

# **Tencent Cloud EdgeOne**

## **Domain Service**

### **Product Documentation**



## Copyright Notice

©2013-2024 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 Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. 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

### Hosting DNS Records

- Modifying DNS Servers

- Configuring DNS Records

- Advanced DNS Configuration

### Domain Connection

- Adding A Domain Name for Acceleration

- Ownership Verification

- Modifying CNAME Records

### HTTPS Certificate

- Overview

- Deploying/Updating SSL Certificate for A Domain Name

- Configuring A Free Certificate for A Domain Name

### HTTPS Configuration

- Forced HTTPS Access

- Enabling HSTS

- SSL/TLS Security Configuration

- Configuring SSL/TLS Security

- TLS Versions and Cipher Suites

- Enabling OCSP Stapling

### Domain alias

- Overview

- Configuration Guide

- Batch Connecting SaaS Domain Names

- Configuring Alias Domain Names for Disaster Recovery

### Traffic Scheduling

- Traffic Scheduling Management

# Domain Service

## Hosting DNS Records

## Modifying DNS Servers

Last updated : 2023-08-10 14:32:31

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 ones displayed in the box below.

**To make your services activated, follow these steps below and modify NS records** [Refresh](#)

**i** To prevent interrupting the DNS resolution service during the process, go to **DNS Records** to import the records first.

**1** Current NS records:



**2** Go to your domain name provider and change the NS records to:



**3** Click "Complete" to activate the EdgeOne service after modification.

The effective time of the change depends on the domain name provider. We will notify you through email, SMS and Message Center w

Configuration guides for major domain registrars:

Tencent Cloud

Alibaba Cloud

Huawei Cloud

Godaddy

Google

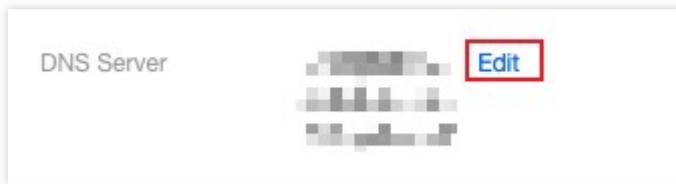
Name

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

Domain	Service Status	DNS Status	Registered	Expires	Auto-renewal
	Normal	DNSPod	2023-05-04	2024-05-04	Disabled <a href="#">Enable</a>

Total items: 1 20 / 1

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.

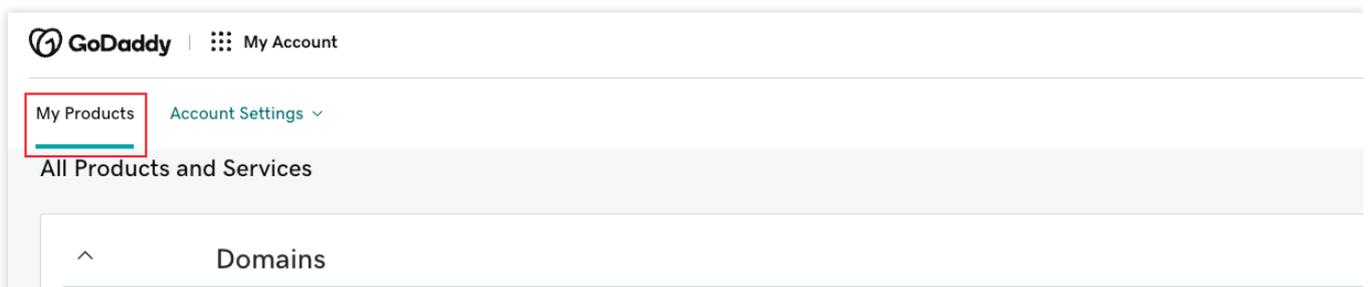
3. On the basic information page, click **Modify**.

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**.

<input checked="" type="checkbox"/>	Domain Name	Status	Expires On	Auto-renew	Estimated Value (USD)	D
<input type="checkbox"/>	<a href="#">[blurred domain name]</a>	Active	[blurred date]	On	Not available	N

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

## Additional Settings



### Don't risk losing your domain

Protect your domain against active threats like domain hijacking and prevent accidental domain loss due to an expired credit card and other billing failures.

Manage DNS

Transfer domain to another GoDaddy acc

Transfer domain away from GoDaddy

Delete domain

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

## Nameservers

Using default nameservers

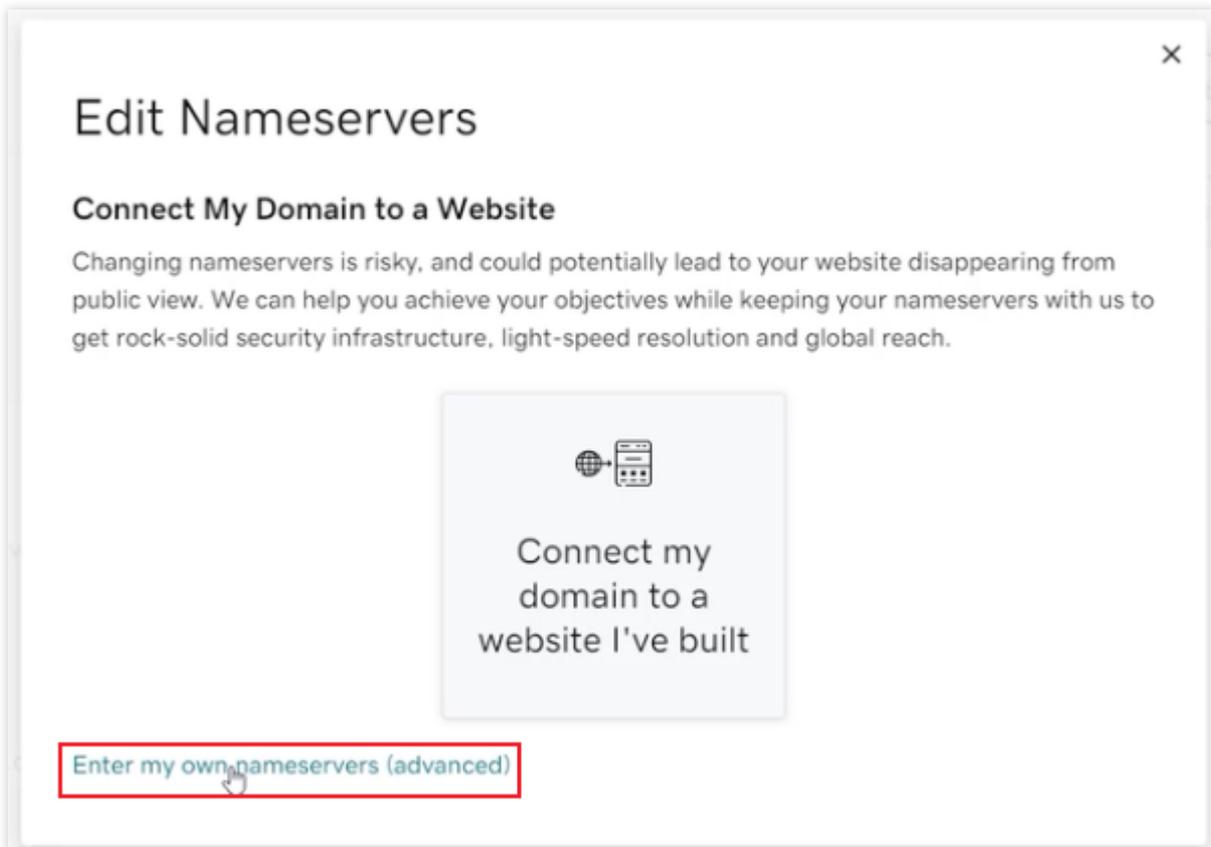
Change

Nameservers ?

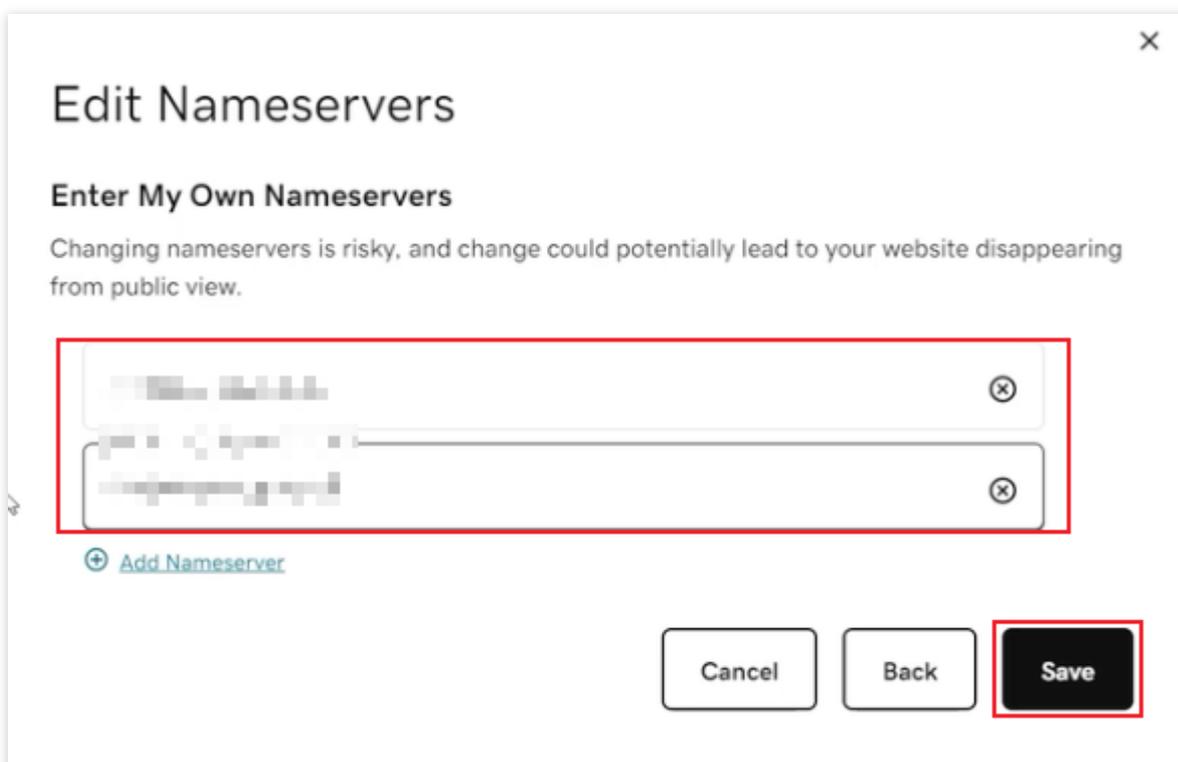
ns61.domaincontrol.com

ns62.domaincontrol.com

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 : 2023-12-26 18:20:47

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](#).

## Directions

### Scenario 1. 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**.

The screenshot shows the 'Add record' button highlighted in red. Below it, there are input fields for 'Record type' (set to 'A'), 'Host record', 'Record value', and 'TTL' (set to 'Automatic'). A blue informational banner provides details on record types:

Record Type	Description	Record Type	Description
A	Resolve host to an IPv4 address, such as 150.109.8.1	AAAA	Resolve host to an IPv6 address
CNAME	Resolve host to another domain name, such as www.example.com	TXT	Commonly used for domain verification
MX	Used for mail servers. Params are provided by the mail registrar. The default priority (5) can be modified.	NS	Designate other DNS services

Total items: 0

### Parameter description:

**Record type** and **Record value**: Different types of records have different purposes.

Record type	Example	Description
A	8.8.8.8	Point a domain name to an IPv4 address, such as 8.8.8.8.
AAAA	2400:cb00:2049:1::a29f:f9	Point a domain name to an IPv6 address.
CNAME	cname.edgeone.com	Point a domain name to another domain name from which the final IP address is resolved.
MX	10 mail.edgeone.com	In the first box, enter the priority of mail servers to receive mails. A smaller value indicates a higher priority. In the second box, enter the mail server, which is usually provided by the mail register.
TXT	ba21a62exxxxxxxxxxcf5f06e audio/video proxy	Identify and describe a domain name. It is usually used for domain name verification and as SPF records (for anti-spam).
NS	ns01.edgeone.com audio/video proxy	If you need to have another DNS provider to resolve the sub-domain, add the NS record. Note that you cannot add an NS record for a root domain name.
SRV	1 5 7001 srvhostname.example.com	Identify a service used by a server. It is commonly used in Microsoft directory management.
CAA	0 issue trustasia.com	Specify CAs that are allowed to issue certificates for a site.

Host record: Prefix of the sub-domain. For example, if the site is `example.com`, and you want to add the domain name `www.example.com`, you need to enter `www`.

TTL: It is the DNS record cache period. A shorter TTL indicates a higher record update frequency. However the DNS resolution speed can be slightly affected.

TTL options: Automatic, 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 200 minutes, 12 hours, and 1 day. If you select **Automatic**, the system will configure TTL to 5 seconds.

How to configure TTL:

If the record value does not change frequently, select 1 hour or longer to speed up DNS resolution.

If the record value changes frequently, select a shorter TTL value such as 1 minute, which, however, may slightly slow down DNS resolution.

**Note:**

1. If the domain name you are resolving needs to be accelerated, click **Enable Acceleration** in the operation column. Only A/AAAA/CNAME records are supported. For common conflicts, see [FAQs](#).

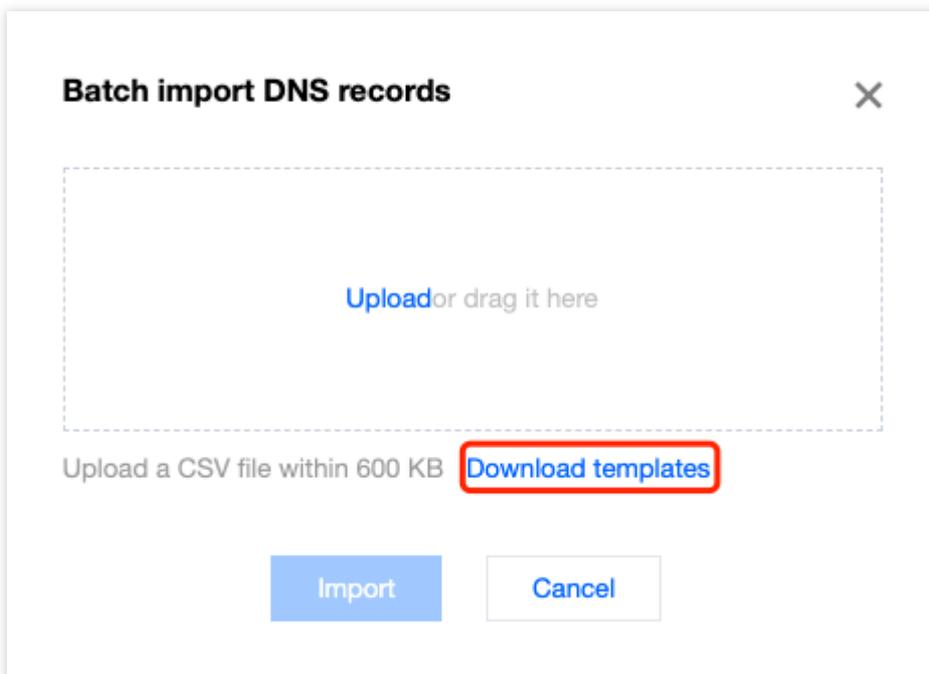
- When you enable acceleration for a domain name, it is moved to **Acceleration**. You can also check it in the **DNS records** page.
- If you want to configure multiple origins, or set a COS bucket as the origin, please see [Adding Acceleration Domain Name](#).

## Scenario 2: Batch Importing DNS Records

- Log in to the [EdgeOne](#) console. Click the target site in the site list to display second-level menus for site management.
- In the left sidebar, click **Domain Name Service > DNS Records**.
- On the DNS records page, click **Batch Import**.



- In the pop-up window that appears, click **Download template**.



- Enter the record type, host record, record value and TTL as instructed in the template. Save the .csv file.

	A	B	C	D
1	Record Type	Host Record	Record Value	TTL
2	A	www	1.2.3.4	Automatic
3	CNAME	ab	oring.com	Automatic
4	MX	mail	15 mailhost.example.com	1 minute

6. In the **Batch import DNS records** pop-up window, click **Upload** to select the .csv file above, or drag and drop it to the specified area. Click **Import**.

# 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.

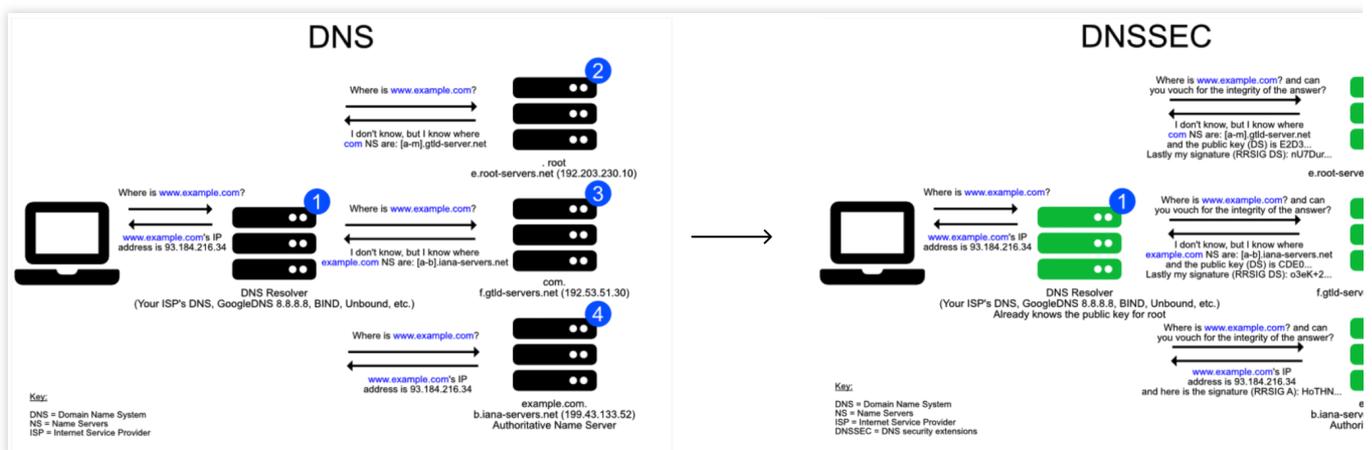
## DNSSEC

### 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.

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, click on



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

4. 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](#).

### DNSSEC

The authentication of the DNS data source provided by DNS to the client (local DNS) can effectively protect the authenticity and reliability of the resolution results. [Details](#)

**Add the following DS records at your domain name registrar:**

DS records		
Summary		
Summary type		
Algorithm		
Public key		
Key label		
Flag		

5. Next, you need to add a DS record at the Domain registration merchant based on the above information.
6. 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
<input type="checkbox"/> A	loopone	1.2.3.4	Automatic
<input type="checkbox"/> CNAME	looptwo	loopone.example.com	Automatic
<input type="checkbox"/> CNAME	looptthree	looptwo.example.com	Automatic

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.
```

# Domain Connection

## Adding A Domain Name for Acceleration

Last updated : 2024-04-01 10:04:18

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

### 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.

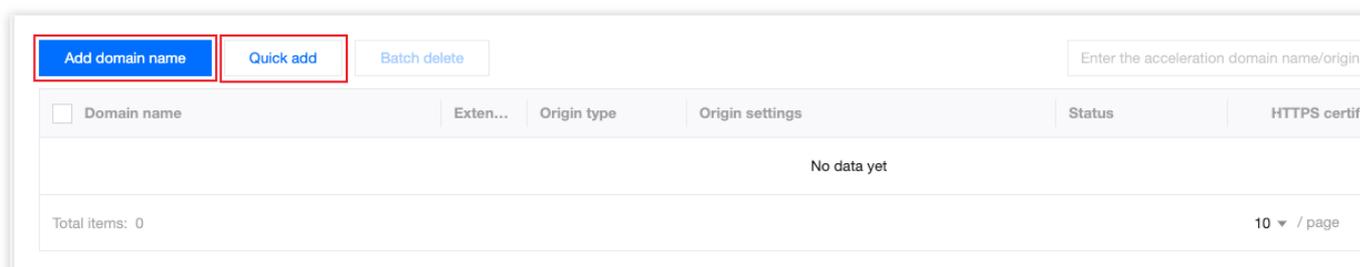
### Directions

The procedure for adding subdomain names varies based on the access mode you have selected.

NS Access

CNAME Access

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 > Acceleration** to go to the domain management page.
3. You can select **Add domain name** or **Quick add**.



Add domain name

Quick add

1. Click **Add domain name** to add an domain name for acceleration.

2. Specify the domain name to be connected to EdgeOne and specify the information of the corresponding origin. Then, click **Next**.

### Add domain name

1 **Domain configuration**
>
2 **Recommended configuration(Optional)**

Domain name

Origin type  IP/Domain name  Object storage origin  Origin Group  VOD on EO

Origin (IP/Domain name)

IPv6 access  Follow site configuration:  Disable  Enable  Disable

Origin Protocol  Follow protocol  HTTP  HTTPS

Origin Port HTTP  HTTPS

Cancel
Next

#### Domain Cor

**IP/Domain na**  
It can be an IP domain name.

**Object storag**  
The object stor storage service supports stora Cloud COS and V4 protocols

**Origin Group**  
Applicable to a back to the ori station, multipl the same origin

**VOD on EO**  
For the authori EO, the deliver all files in the a specified buck

Item	Description
Domain name for acceleration	The domain name accessible to the client. You can enter the value of the host record. EdgeOne supports connecting wildcard domain names. If you want to access the root domain, enter @ . For example, if the domain name is www.example.com , enter www .
Origin settings	Origin is the address of the resource that is accessed when the client initiates a request. Options: <b>IP/Domain name</b> , <b>Object storage origin</b> , and <b>Origin group</b> . <b>IP/Domain name</b> : Select this option to add a single IP address or domain name as the origin.

	<p><b>Object storage origin:</b> This is utilized for the addition of Tencent Cloud COS and buckets that have already activated private read-write permissions of buckets of S3 compatible type. If the bucket is public read-write. IP address/domain access can also be employed.</p> <p><b>Origin group:</b> Select this option to add multiple IP addresses as the origin. For example, you have built a cross-border e-commerce site based on CVM, and hosted it on a server whose IP address is <code>10.1.1.1</code>, you can select <b>IP/Domain name</b> and enter <code>10.1.1.1</code> in the <b>IP/Domain name</b> field.</p> <p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. It is suggested that your origin should be configured in the same region as the acceleration availability zone. For example, if the acceleration zone is the Chinese mainland availability zone, please configure the origin-pull to be domestic. If the origin is located in the Global availability zone (excluding Chinese mainland), cross-border access may exist during origin-pull, and we cannot ensure the origin-pull effect. If you need to accelerate the access of customers in the Chinese mainland, and the origin is in the Global availability zone (excluding Chinese mainland), you can refer to <a href="#">cross-region security acceleration (overseas site)</a>.</li> <li>2. If your acceleration zone is the Global availability zone, you can add corresponding rules in the rule engine, select Client geographic location as the matching condition, select Modify origin as the operation, and origin-pull to different origins based on different regions to ensure the origin-pull effect.</li> </ol>
IPv6 access	Select whether to enable support for access via IPv6. Refer to the document: <a href="#">IPv6 Access</a> .
Origin-pull protocol	<p>Choose the access protocol supported by your origin. Options include:</p> <p><b>Follow protocol:</b> The protocol used during origin-pull is identical to the user's access request protocol.</p> <p><b>HTTP:</b> The HTTP protocol is used for origin-pull.</p> <p><b>HTTPS:</b> The HTTPS protocol is used for origin-pull.</p>
Origin-pull port	Specify the port to be used during origin-pull. Please ensure that the designated port of your origin server is accessible.

3. (Optional) After you add the domain name, EdgeOne provides you with recommended configurations for different business scenarios to ensure that your business runs securely and smoothly. You can select a recommended configuration as needed, and the configuration is displayed in the **Rule Engine** module. Click **Complete** to deploy the configuration, or click **Skip**.

### Add domain name ✕

1 Domain configuration

2 Recommended configuration(Optional)

EdgeOne recommends enabling the following configurations based on different business scenarios to ensure the security and smooth operation of your business. Once these configurations are selected, a rule will be generated in the 'Rule Engine'. After adding the domain name, you can view it in the 'Rule Engine'. Alternatively, you can directly [Skip this step](#). After the domain name is added, go to the 'Rule Engine' to configure it manually.

**website acceleration** Details

It is suitable for e-commerce, websites, UGC communities and other business scenarios that mainly use small static resources (such as web page styles, pictures and small files).

**large file download** Details

Applicable to large files, such as game installation packages, application updates, application package downloads and other business scenarios.

**audio and video on demand** Details

Applicable to on-demand acceleration business scenarios of audio and video files such as online audio and video on demand.

**API acceleration** Paid Add-on Details

Applicable to scenarios where dynamic resources (API interfaces, etc.) are the mainstay, such as account login, order transactions, API calls, and real-time queries.

Enabling API acceleration will activate the smart acceleration feature in the rule engine, which will incur additional charges.

Price explanation:1 VAU/10K requests, 0.1USD/VAU, [VAU Fee](#)

**WordPress website development** Details

Suitable for business scenarios through developing websites with WordPress.

Back
Skip, no recommendation needed.
Complete

1. Click **Quick add** to add an domain name for acceleration.
2. Specify the domain name to be connected to EdgeOne and specify the information of the corresponding origin.

Add domain name
Quick add
Batch delete
Batch set CNAME

Enter the domain name/origin type/origin a

Domain name	Exten...	Origin type	Origin settings	Status	CNAME	HTTPS certificate	Ope
Enter the dor	[icon]	IP/Domain nar	Please enter the origin inform	-	-	-	Se

Enter the prefix of the domain name [Learn more](#)

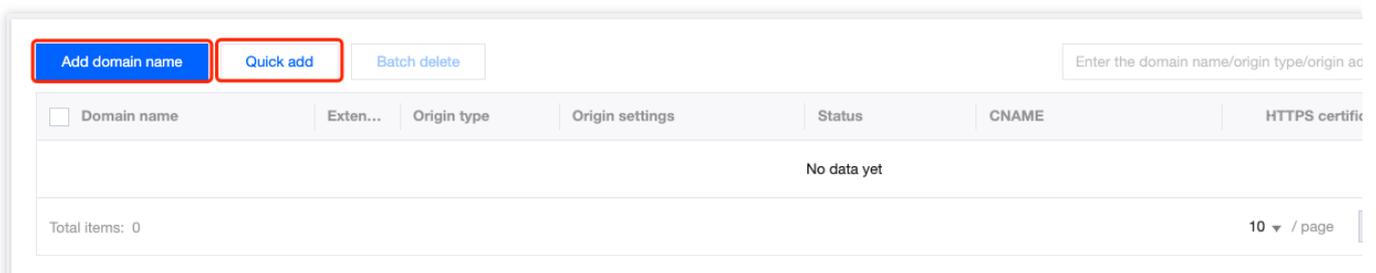
@ Connect the domain name  test Connect the subdomain name   
www Connect the subdomain  Connect the wildcard domain name

Item	Description
Domain name for acceleration	<p>The domain name accessible to the client. You can enter the value of the host record. EdgeOne supports connecting wildcard domain names. If you want to access the root domain, enter <code>@</code>.</p> <p>For example, if the domain name is <code>www.example.com</code>, enter <code>www</code>.</p>

Origin settings	<p>Origin is the address of the resource that is accessed when the client initiates a request. Options: <b>IP/Domain name</b>, <b>Object storage origin</b>, and <b>Origin group</b>.</p> <p><b>IP/Domain name:</b> Select this option to add a single IP address or domain name as the origin.</p> <p><b>Object storage origin:</b> Select this option to add a Tencent Cloud COS bucket or an AWS S3 bucket as the origin.</p> <p><b>Origin group:</b> Select this option to add multiple IP addresses as the origin. For example, you have built a cross-border e-commerce site based on CVM, and hosted it on a server whose IP address is <code>10.1.1.1</code>, you can select <b>IP/Domain name</b> and enter <code>10.1.1.1</code> in the <b>IP/Domain name</b> field.</p> <p><b>Note:</b></p> <ol style="list-style-type: none"> <li>It is suggested that your origin should be configured in the same region as the acceleration availability zone. For example, if the acceleration zone is the Chinese mainland availability zone, please configure the origin-pull to be domestic. If the origin is located in the Global availability zone (excluding Chinese mainland), cross-border access may exist during origin-pull, and we cannot ensure the origin-pull effect. If you need to accelerate the access of customers in the Chinese mainland, and the origin is in the Global availability zone (excluding Chinese mainland), you can refer to cross-region security acceleration (overseas site).</li> <li>If your acceleration zone is the Global availability zone, you can add corresponding rules in the rule engine, select Client geographic location as the matching condition, select Modify origin as the operation, and origin-pull to different origins based on different regions to ensure the origin-pull effect.</li> </ol>
-----------------	--

### 3. Click **Save**.

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 > Acceleration** to go to the domain management page.
3. You can select **Add domain name** or **Quick add**.



### Add domain name

#### Quick add

1. Click **Add domain name** to add an domain name for acceleration.

2. Specify the domain name to be connected to EdgeOne and specify the information of the corresponding origin. Then, click **Next**.

### Add domain name

1 **Domain configuration** > 
 2 **Recommended configuration(Optional)** > 
 3 **Configure CNAME**

Domain name

Origin type  IP/Domain name  Object storage origin  Origin Group  VOD on EO

Origin (IP/Domain name)

IPv6 access  Follow site configuration: Disable  Enable  Disable

Origin Protocol  Follow protocol  HTTP  HTTPS

Origin Port HTTP  HTTPS

**Domain Co**

**IP/Domain na**  
It can be an IP domain name.

**Object storag**  
The object sto storage servic supports stora Cloud COS ar V4 protocols

**Origin Group**  
Applicable to : back to the or station, multip the same origi

**VOD on EO**  
For the author EO, the delive all files in the : specified buck

Cancel
Next

Item	Description
Domain name for acceleration	The domain name accessible to the client. You can enter the value of the host record. EdgeOne supports connecting wildcard domain names. If you want to access the root domain, enter @ . For example, if the domain name is www.example.com , enter www .
Origin settings	Origin is the address of the resource that is accessed when the client initiates a request. Options: <b>IP/Domain name</b> , <b>Object storage origin</b> , and <b>Origin group</b> . <b>IP/Domain name</b> : Select this option to add a single IP address or domain name as the origin.

**Object storage origin:** Select this option to add a Tencent Cloud COS bucket or an AWS S3 bucket as the origin.

**Origin group:** Select this option to add multiple IP addresses as the origin.

For example, you have built a cross-border e-commerce site based on CVM, and hosted it on a server whose IP address is `10.1.1.1`, you can select **IP/Domain name** and enter `10.1.1.1` in the **IP/Domain name** field.

**Note:**

1. It is suggested that your origin should be configured in the same region as the acceleration availability zone. For example, if the acceleration zone is the Chinese mainland availability zone, please configure the origin-pull to be domestic. If the origin is located in the Global availability zone (excluding Chinese mainland), cross-border access may exist during origin-pull, and we cannot ensure the origin-pull effect. If you need to accelerate the access of customers in the Chinese mainland, and the origin is in the Global availability zone (excluding Chinese mainland), you can refer to [cross-region security acceleration \(overseas site\)](#).
2. If your acceleration zone is the Global availability zone, you can add corresponding rules in the rule engine, select Client geographic location as the matching condition, select Modify origin as the operation, and origin-pull to different origins based on different regions to ensure the origin-pull effect.

3. (Optional) After you add the domain name, EdgeOne provides you with recommended configurations for different business scenarios to ensure that your business runs securely and smoothly. You can select a recommended configuration as needed, and the configuration is displayed in the **Rule Engine** module. Click **Next** to deploy the configuration, or click **Skip**.

## Add domain name

- 1 Domain configuration > 2 Recommended configuration(Optional) > 3 Configure CNAME

EdgeOne recommends enabling the following configurations based on different business scenarios to ensure the security and smooth operation of your business. Once these configurations are selected, a rule will be generated in the 'Rule Engine'. After adding the domain name, you can view it in the 'Rule Engine'. Alternatively, you can directly [Skip this step](#). After the domain name is added, go to the 'Rule Engine' to configure it manually.

**website acceleration**[Details](#)

It is suitable for e-commerce, websites, UGC communities and other business scenarios that mainly use small static resources (such as web page styles, pictures and small files).

**large file download**[Detail](#)

Applicable to large files, such as game installation packages, application updates, application package downloads and other business scenarios.

**audio and video on demand**[Details](#)

Applicable to on-demand acceleration business scenarios of audio and video files such as online audio and video on demand.

**API acceleration** Paid Add-on[Detail](#)

Applicable to scenarios where dynamic resources (API interfaces, etc.) are the mainstay, such as account login, order transactions, API calls, and real-time queries.

Enabling API acceleration will activate the smart acceleration feature in the rule engine, which will incur additional charges.

Price explanation: 1 VAU/10K requests, 0.1USD/VAU, [VAU Fee](#)

**WordPress website development**[Details](#)

Suitable for business scenarios through developing websites with WordPress.

[Back](#)[Skip, no recommendation needed.](#)[Next](#)

4. You must complete the CNAME configuration to direct the DNS resolution of the domain name to EdgeOne and then enable domain acceleration. EdgeOne will assign a CNAME address to the domain name. Please visit the DNS provider and [configure CNAME records](#) for the domain name.

**Add domain name**

✓ Domain configuration > 
 ✓ Recommended configuration(Optional) > 
 3 Configure CNAME

Add these resolution records at your DNS service provider, so that access requests can be directed to the EdgeOne node for acc  
[Learn more](#)

*To modify the recommended configuration, click "Complete" and add the records after your modification.*

Host record [input field]

Record type **CNAME** [dropdown]

CNAME [input field]

**Complete**

5. Complete the CNAME configuration, and then click **OK**.

1. Click **Quick add** to add a domain name for acceleration.

2. Specify the domain name to be connected to EdgeOne and specify the information of the corresponding origin.

Add domain name Quick add Batch delete Batch set CNAME Batch configuration of certificates

Please enter accelerated domain name/c

Domain name	Extended service	Origin type	Origin settings	Status	CNAME	HTTPS cer
Enti ...		IP/Domain nar	Please enter the origin informatio	-	-	-

An origin address is used as the record value during origin-pull. Configure your origin based on the selected record type.

- IPv4** Point the origin to an IPv4 address, such as 150.109.8.1
- IPv6** Direct the origin to an IPv6 address (such as "2012:da00:e0a1::a38f:1")
- Domain name** Direct the origin server to another domain name, such as www.example.com

The host header defaults to the accelerated domain name. You can [rewrite the host header](#) at [Rule Engine](#).

Item	Description
Domain name for acceleration	The domain name accessible to the client. You can enter the value of the host record. EdgeOne supports connecting wildcard domain names. If you want to access the root domain, enter @ . For example, if the domain name is www.example.com , enter www .
Origin settings	Origin is the address of the resource that is accessed when the client initiates a request. Options: <b>IP/Domain name</b> , <b>Object storage origin</b> , and <b>Origin group</b> . <b>IP/Domain name</b> : Select this option to add a single IP address or domain name as the origin. <b>Object storage origin</b> : Select this option to add a Tencent Cloud COS bucket or an AWS S3 bucket as the origin.

**Origin group:** Select this option to add multiple IP addresses as the origin.

For example, you have built a cross-border e-commerce site based on CVM, and hosted it on a server whose IP address is `10.1.1.1`, you can select **IP/Domain name** and enter

`10.1.1.1` in the **IP/Domain name** field.

**Note:**

1. It is suggested that your origin should be configured in the same region as the acceleration availability zone. For example, if the acceleration zone is the Chinese mainland availability zone, please configure the origin-pull to be domestic. If the origin is located in the Global availability zone (excluding Chinese mainland), cross-border access may exist during origin-pull, and we cannot ensure the origin-pull effect. If you need to accelerate the access of customers in the Chinese mainland, and the origin is in the Global availability zone (excluding Chinese mainland), you can refer to [cross-region security acceleration \(overseas site\)](#).

2. If your acceleration zone is the Global availability zone, you can add corresponding rules in the rule engine, select Client geographic location as the matching condition, select Modify origin as the operation, and origin-pull to different origins based on different regions to ensure the origin-pull effect.

3. Click **Save**.

4. You must complete the CNAME configuration to direct the DNS resolution of the domain name to EdgeOne and then enable domain acceleration. EdgeOne will assign a CNAME address to the domain name. Please visit the DNS provider and [configure CNAME records](#) for the domain name.

加速域名	拓展服务	源站类型	源站配置	状态	CNAME	HTTPS 证书
<input type="checkbox"/>		IP/域名		<span style="border: 1px solid red; padding: 2px;">! 请配置 CNAME</span>		未配置 <a href="#">编辑</a>

## Verifying Domain Name Acceleration

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

NS Access

CNAME 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.

```
C:\Users\<blurred>>nslookup -qt=A <blurred>
Server: pr1-local-ns-server.shared
Address: 10.211.55.1

Non-authoritative answer:
Name: <blurred>
Addresses: 43.159.118.152
           43.159.119.156
```

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.

IP location query gives information about an IP: Whether it's on EdgeOne nodes, location and ISP.

IP  
43.159.118.152  
43.159.118.156

Enter IPv6 addresses, one per line. Max: 100 IPs.

**Search**

**Query results**

IP	EdgeOne IP	Location
43.159.118.152	Yes	United States California
43.159.118.156	Yes	United States California

Total items: 2

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.

```
Last login: Wed Feb 22 17:42:01 on ttys000
[tiaoshouzhou@bogon ~ % dig [redacted]

; <<>> DiG 9.10.6 <<>> [redacted]
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15282
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:

;; QUESTION SECTION:
; [redacted]                IN      A

;; ANSWER SECTION:
[redacted] 1      IN      A      43.132.70.128

;; Query time: 7 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Feb 22 18:00:37 CST 2023
;; MSG SIZE rcvd: 78
```

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.

IP

Enter IPv6 addresses, one per line. Max: 100 IPs.

**Search**

**Query results**

IP	EdgeOne IP	Location
43.132.70.128	Yes	Japan Tokyo

Total items: 1

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.

```
C:\Users\>nslookup -qt=cname www.example.com
Server: pr1-local-ns-server.shared
Address: 10.211.55.1

Non-authoritative answer:
                canonical name = www.example.com.edgeone.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 www.example.com
; <<>> DiG 9.10.6 <<>>
;; 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:
;www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 298 IN CNAME www.example.com.edgeone.com.
www.example.com. 298 IN CNAME www.example.com.edgeone.com.
www.example.com. 58 IN A 175.99.198.121
```

# Ownership Verification

Last updated : 2023-11-24 16:52:10

## 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` .

Siteverification: If you have permission to configure DNS root domain resolution or root name server, use this method to reduceoperating costs.

Once youownership of the site is verified by EdgeOne, you can directly add itssubdomain names

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

Domainverification: If your company is a multi-levelbusiness or provides domain operations and maintenance and you only havepermission to configure DNS resolution and the origin server for the subdomainnames, you can skip verification when connecting the site. However, all itssubdomain names need to be verified before being added.

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

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

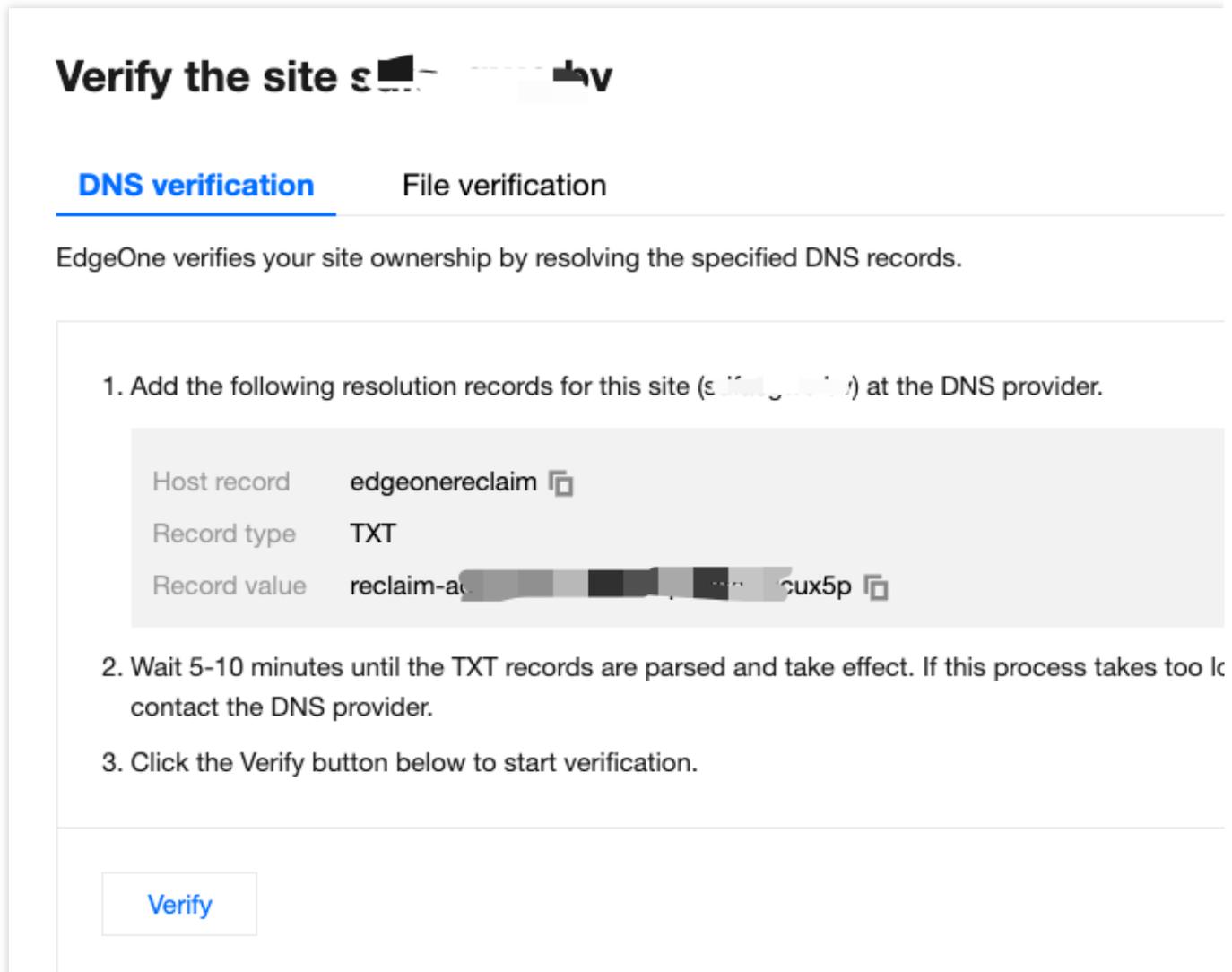
## Steps to Verify the Site or Domain Name Ownership

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.



The screenshot shows the 'Verify the site' interface. At the top, there are two tabs: 'DNS verification' (which is selected and underlined) and 'File verification'. Below the tabs, a text box states: 'EdgeOne verifies your site ownership by resolving the specified DNS records.' Underneath this, there is a numbered instruction: '1. Add the following resolution records for this site (example.com) at the DNS provider.' This instruction is followed by a table with three rows: 'Host record' with the value 'edgeonereclaim', 'Record type' with the value 'TXT', and 'Record value' with the value 'reclaim-abcdefghijklmnopqrstuvwxyz5p'. Below the table, there are two more numbered instructions: '2. Wait 5-10 minutes until the TXT records are parsed and take effect. If this process takes too long, contact the DNS provider.' and '3. Click the Verify button below to start verification.' At the bottom of the instruction area, there is a blue 'Verify' button.

## Verify the site

**DNS verification** File verification

EdgeOne verifies your site ownership by resolving the specified DNS records.

1. Add the following resolution records for this site (example.com) at the DNS provider.

Host record	edgeonereclaim
Record type	TXT
Record value	reclaim-abcdefghijklmnopqrstuvwxyz5p

2. Wait 5-10 minutes until the TXT records are parsed and take effect. If this process takes too long, contact the DNS provider.
3. Click the Verify button below to start verification.

[Verify](#)

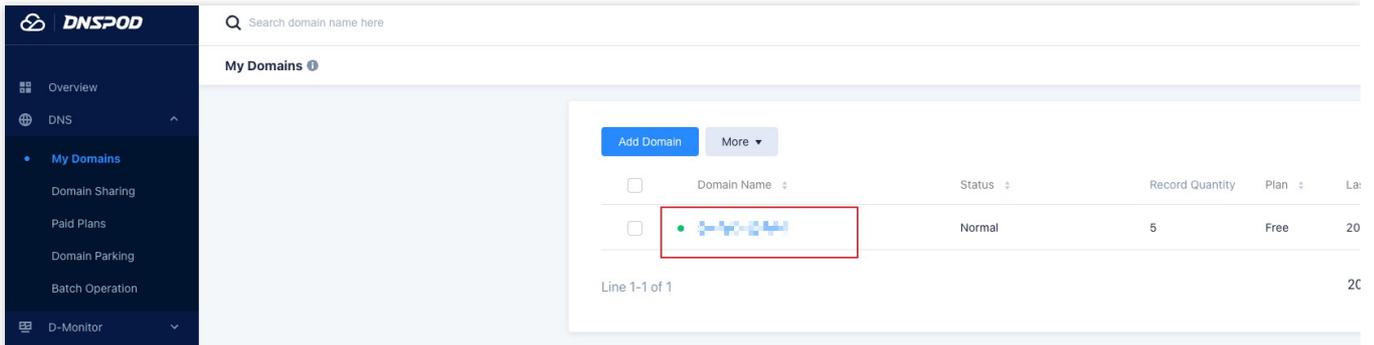
2. Log in to the console of the DNS service provider of the domain name and add a TXT record for the verification of the site ownership. The following examples describe how to add the TXT record in the console of different DNS service providers.

Tencent Cloud DNSPod

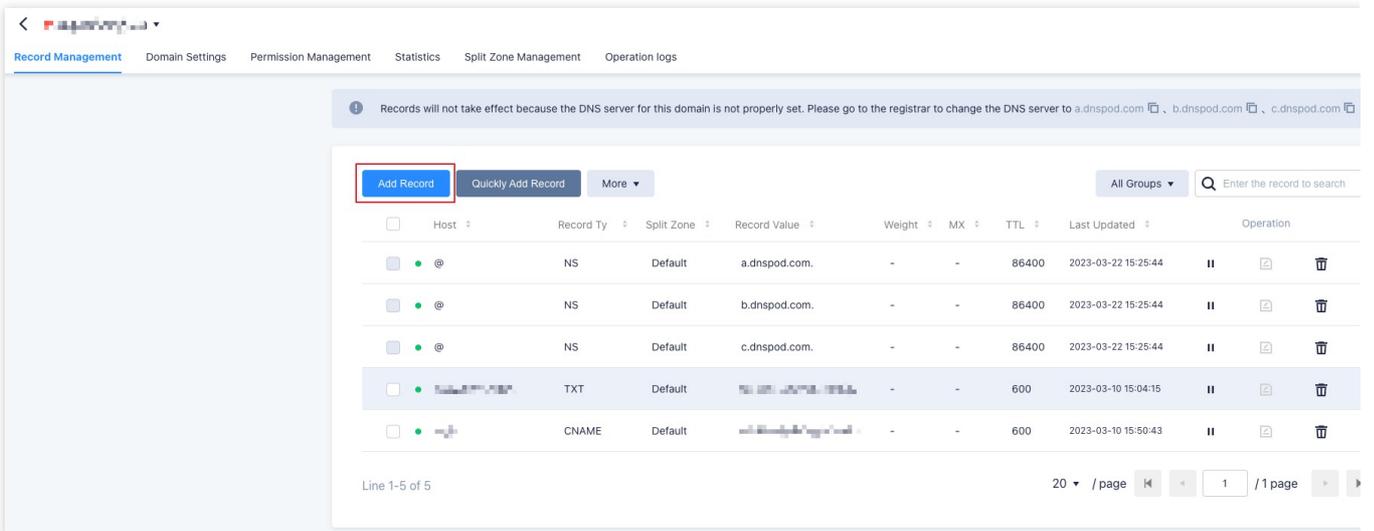
Alibaba Cloud DNS

Godaddy

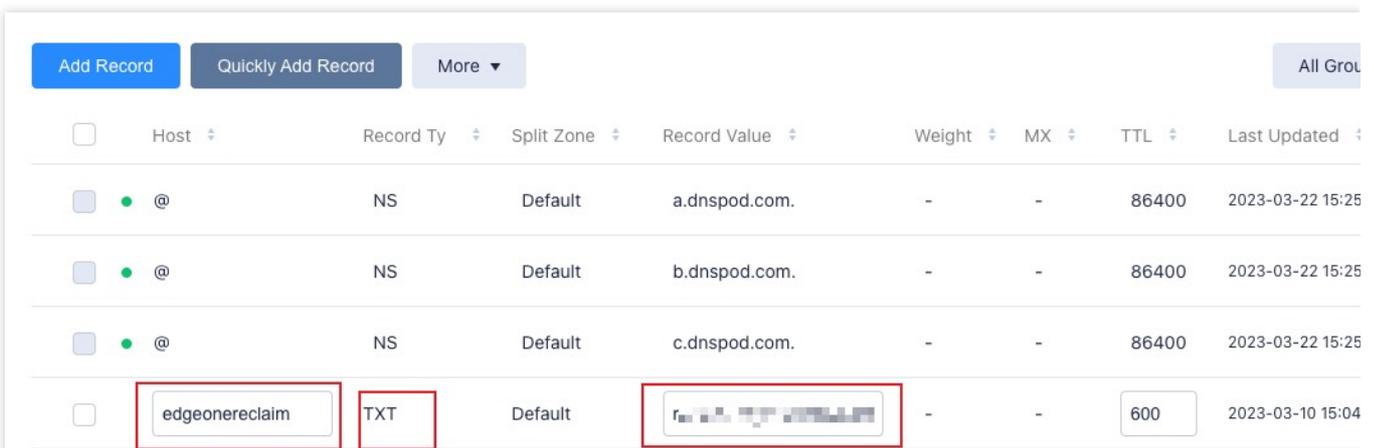
- a. Log in to the [DNSPod console](#) and click **My Domains** in the left sidebar. On the page that appears, click the target domain name to enter its configuration page.



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 .



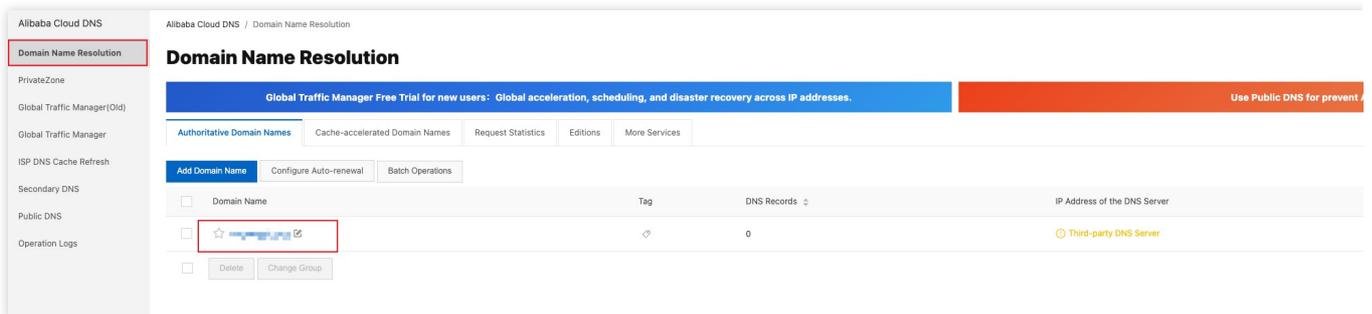
Parameter	Description
Record Type	TXT
Host	edgeonereclaim
Split Zone	Default

Text content	Enter the record value provided by EdgeOne
TTL	600

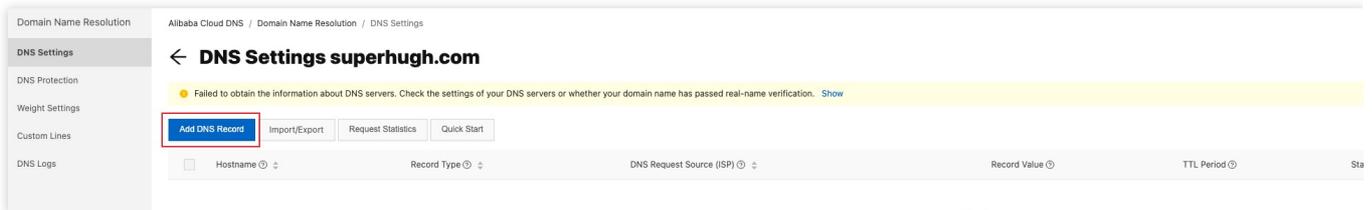
d. Click **OK**.

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.

### Add DNS Record

**Record Type** ?

TXT- Serves as an SPF record to protect against spam and can be up to 512 characters in length.

**Hostname** ?

Enter your domain name prefix

**DNS Request Source**

The region in which the domain name visitor is located and the carrier network that the domain name visitor uses.

Default - Required. If no DNS line is matched for intelligent DNS resolution, resolution results are returned bas...

**\* Record Value** ?

Enter a record value, which is generally a server IP address, a CDN domain name, or a mail server domain name

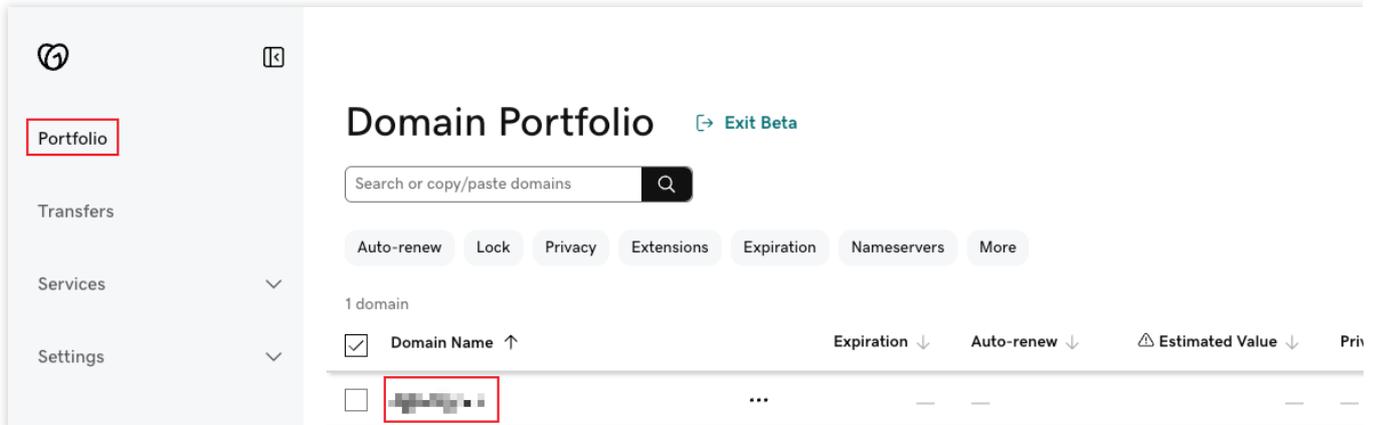
**\* TTL Period** ?

10 Minutes

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.

[TXT records](#) are used to verify domain ownership, SSL verification, and [email sender policies](#).

Type*	Name *	Value *
TXT	@ or email	String of characters

**Add record** **Clear**

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.

```
C:\Users\Administrator>nslookup -qt=txt edgeonereclaim.
Server: UnKnown
Address:

Non-authoritative answer:
edgeonereclaim          text =
"reclaim-006h5khbcwwkmpyk6od6nq73rj5bt0s"
```

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.

```
~ % dig txt edgeonereclaim.

; <<> DiG 9.10.6 <<> txt edgeonereclaim.
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 54753
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4096
;; QUESTION SECTION:
;edgeonereclaim.      IN      TXT

;; ANSWER SECTION:
edgeonereclaim.      600 IN    TXT    "reclaim-006h5khbcwwkmpyk6od6nq73rj5bt0s"

;; Query time: 92 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Apr 21 15:20:26 CST 2023
;; MSG SIZE rcvd: 109
```

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

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



Windows Linux

1. Create a verification directory (.well-known/teo-verification) under the root directory of the site [REDACTED]
2. Download [REDACTED] and upload it to the verification directory.
3. Make sure that you can access either of the following addresses:  
[http://\[REDACTED\]](http://[REDACTED])  
[https://\[REDACTED\]](https://[REDACTED])
4. Click the Verify button below to start verification.

Verify

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.

Windows Linux

1. Log in to the server of the site ([REDACTED], [REDACTED]), open a command prompt and get to the web server's root directory.
2. Run the shell command:

```
mkdir -p .well-known/teo-verification && echo [REDACTED] > .well-known/teo-verification/[REDACTED]
```
3. Make sure that you can access either of the following addresses:  
[http://\[REDACTED\]](http://[REDACTED])  
[https://\[REDACTED\]](https://[REDACTED])
4. Click the Verify button below to start verification.

Verify

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 : 2023-07-06 16:24:53

This document describes how to change the CNAME of a domain name.

## Note:

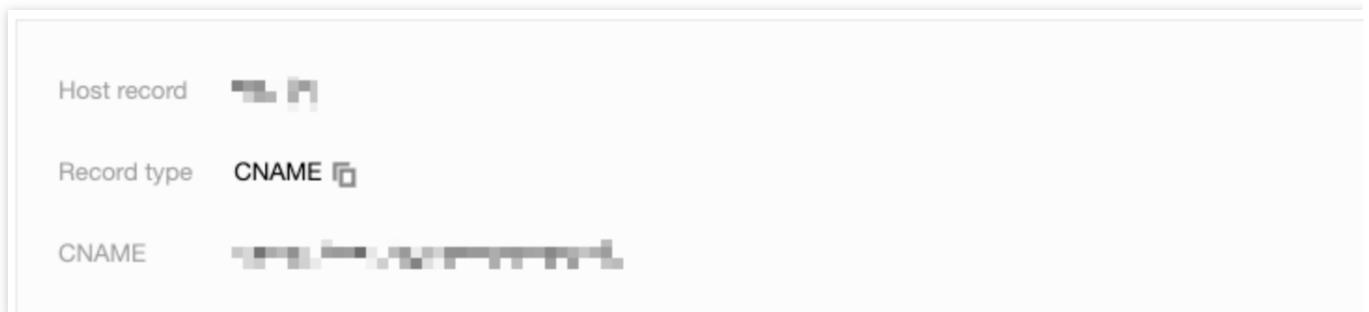
This is only required for sites connected via the CNAME. You don't need to do this for sites connected via the NS.

## Scenarios

In CNAME access mode, besides adding an acceleration domain name or alias domain, you also need to configure the CNAME record at your DNS service provider before you can direct user access to EdgeOne nodes and make the acceleration take effect.

## Directions

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



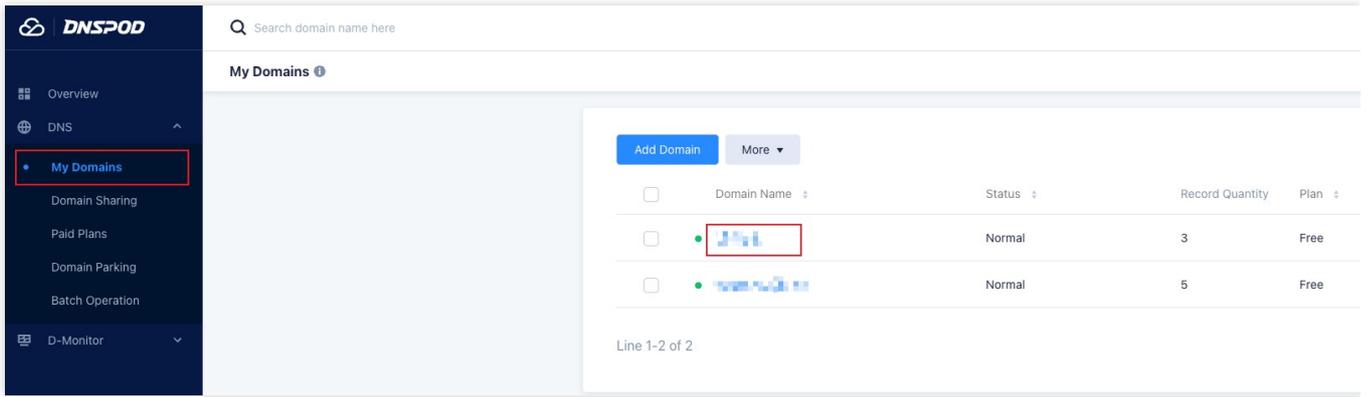
2. Go to the DNS service provider of the domain name and add a CNAME record. See below for examples for different DNS service providers.

Tencent Cloud DNSPod

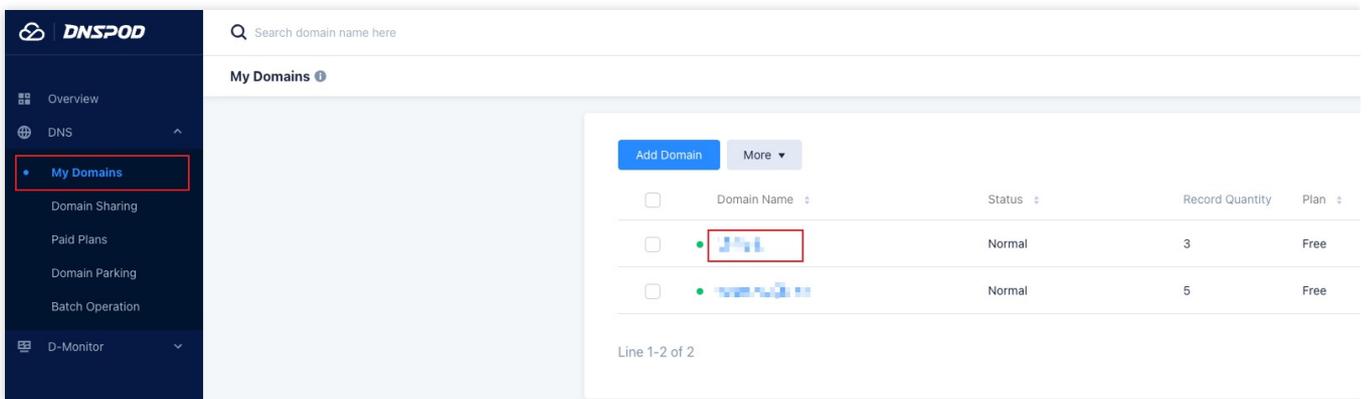
Alibaba Cloud DNS

Godaddy

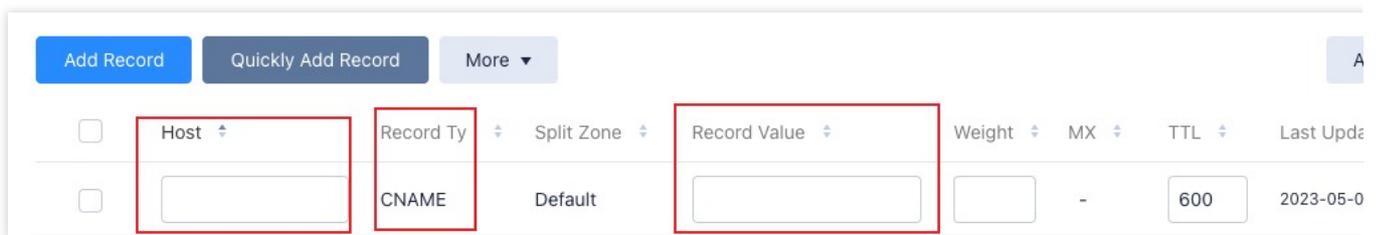
- a. Log in to the [DNSPod console](#). Find the domain to verify in **My Domains**. Click the domain to enter the domain name configuration page.



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.

The screenshot shows the Godaddy Domain Portfolio console. On the left is a navigation menu with 'Portfolio' highlighted in a red box. The main area is titled 'Domain Portfolio' with an 'Exit Beta' link. Below the title is a search bar and several filter buttons: 'Auto-renew', 'Lock', 'Privacy', 'Extensions', 'Expiration', 'Nameservers', and 'More'. A table below shows '1 domain' with columns for 'Domain Name', 'Expiration', 'Auto-renew', and 'Estimated'. The 'Domain Name' column has a red box around a blurred domain name.

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

The screenshot shows the GoDaddy DNS Management interface. At the top, there are navigation menus for 'Domains', 'Buy & Sell', 'DNS', 'Settings', and 'Help'. The main heading is 'DNS Management'. Below this, there is a 'DNSSEC' section with a purple banner containing an information icon and the text: 'This domain is registered elsewhere. To use these DNS records on your domain, set your domain to these nameservers at your registrar: ns59.domaincontrol.com, ns60.domaincontrol.com'. Underneath is the 'DNS Records' section with a brief explanation: 'DNS records define how your domain behaves, like showing your website content and delivering your email.' At the bottom of this section are 'Delete' and 'Copy' buttons.

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

The screenshot shows the 'Add Record' form. It includes a descriptive sentence: 'CNAME records are a type of subdomain, or alias, that points to another domain name.' The form has three main fields: 'Type' with a dropdown menu showing 'CNAME', 'Name' with the text 'blog or shop', and 'Value' with the text 'coolexample.com'. At the bottom left is an 'Add record' button, and at the bottom right is a 'Clear' link.

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"/>	[blurred]	 	IP/Domain name	[blurred]	<span style="border: 1px solid red; padding: 2px;">Activated</span>	[blurred]	Not config
--------------------------	-----------	---	----------------	-----------	---	-----------	------------

## 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"/>	[blurred]	 	IP/Domain name	[blurred]	<span style="border: 1px solid red; padding: 2px;">Activated</span>	[blurred]	Not co
--------------------------	-----------	---	----------------	-----------	---	-----------	--------

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\[blurred]>nslookup -qt=cname www.[blurred]
Server:  pr1-local-ns-server.shared
Address: 10.211.55.1

Non-authoritative answer:
[blurred] canonical name = [blurred]
```

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
; <<>> DiG 9.10.6 <<>>
;; 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 IN A

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

# HTTPS Certificate

## Overview

Last updated : 2023-10-11 11:06:23

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.

## Supported Certificate Types and Encryption Algorithms

Certificate type	Encryption algorithm
International standard certificates	RSA, ECC
Chinese SM standard certificates	SM2

## Differences Between Free and Paid Certificates

EdgeOne provides you with free and paid certificates.

If you want to configure a certificate for the domain of a SME site or personal blog to support access over HTTPS, please [configure a free certificate for the domain](#).

If you want to configure a certificate issued by an authority with higher credibility, or if you already have a self-owned certificate, please [configure a self-owned certificate for the domain](#).

# Deploying/Updating SSL Certificate for A Domain Name

Last updated : 2024-03-27 10:52:40

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.

### HTTPS certificate configuration

- To buy a certificate or upload your own certificate, go to [SSL console](#)
- At most one ECC certificate, one RSA certificate, and one SM2 certificate can be deployed to the same domain name.

Domain name

Certificate type  Off  Managed SSL certificate  Free certificate

Certificate ID/Re...	Bound domain	Certificate brand	Encryption algorithm	Expiration ti...
<input checked="" type="checkbox"/> ID: [redacted] Remarks: [redacted]	[redacted]	TrustAsia TLS RSA CA	RSA 2048	2024-08-10 07:5...
<input type="checkbox"/> ID: [redacted] Remarks: [redacted]	[redacted]	TrustAsia TLS RSA CA	RSA 2048	2023-08-03 07:5...

OK

Cancel

#### 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.

The screenshot shows the EdgeOne console interface. At the top, there are buttons for "Add domain name", "Quick add", "Batch delete", and "Batch set CNAME". Below is a table with columns: Domain name, Exten..., Origin type, Origin settings, Status, and CNAME. A single domain ".cn" is listed with a status of "Activated". A tooltip is displayed over the "Configured" status, showing the current HTTPS certificate details: Certificate ID (6n), Encryption algorithm (RSA 2048), and Expiration time (2024-03-23 07:59:59). The tooltip also includes a "Configured" status and an "Edit" link.

### 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.

### Batch configuration of certificates

1 **Configure certificate** > 2 **Domain configuration**

Please enter the certificate ID/domain keyword.

Certificate information ▾	Bound domain	Certificate brand	Encryption algorithm	Expiration time ↓	Bound domain
<input type="radio"/> ID: 8 [redacted] Remarks: 上传证书	[redacted]	MySSL.com	RSA 2048	2024-09-13 10:16:33	0
<input checked="" type="radio"/> ID: 7 [redacted]	[redacted]	TrustAsia TLS RSA CA	RSA 2048	2024-08-10 07:59:59	2
<input type="radio"/> ID: 5 [redacted]	[redacted]	TrustAsia TLS RSA CA	RSA 2048	2024-05-30 07:59:59	1
<input type="radio"/> ID: 5 [redacted]	[redacted]	TrustAsia TLS RSA CA	RSA 2048	2024-05-30 07:59:59	1
<input type="radio"/> ID: 5 [redacted]	[redacted]	TrustAsia TLS RSA CA	RSA 2048	2024-05-19 07:59:59	0
<input type="radio"/> ID: 3 [redacted]	[redacted]	TrustAsia TLS RSA CA	RSA 2048	2024-02-29 07:59:59	0
		TrustAsia TLS		2024-02-25	

Total items: 16
10 / page

⏪ ⏩ 1

Cancel
Next

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.

### Batch configuration of certificates

1 **Configure certificate** > 2 **Domain configuration**

Only display domain names that have not deployed this certificate.

choose Domain name, You can choose 100 at most

Search by domain name

<input checked="" type="checkbox"/> Domain name	Status	Is this certificate d...
<input checked="" type="checkbox"/> [redacted]	Activated	Yes
<input checked="" type="checkbox"/> [redacted]	Activated	Yes

Selected (2)

Domain name	Status
[redacted]	Activated
[redacted]	Activated

## 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 : 2024-04-16 16:54:34

## 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.

### Notes:

1. Free Certificates are issued by the [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 3 months. The platform will automatically apply for renewal 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. For domain names connected via the CNAME, you need to configure CNAME and wait till the CNAME takes effect.

## 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.

### HTTPS certificate configuration

- To buy a certificate or upload your own certificate, go to [SSL console](#)
- One domain name can have two different certificates: ECC and RSA.

Domain name

Certificate type  Off  Managed SSL certificate  Free certificate

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.

<input type="checkbox"/> Domain name	Exten...	Origin type	Origin settings	Status	CNAME
<input type="checkbox"/> [blurred]		IP/Domain name	[blurred]	Activated	[blurred]
<input type="checkbox"/> [blurred]		IP/Domain name	[blurred]	Activated	[blurred] e4....

Total items: 2

Current HTTPS certificate  
 Encryption algorithm  
 Expiration time  
 Auto-renewal

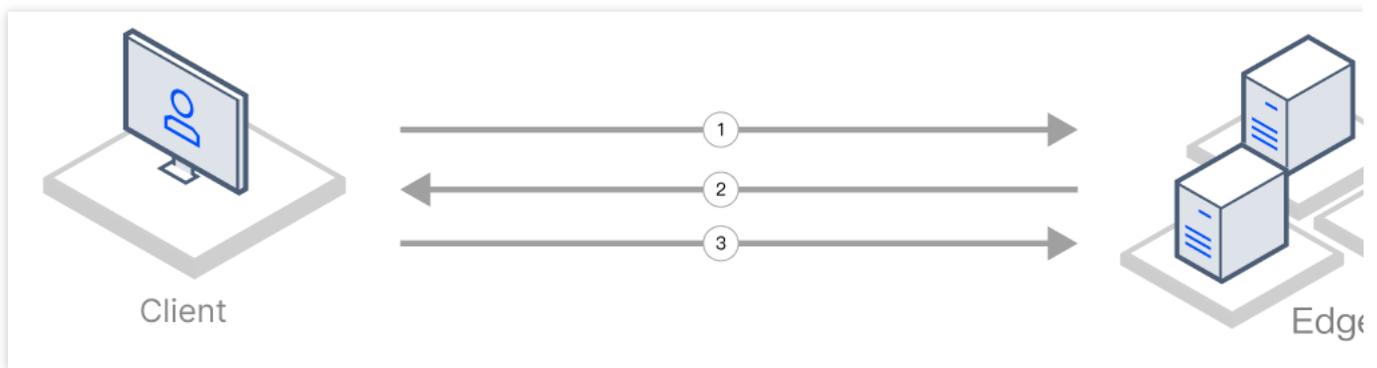
# HTTPS Configuration

## Forced HTTPS Access

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

### 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.

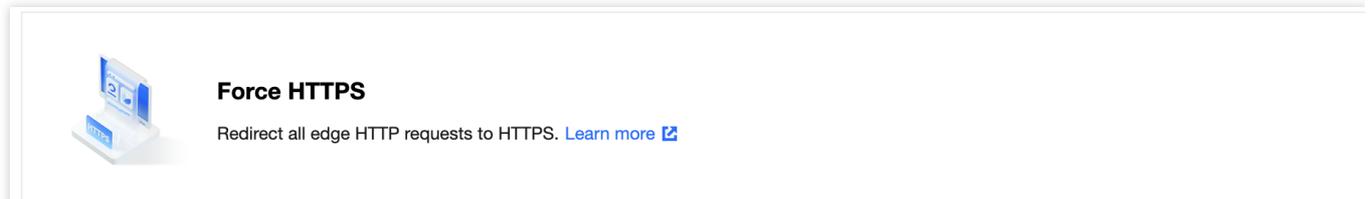
### Prerequisites

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, choose **Site Acceleration > HTTPS** to go to the HTTPS page.

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 **Rule Engine**.
3. On the rule engine management page, click **Create 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 **Operation** drop-down list, select **Forced HTTPS**. Then, select a redirect method.

**IF** [+ Comment](#)

Matching type ⓘ	Operator	Value
HOST ▾	Equal to ▾	

[+ And](#) [+ Or](#)

Action ⓘ	Redirect mode	On/Off
Force HTTPS	301 ▾	<input checked="" type="checkbox"/>

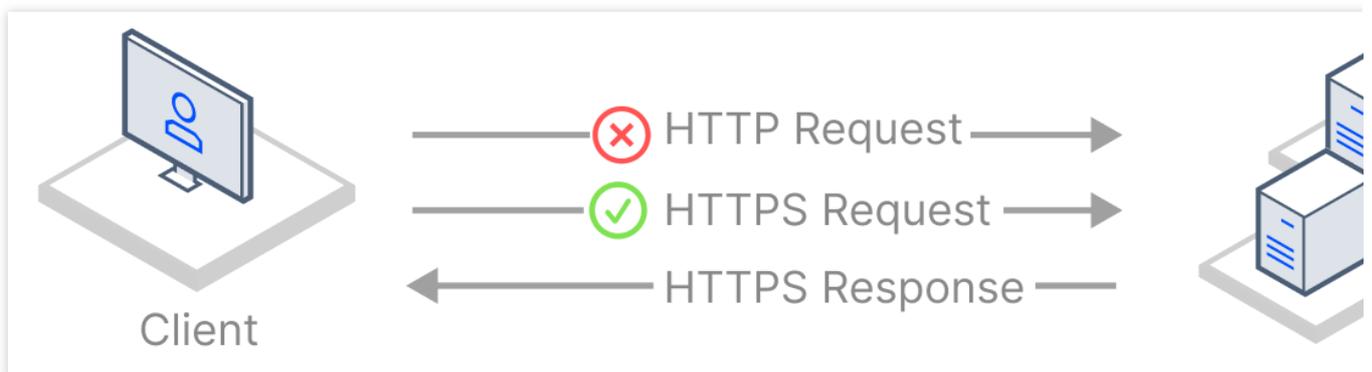
6. Click **Save and publish**.

# Enabling HSTS

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

## 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, choose **Site Acceleration** > **HTTPS** to go to the HTTPS page.
3. On the HSTS configuration card, toggle on the **Site-wide setting** switch to configure HSTS.



### HTTP Strict Transport Security (HSTS)

Force clients (such as browser) to use HTTPS to create links with edge nodes, encrypting websites globally. [Learn more](#)

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

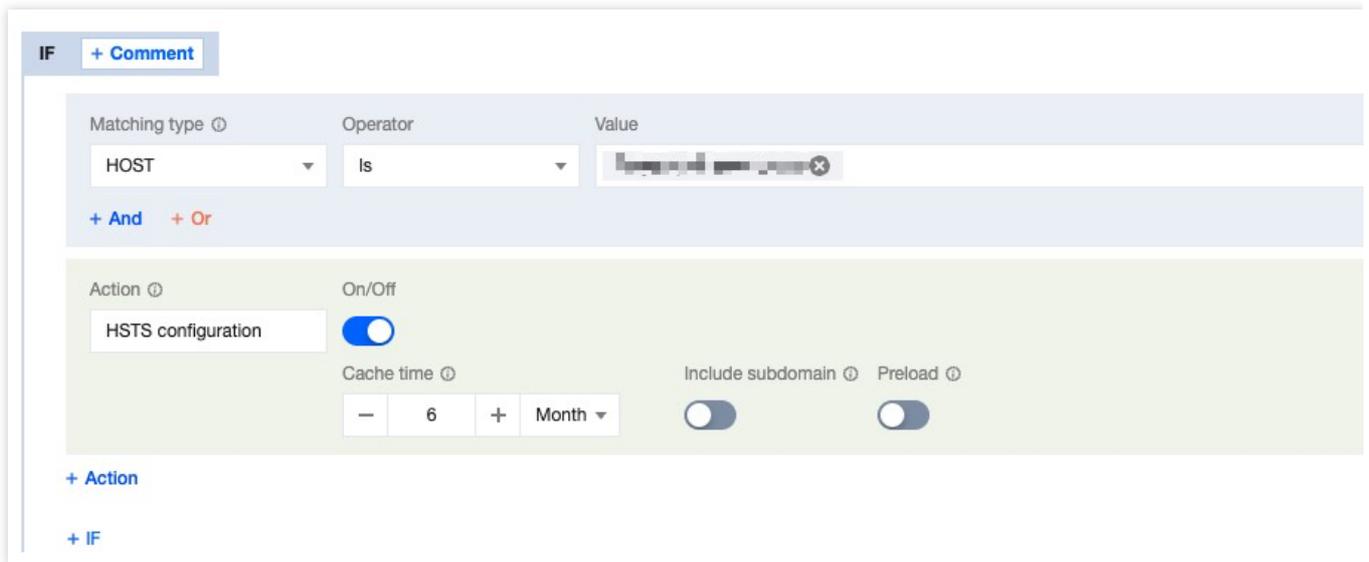
To enable HSTS for specified domain names or differentiate the HSTS configuration for different domain names, refer to the following information.

## 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 **Rule Engine**.
3. On the rule engine management page, click **Create 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 **Operation** drop-down list, select **HSTS**. Then, configure the settings that appear.



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-time&gt;</code>	The validity period of the HSTS header, measured in seconds. Within this 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. 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 : 2023-11-23 20:38:56

### 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

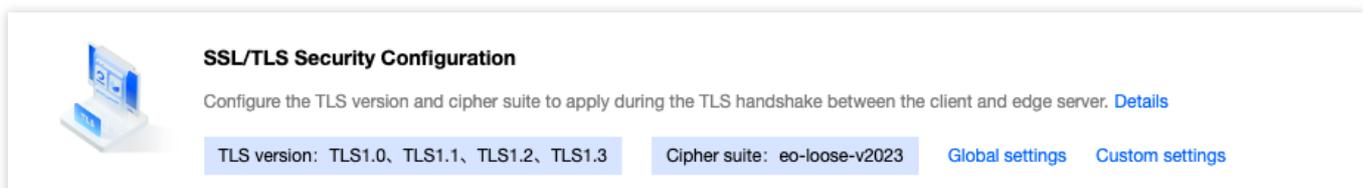
To configure required SSL/TLS versions for all domain names used to access a site, refer to the following information.

### 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, choose **Site Acceleration > HTTPS** to go to the HTTPS page.
3. On the **SSL/TLS Security Configuration** card, click **Global settings** to modify the configuration.



**SSL/TLS Security Configuration**

Configure the TLS version and cipher suite to apply during the TLS handshake between the client and edge server. [Details](#)

TLS version: TLS1.0, TLS1.1, TLS1.2, TLS1.3      Cipher suite: eo-loose-v2023      [Global settings](#)      [Custom settings](#)

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 **Rule Engine**.
3. On the rule engine management page, click **Create 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 **Operation** drop-down list, select **SSL/TLS security configuration**. Then, select TLS versions as needed.

The screenshot shows a configuration interface for a rule. At the top left, there is a tab labeled 'IF' with a '+ Comment' button. Below this, there are two main sections. The first section is for matching conditions, with columns for 'Matching type', 'Operator', and 'Value'. 'Matching type' is set to 'HOST', 'Operator' is 'Equal to', and 'Value' is an empty text box. Below this section are '+ And' and '+ Or' buttons. The second section is for the action, with columns for 'Action', 'TLS version', and 'Cipher suite'. 'Action' is 'SSL/TLS Security Con...', 'TLS version' has radio buttons for 'TLS1.0', 'TLS1.1', 'TLS1.2', and 'TLS1.3', with 'TLS1.2' and 'TLS1.3' selected, and 'Cipher suite' is 'eo-strict-v2023'.

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

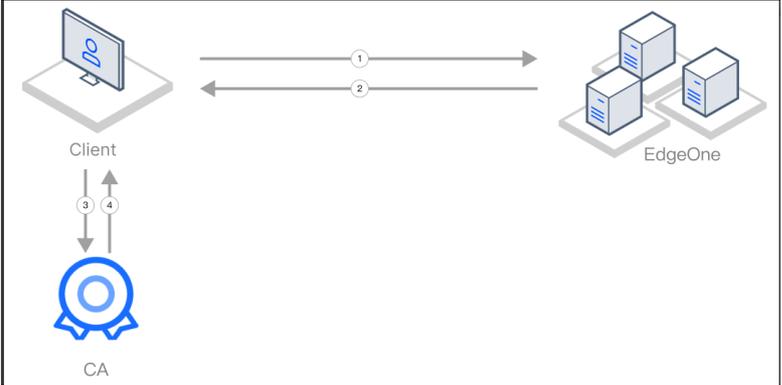
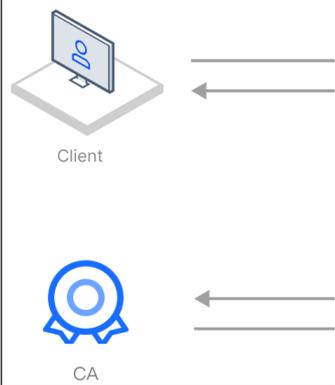
Last updated : 2023-05-08 10:00:27

## 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
	
<ol style="list-style-type: none"> <li>1. The client initiates a TLS handshake.</li> <li>2. EdgeOne responds to the TLS handshake (by returning the certificate).</li> <li>3. The client initiates an OCSP query.</li> <li>4. The CA returns the result.</li> </ol>	<ol style="list-style-type: none"> <li>1. The client initiates a TLS handshake.</li> <li>2. EdgeOne initiates an OCSP query.</li> <li>3. The CA returns the result, and EdgeOne caches it.</li> <li>4. EdgeOne responds to the TLS handshake (by returning the certificate and OCSP information).</li> </ol> <p>Because OCSP information is cached on EdgeOne servers, the client does not need to query the CA to respond to subsequent query requests.</p>

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

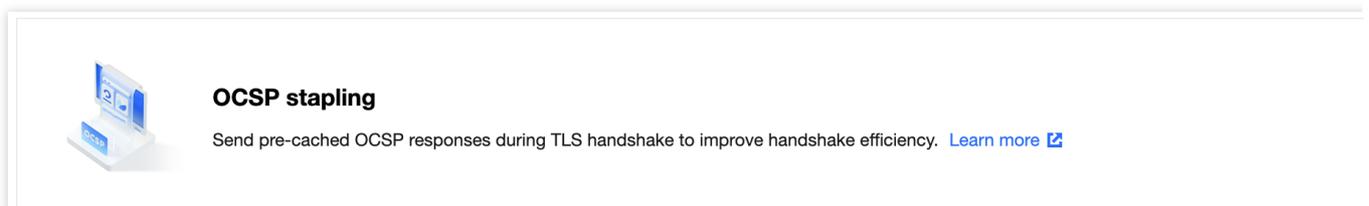
To enable OCSP stapling for all domain names used to access a site, refer to the following information.

### 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, choose **Site Acceleration** > **HTTPS** to go to the HTTPS page.
3. On the OCSP stapling configuration card, toggle on the **Site-wide setting** switch.



**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 **Rule Engine**.
3. On the rule engine management page, click **Create 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 **Operation** drop-down list, select **OCSP stapling**.

6. Click **Save and publish**.

# Domain alias

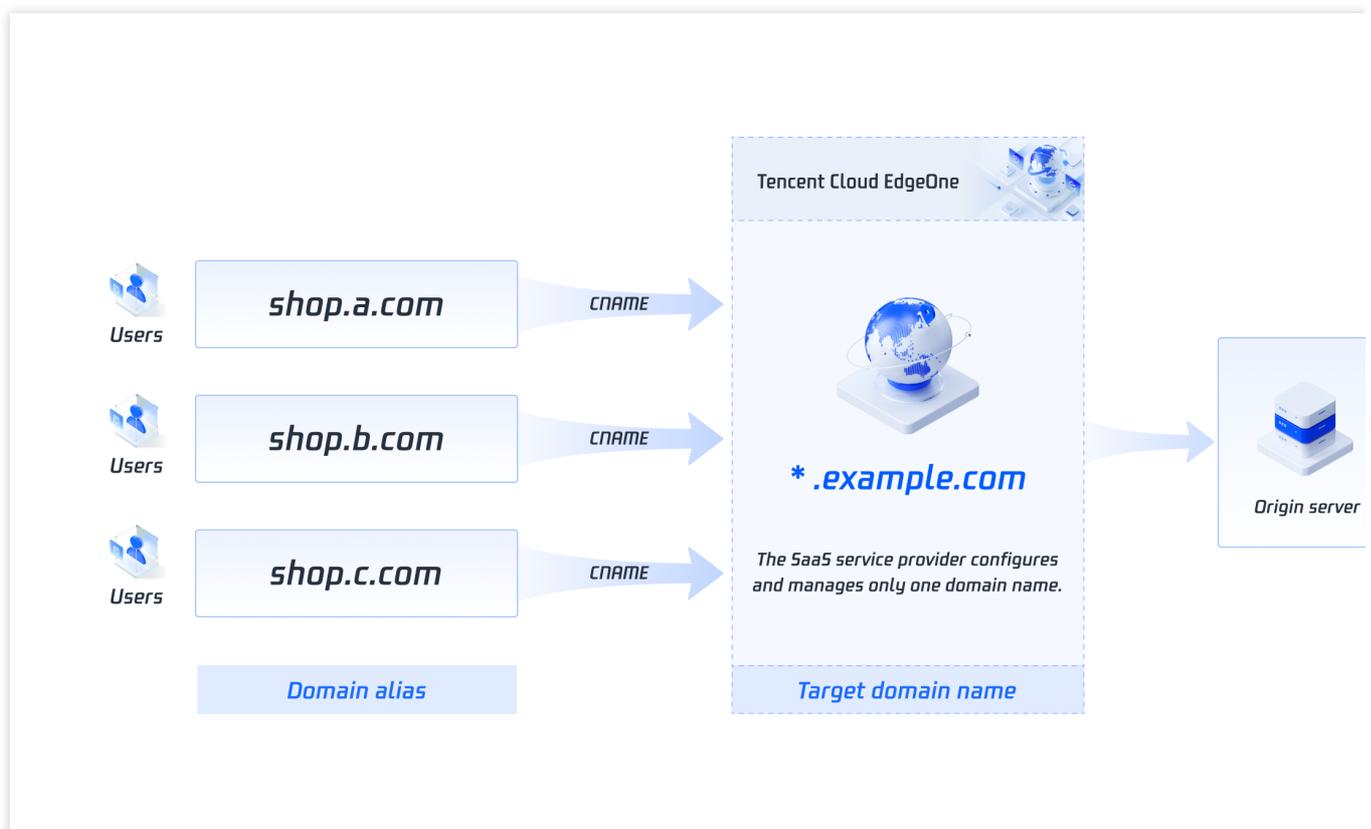
## Overview

Last updated : 2023-06-21 14:47:34

You might be stuck with a huge and repetitive workload when connecting large quantities of domain names to security acceleration services and ensuring they are configured identically, or when adding and changing configuration, deploying, verifying and maintaining HTTPS certificates for these domain names.

With alias domain names, EdgeOne's security acceleration capabilities of one domain name can be extended to others. EdgeOne also supports certificate application and auto-update, reducing your certificate purchase and maintenance costs.

## How It Works



As shown in the figure above, multiple alias domain names are resolved to the target domain name via CNAME, that is, when users access these alias domain names, they will point to the target domain name and its rule configuration

will be automatically applied to these alias domain names.

## Applicable Scenarios

**SaaS business:** Allow SaaS companies to get fast access to security acceleration services and easy configuration synchronization for large quantities of domain names.

**Disaster recovery:** Allow users to configure multiple alternate domain names with the same configuration and enable them when encountering DNS resolution failures.

## Benefits

**Operational convenience:** Maintain multiple domain names synchronously with one domain name.

**Fast access:** Configure large quantities of domain names through simple steps.

# Configuration Guide

Last updated : 2023-11-23 21:15:32

This document describes how to create, edit, and delete a domain alias, configure the CNAME record of the domain alias to point to the target domain name, and configure a certificate for the domain alias.

## Prerequisites

[Purchase](#) the EdgeOne Enterprise plan, [connect your site](#) to EdgeOne, and create the target domain name.

## Creating a Domain Alias

### Step 1. Create a domain alias

1. Log in to the [EdgeOne console](#), click on the site list in the left menu bar, and click on the site to be configured within the site list.
2. On the site details page, click on the **Alias domain name**.
3. On the alias domain name list page, click **Create**, configure the relevant parameters, and click **OK**.

i • You can accelerate alias domain names you configured securely.

• You can request a free certificate after an alias domain name's CNAME is pointed to the target domain name. The certificate will be renewed automatically.

Alias domain name

Target domain name Please select ↻ Create

Configure certificate  Off  Managed SSL certificate  Free certificate ! To purchase a certificate or upload your own certificate, please go to [SSL.com](#)

OK
Cancel

Parameter	Description
Alias domain name	It can contain up to 81 characters. Wildcard domain names such as <code>*.test.com</code> are not supported. If the acceleration region of your site is in the Chinese mainland, you must obtain an ICP filing number for your domain alias.
Target domain name	You can select a domain name of the current site in the <b>Activated</b> or <b>Deploying</b> state. For more information, see <a href="#">Connecting via CNAME</a> and <a href="#">Connecting via NS</a> .

### Configure certificate

**Off:** It indicates not to configure the HTTPS certificate. If you select this option, the domain alias supports only HTTP access.

**Managed SSL certificate:** It indicates to select a certificate managed in SSL. To purchase or upload an external certificate, [contact us](#).

**Free certificate:** EdgeOne supports application and auto-renewal of free certificates. Note that you need to first create the domain alias and point its CNAME record to the target domain name at your DNS service provider.

## Step 2. Add the CNAME record of the domain alias that points to the target domain name

1. After the domain alias is added, it is in the **CNAME not configured** state by default.

Alias domain name	Status	HTTPS	Target domain name	Creation time
<input type="checkbox"/>	<span style="border: 1px solid red; padding: 2px;">❗ CNAME not configured</span>	<input checked="" type="checkbox"/> Configured <a href="#">Configure</a>		2022-12-27 11:32:31

2. Go to your DNS service provider and add a CNAME record that points to the target domain name to activate the domain alias.

3. EdgeOne automatically checks for updates, and changes the status of the domain alias to **Activated**.

## Step 3. Apply for a free certificate (optional)

If you have pointed the CNAME record of the domain alias to the target domain name at your DNS service provider, you can apply for a free certificate in EdgeOne.

1. On the [domain alias list page](#), click **Edit** and select **Free certificate**.

❗ You can accelerate alias domain names you configured securely.  
• You can request a free certificate after an alias domain name's CNAME is pointed to the target domain name. The certificate will be renewed automatically.

Alias domain name:

Target domain name:  [Create](#)

Configure certificate:  Off  Managed SSL certificate  Free certificate

To purchase a certificate or upload your own certificate, please go to [SSL console](#)

OK
Cancel

2. Click **OK**.

## Editing a Domain Alias

1. On the [domain alias list page](#), select the target domain alias and click **Edit**.
2. Modify the target domain name and certificate configuration type as needed and click **OK**.

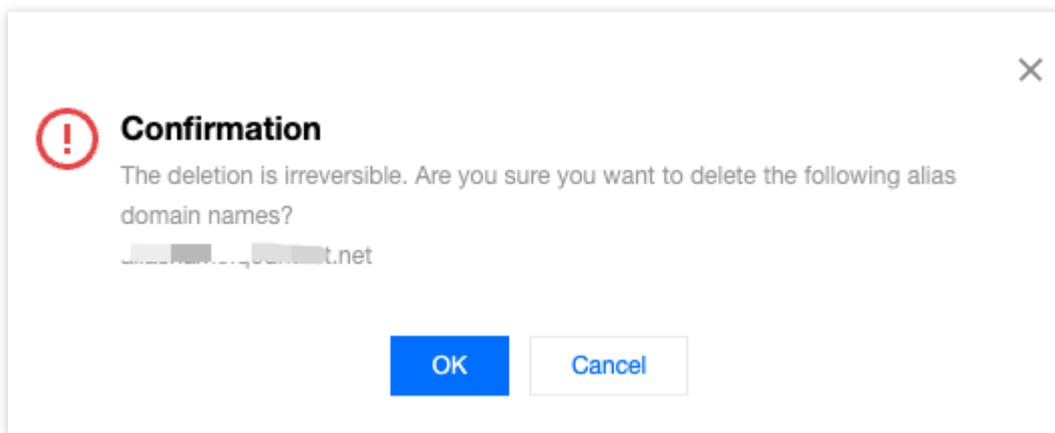
## Deleting a Domain Alias

### Note

A domain alias can be deleted only after it is disabled.

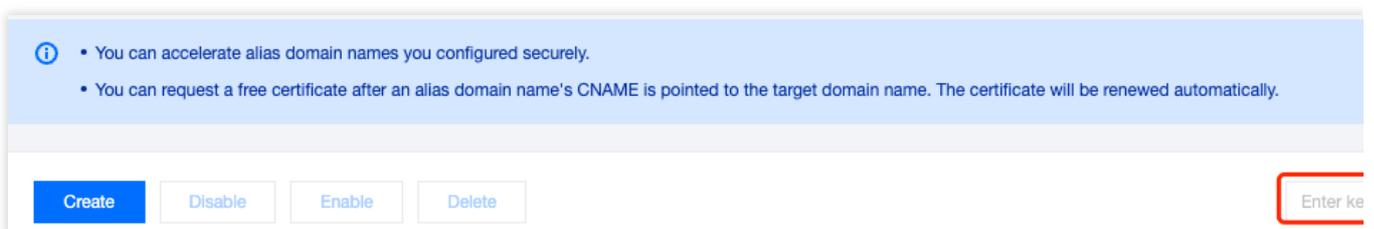
The data cannot be recovered once a domain alias is deleted.

1. On the [domain alias list page](#), select the target domain alias, click **Disable**, and then click **Delete**.
2. In the pop-up window, click **OK**.



## Searching for a Domain Alias

On the [domain alias list page](#), enter a keyword in the search input box and press Enter to search for a domain alias.



# Batch Connecting SaaS Domain Names

Last updated : 2023-06-29 15:06:27

Using alias domain names makes it easy for SaaS businesses to sync the configuration of one domain name to others to achieve batch connection.

## Purpose

Reading this document may take 10 minutes, which helps you understand:

What challenges for SaaS business can be overcome with alias domain names.

How to use alias domain names to relieve the workload of maintaining multiple domain names for the same business.

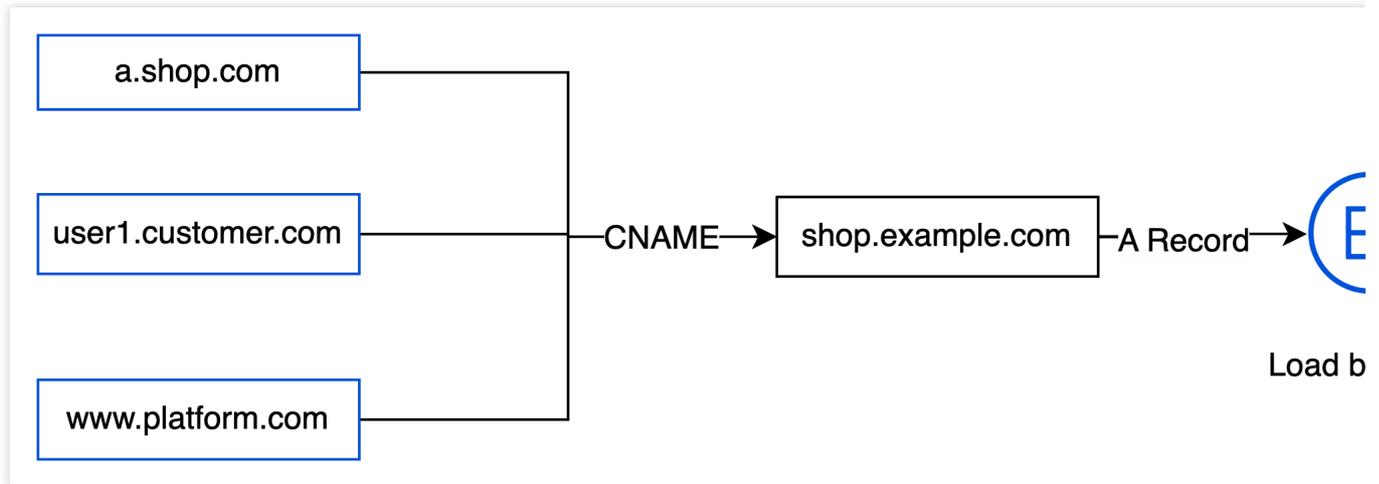
## Background

SaaS providers offer customers preset templates that is customizable for various purposes without coding, such as corporate homepages, e-commerce platforms and tutoring websites. Customers are only responsible for site content as SaaS providers will take care of operation and maintenance. Customer requirements for sites can be identified as follows:

1. Sites can support personalized use of exclusive domain names.
2. HTTPS can be enabled for site security and trustworthiness.
3. Users can have fast, secure access to sites.

### Current solution and pain points

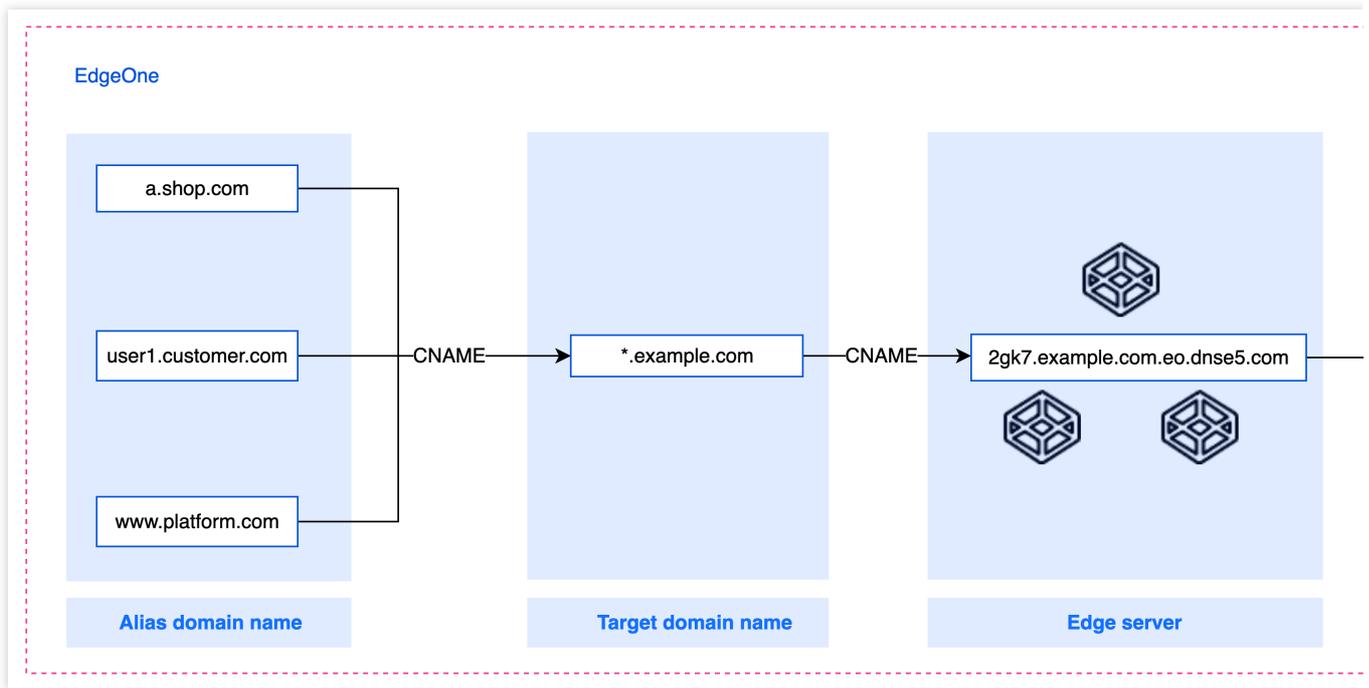
For SaaS providers, the support required by users is basically identical, except for the site content. Thus, an architecture that can facilitate operation and maintenance is used:



It allows customer-defined domain names to associate with SaaS providers' domain names via CNAME, and supports sending SNI requests to origins via the HTTPS certificate, which is deployed in load balancers and web service clusters. However, this architecture has drawbacks:

1. The access performance can be affected when the web service clusters fail to handle volumes of concurrent requests.
2. Security capabilities against network attacks are not provided.
3. While maintaining customers' HTTPS certificates, the clusters cannot guarantee updates of numerous domain names.

## EdgeOne Alias Names



With alias domain names, customer-defined domain names can be linked to the same SaaS website, which is a wildcard domain name connected with EdgeOne and specified as the target domain name. For details about how alias domain names work, see [Overview](#). Using this feature, SaaS website builder can solve these problems:

1. When the target domain name is added to EdgeOne, it can access security and content acceleration services, which are also reachable for the alias domain names.
2. SaaS website builders can greatly reduce costs as a result of maintaining target domain names only.
3. Customer-defined domain names can be separately added to EdgeOne where applications for free certificates and auto-update are provided.

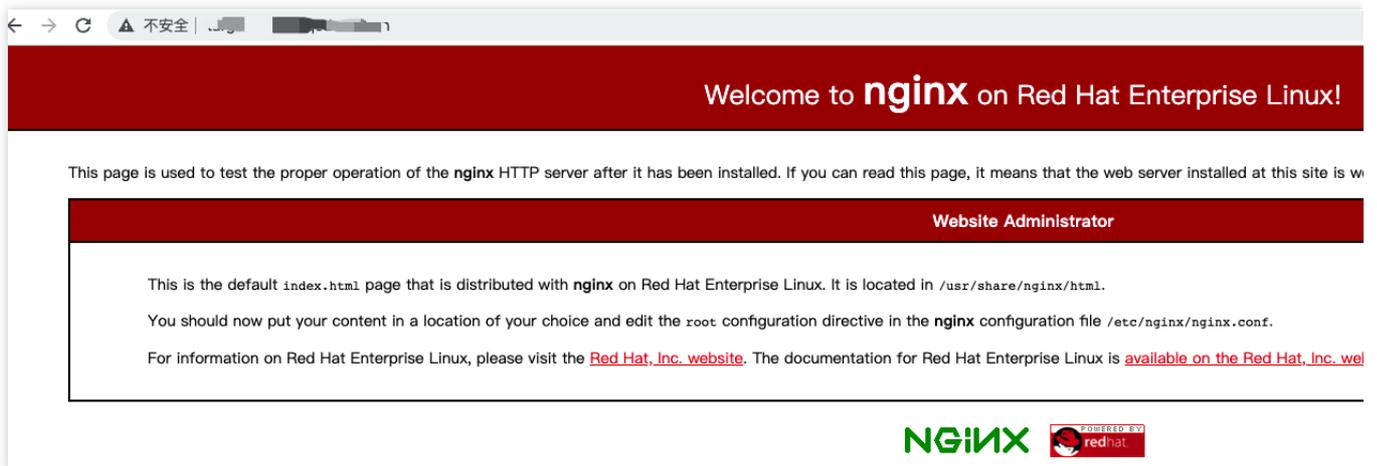
## Prerequisites

You have purchased the [EdgeOne Enterprise plan](#) for your site.

Your site has been connected to EdgeOne. For more information, see [Adding Sites](#).

## Before You Start

1. Set up a SaaS site, such as `site1.example.com`, `site2.example.com`, and `site3.example.com`, where `site1.example.com` can be accessed from a browser, as shown below:



2. Add a wildcard domain name of the SaaS site as an [EdgeOne acceleration domain name](#) and specify it as the target domain name, for example, `*.example.com`.

#### Note:

Since alias domain names share the same configuration and cache as the target domain name, using a wildcard domain name as the target domain name is recommended. This allows different SaaS sites to create their own cached resources to avoid cache conflicts.

3. Add customer-defined domain names as alias domain names. See the table below:

Customer-defined domain names	Sites
a.shop.com	site1.example.com
user1.customer.com	site2.example.com
www.platform.com	site3.example.com

## Directions

### Step 1. Create an alias domain name

1. Log in to the [EdgeOne console](#). Navigate to **Site List** and select a site for management.
2. In the left sidebar, click **Alias Domain Names**. On the page that appears, click **Create**.
3. Enter `a.shop.com` as the alias domain name, select `*.example.com` as the target domain name, and set **Off** for certificate configuration. Click **OK**.

## Step 2. Add a CNAME record that points to the target domain name

You must add a CNAME record that points to the target domain name to the alias domain name. Only activated alias domain names support applications for free certificates.

1. When the alias domain name is added, the status is default to **Not activated**. You need to go to the DNS provider where the alias domain name is located and add a CNAME record pointing to the target domain name. For details about modifying CNAME, see [Modifying CNAME Records](#).

Alias domain name	HTTPS	Target domain name	Creation time
alias.taylorjeonline	Not configured	target.taylorjeonline	2022-12-08 20:23:43
...	...	...	...

2. When the CNAME record is added, EdgeOne automatically checks for updates and changes the status of the domain alias to **Activated**.

You can accelerate alias domain names you configured securely.  
 You can request a free certificate after an alias domain name's CNAME is pointed to the target domain name. The certificate will be renewed automatically.

<input type="checkbox"/> Alias domain name	Status	HTTPS	Target domain name	Creation time
<input type="checkbox"/> alias1.customer.com	<span style="border: 2px solid red; padding: 2px;">✔ Activated</span>	Not configured <a href="#">Configure</a>	target.tencent.com	2022-12-08 20:23:43

Total items: 1

### Step 3. Verify the configuration

Access the alias domain name `a.shop.com` via your browser to verify whether it provides the same content as `site1.example.com`.

target.tencent.com

Welcome to **nginx** on Red Hat Enterprise Linux!

This page is used to test the proper operation of the **nginx** HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site

**Website Administrator**

This is the default `index.html` page that is distributed with **nginx** on Red Hat Enterprise Linux. It is located in `/usr/share/nginx/html`.

You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.

For information on Red Hat Enterprise Linux, please visit the [Red Hat, Inc. website](#). The documentation for Red Hat Enterprise Linux is [available on the Red Hat, Inc. website](#).

**NGINX**

Other alias domain names `user1.customer.com` and `www.platform.com` can be verified in the same way.

### Step 4. Apply for a free certificate (optional)

After you configure the CNAME record for the alias domain name by following Step 2, apply for a free HTTPS certificate as follows:

1. On the alias domain name list page, find `alias1.site.com` and click **Configure** in the **HTTPS** column. In the pop-up window, select **Free certificate** and click **OK**.

### HTTPS certificate configuration

Domain name

Certificate type  Off  Managed SSL certificate  Free certificate

To purchase a certificate or upload your own certificate, please go to [SSL console](#)

2. On the alias domain name list page, move the pointer over



to view the information about the certificate:

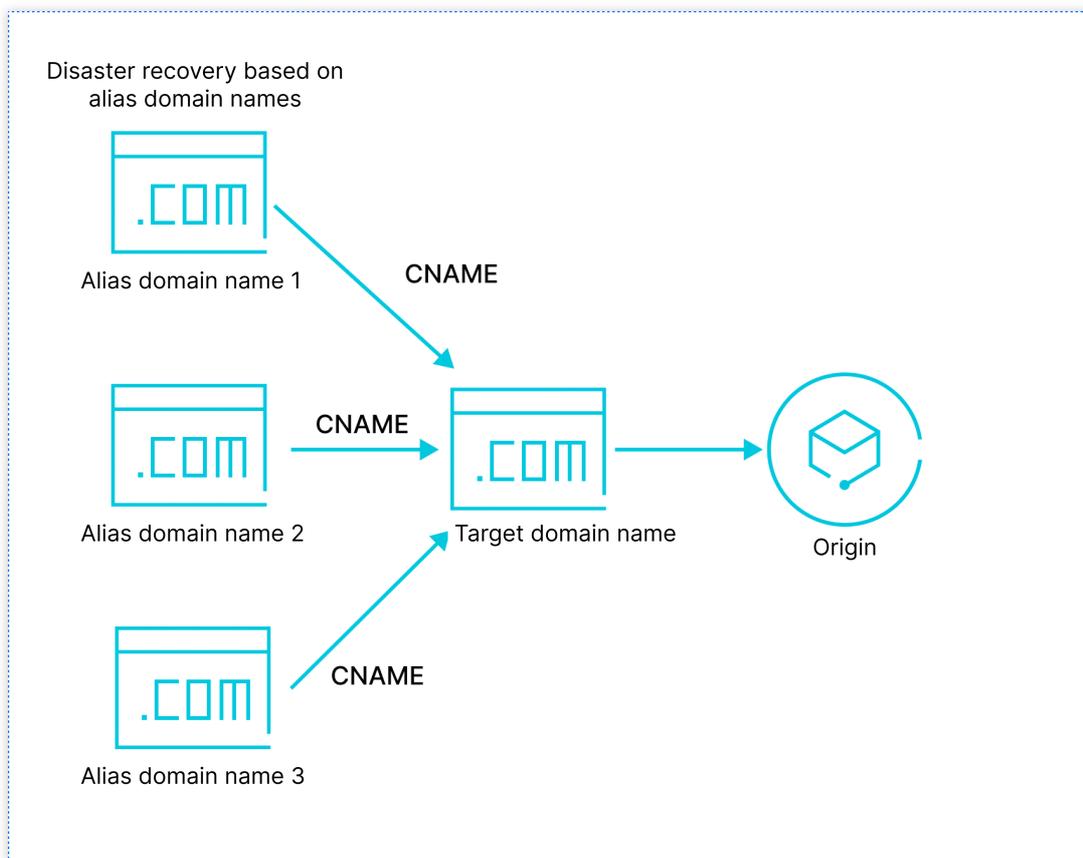
Alias domain name	Status	Current HTTPS certificate	Target domain name	Creation time
<input type="checkbox"/>	Activated	Encryption algorithm: RSA 2048 Expiration time: 2023-07-12 17:14:56 Auto-renewal: Yes		2023-04-13 18:05:02
<input type="checkbox"/>	Activated	Configured <a href="#">Configure</a>		2023-04-13 18:04:44
<input type="checkbox"/>	Activated	Configured <a href="#">Configure</a>		2023-04-13 18:04:32

Total items: 3

# Configuring Alias Domain Names for Disaster Recovery

Last updated : 2023-06-21 14:48:08

This document describes how to achieve business disaster recovery by using EdgeOne alias domain names. If a domain name becomes unavailable due to, for example, DNS exceptions, the alias domain name can provide the service instead.



## Purpose

Reading this document may take 10 minutes, which helps you learn:

1. How to use alias domain names to relieve the workload of maintaining multiple domain names for the same business.
2. How to verify that an alias domain name is working as expected.
3. How to improve business disaster recovery by using alias domain names.

4. How to apply for and maintain free certificates for alias domain names.

## Background

When promoting your business with many top-level domain names or with many alternate domain names in expectation for keeping your business uninterrupted, normally you need to configure these domain names one by one while ensuring each of them is configured identically in EdgeOne. This can result in a huge maintenance workload when it comes to adding/modifying configuration and applying for/renewing HTTPS certificates.

EdgeOne synchronizes the security and acceleration capabilities of one domain name to others by pointing multiple alias domain names to a target domain name. The configuration of the target domain name will then be synced among these alias domain names. Free HTTPS certificates can also be applied for and auto-renewed.

## Prerequisites

1. You have purchased the [EdgeOne Enterprise plan](#).
2. You have connected a site to EdgeOne. For more information, see [Adding Sites](#).
3. You have added the target domain name in EdgeOne.

## Sample Scenario

In this scenario, you have connected `target.example.com` to EdgeOne and want these domain names to serve as alternatives:

1. `alias1.site.com`
2. `www.shop.com`
3. `backup.website.com`

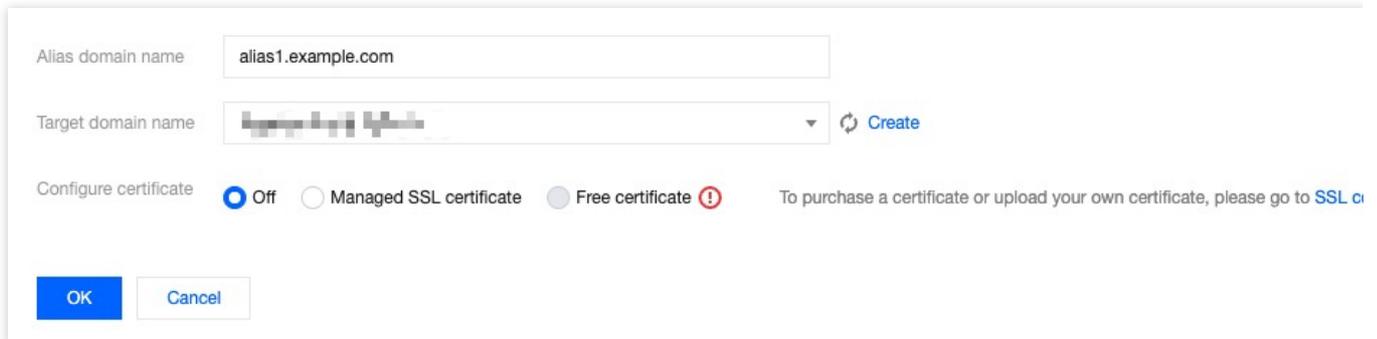
To do so, add these domain names as alias domain names to `target.example.com`, and make sure that they have the same accessibility as `target.example.com` via browser:



## Directions

### Step 1. Create an alias domain name

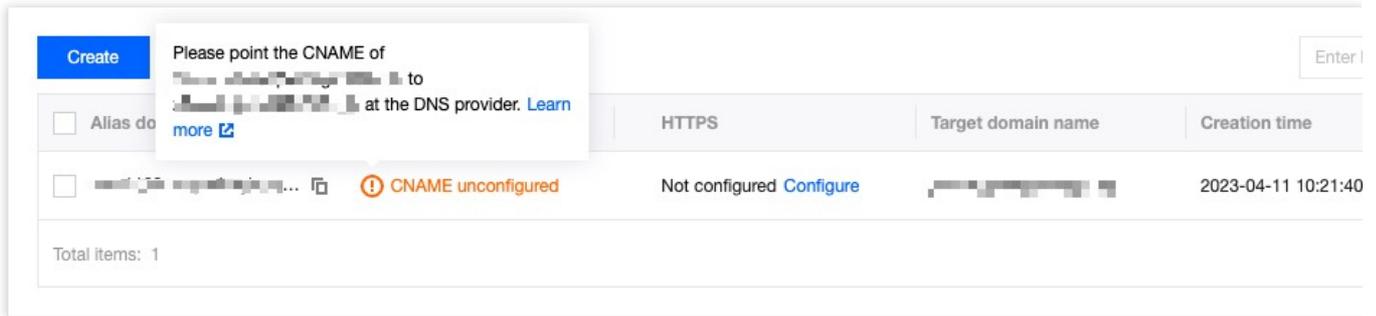
1. Log in to the [EdgeOne console](#). Navigate to **Site List** and select a site for management.
2. In the left sidebar, click **Alias Domain Names**. On the page that appears, click **Create**.
3. Enter `alias1.site.com` as your alias domain name, select `target.example.com` as your target domain name, and set **Off** for certificate configuration. Click **OK**.



### Step 2. Add a CNAME record that points to the target domain name

You must add a CNAME record that points to the target domain name to the alias domain name. Only activated alias domain names support applications for free certificates.

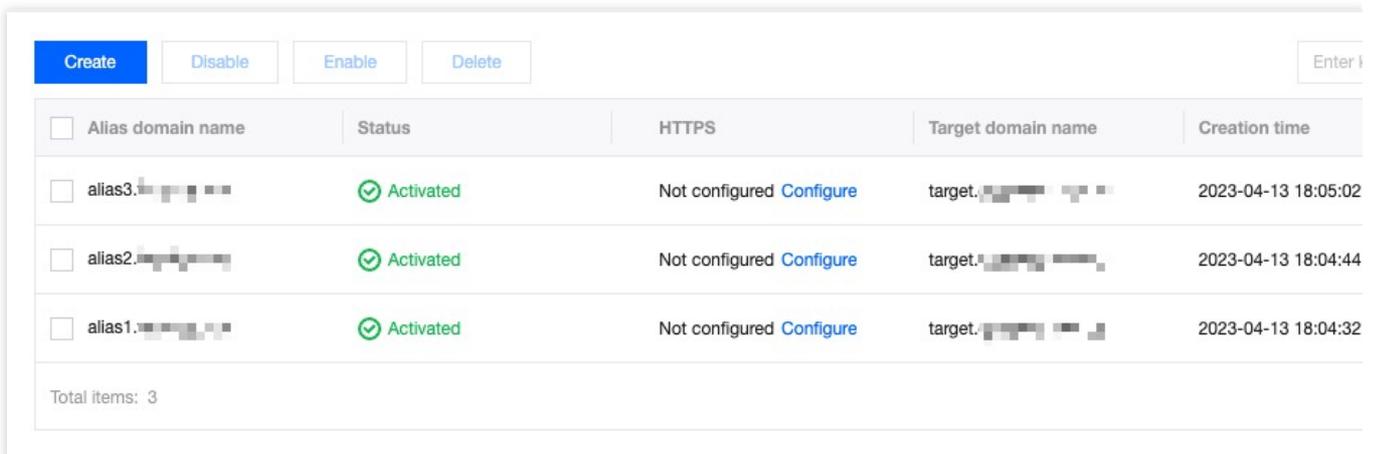
1. When your alias domain name is added, the status is default to **Not activated**, as shown in the figure below:



2. Go to the DNS provider where the alias domain name is located and add a CNAME record pointing to the target domain name. For details about modifying CNAME, see [Modifying CNAME Records](#).

3. When the CNAME record is added, EdgeOne automatically checks for updates and changes the status of the domain alias to **Activated**.

4. Perform the same steps to add and activate `www.shop.com` and `backup.website.com`, as shown below:



### Step 3. Verify the configuration

Access the alias domain names `alias1.site.com`, `www.shop.com` and `backup.website.com` via your browser to verify whether the configuration has taken effect.



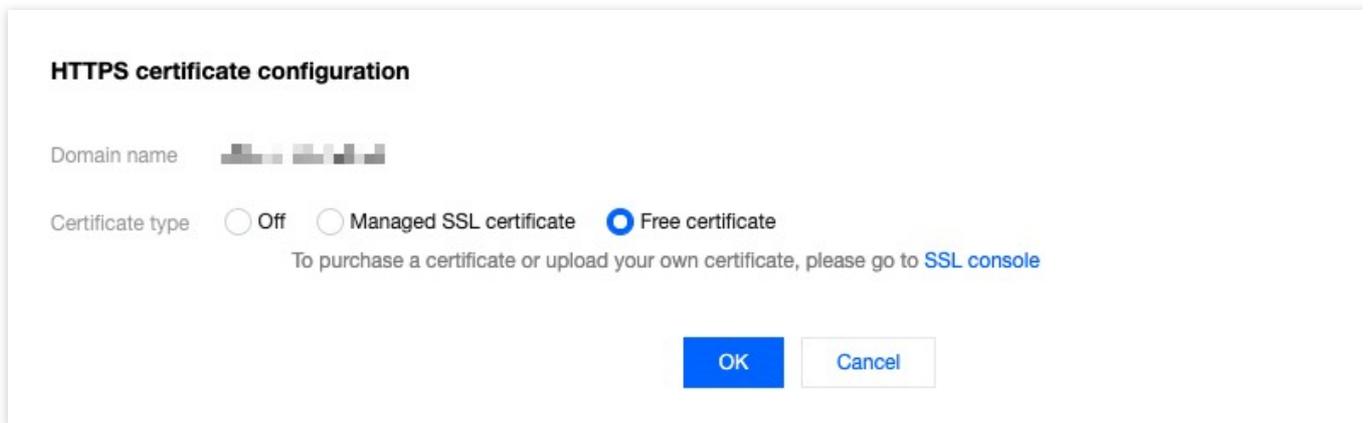
As shown above, the same response is obtained for the access requests to the alias domain names and target domain name. This indicates that the alias domain names have taken effect as expected.

If `alias1.example.com` becomes **Not activated** due to DNS resolution failures, `alias1.site.com`, `www.shop.com` and `backup.website.com` can keep providing services.

#### Step 4. Apply for a free certificate (optional)

After you configure the CNAME record for your alias domain name by following Step 2, apply for a free HTTPS certificate as follows:

1. On the alias domain name list page, find `alias1.site.com` and click **Configure** in the **HTTPS** column. In the pop-up window, select **Free certificate** and click **OK**.



2. On the alias domain name list page, move the pointer over



to view the information about the certificate:

Current HTTPS certificate:

Encryption algorithm RSA 2048

Expiration time 2023-07-12 17:14:56

Auto-renewal Yes

Enter keywords in the alias dom

<input type="checkbox"/> Alias domain name	Status		Target domain name	Creation time	Update tim
<input type="checkbox"/> [blurred]	Deploying	Configured	[blurred]	2023-04-13 18:05:02	2023-04-13
<input type="checkbox"/> [blurred]	Activated	Not configured	[blurred]	2023-04-13 18:04:44	2023-04-13
<input type="checkbox"/> [blurred]	Activated	Not configured	[blurred]	2023-04-13 18:04:32	2023-04-13

Total items: 3

10 / page

# Traffic Scheduling

## Traffic Scheduling Management

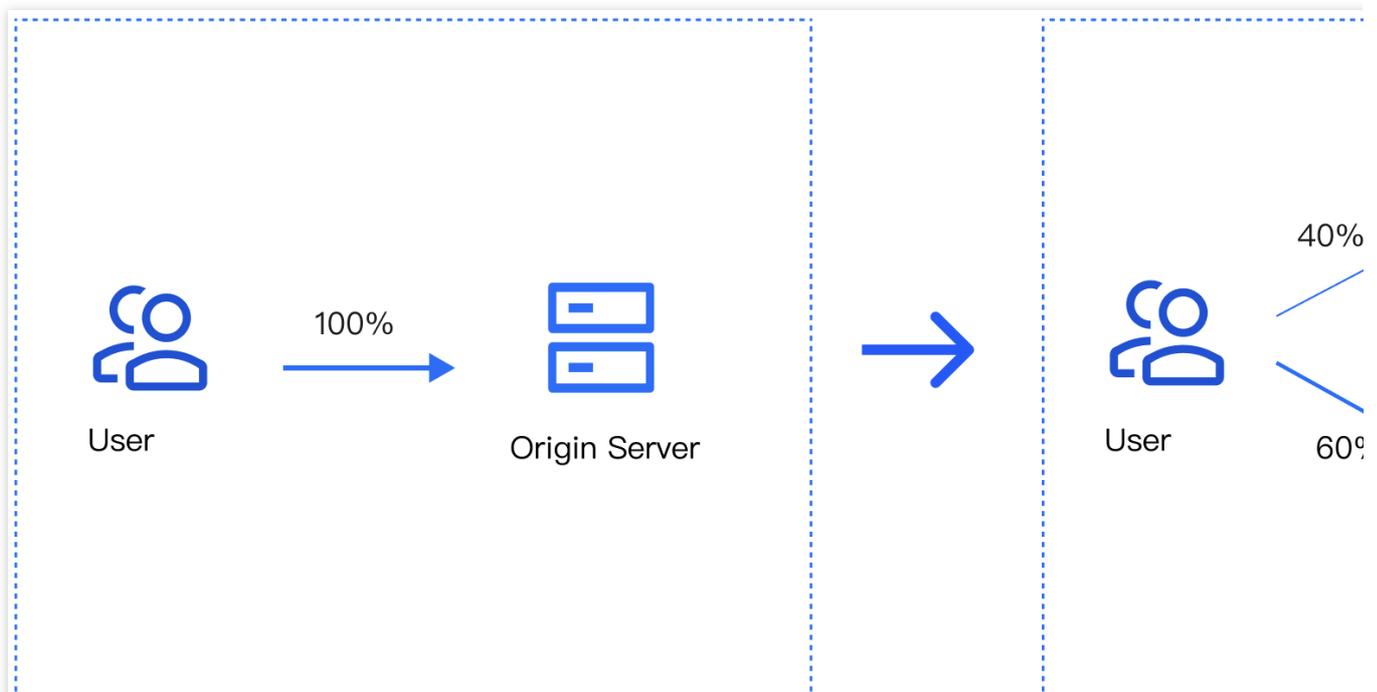
Last updated : 2024-04-16 17:06:58

### Overview

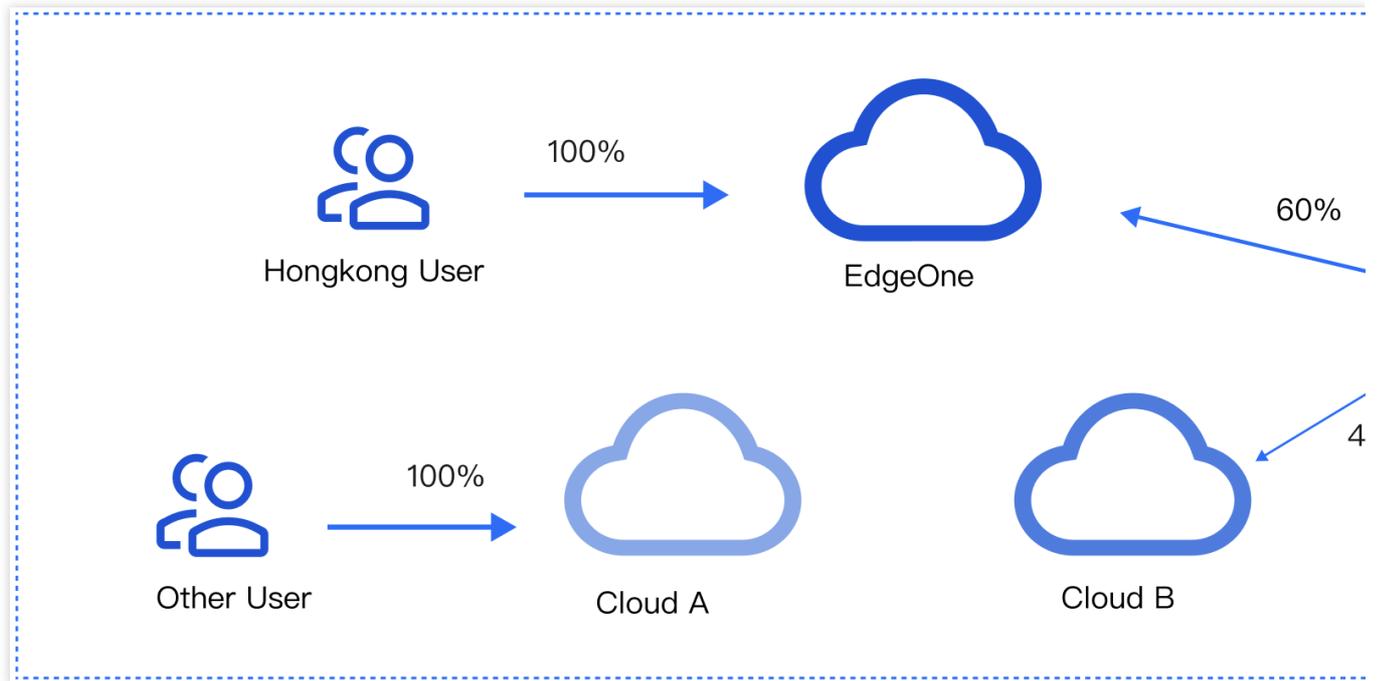
Traffic scheduling management is a multi-CDN smart resolution and scheduling tool provided by EdgeOne. It supports custom traffic scheduling policies between the origin and service providers to implement smooth canary migration of traffic and flexible allocation of services, thereby ensuring a high service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

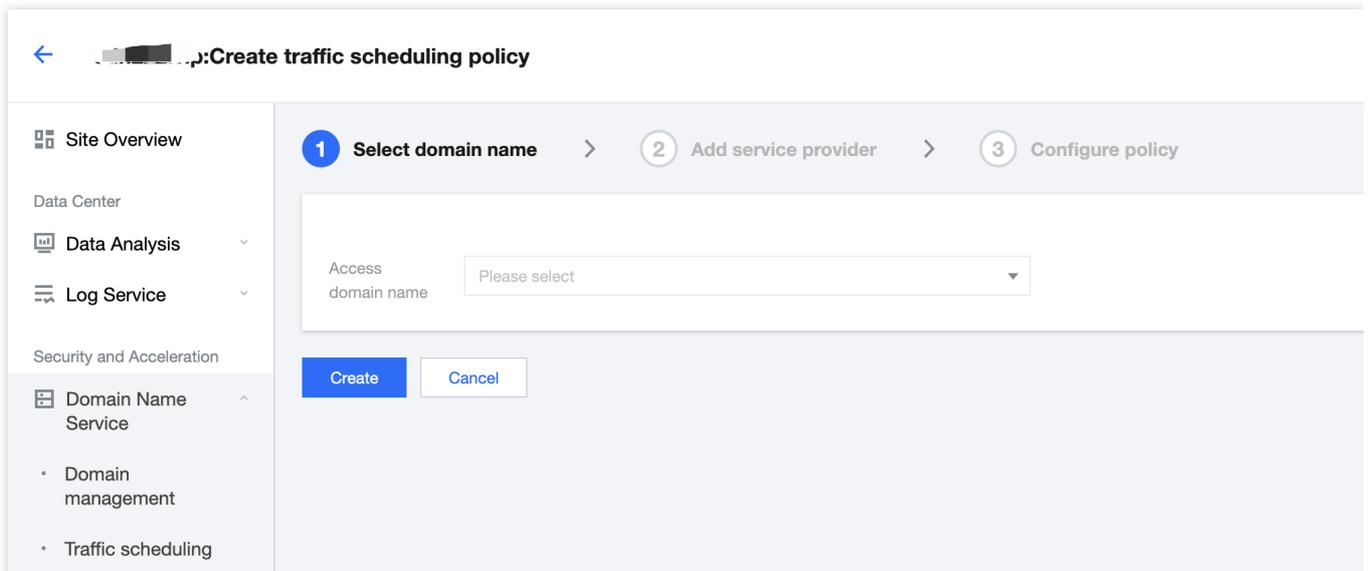
Multiple scenarios: You can use either the origin or services provided by other CDN vendors, implement canary switch, and use services from different vendors at the same time.

## Prerequisites

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

## Adding Traffic Scheduling Policies

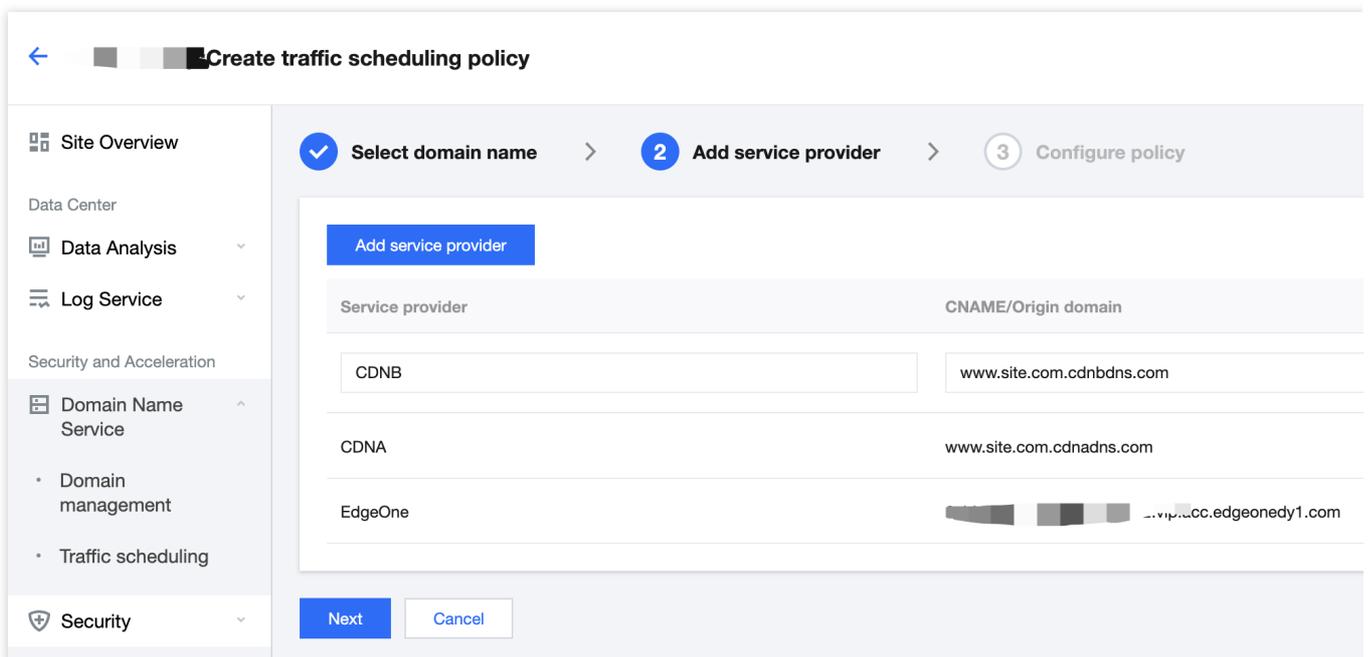
1. Log in to the [EdgeOne console](#), and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. On the site details page, click **Domain Name Service > Traffic Management**.
3. On the **Traffic scheduling** tab, click **Add scheduling policy**.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



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.



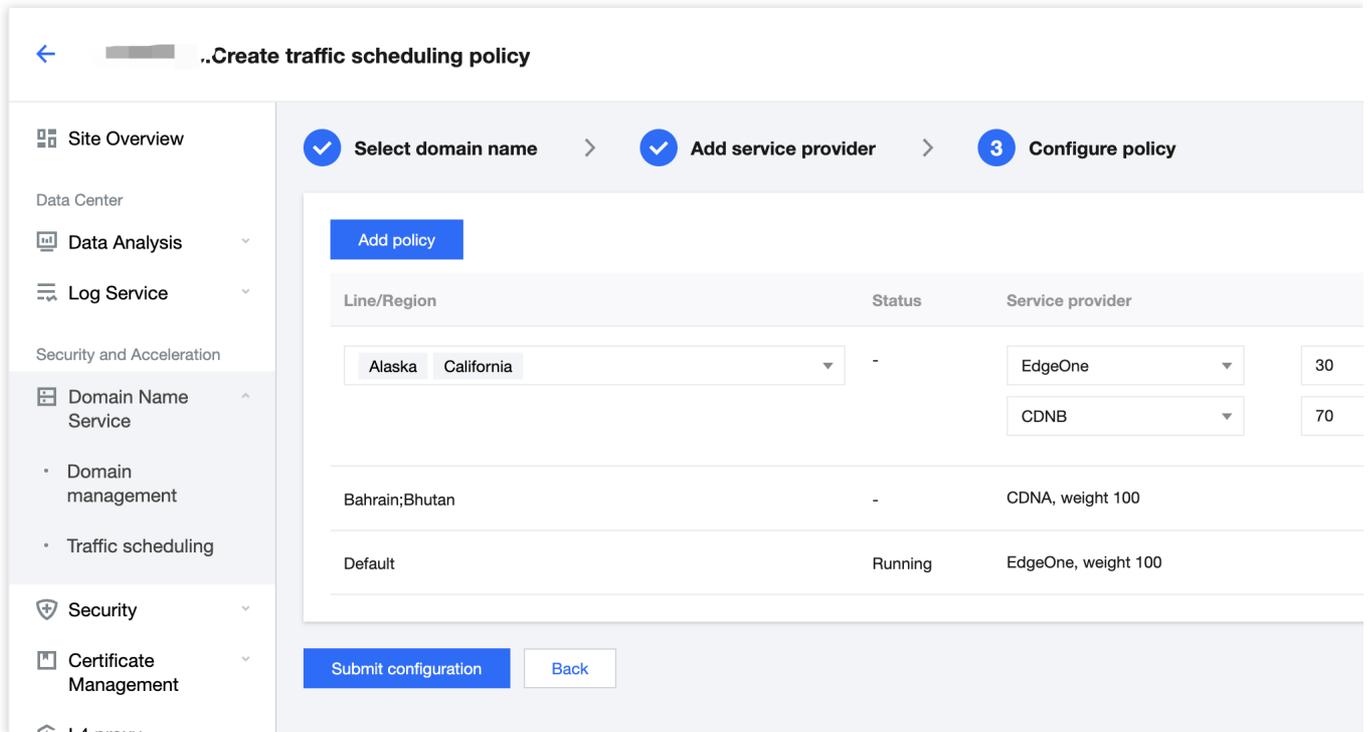
5. Click **Add policy**, select the line/region, and complete the policy configuration. You can select multiple service providers and specify their weights to configure a multi-service provider scheduling policy. After the configuration is complete, click **Submit configuration**.

**Note:**

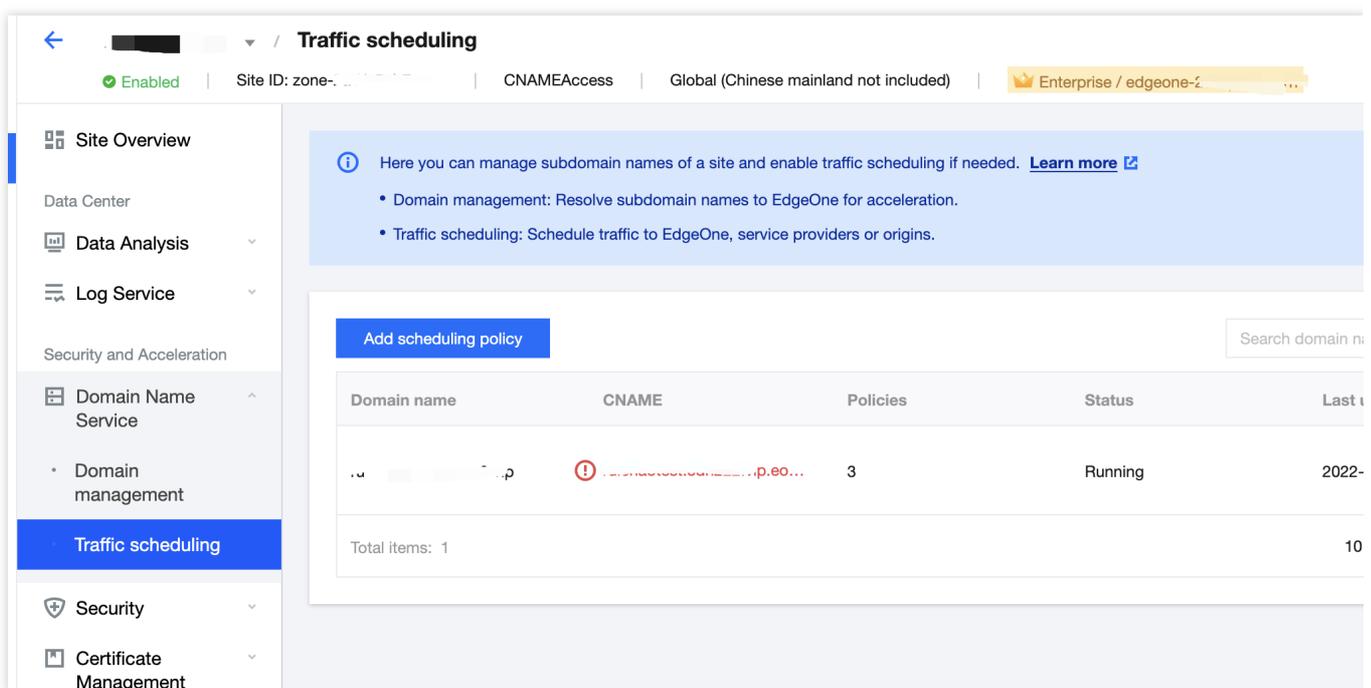
By default, all traffic passes EdgeOne. This is the base policy, which cannot be deleted but can be changed to another service provider.

**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.



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.



# 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.

← [Redacted]

- 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 [Redacted]

CNAME [Redacted]

### Acceleration service provider

[Add service provider](#)

Service provider	CNAME/Origin domain
CDNB	www.site.com.cdnbdns.com
CDNA	www.site.com.cdnadns.com
EdgeOne	[Redacted]hedy1.com

### Scheduling policy

[Add policy](#)

Line/Region	Status	Service provider
Default	-	CDNA
Bahrain Bhutan	-	EdgeOne 50
		CDNB 50
Alaska;California	Running	CDNA, weight 100