>	IP/Domain name	Activated	Not configured	Edit	Disable	Delete
--------------------------	----------------	-----------	----------------	------	---------	--------

## Verifying CNAME Records

After you complete the CNAME configuration, EdgeOne automatically detects whether the CNAME configuration has taken effect. In the domain list, if the **Status** column of the accelerated domain is **Activated**, the domain is correctly configured and accelerated.

<input type="checkbox"/>	IP/Domain name	Activated	Not configured	Edit	Disable	Delete
--------------------------	----------------	-----------	----------------	------	---------	--------

If you have correctly configured the CNAME record, but the status is **CNAME unconfigured**, this may be caused by the CNAME resolution latency of the DNS provider. In this case, you can manually verify the connection by using the following methods:

Windows

Mac/Linux

Open the command prompt and run the `nslookup -qt=cname www.example.com` command. Then, check the CNAME information of the domain. If the CNAME information is the same as that provided by EdgeOne, DNS of the accelerated domain has been switched to EdgeOne.

```
C:\Users\>nslookup -qt=cname www.example.com
Server:  prl-local-ns-server.shared
Address:  10.211.55.1

Non-authoritative answer:
canonical name = .eo.dnse4.com
```

Open the terminal and run the `dig www.example.com` command. Then, check the CNAME information of the domain. If the CNAME information is the same as that provided by EdgeOne, DNS of the accelerated domain has been switched to EdgeOne.

```
[(base) % dig v [REDACTED]

; <<>> DiG 9.10.6 <<>> [REDACTED]
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46159
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;w [REDACTED] IN A

;; ANSWER SECTION:
[REDACTED] 298 IN CNAME w [REDACTED] eo.dnse2.com.
[REDACTED] eo.dnse2.com. 298 IN CNAME w [REDACTED] .acc.edgeoned1.co
[REDACTED] .acc.edgeoned1.com. 58 IN A 175.99.198.121
```

# Verify Business Access

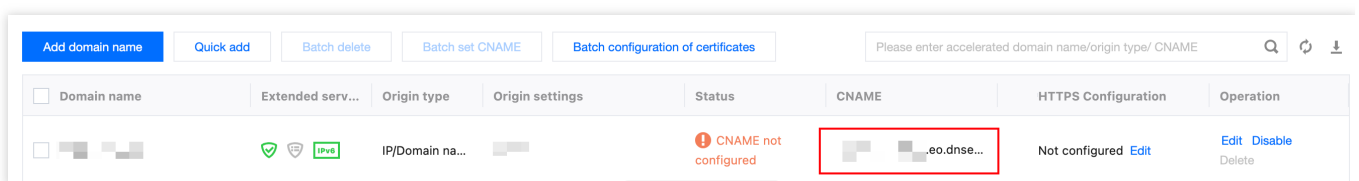
Last updated : 2024-12-23 15:26:59

After your domain is connected to EdgeOne, you need to switch DNS resolution and add the CNAME record assigned by EdgeOne to make the service effective. Before performing this operation, it is recommended to fully test and verify to ensure that your business can be accessed normally after the switch. This document will guide you on how to perform verification.

For example, if your current acceleration domain name is `www.example.com`, the verification steps after access are as follows:

1. Log in to the [EdgeOne console](#), and select the required **Site** from the **Site List**.
2. On the left sidebar, click **Domain Name Service > Domain Management**.
3. In the Domain Management page, if you have already added a domain, you can see the CNAME address allocated by EdgeOne for that domain.

For example: `www.example.com.eo.dnse5.com`.



<a href="#">Add domain name</a>	<a href="#">Quick add</a>	<a href="#">Batch delete</a>	<a href="#">Batch set CNAME</a>	<a href="#">Batch configuration of certificates</a>	Please enter accelerated domain name/origin type/ CNAME		
Domain name	Extended serv...	Origin type	Origin settings	Status	CNAME	HTTPS Configuration	Operation
<input type="checkbox"/>		IP/Domain na...		<span style="color: red;">! CNAME not configured</span>	<span style="border: 1px solid red;">eo.dnse5...</span>	Not configured <a href="#">Edit</a>	<a href="#">Edit</a> <a href="#">Disable</a> <a href="#">Delete</a>

4. Use the TCCLI (CMD running tool or terminal) and the `nslookup` command to get the edge IP resolved from the above CNAME. For example, `nslookup www.example.com.eo.dnse5.com`. The obtained IPs, such as `59.56.100.101` or `175.6.193.206`, are EdgeOne edge node IPs.

```

-Air ~ % nslookup
Server:
Address:

Non-authoritative answer:
canonical name = eo.dnse5.com.
eo.dnse5.com canonical name = .acc.tyxcn.com
Name: .acc.tyxcn.com
Address: 59.56.100.101
Name: .acc.tyxcn.com
Address: 175.6.193.206
```

5. You can continue to refer to the following two methods for verification:

Bind Host verification

Verification using the curl command

Depending on your operating system, you can refer to the following methods to bind the host for testing verification:

Windows

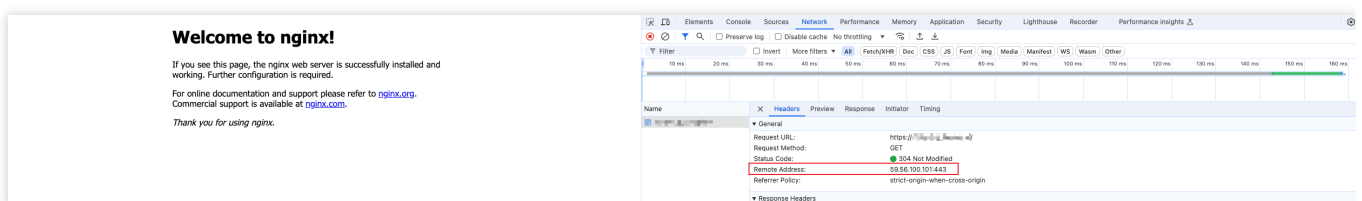
Mac

Find the hosts file in the system and bind the IP address to your acceleration domain name. Bind any node IP ( 27.152.181.195 ) obtained in step 4 and the acceleration domain name ( `www.example.com` ) to the local hosts file on your computer. The format should be the IP address followed by the acceleration domain name, with a space between them, as shown below:

#### Note:

The directory of the hosts file in the Windows system is: `C:\\Windows\\System32\\drivers\\etc` . If you do not have the permission to edit the file in this directory, you can copy the file, edit the copy, and then replace the original file with the edited copy.

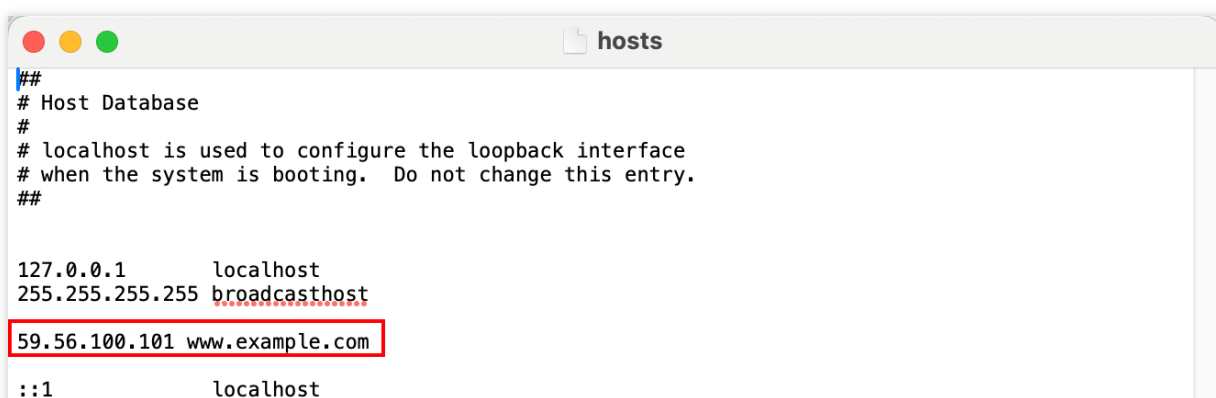
After completing and saving the configuration, perform a business access test through the browser. Directly access the test URL of the current acceleration domain name, open the browser's developer tools, and check whether the accessed IP is the currently bound edge node IP. At the same time, check whether the access performance meets your expectations.



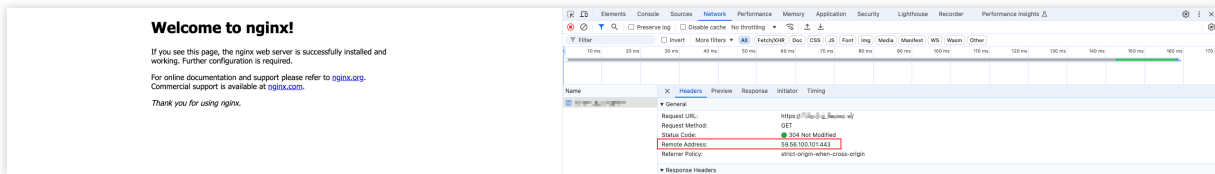
Find the hosts file in the system and bind the IP address to your acceleration domain name. Bind any node IP ( 27.152.181.195 ) obtained in step 4 and the acceleration domain name ( `www.example.com` ) to the local hosts file on your computer. The format should be the IP address followed by the acceleration domain name, with a space between them, as shown below:

#### Note:

The directory of the hosts file in the Mac system is: `/etc/` . If you do not have permission to edit the file in this directory, you can copy the file, edit the copy, and then replace the original file with the edited copy.



After completing and saving the configuration, perform a business access test through the browser. Directly access the test URL of the current acceleration domain name, open the browser's developer tools, and check whether the accessed IP is the currently bound edge node IP. At the same time, check whether the access performance meets your expectations.



You can refer to the following curl command.

```
curl --resolve <hostname>:<port>:<ip> <url> -v
```

The hostname is the domain name you need to access, such as `www.example.com`. The port is the specified port number for access, which is port 443 for HTTPS access and port 80 for HTTP access. The ip is the IP address obtained in step 4, and the url is the URL used for the current access test. For example: `curl --resolve www.example.com:443:59.56.100.101 https://www.example.com/ -v`.

Check whether the request result is normal and meets your expectations.

```
[MacBook-Air ~ % curl --resolve [redacted]:443:59.56.100.101 https://[redacted].cn/ -v]
* Added [redacted]:443:59.56.100.101 to DNS cache
* Hostname [redacted] was found in DNS cache
* Trying 59.56.100.101:443...
* Connected to [redacted] (59.56.100.101) port 443
* ALPN: curl offers h2,http/1.1
* (304) (OUT), TLS handshake, Client hello (1):
* CAfile: /etc/ssl/cert.pem
* CApath: none
* (304) (IN), TLS handshake, Server hello (2):
* (304) (IN), TLS handshake, Unknown (8):
* (304) (IN), TLS handshake, Certificate (11):
* (304) (IN), TLS handshake, CERT verify (15):
* (304) (IN), TLS handshake, Finished (20):
* (304) (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / AEAD-AES256-GCM-SHA384 / [blank] / UNDEF
* ALPN: server accepted h2
* Server certificate:
* subject: CN=[redacted]
* start date: Sep 16 12:20:26 2024 GMT
* expire date: Dec 15 12:20:25 2024 GMT
* subjectAltName: host "[redacted]" matched cert's "[redacted]"
* issuer: C=US; O=Let's Encrypt; CN=R10
* SSL certificate verify ok.
* using HTTP/2
* [HTTP/2] [1] OPENED stream for https://[redacted]/
* [HTTP/2] [1] [:method: GET]
* [HTTP/2] [1] [:scheme: https]
* [HTTP/2] [1] [:authority: [redacted]]
* [HTTP/2] [1] [:path: /]
* [HTTP/2] [1] [user-agent: curl/8.6.0]
* [HTTP/2] [1] [accept: */*]
> GET / HTTP/2
> Host: [redacted]
> User-Agent: curl/8.6.0
> Accept: */*
>
< HTTP/2 200
< etag: "6179061b-267"
< server: nginx/1.21.3
< content-type: text/html; charset=utf8
< ohc-mp4-bitrate: 300kbps
```

6. Once the access is verified to meet expectations, you can switch your domain name resolution to the EdgeOne Service. For details, refer to: [Modify CNAME resolution](#).

# Traffic Scheduling

## Traffic Scheduling Management

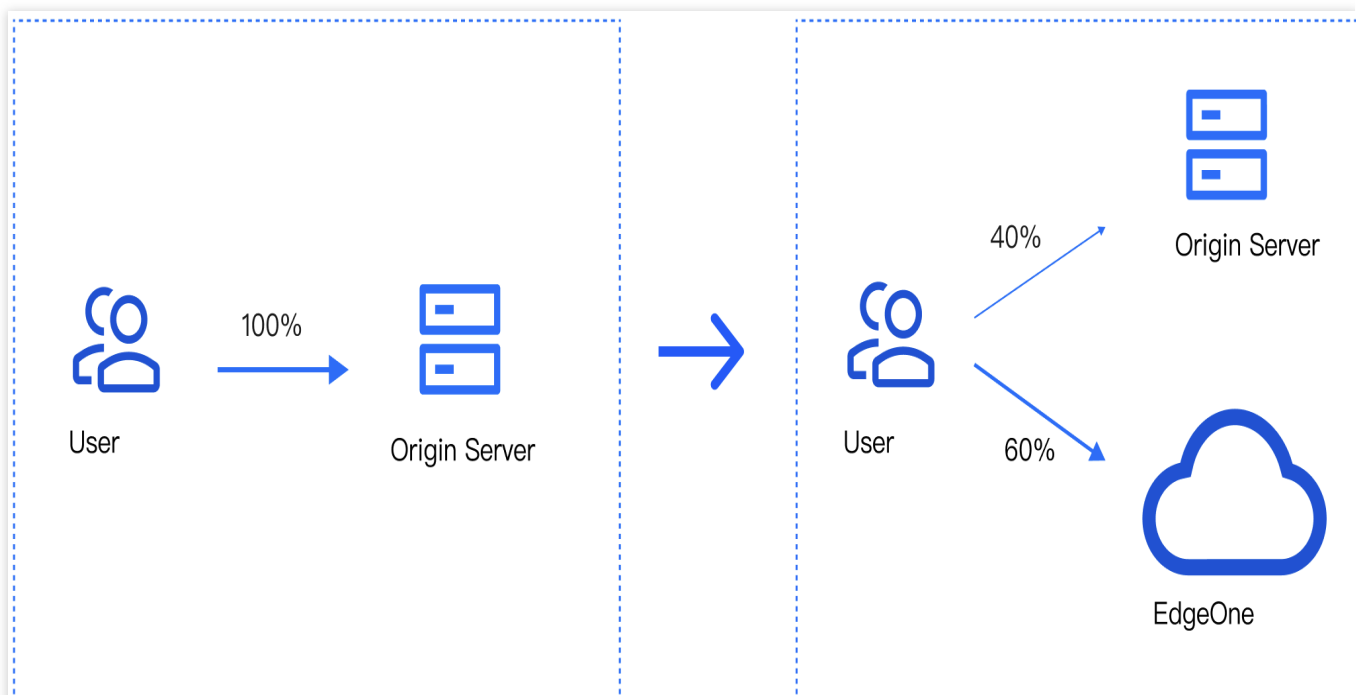
Last updated : 2024-04-16 17:06:58

### Overview

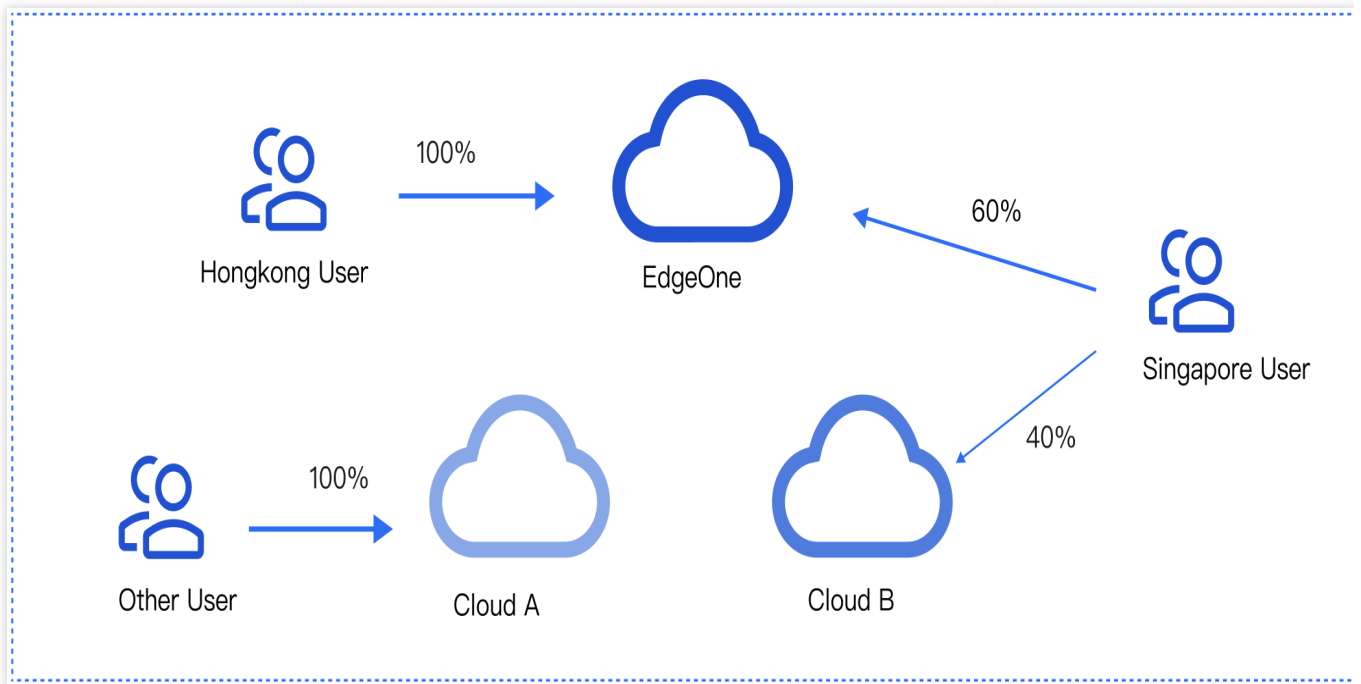
Traffic scheduling management is a multi-CDN smart resolution and scheduling tool provided by EdgeOne. It supports custom traffic scheduling policies between the origin and service providers to implement smooth canary migration of traffic and flexible allocation of services, thereby ensuring a high service availability.

#### Use cases

Canary migration: When a new service provider is added, canary switch is required to ensure the service availability and smooth migration.



Cross-vendor scheduling: For large-scale services that contain sensitive data, it's recommended to distribute traffic to multiple vendors for disaster recovery.



## Features

Simple management: Select a domain name, add service providers, and add scheduling policies.

Quick access: Add the CNAME record assigned by EdgeOne at your DNS service provider

Scheduling modes: Support ratio-based and region-based scheduling.

Multiple scenarios: You can use either the origin or services provided by other CDN vendors, implement canary switch, and use services from different vendors at the same time.

## Prerequisites

[Purchase](#) an EdgeOne Enterprise plan and [connect your site to it](#) in CNAME mode.

## Adding Traffic Scheduling Policies

1. Log in to the [EdgeOne console](#), and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. On the site details page, click **Domain Name Service > Traffic Management**.
3. On the **Traffic scheduling** tab, click **Add scheduling policy**. On the page that appears, select the target domain name and click **Create**.

The screenshot shows the 'Create traffic scheduling policy' page in the Tencent Cloud console. The left sidebar contains navigation options: Site Overview, Data Center, Data Analysis, Log Service, Security and Acceleration, Domain Name Service, and Security. The main area has a progress bar with three steps: 1. Select domain name (active), 2. Add service provider, and 3. Configure policy. Below the progress bar, there is a form with a label 'Access domain name' and a dropdown menu showing 'Please select'. At the bottom of the form are 'Create' and 'Cancel' buttons.

4. Click **Add service provider**, configure parameters such as the service provider name and CNAME record as needed, and click **Next**.

**Note:**

The default service provider is EdgeOne, which cannot be modified or deleted. You can add the domain name of origins or the CNAME domain name of other CDN service providers.

The screenshot shows the 'Create traffic scheduling policy' page in the Tencent Cloud console, Step 2: Add service provider. The progress bar shows Step 1 as completed and Step 2 as active. An 'Add service provider' button is at the top. Below it is a table with columns: Service provider, CNAME/Origin domain, and Operation.

Service provider	CNAME/Origin domain	Operation
CDNB	www.site.com.cdnbdns.com	Save Cancel
CDNA	www.site.com.cdnadns.com	Edit Delete
EdgeOne	www.cc.edgeoneddy1.com	

At the bottom of the table are 'Next' and 'Cancel' buttons.

5. Click **Add policy**, select the line/region, and complete the policy configuration. You can select multiple service providers and specify their weights to configure a multi-service provider scheduling policy. After the configuration is complete, click **Submit configuration**.

**Note:**

By default, all traffic passes EdgeOne. This is the base policy, which cannot be deleted but can be changed to another service provider.

**Line/Region** can be countries/regions, ISPs and provinces in the Chinese mainland, and states in the US and India.

A policy with a more specific regional division takes the higher priority. For example, if you set **Origin domain** for Beijing, **Service provider A** for the Chinese mainland, and **Service provider B** for the default line, then requests from Beijing go to the origin, requests from other Chinese mainland regions go to Service provider A, and requests from regions outside the Chinese mainland go to Service provider B.

← **..Create traffic scheduling policy**

Site Overview

Data Center

Data Analysis

Log Service

Security and Acceleration

Domain Name Service

Domain management

Traffic scheduling

Security

Certificate Management

1. Select domain name

2. Add service provider

3. Configure policy

Add policy

Line/Region	Status	Service provider		Operation
Alaska California	-	EdgeOne	30	+ Add
		CDNB	70	
Bahrain;Bhutan	-	CDNA, weight 100		Edit Delete
Default	Running	EdgeOne, weight 100		Edit

Submit configuration Back

6. If the domain name resolution has been migrated to EdgeOne, the policy takes effect automatically. Otherwise, you need to switch the domain name resolution at your DNS service provider.

← **Traffic scheduling**

Enabled Site ID: zone- CNAMEAccess Global (Chinese mainland not included) Enterprise / edgeone-2 Site

Site Overview

Data Center

Data Analysis

Log Service

Security and Acceleration

Domain Name Service

Domain management

Traffic scheduling

Security

Certificate Management

Here you can manage subdomain names of a site and enable traffic scheduling if needed. [Learn more](#)

- Domain management: Resolve subdomain names to EdgeOne for acceleration.
- Traffic scheduling: Schedule traffic to EdgeOne, service providers or origins.

Add scheduling policy Search domain names

Domain name	CNAME	Policies	Status	Last updated	Operation
		3	Running	2022-12-08 21:30:25	Manage Disable Delete

Total items: 1 10 / page 1 / 1 page

# Managing Traffic Scheduling Policies

1. Log in to the [EdgeOne console](#), and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. On the site details page, click **Domain Name Service > Traffic Scheduling Management**.
3. On the Traffic Scheduling Management page, you can edit, disable, enable, and delete the policies.

## Disabling a policy

When the traffic scheduling policy is disabled, all traffic is scheduled to EdgeOne nodes by default.

## Enabling a policy

When the traffic scheduling policy is enabled, the traffic is scheduled as configured, rather than going to EdgeOne nodes.

## Deleting a policy

After a policy is disabled, you can delete it. This does not affect the service. But the policy cannot be recovered.

## Editing a policy

Click **Manage** to enter the scheduling policy management page, where you can add, delete, modify, and disable service providers and scheduling policies for a domain name.

### Note:

Changing the service provider referenced by a policy takes effect immediately.

Deleting, modifying, enabling, and disabling a policy take effect immediately.

A service provider cannot be deleted if it is referenced by a policy.

Site Overview

Data Center

Data Analysis

Log Service

Security and Acceleration

Domain Name Service

Domain management

Traffic scheduling

Security

Certificate Management

L4 proxy

Site Acceleration

Origin settings

Rule engine

EdgeOne +

Speed Test Tools

Edge function

Alias domain name

EdgeOne Service

Plan usage

Access domain name

Domain name

CNAME

Acceleration service provider

Add service provider

Service provider	CNAME/Origin domain	Operation
CDNB	www.site.com.cdnbdns.com	Save Cancel
CDNA	www.site.com.cdnadns.com	Edit Delete
EdgeOne	www.site.com.edgely1.com	

Scheduling policy

Add policy

Line/Region	Status	Service provider	Operation
Default	-	CDNA	+ Add Save Cancel
Bahrain Bhutan	-	EdgeOne	50 Save Cancel
		CDNB	50 + Add Save Cancel
Alaska,California	Running	CDNA, weight 100	Edit Disable Delete

# HTTPS Certificate

## Overview

Last updated : 2024-11-08 15:55:01

This document describes the advantages of HTTPS over HTTP, and the supported certificate types and encryption algorithms.

## HTTPS Overview

As an extension of HTTP, HTTPS supports identity verification and encrypted transmission through the SSL protocol. SSL uses HTTPS certificates to verify the server's identity and establish an encrypted transmission channel between the client browser and the server. Compared to HTTP, HTTPS offers the following advantages:

**Higher security:** HTTPS encrypts the data exchanged between clients and servers to prevent the data from being hijacked, tampered, or listened to.

**Increased website credibility:** When users access a website over HTTPS, they can verify the website credibility based on its certificate. If the website is trustworthy, a green security identifier is displayed in the browser. This improves the website credibility and prevents users from accessing phishing websites.

**Improved website SEO:** Search engines prioritize trustworthy websites that support HTTPS. Enabling HTTPS access to a website can improve the website ranking in search engine results.

## HTTPS Certificate Capabilities Supported by EdgeOne

Feature	Description
Edge HTTPS Certificates	<p>Edge HTTPS certificates enable users to securely communicate with EdgeOne edge nodes via HTTPS when accessing the current domain name. Currently, EdgeOne supports configuring Edge HTTPS certificates in the following ways.</p> <p><a href="#">Tencent Cloud SSL Certificates</a>: If you already have a domain name certificate, you can deploy the certificate uploaded to the Tencent Cloud SSL console to an EdgeOne edge node. You can deploy at most one RSA, ECC, or SM2 certificate to the EdgeOne node simultaneously.</p> <p><a href="#">Applying for Free Certificates</a>: If you have not yet purchased SSL certificates, you can use EdgeOne to automatically complete the application, deployment, and renewal of free certificates, so as to reduce the operational workload. The currently applied free certificates are RSA certificates from Let's Encrypt.</p>
Edge Mutual	Edge mutual authentication means that during the communication process, both the client

Authentication	and the server need to prove their identities to each other. This is typically used in scenarios with high security requirements, such as corporate internal networks or financial transactions. EdgeOne supports enabling mutual authentication within edge nodes and requires the client to carry a trusted client certificate for verification during access, so as to further enhance the security of communication.
Forced HTTPS Access	Forced HTTPS access can redirect client HTTP requests to HTTPS via 301/302 and ultimately access EdgeOne via HTTPS, so as to ensure that all clients initiate requests to the EdgeOne node via HTTPS and ensure the security of communication.
HSTS	HTTP Strict Transport Security (HSTS) is a web security protocol promoted by the Internet Engineering Task Force (IETF). The protocol is used to instruct web browsers to access a site over the more secure HTTPS protocol. You can configure HSTS to improve the security and credibility of your website if you have any of the following needs: to prevent malicious attackers from stealing sensitive user information through man-in-the-middle attacks, to comply with data privacy protection regulations, or to enhance users' trust in your website.
SSL/TLS Security Configuration	When HTTPS access is enabled for your website, EdgeOne supports multiple SSL/TLS versions to ensure compatibility with different user terminals by default. Normally, you do not need to modify this configuration. However, if your website requires a high level of security and you need to prevent users from accessing your website through less secure SSL/TLS versions, you can customize this configuration by specifying the required SSL/TLS versions.
OCSP stapling	<p>Online Certificate Status Protocol (OCSP) is provided by certificate authorities (CAs) to check the authenticity and validity of digital certificates. Whenever a user accesses a website over HTTPS, the browser initiates an OCSP query to verify whether the certificate of the website is still valid.</p> <p>When OCSP stapling is enabled, EdgeOne performs OCSP queries and caches the results on servers. When a client initiates a TLS handshake with EdgeOne, EdgeOne responds with the OCSP information and certificate required for verification so that the client does not need to send a query request to the CA. This significantly improves the efficiency of the TLS handshake, reduces the time for verification, and improves the HTTPS request speed.</p>

# Deploying/Updating SSL Certificate for A Domain Name

Last updated : 2025-04-03 18:01:57

This document describes how to deploy or update a self-owned certificate for a domain name via the EdgeOne console and the SSL console.

## Deploying Certificate

### Prerequisite

Purchase an SSL certificate in the [SSL Certificate Service console](#), or upload a self-owned certificate and manage it in SSL.

### Scenario 1: Configuring A Self-Owned Certificate via the EdgeOne Console

You can manage and use a self-owned certificate via the EdgeOne console as instructed below.

1. Log in to the [EdgeOne console](#) and click the target site in the site list to display second-level menus for site management.
2. In the left sidebar, click **Domain Name Service > Domain Management**.
3. In the domain name list that appears, find the domain name for which the managed SSL certificate is to be configured and click **Edit** in the HTTPS column of the domain name.
4. In the pop-up window, set **Certificate type** to **Managed SSL certificate**. In the certificate list that appears, select the ID of the certificate to be associated and click **OK**. Then the certificate configuration is delivered.

### Note:

Up to one ECC, one RSA, and one national secret SM2 encryption algorithm certificate can be deployed to the same domain.

5. In the domain name list, hover over the icon before **Configured** in the record of the target domain name, and you can see the information of the deployed certificate.

### Scenario 2: Batch Certificate Configuration through EdgeOne console

If your certificate is a multi-domain or wildcard domain name certificate, and you expect to select multiple domain names in EdgeOne and deploy the same certificate to reduce the operation of configuring the same certificate for multiple different domain names, then batch configuration of certificates is suitable for this scenario. The specific operation steps are as follows:

1. Log in to the [EdgeOne console](#), select the site to be configured through the site list, and enter the site management secondary menu.
2. In the left navigation bar, click **Domain Name Service > Domain Management**.
3. On the Domain Management page, click **Batch Configuration of Certificate**, and in the steps of batch configuration certificate, select the certificate to be configured.
4. Click **Next** to enter the domain name configuration step. Select the domain names to be deployed in batches, and click Complete to issue the certificate deployment.

**Note :**

1. Up to 100 domain names can be selected at once. If the certificate needs to be deployed to more than 100 domain names, please operate in batches.
2. If you need to quickly filter out domain names that have already deployed this certificate, please check: Show only domain names that have not deployed this certificate.

## Updating Certificate

**Scenario 1:** If your certificate is a self-owned certificate, upload it to the SSL certificate management, and when it needs to be updated, you need to re-upload the new certificate content to the SSL certificate console, and then refer to the [deploying certificate](#) method to update it after redeployment.

**Scenario 2:** If you have purchased an SSL certificate in the SSL certificate console, it is suggested that you enable certificate management to implement automatic renewal and update of the certificate. You can refer to [certificate management](#).

# Configuring A Free Certificate for A Domain Name

Last updated : 2025-07-02 10:46:53

## Overview

If you haven't purchased an HTTPS certificate for the website, and the accelerated domain names do not contain any wildcard domain name, you can configure a free certificate.

### Note:

1. Free Certificates are issued by the [TrustAsia](#) and [Let's Encrypt](#). If your site is currently accessed through NS, you can apply for a wildcard domain name certificate. If it is accessed through CNAME, EdgeOne only supports the application of single domain name certificates and does not support the application of wildcard domain name certificates.
2. The certificate has a validity period of 90 days. The platform will automatically apply for renewal 15 days before expiry, so there is no need for you to manually update it. If you are currently using NS access and switch to CNAME access, the applied wildcard domain name certificate will not be able to auto-renew upon expiration.
3. Free certificates do not support downloading.
4. If the domain is accessed via CNAME or DNSPod hosted access, you need to complete the CNAME configuration and wait for the CNAME status to take effect before applying for a free SSL certificate for the domain. In the CNAME or DNSPod hosted access mode, EO will apply for the free certificate through HTTP verification. During the verification process, the EO node will directly respond with the verification value. It is recommended to avoid using line/region-based resolution when configuring CNAME records, as this may lead to difficulties in obtaining the correct verification value, resulting in the failure of the free certificate application.

## Directions

1. Log in to the [EdgeOne console](#). Click the target site in the site list to display second-level menus for site management.
2. In the left sidebar, click **Domain Name Service > Domain Management**.
3. In the domain name list that appears, find the domain name for which the certificate is to be configured and click **Edit** in the HTTPS column of the domain name.
4. Set **Certificate type** to **Free certificate** and click **OK**. Then the free certificate is delivered and installed.

5. In the domain name list, hover over the icon before **Configured** in the record of the target domain name, and you can see the information of the deployed certificate.

# Mutual Authentication

Last updated : 2024-11-08 15:55:01

## Overview

HTTPS mutual authentication, also known as mutual TLS (mTLS) authentication or client authentication, is a secure communication protocol that requires both the server and the client to verify the identity of the opposite side. For standard HTTPS, the server proves its identity to the client (through a server certificate) in most cases, thereby establishing a secure, encrypted communication channel. On this basis, mutual authentication further requires the client to provide a certificate for the server to verify the client identity. This method is often used in systems with high security requirements to ensure both communication parties are trustworthy.

## Preparations

One server certificate, consisting of server.pem and server.key;

One client certificate, consisting of client.pem and client.key;

Root certificate: CA.pem. The certificate requires the complete certificate chain to be uploaded in advance to the [Tencent Cloud SSL console](#). The certificate needs to include the complete certificate chain. For format requirements, refer to [CA Certificate Format and Certificate Chain Specification](#).

### Note:

If you have not purchased server certificates and client certificates yet, you can also refer to [Using OpenSSL to Generate Self-Signed Certificates](#) to generate self-signed certificates in a testing environment.

## Use Limits

Currently, each domain name supports configuring only 1 client CA certificate and supports RSA, ECC, or SM2 national encryption algorithm certificates.

If the server is configured with a national encryption algorithm certificate, the client CA certificate must also be a national encryption algorithm certificate.

## Directions

For example, you need to configure mutual authentication for the domain name `www.example.com`, and the client CA certificate has been uploaded to the Tencent Cloud SSL console.

1. Log in to the [EdgeOne console](#), click **Site List** in the left sidebar, and then click the **site** you want to configure in the site list.
2. On the site details page, click **Domain Name Service > Domain Name Management**.
3. On the domain name management page, select the domain name to be configured with a certificate and click **Edit** in the HTTPS column. The HTTPS certificate configuration page will pop up. In mTLS configuration, enable Edge mTLS and select an existing client CA certificate to configure.

**mTLS configuration**

If you need to upload a client CA certificate, you can go to [Tencent Cloud SSL Console](#) to upload/manage.

Edge mTLS ☒

After enabling, EdgeOne will use mTLS in the handshake process with the client's request. You need to deploy the current client's CA certificate within EdgeOne to ensure that EdgeOne can complete the client certificate authentication.

Client CA certificate

	Certificate ID/Remarks	Certificate Subject	Issuer	Encryption algorithm	Expiration time ↕	Status
<input type="radio"/>	ID: [REDACTED] Re [REDACTED] _ [REDACTED]	MiddleCA for Test	RootCA for Test	SM2	2035-12-31 00:00:00	Issued
<input type="radio"/>	ID: [REDACTED] Re [REDACTED] _rc [REDACTED]	TrustAsia RSA DV TL...	AAA Certificate Servi...	RSA 3072,RSA 2048	2029-01-01 07:59:59	Issued
<input type="radio"/>	ID: [REDACTED] Re [REDACTED]	MySSL.com	MySSL.com	SM2	2033-11-21 14:42:35	Issued

4. Click **Confirm** to issue the configuration. It will take effect immediately after the deployment is completed. After configuration, the client must carry the client certificate issued by the client CA certificate for access, otherwise the HTTPS handshake cannot be completed. You can also verify whether the handshake is successful by following the CURL command below to carry the client certificate information:

```
curl https://www.example.com --cert client.crt --key client.key -v -k
```

In this command, --cert indicates the local path of the client's public key certificate, and --key indicates the local path of the client's private key certificate.

## FAQs

### What Should I Do If An Error Is Reported During Testing with the Response Message: Empty Reply From Server?

In this case, the most common possibility is that the certificate chain of the currently configured client CA certificate is incomplete. You need to concatenate the complete certificate chain content together and upload it to the Tencent

Cloud SSL console. The concatenation order needs to be in strict accordance with the [CA Certificate Format and Certificate Chain Specification](#).

# Using Keyless Certificate

Last updated : 2025-04-14 17:48:48

Usually, if a domain name provides HTTPS access, the public and private keys of the certificate must be deployed on the server to complete communication encryption and decryption during the handshake process. If your domain name needs to connect to EdgeOne for security acceleration, you also need to upload and deploy both the public and private key of the certificate at EdgeOne's edge nodes. If you prefer to keep your certificate's private key more securely and do not want to upload it to the Tencent Cloud SSL console, EdgeOne supports the Keyless certificate deployment solution. This document describes how to use the Keyless certificate solution for EdgeOne.

## Note:

This feature is currently undergoing internal testing. If you need to use it, please [contact us](#).

Currently, the Keyless solution only supports the RSA algorithm certificate.

## Solution Description

### Handshake Process for HTTPS One-Way Authentication (Taking the RSA Key Exchange Algorithm as an Example)

Under normal circumstances, if an HTTPS certificate is configured on EdgeOne, the process for the client to initiate an HTTPS handshake request is as follows (taking the RSA key exchange algorithm as an example):

1. The client sends a hello request to EdgeOne, including a random number generated by the client and information about supported encryption suites;
2. Once EdgeOne receives the request, it generates a random number on the server side and sends the public key of the HTTPS certificate configured for the current domain name to the client;
3. After receiving the server's random number and the public key certificate for the current domain name, the client verifies the certificate using a CA certificate to ensure it is valid and trusted;
4. Once the certificate is confirmed to have passed the verification, the client generates a pre-master key based on the current encryption algorithm, encrypts it with the public key from the certificate, and sends it to EdgeOne;
5. EdgeOne receives the encrypted pre-master key and decrypts it with the private key from the certificate to obtain the pre-master key;
6. At this point, both the server and the client have the complete information on the client's random number, the server's random number, and pre-master key, which will be combined to generate a session key. Both the client and the server use this session key for communication.

The security of the above encrypted communication session lies in the fact that the private key of the certificate on the server is secure. If it is leaked, it could be exploited by attackers, leading to session information leakage.

## Handshake Process in the Keyless Certificate Solution (Taking the RSA Key Exchange Algorithm as an Example)

EdgeOne currently supports the Keyless certificate solution. To further ensure the security of the private key of the certificate, it supports users to deploy only the public key of the domain name certificate to EdgeOne's edge nodes. Users can store the private key themselves and request the Keyless storage server to use the private key to decrypt related data when needed. The main difference from the normal handshake process for HTTPS one-way authentication is that after the server receives the encrypted pre-master key, EdgeOne will forward the information to the Keyless Server, which will then complete the decryption and return the decrypted pre-master key information to EdgeOne via encrypted communication.

### Note:

By default, HTTPS secure encrypted communication can be configured between EdgeOne's edge nodes and the Keyless Server. If you need to configure the HTTPS two-way authentication handshake to further ensure the security of the session, please [contact us](#).

## Preparations

1. Prepare a server for installing the Keyless Server, for example: `1.1.1.1` .
2. Prepare a domain name that needs to use Keyless, for example: `example.com` . This domain name has been connected to EdgeOne, and its corresponding certificates are: `example.com.crt` and `example.com.key` .
3. Prepare the server certificate that needs to be configured currently, including the client public and, private keys, for example: `server.crt` and `server.key` .

### Note:

You may also prepare the certificates required for testing by generating self-signed certificates, for which you can refer to [Using OpenSSL to Generate Self-Signed Certificates](#). It is important to note that self-signed certificates are solely for testing purposes and are not trusted by browsers, thus they should not be used in actual business scenarios.

## Directions

### Step 1: Install the Keyless Server Service on the Server

1. Log into the server where you plan to install the Keyless Server and ensure the following dependencies are installed. The requirements for the dependent environments are as follows:

[Go](#): The version should be go1.20 or higher.

[tRPC cmdline tools](#): Used for generating PB (protobuf) protocol code.

[trpc-go](#): The version should be v1.0.3 or above.

**Openssl:** The necessary libraries include openssl-static(1:1.1.1k-12.tl3.1), openssl-devel(1:1.1.1k-12.tl3.1), and zlib-devel(1.2.11-25.tl3).

2. Upon verifying that all initial installations have been completed, execute the following command to download the open-source Keyless server project code, provided by Tencent Cloud EdgeOne, from GitHub into your designated installation directory.

```
git clone https://github.com/Tencent/edgeone-keyless-server.git
```

3. Navigate to the root directory of the Keyless project.

```
cd /edgeone-keyless-server
```

4. Within the root directory, establish a directory named `/ssl` designated for the storage of Keyless public and private key certificates; furthermore, create a directory `/ssl/mutual_ssl` intended for housing the certificates utilized during the HTTPS handshake when the server receives Keyless requests.

```
mkdir ssl
mkdir ssl/mutual_ssl
```

**Note:**

Upon receiving a request for Keyless SSL acceleration, the Keyless server, by default, retrieves the certificate's private key for decryption by accessing the certificate stored in the `/ssl` directory. Should you wish to customize the storage path for the certificate, it is necessary to amend the `private_key_path` in `/config/keyless.yaml` to reflect the current path where the certificate is stored.

5. Upload the Keyless public and private key certificates for the current domain to the `/ssl` directory; for instance: `example.com.crt` , `example.com.key` . For the server certificates required for the handshake between EdgeOne edge nodes and the Keyless server, upload the public and private key files of the certificate to the `./ssl/mutual_ssl/` directory, such as `server.crt` , `server.key` .

**Note:**

The filenames of the public and private key certificates for Keyless must remain consistent.

Should you desire to employ HTTPS mutual authentication handshake between EdgeOne edge nodes and the Keyless server, please upload the client's CA certificate to the `./ssl/mutual_ssl/` directory as well.

Additionally, you will need to configure the client certificate that the EdgeOne edge node carries when initiating access to the Keyless server. For this certificate configuration, please [contact us](#).

6. Run the following command to get the local IP address, for example: `172.16.64.24` .

```
ifconfig -a
```

7. Modify the configuration file.

```
vim trpc_go.yaml
```

7.1 Press **i** to enter the insert mode to begin editing the configuration file. Modify the following five parameters, while keeping the other parameters as default:

IP: The local IP address obtained in Step 6;

Port: The service port for external access. It is recommended to use 443, and it is necessary to ensure that the port is accessible;

tls\_cert: The path of the server certificate's public key uploaded in Step 5;

tls\_key: The path of the server certificate's private key uploaded in Step 5;

ca\_cert: By default, no configuration is needed. If the configuration of the two-way authentication handshake is required, this item is used to specify the CA certificate path for the client certificate, which is the client CA certificate path uploaded in Step 5.

7.2 Press **Esc** to exit the insert mode, then enter **:wq** to save and exit.

8. Upon completing the basic configuration, proceed to compile the project.

```
go build -o keyless main.go && chmod a+x keyless
```

9. Run the following command to launch the keyless server service.

```
sudo nohup /edgeone-keyless-server/keyless >/dev/null 2>&1 &
```

10. Run the following command to check whether the current service has been launched successfully. If launch success is displayed, it means the service has been launched successfully.

```
tail -f log/keyless.log
```

## Step 2: Upload the Certificate to the Tencent Cloud SSL Certificate Console

Upload the certificate to be configured for the current domain name (including the public key only) to the Tencent Cloud SSL console. For the steps, refer to: [Uploading a Certificate to the Tencent Cloud SSL Console](#).

### Note:

If you need to upload a server certificate containing solely the public key, please [contact us](#) to enable allowlist access to Tencent Cloud's SSL product for you.

## Step 3: Configure the Domain Name in the EdgeOne Console to Use the Keyless Certificate

1. Log in to the [EdgeOne console](#), click **Site List** in the left menu bar, and click the **site** to be configured on the site list.

2. On the site details page, click **Domain Name Service** > **Domain Management**.

3. Find the domain name to be configured, click **Edit** in the HTTPS configuration column to go to the HTTPS configuration page, and choose to use the Keyless certificate.

4. Configure the address of the Keyless server. This address is the server address and port number you prepared in [Step 1](#).
5. Select the HTTPS certificate to be used. This certificate is the one you uploaded in [Step 2](#).
6. Click **OK** and wait for the configuration to be deployed so that it can take effect.

## Step 4: Verify Access

Use curl to perform access verification and check if the HTTPS handshake can be accessed successfully. You can refer to the following curl command:

```
curl https://example.com/ -v -k
```

## Updating a Keyless Certificate

1. Log in to the Keyless server, go to the currently installed Keyless directory, and upload the public key and private key certificates to be updated to the `./ssl/` directory;

### Note:

The file names of the Keyless public key and private key certificates must remain consistent. When updating the certificates, do not directly overwrite the old domain name certificates. It is recommended to use new file names for storage. For example, if original certificate names are `example.com.crt` and `example.com.key`, new certificate names can be `example.com.new.crt` and `example.com.new.key`.

2. After the upload is complete, execute the following command to reload the Keyless certificates:

```
curl http://127.0.0.1/KeylessReloadCerts -v
```

If the curl request is as follows and responds with 200, it means the loading is successful:

3. Upload the certificate to be updated currently (including the public key only) to the Tencent Cloud SSL console. For the steps, refer to: [Uploading a Certificate to the Tencent Cloud SSL Console](#).
4. Log in to the [EdgeOne console](#), click **Site List** on the left sidebar, and click the **site** to be configured on the site list.
5. On the site details page, click **Domain Name Service > Domain Management**.
6. Find the domain name to be configured, click **Edit** in the HTTPS configuration column to go to the HTTPS configuration page, and choose to use the Keyless certificate.
7. Change the HTTPS certificate to the one you newly uploaded, and then click **OK**. It will take effect once the configuration is deployed and issued.



# HTTPS Configuration

## Forced HTTPS Access

Last updated : 2025-05-26 17:03:11

### Overview

You can use 301 or 302 redirects to redirect HTTP client requests to HTTPS requests and send them to EdgeOne. Forced HTTPS access is used to improve website security and protect user privacy. If your business needs to safeguard user privacy and other sensitive information, we recommended you enable this feature to ensure that data is encrypted during transmission.

1. The client initiates an HTTP request.
2. The EdgeOne node responds with a 301 or 302 status code.
3. The client is redirected to initiate an HTTPS request.

### Scenario 1: Enabling Forced HTTPS Access for All Domain Names

To enable forced HTTPS access for all domain names used to access the current site, refer to the following information.

#### Prerequisites

You have configured SSL certificates for all domain names used to access the current site as instructed in [Certificate Configuration](#).

#### Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page. Then click **HTTPS** in the right sidebar.
3. On the forced HTTPS configuration card, toggle on the **Site-wide setting** switch to enable this feature for the entire site.

Off (default): EdgeOne does not perform any redirection, regardless of the request protocol used by a client. The client accesses an EdgeOne node via the original protocol.

On: You may choose to redirect HTTP requests made by a client to HTTPS by using a 301 or 302 redirect. HTTPS requests made by a client will not be redirected.

## Scenario 2: Enabling Forced HTTPS Access for Specified Domain Names

To enable forced HTTPS access for specified domain names used to access the current site, refer to the following information.

### Prerequisites

You have configured SSL certificates for the specified domain names used to access the current site as instructed in [Certificate Configuration](#).

### Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page. Then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.
4. On the page that appears, select **HOST** from **Matching type** and specify an operator and a value to match the requests of specified domain names.
5. From the **Action** drop-down list, select **Forced HTTPS**. Then, click **Switch**.
6. Click **Save and publish**.

# Enabling HSTS

Last updated : 2025-05-26 17:03:56

## Overview

HTTP Strict Transport Security (HSTS) is a web security protocol promoted by the Internet Engineering Task Force (IETF). The protocol is used to instruct web browsers to access a site over the more secure HTTPS protocol. You can configure HSTS to improve the security and credibility of your website if you have any of the following needs: to prevent malicious attackers from stealing sensitive user information through man-in-the-middle attacks, to comply with data privacy protection regulations, or to enhance users' trust in your website.

When a client initiates a request to an EdgeOne node over HTTP, this HTTP request may still be intercepted or tampered even though [forced HTTPS access](#) is enabled.

To improve access security, HSTS can be used to force browsers to directly initiate HTTPS requests. When HSTS is enabled, EdgeOne adds the `Strict-Transport-Security` header to HTTPS responses. The header tells browsers to send HTTPS requests in a specified period of time.

### Note:

1. The `Strict-Transport-Security` header applies to only HTTPS requests. Therefore, we recommend that you configure [forced HTTPS access](#) before you enable HSTS. This ensures that a user's initial access request is made over HTTPS and the configuration takes effect.
2. When the HSTS header is included in responses, browsers will alert users and intercept the access to the current site if a certificate security risk is detected. This further protects user data security.

## Scenario 1: Enabling HSTS for All Domain Names

To enable HSTS for all domain names used to access the current site, refer to the following information.

### Prerequisites

You have configured SSL certificates for all domain names used to access the current site as instructed in [Certificate Configuration](#).

### Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.

2. On the site details page, click **Site Acceleration** to enter the global site configuration page. Then click **HTTPS** in the right sidebar.
3. On the HSTS configuration card, toggle on the **Site-wide setting** switch to configure HSTS.

4. Configure the `Strict-Transport-Security` header in the pop-up window.

**On/Off:** Enable or disable HSTS.

**Cache time:** The value of the `max-age` field, which can be set to an integer from 1 to 31536000.

**Contain subdomain name:** When enabled, the `includeSubDomains` instruction is contained.

**Preload:** When enabled, the `preload` instruction is contained.

## Scenario 2: Enabling HSTS for Specified Domain Names

To enable HSTS for specified domain names or differentiate the HSTS configuration for different domain names, refer to the following information.

### Prerequisites

You have configured SSL certificates for the domain names for which you want to enable HSTS as instructed in [Certificate Configuration](#).

### Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page. Then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.
4. On the page that appears, select **HOST** from **Matching type** and specify an operator and a value to match the requests of specified domain names.
5. From the **Action** drop-down list, select **HSTS**. Then, configure the settings that appear. Then, click **Switch**.
6. Click **Save and publish**.

## More Information

The following table describes fields in the `Strict-Transport-Security` header:

Field	Description
<code>max-age=&lt;expire-</code>	The validity period of the HSTS header, measured in seconds. Within this

<code>time&gt;</code>	period, browsers always send requests over HTTPS.
<code>includeSubDomains</code> (optional)	Enable HSTS for the current domain name and all of its subdomain names.
<code>preload</code> (optional)	<p>Add the current domain name to the HSTS preload list of all major browsers. In this case, the browsers always send HTTPS requests to the domain name.</p> <p>Requirements:</p> <ul style="list-style-type: none"><li><code>max-age</code> is no less than 31536000 (one year).</li><li><code>includeSubDomains</code> is contained.</li><li><code>preload</code> is contained.</li></ul> <p>You can view the <a href="#">HSTS preload list</a> to check if the current domain name is in the browser's preload list. Major browsers regularly write the HSTS preload list into their version updates by hard coding.</p>

# SSL/TLS Security Configuration

## Configuring SSL/TLS Security

Last updated : 2025-05-26 17:06:47

### Use Cases

When HTTPS access is enabled for your website, EdgeOne supports multiple SSL/TLS versions to ensure compatibility with different user terminals by default. Normally, you do not need to modify this configuration. However, if your website requires a high level of security and you need to prevent users from accessing your website through less secure SSL/TLS versions, you can customize this configuration by specifying the required SSL/TLS versions.

#### Note:

For differences between different TLS versions and cipher suites, see [TLS Versions and Cipher Suites](#).

## Scenario 1: Modifying SSL/TLS Security Configuration for All Domain Names

To configure required SSL/TLS versions for all domain names used to access a site, refer to the following information.

### Prerequisites

You have configured SSL certificates for all domain names used to access the current site as instructed in [Certificate Configuration](#).

### Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page. In the right navigation bar, click **HTTPS**.
3. On the **SSL/TLS Security Configuration** card, click **Global settings** to modify the configuration.

Default configuration:

Supported TLS versions: `TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3` .

Cipher suite strength: `eo-loose-v2023` .

## Scenario 2: Modifying SSL/TLS Security Configuration for Specified Domain Names

To configure required SSL/TLS versions for specified domain names, refer to the following information.

### Prerequisites

You have configured SSL certificates for the specified domain names used to access the current site as instructed in [Certificate Configuration](#).

### Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page, then click the **Rule Engine** tab.
3. On the Rule Engine page, click **Create rule** and select **Add blank rule**.
4. On the page that appears, select **HOST** from **Matching type** and specify an operator and a value to match the requests of specified domain names.
5. From the **Action** drop-down list, select **SSL/TLS security configuration**. Then, select TLS versions as needed.
6. Click **Save and publish**.

# TLS Versions and Cipher Suites

Last updated : 2023-05-08 10:00:27

This document describes the TLS protocols and cipher suites that are supported by EdgeOne during a Transport Layer Security (TLS) handshake.

## TLS Protocol Versions

TLS is the successor protocol to Secure Sockets Layer (SSL) and is used to encrypt network communication between client and server applications. TLS has several versions, including TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. TLS 1.3 is the latest version that offers the most secure and efficient encryption mechanism.

## Cipher Suites

A cipher suite is a set of encryption algorithms used for secure connections via TLS. A cipher suite consists of an authentication algorithm, an encryption algorithm, and a message authentication code (MAC) algorithm. These algorithms protect data in transit from being stolen by third parties. During a TLS handshake, the client and server negotiate a cipher suite based on their lists of supported cipher suites. The cipher suite will encrypt communication between the client and server.

## Use Cases

By default, EdgeOne enables all TLS versions and uses the cipher suite `eo-loose-v2023`, which can meet the needs of most customers. If you require a higher level of security, you can adjust the settings accordingly.

Business Scenario	TLS Version	Cipher Suite
Compatibility with earlier browser versions is prioritized while security requirements can be relaxed accordingly.	TLS 1.0, TLS 1.1, and TLS 1.2	<code>eo-loose-v2023</code>
A balanced approach is needed to ensure a moderate level of security and browser version compatibility.	TLS 1.2 and TLS 1.3	<code>eo-general-v2023</code>
A high level of security is required while browser version compatibility may be sacrificed accordingly. All TLS versions and cipher suites	TLS 1.2 and TLS 1.3	<code>eo-strict-v2023</code>

that may have security vulnerabilities must be blocked.

## TLS Protocols and Cipher Suites Supported by EdgeOne

EdgeOne supports the following versions of TLS:

TLS 1.0

TLS 1.1

TLS 1.2

TLS 1.3

OpenSSL Cipher Suite	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
TLS_AES_256_GCM_SHA384	✓	-	-	-
TLS_CHACHA20_POLY1305_SHA256	✓	-	-	-
TLS_AES_128_GCM_SHA256	✓	-	-	-
TLS_AES_128_CCM_SHA256	✓	-	-	-
TLS_AES_128_CCM_8_SHA256	✓	-	-	-
ECDHE-ECDSA-AES256-GCM-SHA384	-	✓	-	-
ECDHE-ECDSA-AES128-GCM-SHA256	-	✓	-	-
ECDHE-RSA-AES256-GCM-SHA384	-	✓	-	-
ECDHE-RSA-AES128-GCM-SHA256	-	✓	-	-
ECDHE-ECDSA-CHACHA20-POLY1305	-	✓	-	-
ECDHE-RSA-CHACHA20-POLY1305	-	✓	-	-
ECDHE-ECDSA-AES256-SHA384	-	✓	-	-
ECDHE-ECDSA-AES128-SHA256	-	✓	-	-
ECDHE-RSA-AES256-SHA384	-	✓	-	-
ECDHE-RSA-AES128-SHA256	-	✓	-	-
ECDHE-RSA-AES256-SHA	-	-	✓	✓
ECDHE-RSA-AES128-SHA	-	-	✓	✓

AES256-GCM-SHA384	-	✓	-	-
AES128-GCM-SHA256	-	✓	-	-
AES256-SHA256	-	✓	-	-
AES128-SHA256	-	✓	-	-
AES256-SHA	-	-	✓	✓
AES128-SHA	-	-	✓	✓

EdgeOne offers users several cipher suite strength options based on the TLS protocol version.

`eo-strict-v2023` : Offers the highest level of security by disabling all insecure cipher suites.

`eo-general-v2023` : Keeps a balance between browser version compatibility and security.

`eo-loose-v2023` (default): Offers the highest compatibility by relaxing security requirements accordingly.

OpenSSL Cipher Suite	eo-strict-v2023	eo-general-v2023	eo-loose-v2023
TLS_AES_256_GCM_SHA384	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓
TLS_AES_128_GCM_SHA256	✓	✓	✓
TLS_AES_128_CCM_SHA256	-	✓	✓
TLS_AES_128_CCM_8_SHA256	-	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓
ECDHE-ECDSA-CHACHA20-POLY1305	✓	✓	✓
ECDHE-RSA-CHACHA20-POLY1305	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	-	✓	✓
ECDHE-ECDSA-AES128-SHA256	-	✓	✓
ECDHE-RSA-AES256-SHA384	-	✓	✓

ECDHE-RSA-AES128-SHA256	-	✓	✓
ECDHE-RSA-AES256-SHA	-	-	✓
ECDHE-RSA-AES128-SHA	-	-	✓
AES256-GCM-SHA384	-	-	✓
AES128-GCM-SHA256	-	-	✓
AES256-SHA256	-	-	✓
AES128-SHA256	-	-	✓
AES256-SHA	-	-	✓
AES128-SHA	-	-	✓

You can choose a TLS version and cipher suite strength. The final supported OpenSSL cipher suites are determined by the selected options in combination.

For instance, if you enable `TLS 1.3` and select `eo-strict-v2023` , the OpenSSL cipher suites supported are `TLS_AES_256_GCM_SHA384` , `TLS_CHACHA20_POLY1305_SHA256` , and `TLS_AES_128_GCM_SHA256` .

## Relevant Documentation

[Configuring SSL/TLS Security](#)

# Enabling OCSP Stapling

Last updated : 2025-05-26 17:04:47

## Overview

Online Certificate Status Protocol (OCSP) is provided by certificate authorities (CAs) to check the authenticity and validity of digital certificates. Whenever a user accesses a website over HTTPS, the browser initiates an OCSP query to verify whether the certificate of the website is still valid.

When OCSP stapling is enabled, EdgeOne performs OCSP queries and caches the results on servers. When a client initiates a TLS handshake with EdgeOne, EdgeOne responds with the OCSP information and certificate required for verification so that the client does not need to send a query request to the CA. This significantly improves the efficiency of the TLS handshake, reduces the time for verification, and improves the HTTPS request speed.

To enhance website performance and improve the efficiency of certificate status validation during HTTPS handshakes, you can enable OCSP stapling.

OCSP Stapling Disabled	OCSP Stapling Enabled
<div>1. The client initiates a TLS handshake.</div> <div>2. EdgeOne responds to the TLS handshake (by returning the certificate).</div> <div>3. The client initiates an OCSP query.</div> <div>4. The CA returns the result.</div>	<div>1. The client initiates a TLS handshake.</div> <div>2. EdgeOne initiates an OCSP query.</div> <div>3. The CA returns the result, and EdgeOne caches the result.</div> <div>4. EdgeOne responds to the TLS handshake (by returning the certificate and OCSP information).</div> <div>Because OCSP information is cached on EdgeOne servers, EdgeOne will respond to subsequent query requests without initiating a new OCSP query.</div>

## Scenario 1: Enabling OCSP Stapling for All Domain Names

To enable OCSP stapling for all domain names used to access a site, refer to the following information.

### Prerequisites

You have configured SSL certificates for all domain names used to access the current site as instructed in [Certificate Configuration](#).

## Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page. Then click **HTTPS** in the right sidebar.
3. Locate the OCSP stapling configuration card. This protocol is disabled by default. Toggle the **switch** to enable it.

Off (default): When a client initiates a TLS handshake, the client must send a certificate verification request to the CA to check the certificate status in real-time.

On: EdgeOne sends a certificate verification request to the CA and caches the query results. When a client initiates an HTTPS request to the EdgeOne node, EdgeOne responds to the request by providing the certificate query results.

## Scenario 2: Enabling OCSP Stapling for Specified Domain Names

To enable OCSP stapling for specified domain names, refer to the following information.

### Prerequisites

You have configured SSL certificates for the specified domain names for which you want to enable OCSP stapling, as instructed in [Certificate Configuration](#).

## Directions

1. Log in to the [EdgeOne](#) console and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page. Then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.
4. On the page that appears, select **HOST** from **Matching type** and specify an operator and a value to match the requests of specified domain names.
5. From the **Action** drop-down list, select **OCSP stapling**, click **Switch** to enable the configuration.
6. Click **Save and publish**.

## Related References

# Using OpenSSL to Generate Self-Signed Certificates

Last updated : 2024-12-19 11:03:27

All server and client certificates usually need to be applied for from a certificate authority (CA) to ensure that they can be trusted by different operating systems and browsers. CA typically charges a certain certificate fee. If you currently need an HTTPS certificate just for testing or for internal use in an enterprise, you can also issue a self-signed certificate using OpenSSL. Refer to the following steps:

## Step 1: Generating a Root Certificate

1. Create a root certificate private key with the following command, which will generate a 2048-bit private key and save it to a .key file.

```
openssl genrsa -out root.key 2048
```

2. Generate a Certificate Signing Request (CSR) file based on the root certificate private key.

```
openssl req -new -key root.key -out root.csr
```

During the generation of a CSR file, you need to provide information such as the organization name and common name, which can be filled in based on the actual usage.

3. Run the following command to create a root certificate.

```
openssl x509 -req -in root.csr -out root.crt -signkey root.key -CAcreateserial  
-days 3650
```

You will get a root certificate, root.crt, with a validity period of 10 years. You can use this root certificate to issue the required server and client certificates later.

## Step 2: Issuing a Certificate

Taking issuing a server certificate as an example, you can start issuing your own certificates using the root certificate generated in [Step 1](#):

1. Generate a private key for the server certificate.

```
openssl genrsa -out server.key 2048
```

2. Generate a CSR file based on the server certificate private key.

```
openssl req -new -out server.csr -key server.key
```

During the generation of a CSR file, similar to that for the root certificate, you need to provide information such as the organization name and common name, which can be filled in based on the actual usage.

3. Generate a server public key certificate.

```
openssl x509 -req -in server.csr -out server.crt -signkey server.key -CA root.crt -
```

Through the above three steps, you will obtain self-signed server certificates, server.crt, and server.key, with a validity period of 10 years. You can repeat these steps to continue generating other required server or client certificates using the same root certificate.



Your certificate should start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----".

Each line should contain 64 characters, with the last line containing no more than 64 characters.

2. If the certificate is issued by an intermediate CA, the CA certificate needs to include a multi-level certificate chain.

The certificate chain structure is as follows:

```
-----BEGIN CERTIFICATE-----
Intermediate CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root CA
-----END CERTIFICATE-----
```

The certificate chain rules are as follows:

There should be no blank lines between certificates.

All certificates should meet the certificate format requirements mentioned above.

## Instructions for Converting Certificates to PEM Format

Generally, HTTPS certificates are in PEM format. For certificates in other formats that need to be converted to PEM format, it is recommended to use the OpenSSL tool for conversion. Below are methods to convert several popular certificate formats to PEM format.

DER to PEM

P7B to PEM

PFX to PEM

CER/CRT to PEM

The DER format is generally used on Java platforms.

Certificate conversion:

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

Private key conversion:

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

The P7B format is generally used on Windows Server and Tomcat.

Certificate conversion:

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

You need to get the content between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" in outcertificate.cer to upload as certificate.

Private key conversion: Private keys can generally be exported on IIS servers.

The PFX format is generally used on Windows Server.

Certificate conversion:

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

Private key conversion:

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

You can convert certificates in CER/CRT format by directly modifying their file extensions. For example, you can directly rename the "servertest.crt" certificate file as the "servertest.pem" certificate file.

# Origin Configuration

## Load Balancing

## Overview

Last updated : 2024-05-29 10:33:37

EdgeOne Load Balancing is ideal for scenarios where high availability of origins is crucial. It supports the configuration of multi-level secondary sources for disaster recovery switching. It can proactively probe the health status of origins. This proactive measure blocks failed origins and directs business traffic to healthy origins.

### Note:

EdgeOne Load Balancing feature is in beta testing. If you want to use it, you can [Contact Us](#).

## Use Cases

Hardware failures, network failures, configuration errors, security attacks, natural disasters, human errors, and other unforeseen circumstances, can affect the availability of the origin. For businesses that require high availability, such as finance, gaming, audio and video, and e-commerce, even brief failures of the origin can result in significant losses. Therefore, it is necessary to implement primary/secondary disaster recovery and health checks for the origin.

**Primary/Secondary Disaster Recovery:** When the primary source becomes unavailable, it is automatically switched to the secondary source to ensure business continuity.

**Proactively Checking origin Health Status:** Preemptively disables failed origins, and redirects business traffic to healthy origins. Prevents a situation where a significant number of legitimate service requests are still directed to malfunctioning origins in the event of a failure.

## Supported Capabilities

1. Supports the configuration of multi-level secondary sources for multi-source disaster recovery.
2. Supports the configuration of health check policies such as ICMP Ping, HTTP/HTTPS, TCP, and UDP to preemptively disable failed origins and redirect business traffic to healthy origins.
3. Provides a fallback retry policy. It retries directing the traffic to alternative healthy origins when real business traffic requests fail.



## More Information

[Quickly Create Load Balancers](#)

[Load Balancing-Related Concepts](#)

[Health Check Policies](#)

# Quickly Create Load Balancers

Last updated : 2024-05-29 10:33:37

This document guides you on how to create a Cloud Load Balancer instance.

## Note:

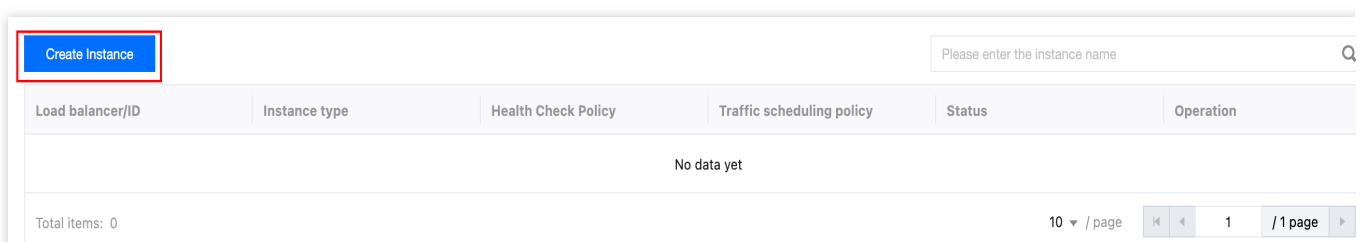
EdgeOne Load Balancing feature is in beta testing. If you want to use it, you can [Contact Us](#).

## Sample Scenario

For example, you currently have an acceleration domain `www.example.com`, with three origins `1.2.3.4`, `2.3.4.5`, and `3.4.5.6`. Under normal circumstances, both `1.2.3.4` and `2.3.4.5` are used as primary origins. You have already configured them as the origin group named `primary_origins` following the [Origin Group Operation Guide](#). The server `3.4.5.6` is used as a standby origin in a group called `backup_origins`, which is only used when the primary origins fail. In cases where a real business request fails, retries are attempted with other healthy servers within the same group. Additionally, there is a requirement for proactive probing to actively identify and disable unhealthy origins.

## Directions

1. Log in to the [Tencent Cloud EdgeOne console](#). In the left menu bar, click the **Site List**. Within this list, click the **Site** that need to be configured to go to the details page.
2. On the site details page, click **Origin Settings > Load Balancing**.
3. On the Load Balancing page, click **Create Instance**.



4. Proceed to step 1 of choosing the origin. You need to fill in the instance name, choose the instance type, and add an origin group.

Taking this scenario as an example, add the origin group `primary_origins` as a priority 1 origin group, add the origin group `backup_origins` as a priority 2 origin group, and click **Next**.

1 Select origin

2 Health Check Policy

3 Traffic scheduling policy

Instance name 
  
1-200 characters, allowed characters are a-z, A-Z, 0-9, \_, -

Instance type ☒ HTTP-specific type ☐ General Type

Add origin group

Priority	Origin Group	Origin type	Origin group information	Operation
1	<input type="text" value="primary_origins"/>	HTTP-specific type	1.2.3.4(50.00%) 2.3.4.5(50.00%)	<a href="#">Delete</a>
2	<input type="text" value="backup_origins"/>	HTTP-specific type	3.4.5.6	<a href="#">Delete</a>
<a href="#">+ Add origin</a>				

Next

Cancel

Parameter	Description
Instance name	Limit to 1-200 characters in length. Allowed characters are a-z, A-Z, 0-9, _, -.
Instance type	<p>HTTP-specific Type: Supports adding both HTTP-specific and general origin groups. It is only applicable for reference by site acceleration-related services, such as domain services and rule engines.</p> <p>General Type: Only supports adding general origin groups. It is applicable for site acceleration services including domain services and rule engines, and reference by L4 proxy service.</p>
Add origin group	<p>In the CLB instance, the smallest configuration dimension for an origin is the origin group. You need to configure the origin into an origin group and add it here. For more details, see <a href="#">Origin Group Configuration</a>.</p> <p>You can set priorities for the added origin groups. Traffic will not be directed to origins in lower-priority origin groups if there are healthy origins in higher-priority origin groups. Up to 10 origin groups can be configured, with lower numbers indicating higher priorities.</p>

5. Proceed to step 2 of health check policy. It supports four types of probes: ICMP Ping, HTTPS/HTTP, TCP, and UDP. Tencent Cloud EdgeOne will actively send probe requests to your origin to check its latency and health status. You can choose the appropriate probe frequency based on the load condition of your origin. Here, choose ICMP Ping as the probe policy. For a detailed introduction to probe policy configuration, see [Introduction to Health Check Policy](#). After configuration is completed, click **Next**.

1 Select origin

2 Health Check Policy

3 Traffic scheduling policy

EdgeOne will detect the latency and health of your origin by proactively sending probing requests to your origin based on the following configuration you select.

### Detection Policy

**ICMP Ping**

Only check network connectivity, host accessibility

**HTTPS/HTTP**

Suitable for applications that need to recognize the content of the request, such as Web applications, app services, etc.

**TCP**

Suitable for scenarios that require high reliability and data accuracy and low transmission speed, such as file transfer, remote login, etc.

**UDP**

Suit for scenarios that require high transmission efficiency and relatively low accuracy, such as instant messaging, online video, etc.

**Disable**

Disable all health check policies

### Basic configuration

Detection frequency: Every 30 seconds

[Expand Advanced Configuration](#)

[Back](#) [Next](#)

**Note:**

If you do not want EdgeOne's nodes to initiate any probe requests to origins, you can choose **Not Enabled**. In this case, the Load Balancing instance will default to traffic scheduling based on the priority order of the origin groups from step 1. If a request to a particular origin fails 5 times within 60 seconds, the corresponding origin will be disabled for 10 minutes according to the default policy.

Using this policy **will not be able to disable the origin of the failure in advance, and it will not be able to automatically and quickly recover the traffic scheduling after the origin returns to normal**. Compared with enabling active probe, using this policy may cause you to encounter more failed requests during the origin failure period. Therefore, if you want your business to have higher availability, it is recommended that you enable active probe.

6. Proceed to step 3 of traffic scheduling policy. The current traffic scheduling policy defaults to failover based on the priority order according to the results of active probes. When real business requests fail to retrieve content from the origin during the backsource process, support for request retry is available. There are two request retry policies available. For details, see [Introduction to Request Retry Policy](#).

Policy 1: When a real business request fails to access a certain origin, it directly retries with another origin within the next lower priority origin group. This is suitable for scenarios where the performance of both origin group 1 and origin group 2 is similar.

Policy 2: When a real business request fails to access a certain origin, it directly retries with another origin within the same priority origin group. This is suitable for scenarios where the performance of origin group 1 is significantly better than that of origin group 2.

✓ Select origin

✓ Health Check Policy

3 Traffic scheduling policy

Traffic scheduling policy

**Failover in order of priority**

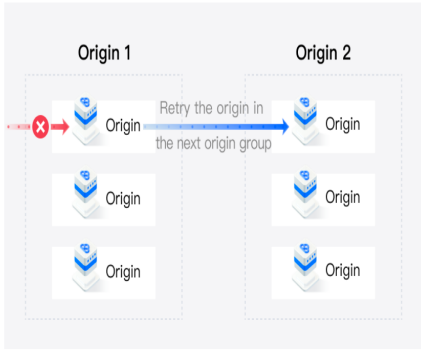
EdgeOne will actively probe the configured origins based on the health check policy you have set, block faulty origin groups in the order of priority, and route traffic to healthy origin groups.

Request retry policy

**The process of origin pulling may fail due to network fluctuations or other reasons, therefore two retry strategies are provided.**

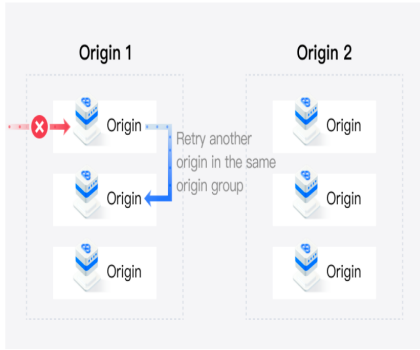
☐ Strategy 1

When a real request fails to access a specific origin, it will directly retry to other origins in the current priority origin group. Applicable scenario: Similar performance between origin group 1 and origin group 2.



☒ Strategy 2

When a real request fails to access a specific origin, it will directly retry to other origins in the current priority origin group. Applicable scenario: Origin group 1 has much better performance than origin server group 2.



Back

Complete

7. Taking this sample scenario as an example, policy 2 can be chosen. Click **Complete** to finish creating the instance.

# Health Check Policies

Last updated : 2025-03-24 17:16:06

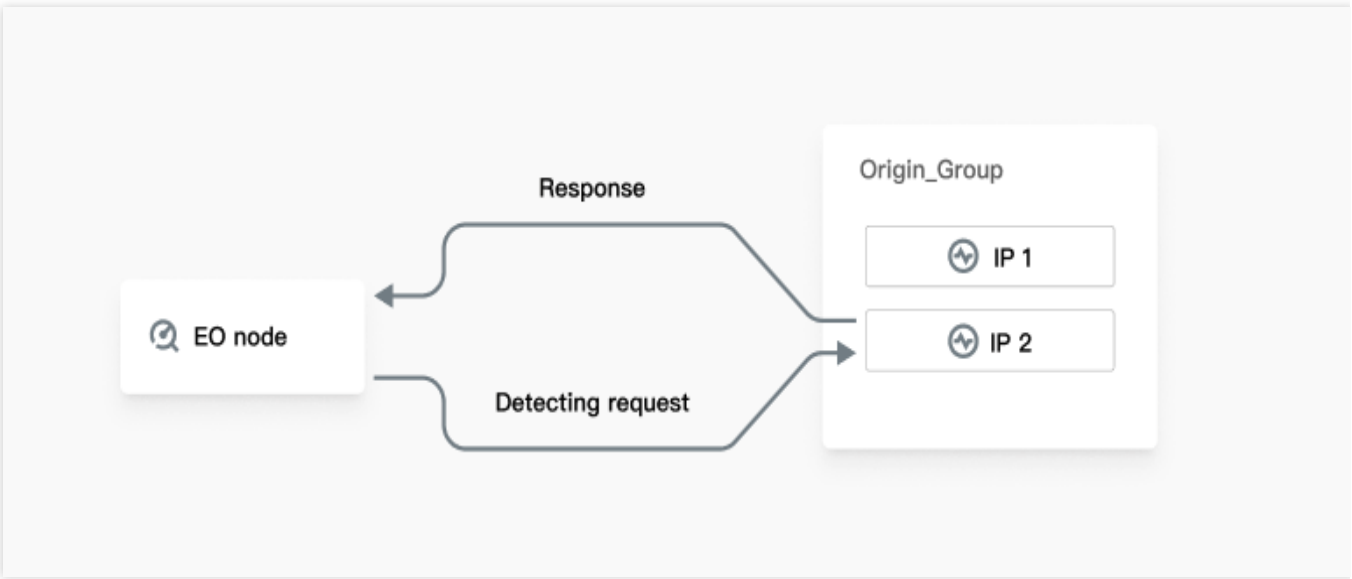
This document introduces the probe methods and their principles within health checks, the origin health determination criteria and the calculation methods.

**Note:**

EdgeOne Load Balancing feature is in beta testing. If you want to use it, you can [Contact Us](#).

## Principle of Health Checks

After configuring health check policies, EdgeOne's probe nodes in different regions will send probe requests to your origin and determine the health status of the origin based on the response results. Health check policies consist of probe methods and origin health determination criteria. The probe method determines the type of probe request, while the origin health determination criteria determine how the response results are processed.



### Probe Method

Currently, supports for ICMP Ping, HTTP/HTTPS, TCP, and UDP as the four methods of probe. For more details, see [The Principle Introduction of Probe Methods](#). The following are the explanations for the corresponding configuration items:

Probe Method	Applicable Scenario	Configuration Item	Description
ICMP Ping	Only probes network connectivity, and host reachability.	Probe Frequency	Required, with optional intervals of every 30 seconds, every 60 seconds, every 3 minutes, every 5 minutes, or every 10 minutes.

HTTP/HTTPS	Applicable for applications that require content recognition in requests, such as web applications and app services.	Probe Frequency	Required, with optional intervals of every 30 seconds, every 60 seconds, every 3 minutes, every 5 minutes, or every 10 minutes.
		URL	Required, the full URL for health checks, for example: <code>www.example.com/test</code> .
		Probe Port	Required, defaulting to port 80. It is recommended not to modify this unless a specific port needs to be designated.
		HTTP Method	Required, the HTTP method for health checks is by default HEAD, with options including GET or HEAD. If the HEAD method is used, the server returns only HTTP header information, which can reduce backend overhead and enhance request efficiency. The corresponding origin service must support HEAD. If the GET method is used, the origin service simply needs to support GET.
		HTTP Status Code	Required, the origin is considered healthy when the status code matches the selected status codes. By default, this includes 2XX, with options to select: 1XX, 2XX, 3XX, 4XX, 5XX.
		Follow Redirects	Disabled by default. When enabled, the probe node will initiate another probe based on the 301/302 redirect address responded by the origin. It Uses the status code of the final redirection response as the determination result for the health status. Up to 3 redirects are supported.
		Custom Request Headers	Optional, custom request headers can be configured to be sent with the health check requests to the origin, with a maximum of 8 configurations allowed, for example: <code>host : www.example.com</code> .
TCP	Suitable for scenarios where high reliability and data accuracy are essential, but	Probe Frequency	Required, with optional intervals of every 30 seconds, every 60 seconds, every 3 minutes, every 5 minutes, or every 10 minutes.
		Probe Port	Required, defaulting to port 80. It is

	transmission speed is of lesser importance, such as file transfers and remote log-ins.		recommended not to modify this unless a specific port needs to be designated.
UDP	Suitable for scenarios where high transmission efficiency is crucial and a relatively lower level of accuracy is acceptable, such as instant messaging and online video streaming.	Probe Frequency	Required, with optional intervals of every 30 seconds, every 60 seconds, every 3 minutes, every 5 minutes, or every 10 minutes.
		Probe Port	Required, defaulting to port 80. It is recommended not to modify this unless a specific port needs to be designated.
		Probe Request	Required, customize the content of the health check request, with a limit of 500 characters.
		Probe Response Result	Required, customize the content of the health check request, with a limit of 500 characters.

## Origin Health Determination Criteria

Choose any of the probe policies: ICMP Ping, HTTP/HTTPS, TCP, and UDP. Click **Show Advanced Configuration** to configure origin health determination criteria. The following are the descriptions for each configuration item:

1 Select origin

2 Health Check Policy

3 Traffic scheduling policy

EdgeOne will detect the latency and health of your origin by proactively sending probing requests to your origin based on the following configuration you select.

Detection Policy

ICMP Ping

Only check network connectivity, host accessibility

HTTPS/HTTP

Suitable for applications that need to recognize the content of the request, such as Web applications, app services, etc.

TCP

Suitable for scenarios that require high reliability and data accuracy and low transmission speed, such as file transfer, remote login, etc.

UDP

Suit for scenarios that require high transmission efficiency and relatively low accuracy, such as instant messaging, online video, etc.

Disable

Disable all health check policies

Basic configuration

Detection frequency

Every 30 seconds

[Collapse Advanced Configuration](#)

Source station health conditions

Timeout period

—

5

+

seconds

the default is 5 seconds.

Unhealthy threshold

—

2

+

times

The number of times to retry when the health check result is "Unhealthy"

Healthy threshold

—

3

+

times

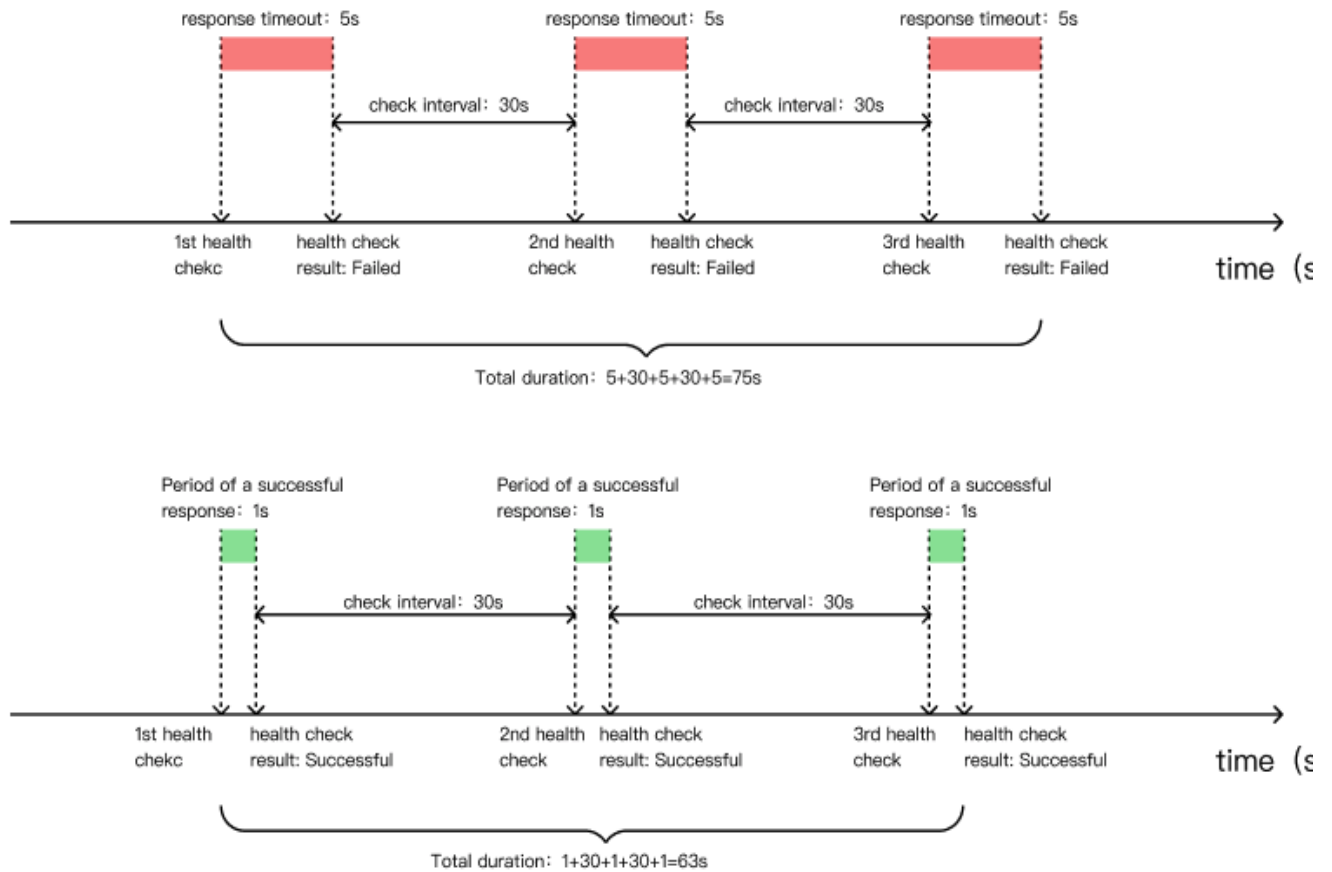
When the origin is healthy for several consecutive times, the origin group is determined to be "healthy" and restored to an available state, default 3 times.

Back

Next

Configuration Item	Description
Timeout	The allowed timeout duration for a single health check request to the origin. If no response is received within this period, the origin is considered Unhealthy. The default is 5 seconds, with a configurable range of [1, 30] seconds.
Unhealthy Threshold	The number of consecutive probe failures required to determine an origin Unhealthy. Once this threshold is reached, the origin is considered Unhealthy. The default is 2 times, with a configurable range of [1, 5]. For example, if this value is set to 2, and an origin is initially Healthy, upon receiving two consecutive Unhealthy probe results, the origin will be considered Unhealthy.
Healthy Threshold	The number of consecutive successful probes required to restore an origin to a Healthy state, making it available again. The default is 3 times, with a configurable range of [1, 5]. For example, if this value is set to 3, and an origin is Unhealthy, after three consecutive Healthy probe results, the origin will be restored to a Healthy status.

### Active Probing Cycle for Origin Health Status Change



For example, suppose the health determination conditions for the origin are set as follows: timeout of 5 seconds, unhealthy threshold of 3 times, healthy threshold of 3 times, and a probe interval of every 30 seconds.

The time required to consider an origin Unhealthy would then be:  $5+30+5+30+5=75$  seconds.

The time required to restore the origin to a Healthy state (assuming a successful active probe response takes 1 second) would be:  $1+30+1+30+1=63$  seconds.

## More Information

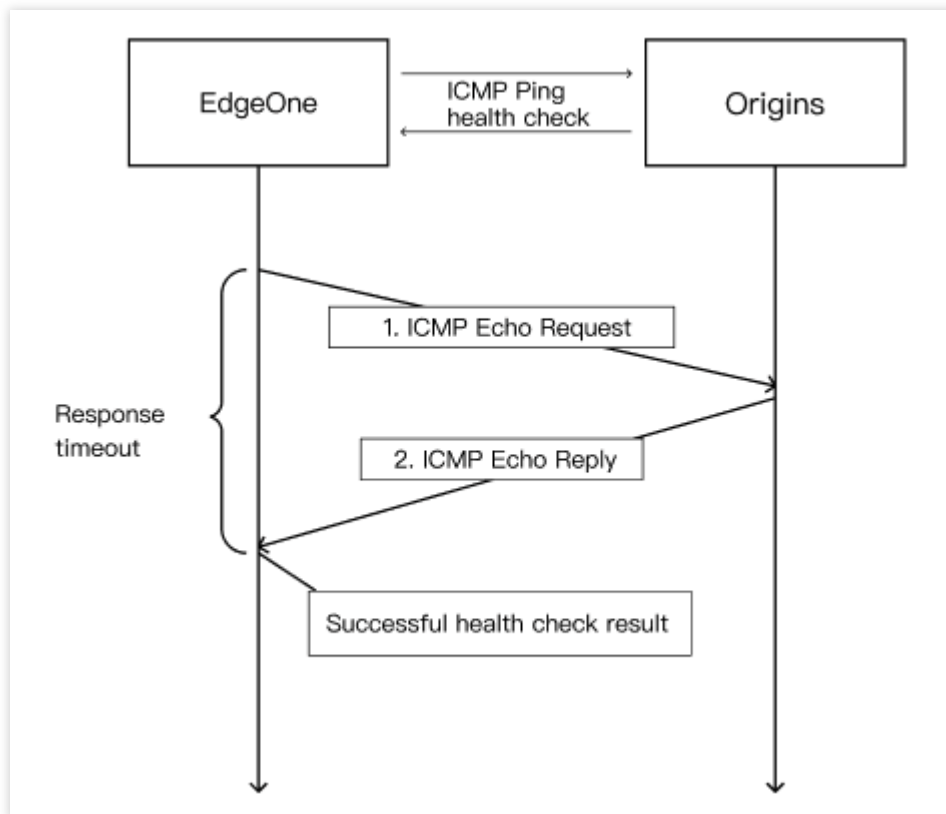
### Introduction to Principle of Probe Method

ICMP Ping

HTTP/HTTPS

TCP

UDP

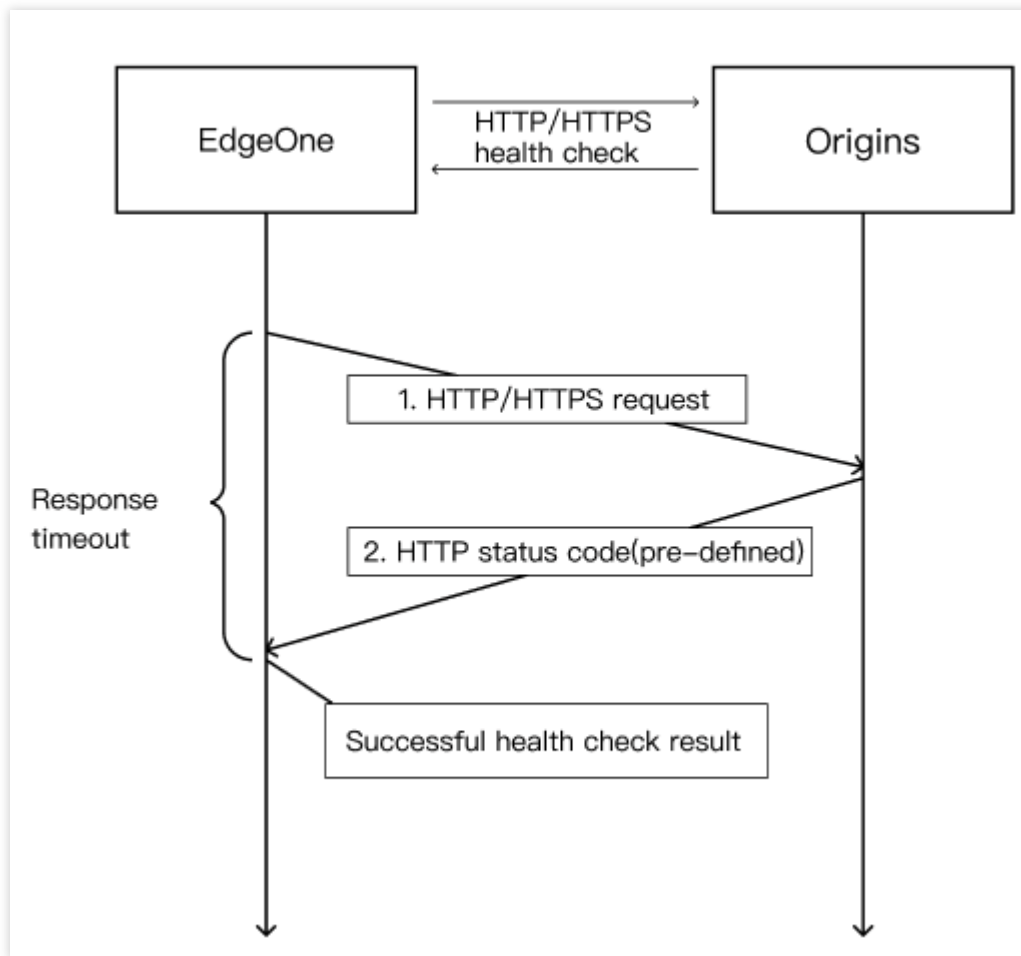


The ICMP Ping health check mechanism is as follows:

1. EdgeOne probe node sends a Ping command to your origin.
2. If the Ping is successful, and within the backsource timeout period, the probe node receive an ICMP reply from the origin, the service is considered normal, and the result of this check is considered healthy.
3. If the Ping fails, and within the backsource timeout period, the probe node does not receive an ICMP reply from the origin, the service is considered abnormal, and the result of this check is considered unhealthy.

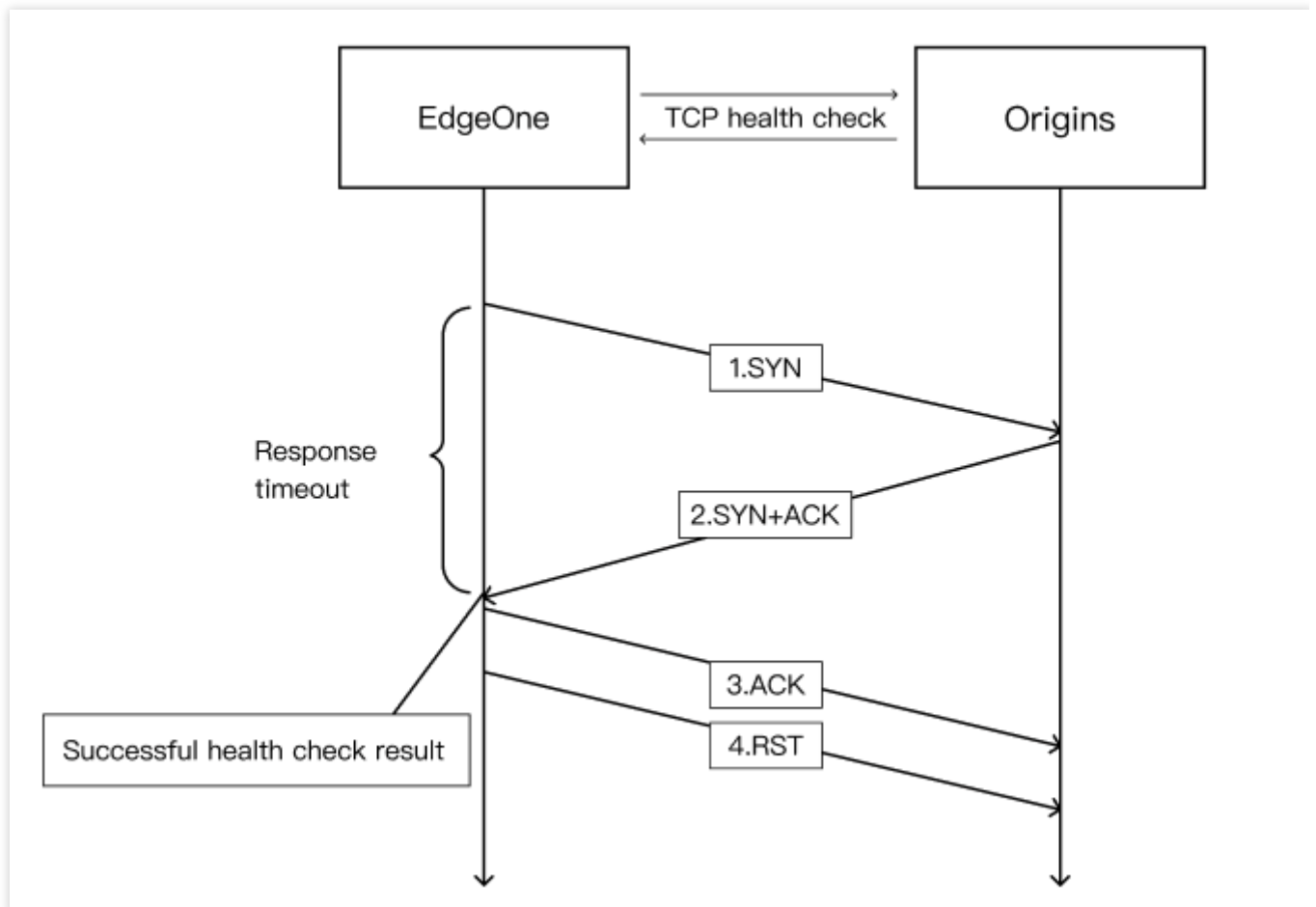
**Note:**

ICMP Ping requires your origin to support Ping.



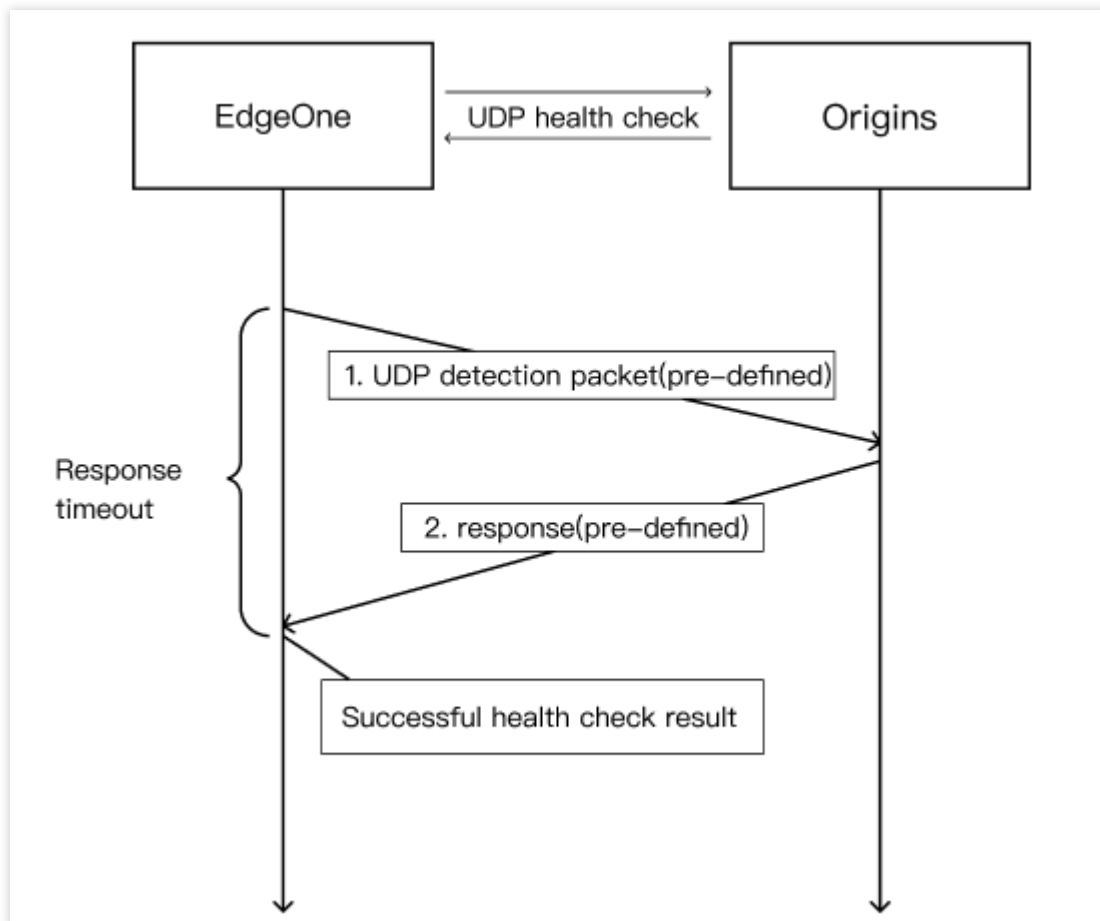
The HTTP/HTTPS health check mechanism is as follows:

1. EdgeOne probe node sends an HTTP request to your origin. It requires configuration of the corresponding URL and port, with the option to include a custom HOST header.
2. If, within the backsource timeout period, the EO probe node receives an HTTP status code from the origin that successfully matches the configured HTTP status codes, the result of this check is considered healthy.
3. If, within the backsource timeout period, the EO probe node does not receive a response from the origin or receives a status code that does not match the configured codes, the result of this check is considered unhealthy.



The TCP health check mechanism is as follows:

1. EdgeOne probe node sends a SYN connection request packet to a specific port (configurable) on your origin.
2. Upon receiving the SYN request packet, if the corresponding port on the origin is in a normal listening state, it will respond with a SYN+ACK packet.
3. If, within the backsource timeout period, the probe node receives a SYN+ACK response packet from the origin, it indicates that the service is running normally. The result of this check is considered healthy. The probe node then replies with an ACK packet to the origin and sends an RST reset packet to terminate the TCP connection.
4. If, within the backsource timeout period, the probe node does not receive a SYN+ACK response packet from the origin, it indicates that the service is running abnormally. The result of this check is considered unhealthy. The probe node sends an RST reset packet to the origin to terminate the TCP connection.



The UDP health check mechanism is as follows:

1. EdgeOne probe node sends a customized probe packet to a specific port (configurable) on your origin.
2. If, within the backsource timeout period, the probe node receives a customized response packet from the origin, it indicates that the service is running normally. The result of this check is considered healthy.
3. If, within the backsource timeout period, the probe node does not receive a customized response packet from the origin or receives a response packet that does not conform to the defined content, it indicates that the service is running abnormally. The result of this check is considered unhealthy.

**Note:**

Both the request content and response content are customized, and you need to configure the corresponding request-response content on your origin.

### Probe Request Identification

Active probes do not carry special request identifiers. When you choose ICMP Ping or TCP probes, there are no related features. When you choose UDP probes, customized content can be configured to serve as identifiers. For HTTP/HTTPS probes, separate customized request headers can be configured to serve as identifiers.

# Viewing the Health Status of Origin Server

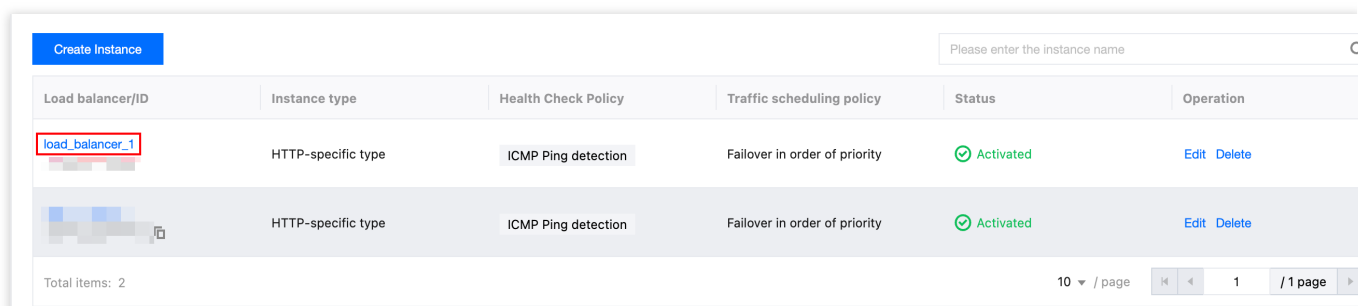
Last updated : 2024-05-29 10:33:37

The node probe results will display the outcomes of probes initiated by EdgeOne from various nodes and regions within the global availability zones towards the current origin group. Users can view these probe results to find whether the origin is healthy across different zones.

## Note:

EdgeOne Load Balancing feature is in beta testing. If you want to use it, you can [Contact Us](#).

1. Log in to the [EdgeOne console](#). In the left menu bar, click the **Site List**. Within this list, click the **Site** need to be configured to go to the details page.
2. On the site details page, click **Origin Settings > Load Balancing**.
3. On the Load Balancing page, click the desired **Load balancer**.



Create Instance		Please enter the instance name			
Load balancer/ID	Instance type	Health Check Policy	Traffic scheduling policy	Status	Operation
load_balancer_1	HTTP-specific type	ICMP Ping detection	Failover in order of priority	Activated	Edit Delete
	HTTP-specific type	ICMP Ping detection	Failover in order of priority	Activated	Edit Delete
Total items: 2		10 / page 1 / 1 page			

4. In the instance details page, click **View details**.

Instance details

Instance name

load\_balancer\_1 HTTP-specific type ICMP Ping detection

Instance ID

Check frequency

Every 30 seconds

The timeout(in seconds) before making the health check failed.

5 seconds

Thresholds to mark origin unhealthy.

2 times

Health threshold

3 times

Traffic scheduling policy

Failover in order of priority

Request retry policy

When an origin is marked unhealthy or request an origin fails, subsequent requests go directly to the next prioritized group of origin.

Origin Group Status

Priority	Origin Group	Origin Health Status	Origin group type	Operation
1	<div></div>	ipv4 <div></div>	HTTP-specific type	<a href="#">View details</a>

5. In the node probe results, nodes are differentiated by the following three colors:

**Green Node:** Indicates that the probe node in the region has considered all origins in the origin group to be healthy.

**Red Node:** Indicates that the probe node in the region has considered one or more origins in the origin group to be unhealthy.

**Gray Node:** Indicates that the probe node in the region cannot probe any origins. Probing is done at the IP level, meaning if the origin is a domain, the domain will be resolved into an IP before it probes. This situation usually occurs if you have entered an incorrect domain origin which cannot be resolved into an IP. In this case, it is recommended to check for potential spelling mistakes in the origin domain or whether the corresponding domain has expired.

#### Detection results

Number of total nodes

17

Number of nodes with all origins healthy

16

Number of nodes with unhealthy origin

1

Number of nodes where no origin is detected

0



#### Note:

Probe nodes in different regions make independent decisions. Edge nodes will route requests back to the origin based on the probe results from the nearest probe nodes in each region.

For example: If your origin is in Hong Kong (China), and the probe node in Singapore considers the origin to be unhealthy whereas the probe node in Germany considers it to be healthy, traffic from the Singapore region will not be routed to that origin, while traffic from the Germany region will continue to be directed to that origin.

In the scenario described above, you can refer to the probe results from other regions for a comprehensive view. If only a few nodes consider the origin to be unhealthy, it might be due to network fluctuations in certain areas. If the majority of nodes consider the origin to be unhealthy, it is recommended to check whether the origin has malfunctioned.



## Related References

# Load Balancing-Related Concepts

Last updated : 2024-05-29 10:33:37

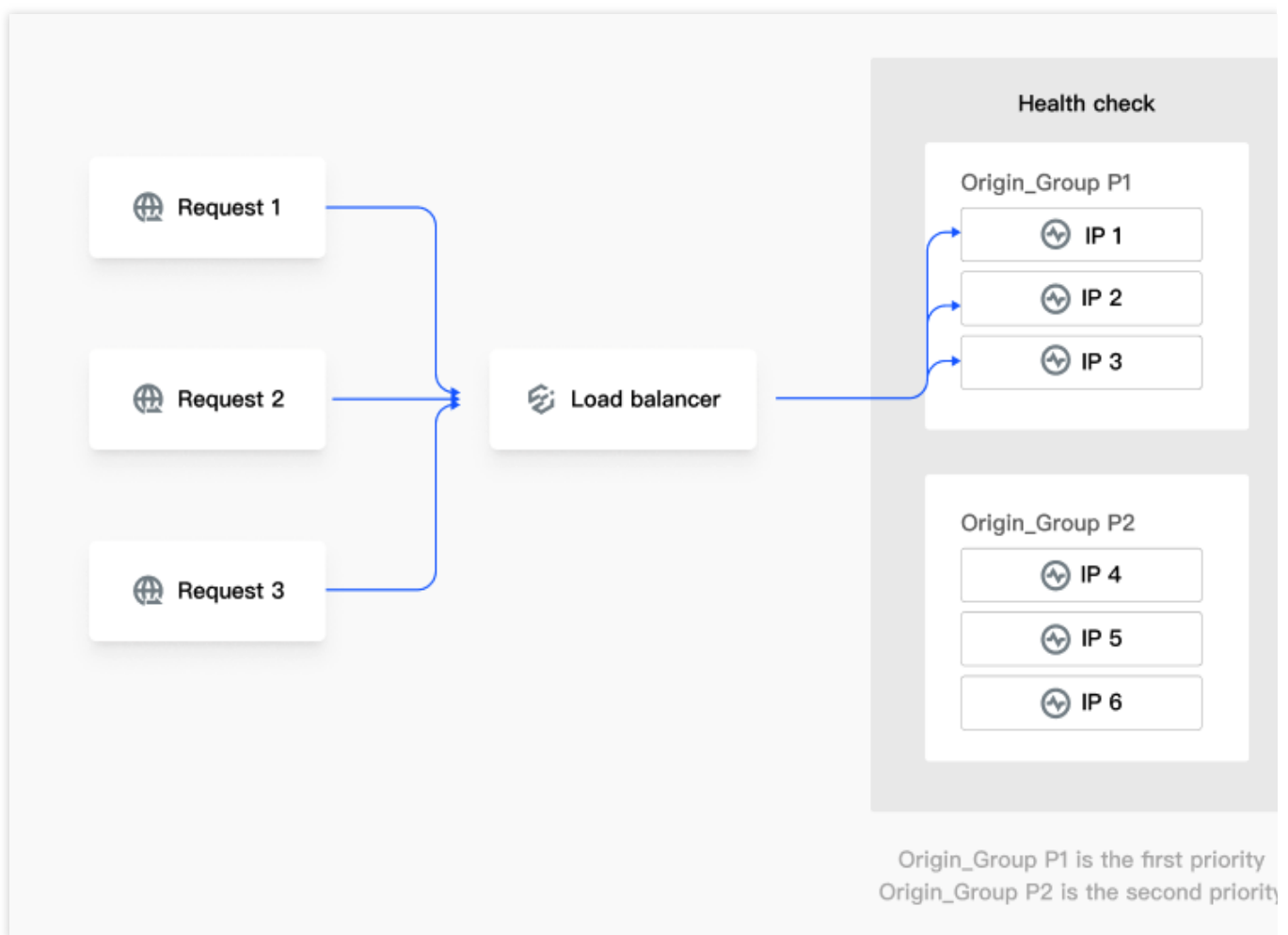
This document introduces the relevant concepts involved in Load Balancing.

### Note:

Tencent Cloud EdgeOne Load Balancing feature is in beta testing. If you want to use it, you can [Contact Us](#).

## Load Balancer

A load balancer is a virtual concept, comprising Origin groups and health check policies. Within a single load balancer, up to ten origin groups can be configured in priority order, accompanied by one health check policy. The load balancer intelligently directs business traffic based on probe results and the configured traffic scheduling policy.



## Origin Group

An origin group is the smallest unit of origin configuration within the Load Balancing. You can add one or more origins. When you add multiple Origin Servers, you can configure weights to adjust traffic load. For more details, see [Origin Group Configuration](#).

## Health Check Policy

The health check policy consists of probe methods and health assessment criteria. Currently, four probe methods are supported: ICMP Ping, HTTP/HTTPS, TCP, and UDP. For more details, see [Detailed Health Checks](#).

## Traffic Scheduling Policy

The traffic scheduling policy only takes effect when the health check policy is enabled. Currently, it supports a Failover-by-Priority-Order policy, that is, based on probe results, it disables failed origins and routes traffic to healthy ones according to the priority order of origin groups.

## Request Retry Policy

In the event of a request failure to a particular origin during normal business operations, the Load Balancing feature, guided by its request retry policy, can schedule the request to another origin for a retry. This helps reduce business request failures due to network issues or origin malfunctions. For more details, see the [Introduction to Request Retry Policy](#).

# Introduction to Request Retry Strategy

Last updated : 2025-03-04 15:35:20

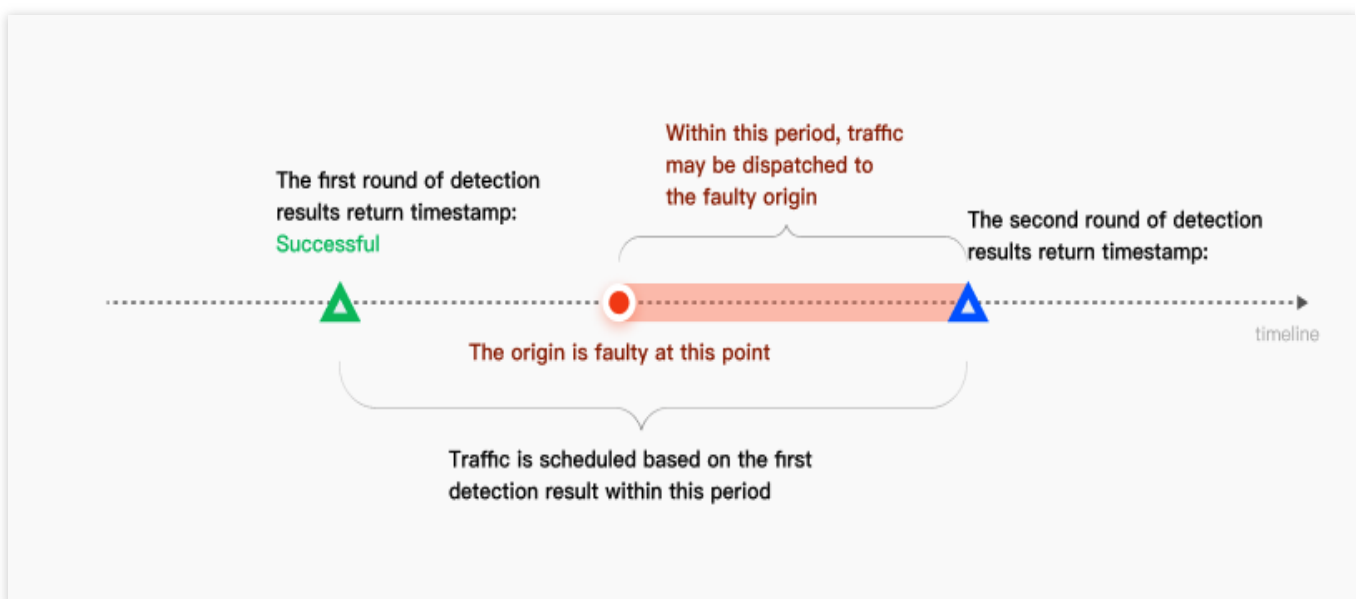
Load Balancing is capable of redirecting a request to an alternative origin for retrial when a request to an initially designated server fails, in accordance with the retry policy. This reduces business request failures caused by network issues or origin fails.

## Note:

EdgeOne Load Balancing feature is in beta testing. If you want to use it, you can [Contact Us](#).

Actual business requests may fail due to the following reasons:

**1. Origin Failure and Have Not Actively Probe to Disable:** After health check policies are configured, active probe is conducted periodically. Traffic is directed based on the results of the previous probe until new results are available. If an origin becomes unhealthy between two probes, business traffic might still be directed to the unhealthy origin. This leads to business request failure.



**2. Network Jitter:** The origin is healthy, but network issues occur during the access. This leads to business request failure.

## Note:

Request failures include origin connection establishment failures and origin response reception failures.

For the situations mentioned above, EdgeOne provides the following two fallback request retry policies:

**Policy 1:** When a real business request fails to access a certain origin, it directly retries with another origin within the next lower priority origin group. This is suitable for scenarios where the performance of both higher and lower priority origin groups is similar.

**Policy 2:** When a real business request fails to access a certain origin, it directly retries with another origin within the same priority origin group. This is suitable for scenarios where the performance of the higher priority origin group is

significantly better than that of the lower priority origin group.

**Note :**

POST requests do not support origin-pull retry.

# Origin Group Configuration

Last updated : 2025-01-15 09:54:54

## Overview

Manage business origins in the form of origin groups. The origin groups configured here can be used in functions such as [adding acceleration domain names](#) and [L4 proxy](#).

## Create Origin Group

1. Log in to [the EdgeOne console](#) and click Site List in the left sidebar. In the **site list**, click the target site to enter the site details page.
2. On the site details page, click **origin configuration > origin group**.
3. Click **Create origin group**.

4. Fill in the origin group name and select the origin type. The specific type descriptions are as follows:

**HTTP Dedicated:** Supports adding **IP/domain name origins** and **object storage origins**, and can only be used for site acceleration-related services (e.g., Domain Name Service and rule engine - Modify origin).

**Universal:** Only supports adding **IP/domain name** as origin, does not support adding **object storage origin**, and can be used for site acceleration services (such as Domain Name Service and rule engine) and L4 proxy.

### Note:

After the configuration is complete, the origin group type cannot be modified.

### Create origin group

Origin group name

1-200 characters ([a-z], [A-Z], [0-9], [-])

Origin group type

☒ HTTP-specific type ☐ General Type

HTTP-specific origin groups support "IP/Domain" and "Object Storage Bucket" as origin, but can only be referenced by the Layer 7 acceleration services (Domain Service and Rule Engine).

Origin server

Origin type	Origin address	Weight ①	Operation
<a href="#">+ Add origin</a>			

Host Header(optional)

Please enter origin Host Header.

If your origin-pull host is different from the accelerated domain name, you can use this feature to rewrite the host to the actual host.  
Note: If you configure the object storage origin, this configuration does not modify the host to ensure that the origin request will not fail.  
At the same time, the rule engine modification of the host-related operations has a higher priority.

Create

Cancel

5. Click the **Add Origin** button to configure the origin. The supported origin types are as follows, with up to 20 origins supported.

**Object storage origin:** Tencent Cloud COS or other object storage buckets compatible with [AWS S3](#).

**IP/domain name origin:** Supports IPv4 addresses, IPv6 addresses, and domain names as origins.

**Note :**

Explanation of weight-related configurations in the origin group:

1. If a weight is set for an origin in the origin group, all origins in the group must also set corresponding weights. Weights can be integers between 0 and 100. If you do not set a weight, all origins in the origin group should not set weights at the same time.

2. When using the combination of [Smart Acceleration](#) and origin server group weights, the following logic will apply:

Scenario	Activation Logic
Configure weights for multiple origin servers in the origin server group and enable Smart Acceleration	Prioritize selecting the origin server based on weight, then Smart Acceleration will optimize the return link.
Configure weights for multiple origin servers in the origin server group without enabling Smart Acceleration.	Origin-pull by weight ratio.
Do not configure weights for multiple origin servers in the origin server group, enable Smart Acceleration.	Origin-pull from the optimal origin server selected by Smart Acceleration.
Do not configure weights for multiple origin servers in the origin server group, do not enable Smart Acceleration.	Poll each origin server in the origin server group, proportional origin return.

**Create origin** ✕

Origin type

IP/Domain Origin ▼

Origin (IP/Domain name)

Please enter IPv4/IPv6/domain or

Weight (optional)

Any integer from 0-100 is supported.

Create

Cancel

6. Click **Create** to complete the origin group creation.

# Origin-pull configuration

## Origin-Pull Timeout

Last updated : 2025-01-15 10:46:06

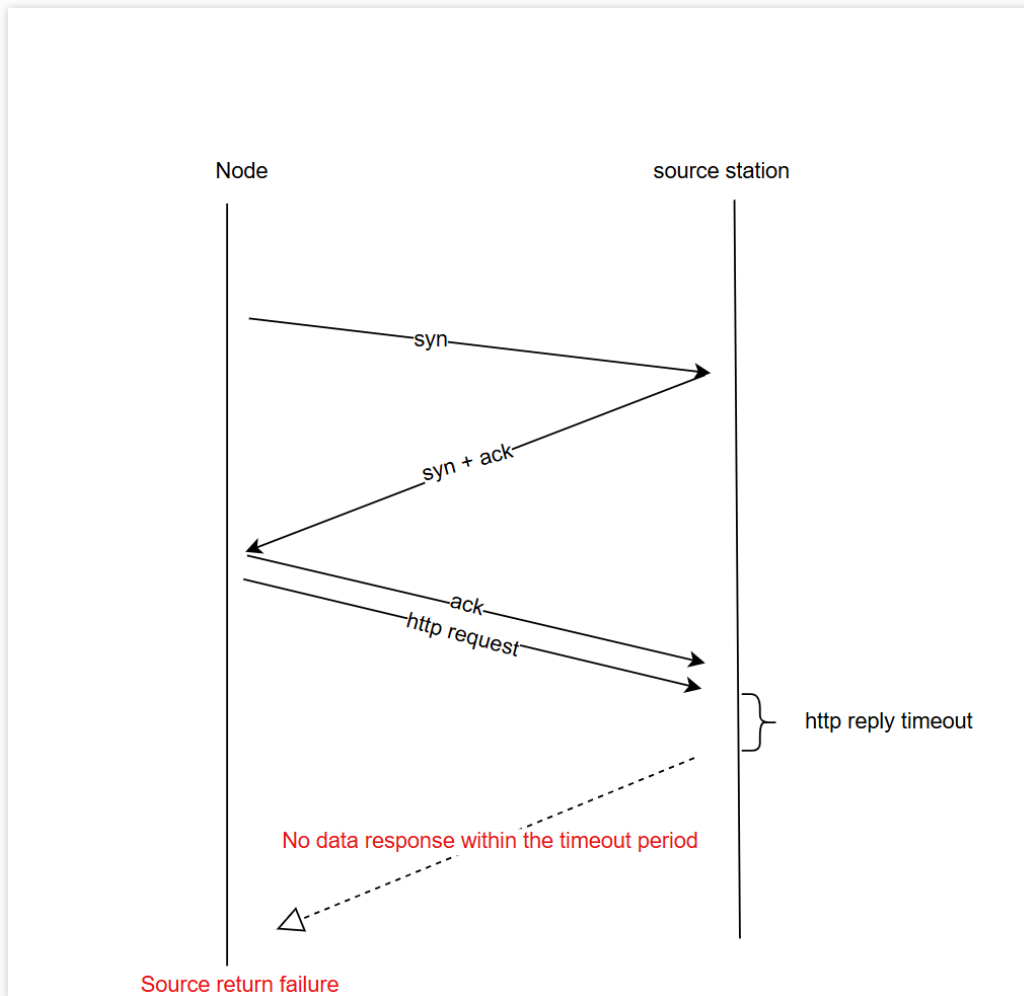
### Overview

The EdgeOne rule engine supports setting custom origin-pull timeouts. You can reasonably set the origin-pull request timeout based on the network link conditions and the data processing capability of the origin server, to ensure normal origin-pull for the request. The origin-pull timeout is defined as follows. If there is no data response from the origin server after a node initiates an origin-pull request, no matter how long the duration is, the node will consider it a timeout and actively disconnect from the origin server.

Currently, it supports configuring the HTTP response timeout (please stay tuned to the support for TCP connection timeout configuration, which is coming soon). The timeout can be set to an integer from 5 to 600, with a default value of 15. It means that after a node is connected to an origin server and initiates an HTTP request, if the origin server does not respond with any data within 15 seconds (including scenarios where there is no data response at all or partial data response is interrupted), the node will consider it an HTTP response timeout, and will respond to the client with a 524 status code.

#### **Note:**

This timeout does not apply to HTTP/2 origin-pull. In the HTTP/2 origin-pull scenario, if no frames are sent/received within 600s (adjustment not supported yet), the connection will timeout and disconnect, and the requests on the connection will also disconnect synchronously.



## Scenario: Configuring the HTTP Response Timeout to 60 Seconds

If the origin server for your business at the `www.example.com` domain name under the `example.com` site is heavily loaded and takes longer processing time, you should extend the timeout to 60 seconds, to avoid access failure due to active disconnection of the node after the default HTTP timeout of 15 seconds. You can refer to the following steps:

1. Log in to the [EdgeOne console](#), click **Site List** in the left sidebar, and then click the **site** you want to configure in the site list.
2. On the site details page, click **Site Acceleration** to enter the global configuration page. Then click the **Rule Engine** tab.
3. On the rule engine page, click **Create rule** and select **Add blank rule**.
4. On the rule editing page, select the matching type as **HOST** and set its value to equal `www.example.com`.
5. Click the **choice box** below **Action** and select the action as **Upstream Timeout** in the pop-up action list. Then configure the HTTP response timeout to 60 seconds.
6. The complete rule configuration is shown below. Click **Save and publish** to finish the rule configuration.

IF

+ Comment

Matching type ⓘ

Operator

Value

HOST

Is

+ And

+ Or

Action ⓘ

HTTP Response Timeout ⓘ

Upstream Timeout

−

60

+

seconds

+ Action

+ IF

# Configuring Origin-Pull HTTPS

Last updated : 2024-08-26 10:54:37

## Overview

You can specify the protocol that EdgeOne uses in the origin-pull request.

In scenarios that requires a high level of security, HTTPS can be used to access a website to ensure the security of website data. When HTTPS is specified as the origin-pull protocol, all origin-pull requests from EdgeOne to the origin use HTTPS, which prevents data tampering or theft during transmission.

In scenarios where fast response is required, HTTP can be used for origin-pull requests to speed up website access. When HTTP is specified as the origin-pull protocol, you can avoid complex SSL handshakes and other operations between EdgeOne and the origin, thus improving the website access speed. If your origin does not support HTTPS, please select HTTP.



1. An EdgeOne node initiates an origin-pull request by using the specified origin-pull protocol.
2. The origin responds to the request and establishes a connection by using the same protocol as the request.

### Note:

The configuration priority of the rule engine is superior. If the origin protocol rule is configured simultaneously within the domain name service and the rule engine, the final standard is determined by the rule engine.

## Scenario 1: Configuring origin-pull HTTPS for multiple domain names in batches in the rule engine

If you need to uniformly change the origin-pull protocol to origin-pull HTTPS for multiple domain names, such as `www.example.com` , `vod.example.com` and `image.example.com` , please refer to the following steps:

1. Log in to the [EdgeOne console](#) and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page, then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.

- On the rule editing page, enter the rule name and select Host matching type to match the request of the specified domain name. In the current scenario, select domain names `www.example.com` , `vod.example.com` and `image.example.com` .
- Click on **Action > Select Box**, select **Origin-pull HTTPS** from the dropdown action list that appears.

- Click on **Save and Publish** to finalize this rule configuration.

## Scenario 2: Configuring origin-pull HTTPS for the specified domain name

If you need to specify a domain name to modify the origin-pull protocol into origin-pull HTTPS, such as `www.example.com`, please follow these steps:

- Log in to the [EdgeOne console](#) and click **Site List** in the left sidebar. In the site list, click the target **Site**.
- Choose **Domain Name Service > Domain Name Management** on the **Site Details** page.
- Select the domain name that needs to be modified and click **Edit** on the **Domain Management** page.

<input type="checkbox"/> Domain name	Extended service	Origin type	Origin settings	Status	HTTPS certificate	Operation
<input type="checkbox"/> [Domain Name]	[Service]	Object storage ori...		<span>Activated</span>	Not configured <a href="#">Edit</a>	<a href="#">Edit</a> Switch to Only DNS <a href="#">Disable</a> Delete

- In the origin-pull protocol, select **HTTPS** and click **Complete** to finish the modification.

Edit domain name

Domain name

Origin type

☒ IP/Domain name

☐ Object storage origin

☐ Origin Group

Origin (IP/Domain name)

IPv6 access

☒ Follow site configuration: Disable

☐ Enable

☐ Disable

Origin Protocol

☒ Follow protocol

☐ HTTP

☐ HTTPS

Origin Port

HTTP

80

HTTPS

443

Origin configuration guide

Follow protocol

Client requests with HTTP or HTTPS protocol, EdgeOne follows the client's protocol to request the origin (the origin needs to support both port 80 and port 443, otherwise it may fail to request origin)

HTTP

Use HTTP protocol request the origin, the default port 80, support the configuration of custom ports.

HTTPS

HTTPS protocol request the origin, the default use of port 443, support the configuration of custom ports.

# Host Header Rewrite

Last updated : 2024-10-28 15:34:17

## Overview

Host header rewriting enables you to rewrite the host header as the actual origin domain name when the origin domain name is different from the acceleration domain name in the origin group list.

## Directions

1. Log in to [EdgeOne console](#) and click **Site List** in the left sidebar. In the site list, click the target **site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page. Then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.
4. On the rule editing page, set the matching type as HOST and configure it as the domain name to be modified, such as `www.example.com`.
5. Click **Action** > **choice box** and select the action as **Rewrite host header** in the dropdown action list. You can select the mode as **Custom** or **Follow origin domain**.

The screenshot displays the 'Rule Engine' configuration page. It features a table with two main sections: 'IF' (conditional) and 'Action'. The 'IF' section is currently empty, with a '+ Comment' button. The 'Action' section contains one rule configuration. The rule is defined by the following fields:

Matching type	Operator	Value
HOST	Is	

Below the 'IF' section, there are buttons for '+ And' and '+ Or'. The 'Action' section has a table with the following fields:

Action	Mode	Target value (supports variables)
Rewrite host header	Custom	www.example.com

At the bottom of the 'Action' section, there are buttons for '+ Action' and '+ IF'.

6. Click **Save and publish** to complete the rule configuration.

# Controlling Origin-pull Requests

Last updated : 2024-08-26 10:54:37

## Overview

By default, when origin-pulling, all query strings and Cookies within the request will be retained. If your business origin only allows specified query strings or Cookie information to be carried in the origin-pull request, you can ensure the normal origin-pull request by deleting the specified origin-pull request parameters.

## Directions

For example, Client requests Request URL: `http://www.example.com/path/demo.jpg?`

`key1=a&key2=b&key3=c&key4=d` , and only `key1=a` parameter needs to be retained when origin-pulling. You can follow the steps below to configure:

1. Log in to the [EdgeOne console](#) and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page, then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.
4. On the rule edit page, select the matching type as HOST equals `www.example.com`.
5. Click on the **action**, and in the pop-up operation list, select the operation as **origin-pull request parameter settings**.
6. Select the mode as retaining specified parameters, Enter the parameters `key1` and `key2` to be retained, up to 10 parameters are allowed.

The screenshot displays the configuration interface for a rule in the Tencent Cloud EdgeOne console. It is divided into two main sections: 'IF' (Condition) and 'Action'.

- IF Section:** Contains a matching rule with 'Matching type' set to 'HOST', 'Operator' set to 'Is', and 'Value' set to 'www.example.com'. Below this are buttons for '+ And' and '+ Or' to add more conditions.
- Action Section:** Contains the 'Origin-pull request parameter settings' action. It has three sub-sections: 'Type' (set to 'Query string'), 'Mode' (set to 'Reserve Specified Parameters'), and 'Parameter' (set to 'key1;key2'). There is a '+ Add' button below the parameter field.
- Bottom Navigation:** Includes buttons for '+ Action' and '+ IF' to add new actions or conditions.

7. Click **Save and Publish** to complete the rule Configuration.

# Redirect Following During Origin-Pull

Last updated : 2024-08-26 10:54:37

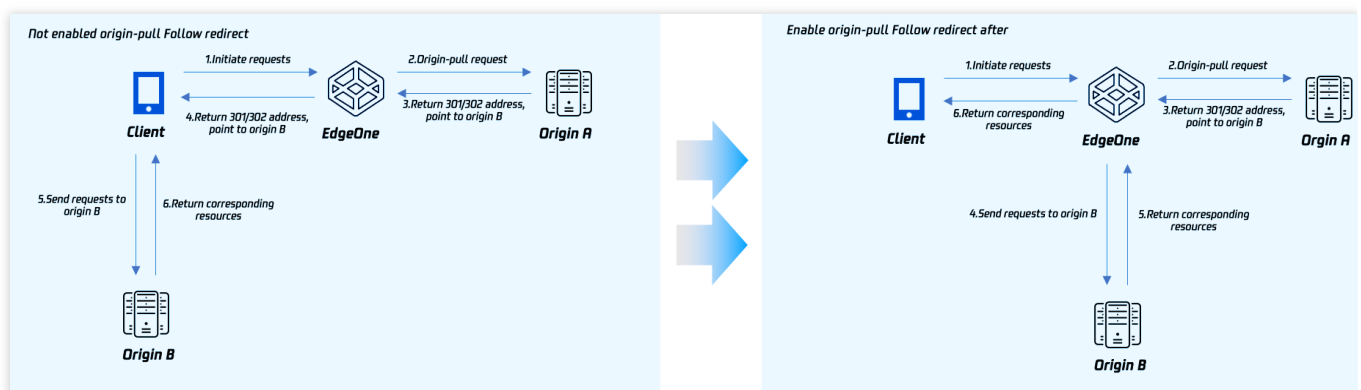
## Overview

Under normal circumstances, when the origin returns a 301/302 request, the node will return the status code to the client by default, and the client will redirect to the corresponding resources for access. EdgeOne supports follow origin redirects. When enabled, if the node receives a 301/302 status code during origin-pull, it will actively follow the redirect (not exceeding the set maximum redirects) to the specified address until the corresponding file is obtained, and then respond to the client with the actual resources, which can improve the user's access response speed.

For example: The client accesses the URL `https://a.example.com/test.jpg`, the origin A redirects the URL 302 to `https://b.example.com/test.jpg`, and the domain `a.example.com` has accessed the EdgeOne Service, while `b.example.com` has not yet accessed the acceleration service. Then:

**Without enabling origin-pull follow redirect:** After the client initiates the visit, if there is no cache in the EdgeOne node, it will visit the origin A and receive the 302 status code, and then respond to the client with the status code, and the client will directly request the origin B for the corresponding resources. At this time, since the origin B has not accessed the acceleration service, the client's self-initiated access speed is slower, and the obtained file cannot be cached. When other users access the same file, the process needs to be repeated.

**Enable origin-pull follow redirect:** After the client initiates the visit, if there is no cache in the EdgeOne node, it will visit the origin A and receive the 302 status code, and then, according to the status code and the corresponding address, directly request the origin B for the corresponding resources, and cache the resources in the node. This process is carried out by the EdgeOne node for origin-pull requests, the request speed is faster, and the obtained file can be cached in the node. When other users access the same file, there is no need to repeat the origin-pull, and the file can be directly hit and responded to the client.



## Directions

For example: If you need to enable origin-pull follow redirect for the specified domain `www.example.com` , with a maximum of 3 redirects. You can refer to the following steps:

1. Log in to the [EdgeOne console](#) and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page, then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.
4. On the rule editing page, select the matching type as HOST equals `www.example.com` .
5. Click on the **Action**, and in the pop-up operation list, select the operation as **follow origin redirect**.
6. Click on the switch, click on the switch to enable, and set the maximum redirects to 3 times. The related configuration instructions are as follows:

**Maximum redirects:** You can set it between 1-5 times. Within the maximum redirects, the node will follow the redirect address until the corresponding resources are obtained. If the maximum redirects are exceeded, the corresponding status code will be directly responded to the client.

The screenshot displays the 'Rule Engine' configuration page. It features two main sections: 'IF' (conditions) and 'Action'. The 'IF' section has a '+ Comment' button and a table with columns for 'Matching type', 'Operator', and 'Value'. The first row shows 'HOST' as the matching type, 'Is' as the operator, and 'www.example.com' as the value. Below this are '+ And' and '+ Or' buttons. The 'Action' section has a '+ Action' button and a table with columns for 'Action', 'On/Off', and 'Maximum redirects'. The first row shows 'Follow origin redirect' as the action, a toggle switch turned on, and '3' as the maximum redirects. There is also a '+ IF' button at the bottom left.

7. Click on **Save and Publish** to complete the rule configuration.

# HTTP/2 Origin-Pull

Last updated : 2024-08-26 16:03:35

## Overview

Support EdgeOne nodes to origin-pull using HTTP/2 protocol. HTTP/2 (i.e., HTTP 2.0, Hypertext Transfer Protocol version 2) is the second major version of the HTTP protocol, which can effectively reduce network latency and improve site page loading speed.

**Note :**

1. When enabled, the origin must support HTTP/2 protocol access.
2. If you need to configure HTTP/2 access, please refer to [HTTP/2](#).

## Use Limits

When HTTP/2 origin-pull is enabled and the origin-pull protocol is set to Follow Protocol, if a client sends an HTTP request, the EdgeOne node will perform origin-pull using H2C. However, if the origin server does not support H2C, the origin-pull will fail.

Therefore, if your current origin server does not support H2C and the origin-pull protocol is set to Follow Protocol, to reduce the risk of origin-pull failure, we recommend keeping HTTP/2 origin-pull disabled for the site/domain name. If your origin-pull protocol is HTTPS, it will not be affected.

**Note:**

H2C is an unencrypted version of HTTP/2, where C stands for clear text, namely plaintext. HTTP/2 is the second major version of the HTTP protocol, with significant performance improvements including multiplexing of requests and responses, reduced latency, optimized data flow, and header compression. However, the HTTP/2 protocol is typically used over secure HTTPS, requiring encryption by TLS (Transport Layer Security Protocol), while H2C allows the use of HTTP/2 without encryption, enabling performance benefits of HTTP/2 when encryption is not needed or cannot be used. Therefore, EdgeOne uses H2C for origin-pull when HTTP/2 origin-pull is enabled and HTTP is used for origin-pull.

## Directions

If you need to enable or disable HTTP/2 origin-pull for the specified domain `www.example.com`, you can follow the steps below:

1. Log in to the [EdgeOne console](#), click **Site List** in the left sidebar, and then click the **site** you want to configure in the site list.
2. On the site details page, click **Site Acceleration** to enter the global configuration page. Then click the **Rule Engine** tab.
3. On the rule engine page, click **Create rule** and select **Add blank rule**.
4. On the rule editing page, select the matching type as HOST equals `www.example.com`.
5. Click the **Action**, and in the pop-up operation list, select the operation as **HTTP/2 origin-pull**. Click the switch to enable/disable HTTP/2 origin-pull.

The screenshot displays the 'Rule Engine' configuration page. At the top, there is a tab labeled 'IF' with a '+ Comment' button. Below this, the configuration is divided into two main sections: 'Matching type' and 'Action'.

**Matching type section:**

- Matching type:** A dropdown menu showing 'HOST'.
- Operator:** A dropdown menu showing 'Is'.
- Value:** A text input field containing 'www.example.com'.

Below the matching type section, there are buttons for '+ And' and '+ Or'.

**Action section:**

- Action:** A dropdown menu showing 'HTTP/2 origin-pull'.
- On/Off:** A toggle switch that is currently turned on (blue).

At the bottom of the configuration area, there are buttons for '+ Action' and '+ IF'.

6. Click **Save and Publish** to complete the rule configuration.

# Range GETs

Last updated : 2024-08-26 15:57:58

## Overview

Range GETs can be enabled to reduce the consumption of large file origin-pulls and response time.

### Why can Range GETs improve the efficiency of large file delivery?

When caching large files, nodes will split them into smaller parts in order to improve cache efficiency. All parts cached expire at the same time and follow the node cache TTL configuration. Range requests are also supported. For example, if a client request carries the HTTP header `Range: bytes = 0-999`, only the first 1000 bytes of the file will be returned to the user.

If Range GETs is enabled: When parts of the file are requested and their caches expire, nodes only pull and cache the requested parts and return them to the user, so that origin-pull consumption and response time are greatly reduced.

If Range GETs is disabled, when the client requests only parts of a file, the node will pull only the requested parts according to the `Range` header in the client request, cache them, and return them to the client at the same time.

However, this may not be able to achieve the optimal performance. In large file scenarios, we recommend you enable Range GETs.

## Use Cases

You can use Range GETs to cache large static files in either of the following cases: The origin server supports Range requests, or you use a Tencent Cloud COS origin server and do not apply any data processing methods such as image processing.

## Notes

The origin server must support Range requests, or the origin-pull may fail.

The origin-pull may fail if Range GETs is enabled for small static files, or if you enable it while using a Tencent Cloud COS origin server and data processing methods such as image processing.

## Directions

For instance, you have a video service website that provides online video watching through

`video.example.com`. The videos are mainly long videos with large files. In order to reduce traffic consumption of large files and improve origin-pull speed, you need to support range requests and origin-pull. You can perform the following steps:

1. Log in to the [EdgeOne console](#) and click **Site List** in the left sidebar. In the site list, click the target **Site**.
2. On the site details page, click **Site Acceleration** to enter the global site configuration page, then click the **Rule Engine** tab.
3. On the rule engine management page, click **Create rule** and select **Add blank rule**.
4. On the rule editing page, select the Matching type as `HOST` equals `video.example.com`.
5. Click on **Action**, in the displayed operation list, choose the operation as **Range GETs**.
6. Click on **On/Off** to enable Range GETs.

The screenshot displays the 'Rule Engine' configuration page. It features two main sections: 'IF' (blue header) and 'Action' (green header). In the 'IF' section, 'Matching type' is set to 'HOST', 'Operator' is 'Is', and 'Value' is 'video.example.com'. Below this, there are '+ And' and '+ Or' options. In the 'Action' section, 'Range GETs' is selected, and the 'On/Off' toggle switch is turned on. At the bottom, there are '+ Action' and '+ IF' buttons.

7. Click on **Save and publish** to complete the configuration of this rule.

# Origin Protection

Last updated : 2025-06-27 14:20:57

This document introduces how to obtain and update EdgeOne's IP address range for configuration of origin server firewall rules, only allowing traffic to the origin server that transits through fixed IP addresses, implementing origin protection.

## Obtaining Origin IP Address Range

1. Log in to the [Tencent Cloud EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.
2. On the site details page, click **Security > Origin Protection**.
3. On the Origin Protection page, click **Use Now**, carefully read the [Origin Protection Enablement Conditions of Use](#), and click **Confirm to Enable** after confirming the content of the "Special Agreement" is acceptable.
4. Click **Enable** for origin protection status, select the site acceleration/Layer 4 proxy resource to be protected, and click **Submit**.
5. After successfully enabled, you can see the current origin-pull IP list used by these resources. Update it to your origin server firewall rules.

### Warning:

1. EdgeOne may update the origin IP range irregularly to enhance network stability and reliability, improve security, handle expansion needs, or respond to compliance requirements. EdgeOne will notify you 14 days, 7 days, 3 days, and 1 day before the change via Message Center, SMS, or email. To ensure you receive the change notification, please verify that you have selected EdgeOne product service notifications in the [Tencent Cloud Message Center Console](#) and configured the correct Message Recipient. For setup details, refer to [message subscription management](#).
2. Upon receiving Tencent's "Origin IP Address Range Change Notification", please complete the update operation for the origin IP address range by referring to [Update Origin IP Address Range](#) within **no more than 14 calendar days**. For example, if EO sends the "Origin IP Address Range Change Notification" at 12:00:00 (GMT+8) on January 1, 2025, you need to complete the update operation for the origin IP address range by 12:00:00 (GMT+8) on January 15, 2025.
3. If you fail to complete the above operations within the agreed time limit, Tencent is authorized to take actions including but not limited to [forcibly updating the origin-pull IP range to the latest version]. Please understand and recognize that any adverse consequences arising therefrom, such as [origin-pull failure] or [live business unavailability], will be borne by you. This situation is not covered under the service availability assurance of the [EdgeOne Service Level Agreement](#).

4. If you cannot complete the update in time, it is advisable to adopt the origin-pull mutual authentication solution to ensure your origin server security. If you need to use this solution, [contact us](#).

## Updating Origin IP Address Range

Upon receiving the notification about the origin IP range change, you need to refer to the following steps to view the updated origin IP and complete the update within 14 calendar days to prevent service disruption caused by origin-pull failure.

1. Log in to the [EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** in the Message Center/email that needs to be changed under **Website Security Acceleration**.
2. On the site details page, click **Security > Origin Protection**.
3. Click **Go to update**.
4. After updating the latest origin IP range to the origin server firewall, click **I have updated to the latest origin IP range**.
5. After confirming the update, the console shows "Origin IP ACL CIDs is the latest version" to indicate the update is complete.

## Special Note

If the origin-pull IP range change operation is not carried out within the agreed deadline, EdgeOne will forcibly update the origin-pull IP range to the latest version according to the [Origin Protection Enablement Conditions of Use](#). You will bear adverse consequences such as [origin-pull failure] and [live business unavailability] arising therefrom. This situation is not within the scope of service availability assurance in the [EdgeOne Service Level Agreement](#).

## Related References

# Id Version Origin Group Compatible Related Issues

Last updated : 2023-10-24 15:45:49

The origin group has carried out a product capability upgrade since October 24, 2023. After the upgrade, the old version of the origin group will be processed for compatibility in the following ways. At the same time, we also suggest you switch to the usage of the new version of the origin group.

## Origin type & Configuration method compatibility

The new version of the origin group will no longer distinguish between **self-owned origin**, **object storage origin**, and **Tencent Cloud COS type origin**. The original origin groups with origin type of **object storage and Tencent Cloud COS** will be automatically updated to the new version of dedicated **HTTP origin group**, and the original origin groups with **self-owned origin** type will be automatically updated to the **universal origin** group.

The origin group will no longer support the configuration of origin-pull by region/protocol. If you have previously configured related origin-pull rules by region/protocol, the rules will be migrated to the rule engine as shown below:

modify origin-http/https

IF

HOST is

IF


Request protocol is HTTP

Modify origin Origin type: Origin Group Origin Group: Origin Protocol: HTTP Port: 80



IF

Request protocol is HTTPS


Modify origin Origin type: Origin Group Origin Group: Origin Protocol: HTTPS HTTPS origin port: 443


modify origin-region 

IF


HOST is  


IF

Client geo location is **Asia** 

Modify origin **Origin type: Origin Group** **Origin Group:**  **Origin Protocol: Follow protocol** **Port: 80** **HTTPS origin port: 443**

IF

Client geo location is **Europe** 

Modify origin **Origin type: Origin Group** **Origin Group:**  **Origin Protocol: Follow protocol** **Port: 80** **HTTPS origin port: 443**

## Origin group port migration description

The new version of the origin group will no longer support port configuration. All port configurations will be migrated to the service configuration entry, such as L4 proxy or Domain Management.

1 Domain configuration

>

2 Recommended configuration(Optional)

>

3 Configure CNAME

Domain name

Origin type

☐ IP/Domain name
 ☐ Object storage origin
 ☒ Origin Group
 ☐ Load balancing

Origin Group

Select from existing origin groups

Origin Protocol

☒ Follow protocol
 ☐ HTTP
 ☐ HTTPS

Origin Port

HTTP

80

HTTPS

443

Domain Configuration

IP/Domain name

It can be an IPv4/IPv6 address or a domain name.

Object storage origin

The object storage source site of cloud storage service providers, currently supports storage buckets of Tencent Cloud COS and Amazon AWS Signature V4 protocols

Origin Group

Applicable to a single domain name back to the origin of multiple origin station, multiple domain names share the same origin station configuration.

Load balancing

Proactively detects the delay and health status of the origin, configures intelligent traffic scheduling policies, and provides safer and faster traffic distribution services.

Cancel

Next

Rule ID	Forward...	Forwarding port ⓘ	Origin type ⓘ	Origin address	Origin port ⓘ	Session persistence (seconds) ⓘ	Pass client IP ⓘ	Rule Tag ⓘ	Status	Operation
-	TCP ▾	100-110	Origin Gr ▾	test ▾	100-110	<input checked="" type="checkbox"/>	TOA ▾	optional	-	<div>Save</div> <div>Ca</div>

## Primary and Standby Origin Configuration Instructions

In the **Domain Management** and **Rule Engine - Modify Origin**, directly configuring primary and standby origins is no longer supported. Existing configurations will not be affected, but modifications are no longer supported. If you currently have a demand for primary and standby origin configurations, please [contact us](#) for support.