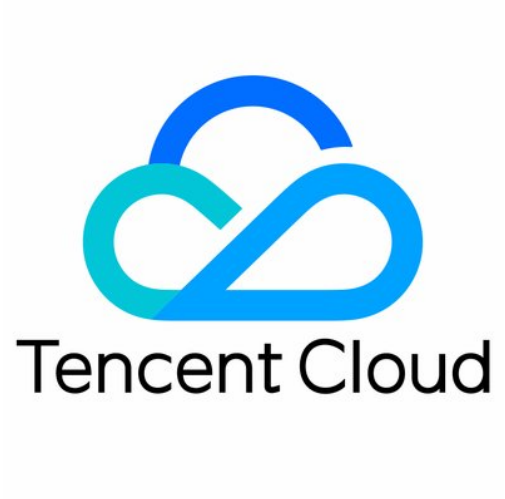
Tencent Cloud EdgeOne

Domain Service

Product Documentation



Contents

Domain Service
Hosting DNS Records
Modifying DNS Servers

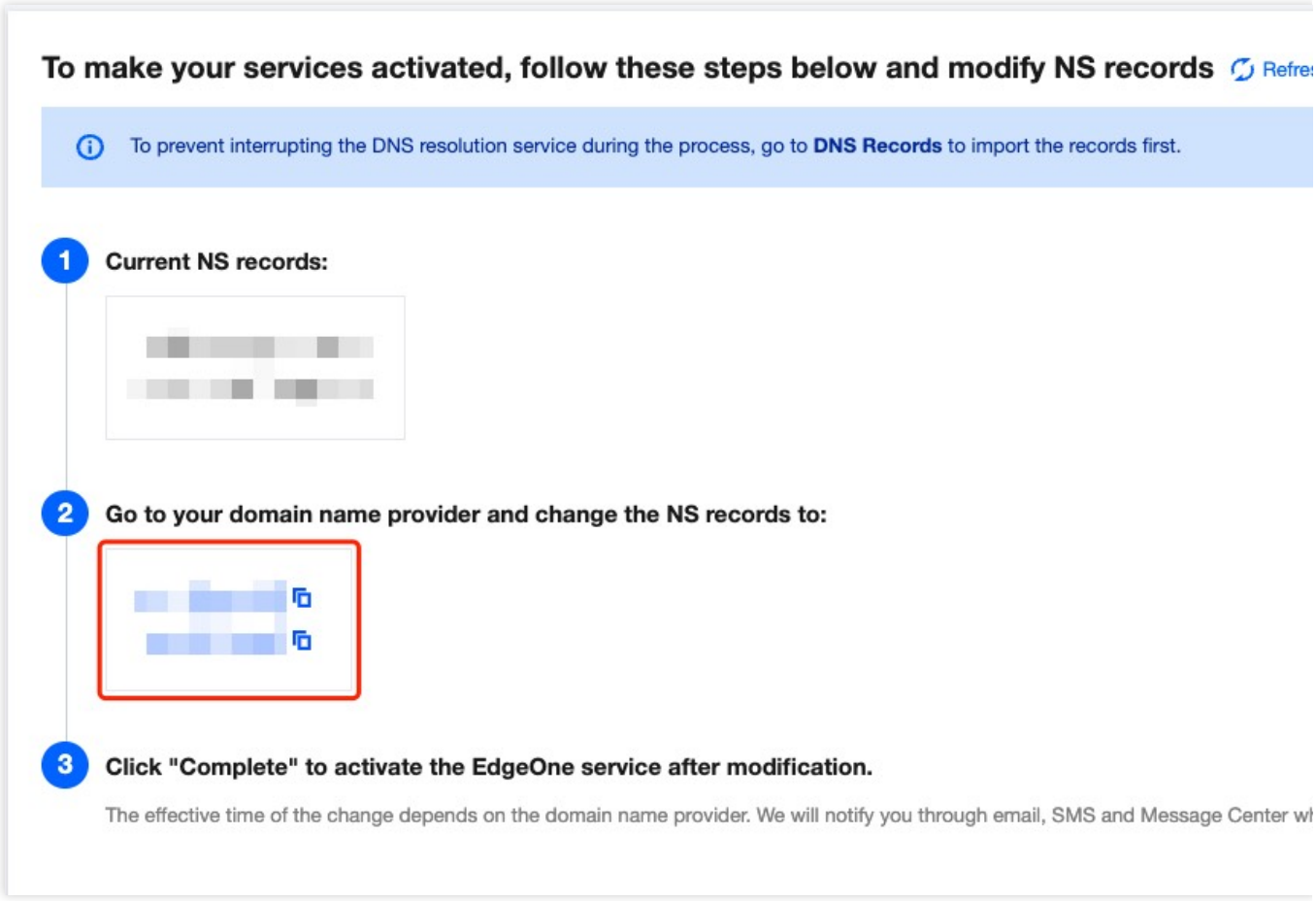
Last updated：2023-08-10 14:32:31

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.



Configuration guides for major domain registrars:

Tencent Cloud

Alibaba Cloud

Huawei Cloud

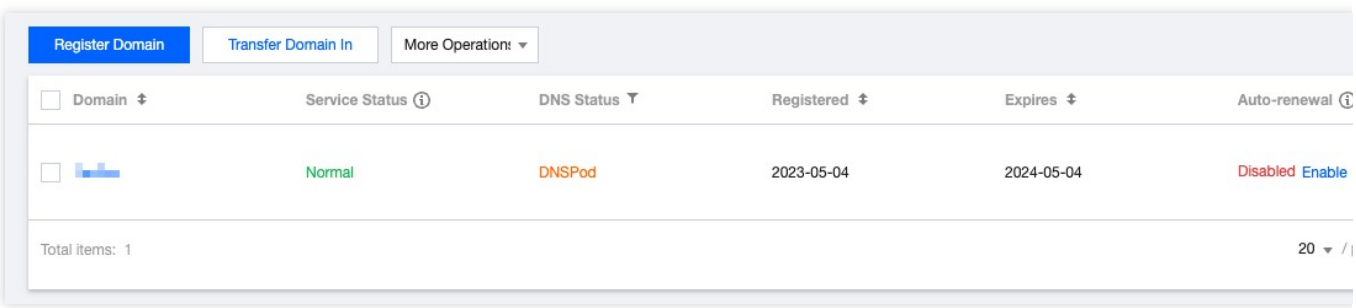
Godaddy

Google

Name

1. Log in to the Domains console.

2. On **My Domains** page**,** locate the target domain, and click **Manage** on the right.



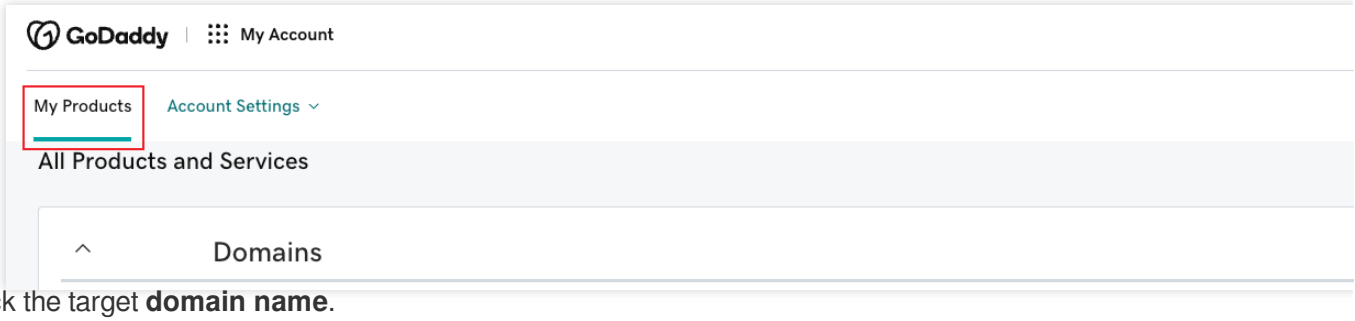
3. In the DNS resolution window, click **Modify DNS servers**.

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

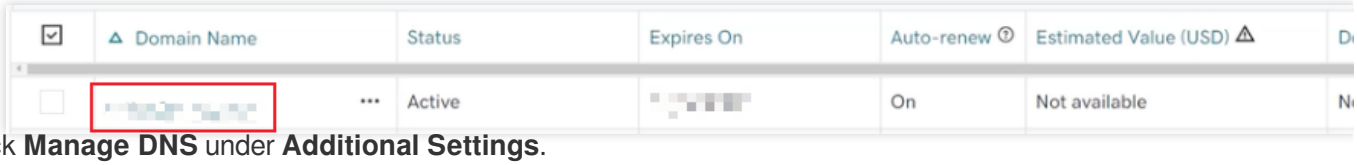
1. Log in to the Alibaba Cloud Domains console.
2. Click **Domains List**, and locate the target domain. Click **Manage** on the right.
3. In the left sidebar, click **Modify DNS**.
4. On the DNS modification page, click **Modify DNS servers**.
5. Enter the DNS server addresses provided by EdgeOne, and then click **OK**.

1. Log in to the Huawei Cloud Domains console.
2. Locate the target domain in the Domains List. Click **More** > **Manage** on the right.
3. On the basic information page, click **Modify**.
4. In the **Modify DNS servers** window, enter the server addresses provided by EdgeOne.
5. Click **OK**.

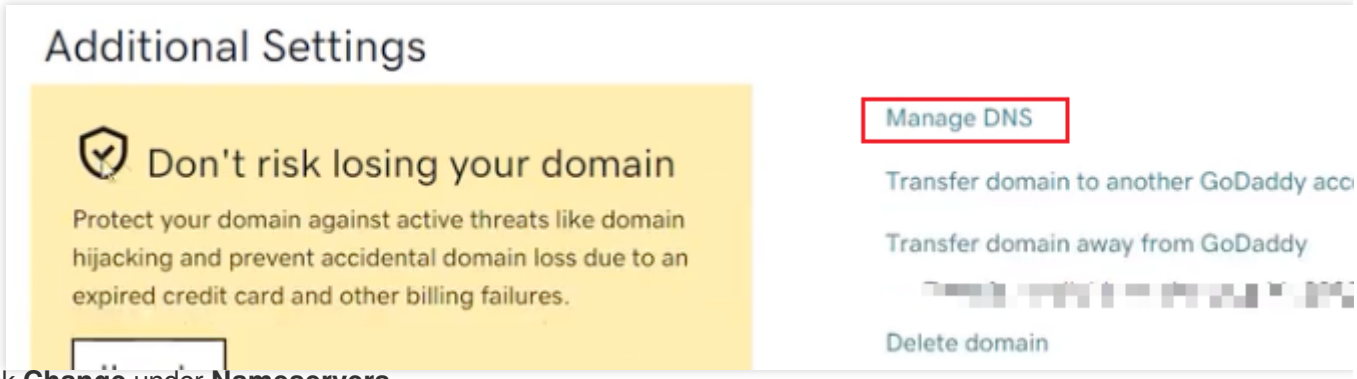
1. Log in to GoDaddy.
2. Click **My Products**, and select **Manage All**.



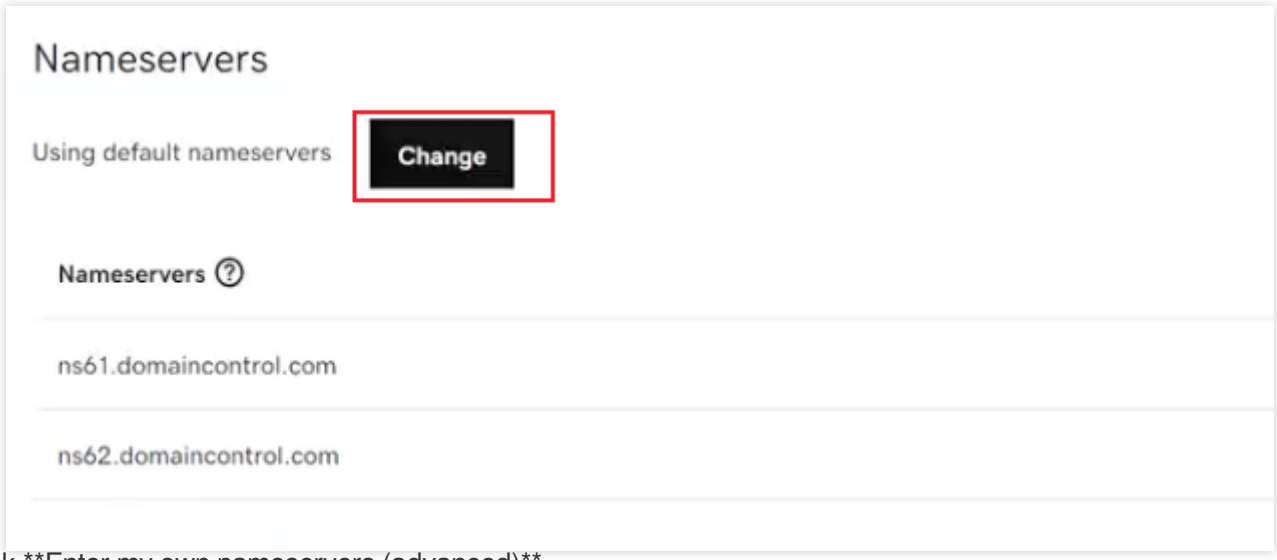
3. Click the target **domain name**.



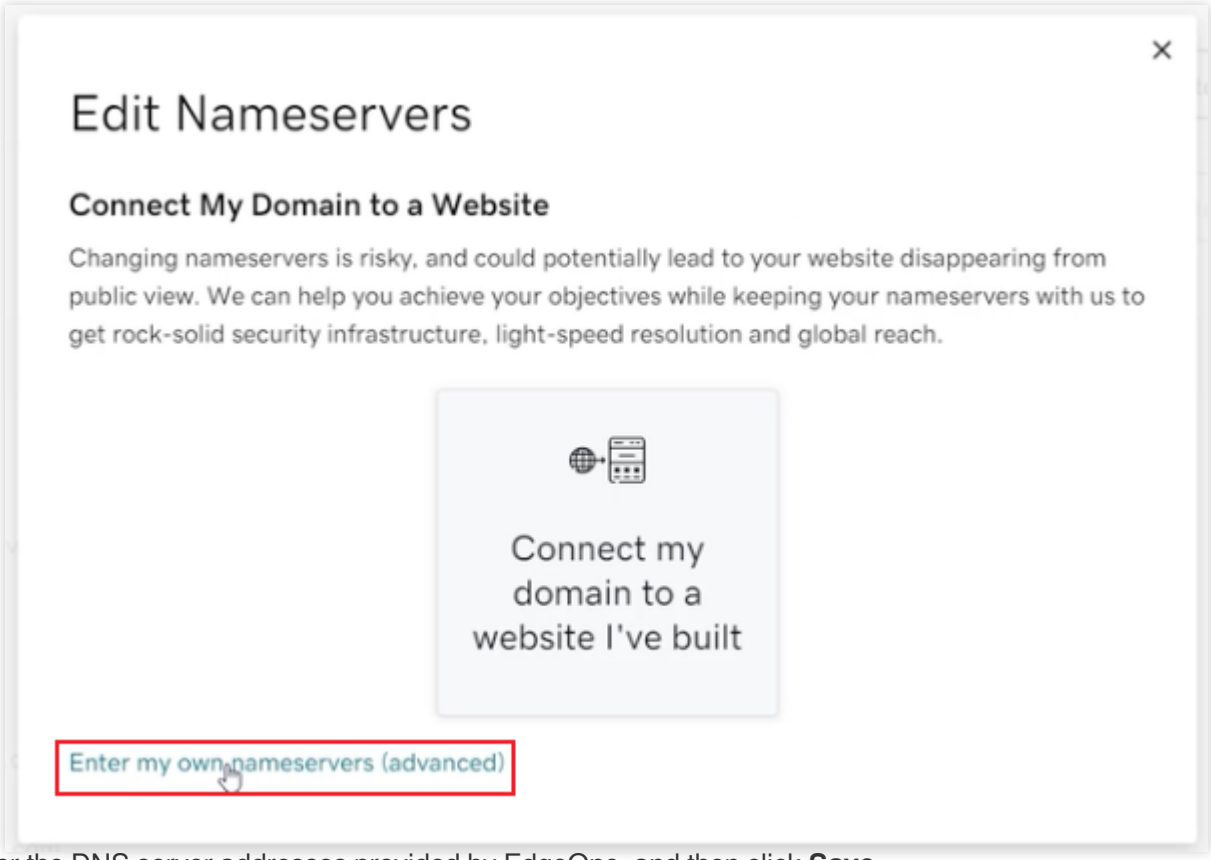
4. Click **Manage DNS** under **Additional Settings**.



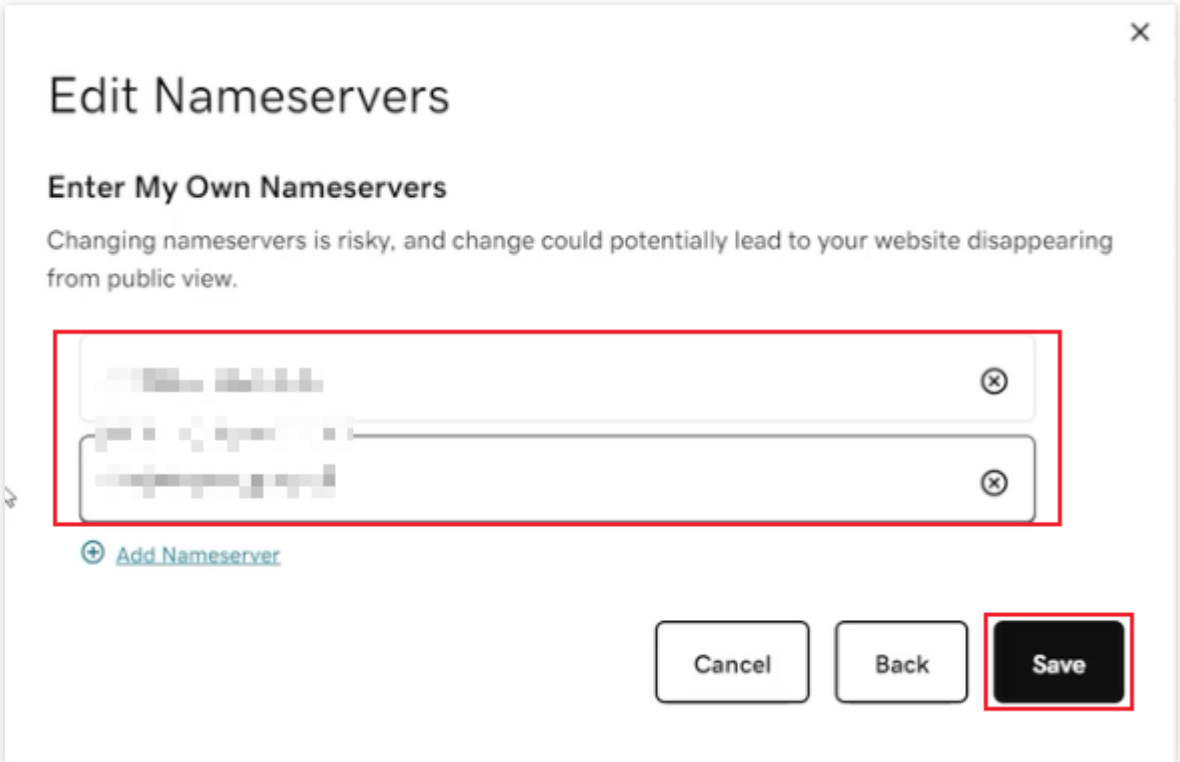
5. Click **Change** under **Nameservers**.



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



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



1. Log in to the Google Domains console.
2. Select the target domain name.
3. Click **Menu** > **DNS** on the top-left corner.

4. Choose to use custom domain servers under **Domain Servers**.
5. Enter the server addresses provided by EdgeOne in the **Domain Servers** field.
6. Click **Save**.

1. Log in to the Name console.
2. Click **My Domains**.
3. Select the target domain name.
4. In the **Nameservers column**, click **Manage Nameservers**.
5. Click **Delete All** to clear the current servers.
6. Enter the DNS server address provided by EdgeOne in the box labeled **Add Nameserver**, and then click **Add**. Only one server address can be added at one time.
7. Click **Save Changes**.

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

Note:

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

Configuring DNS Records

Last updated：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.

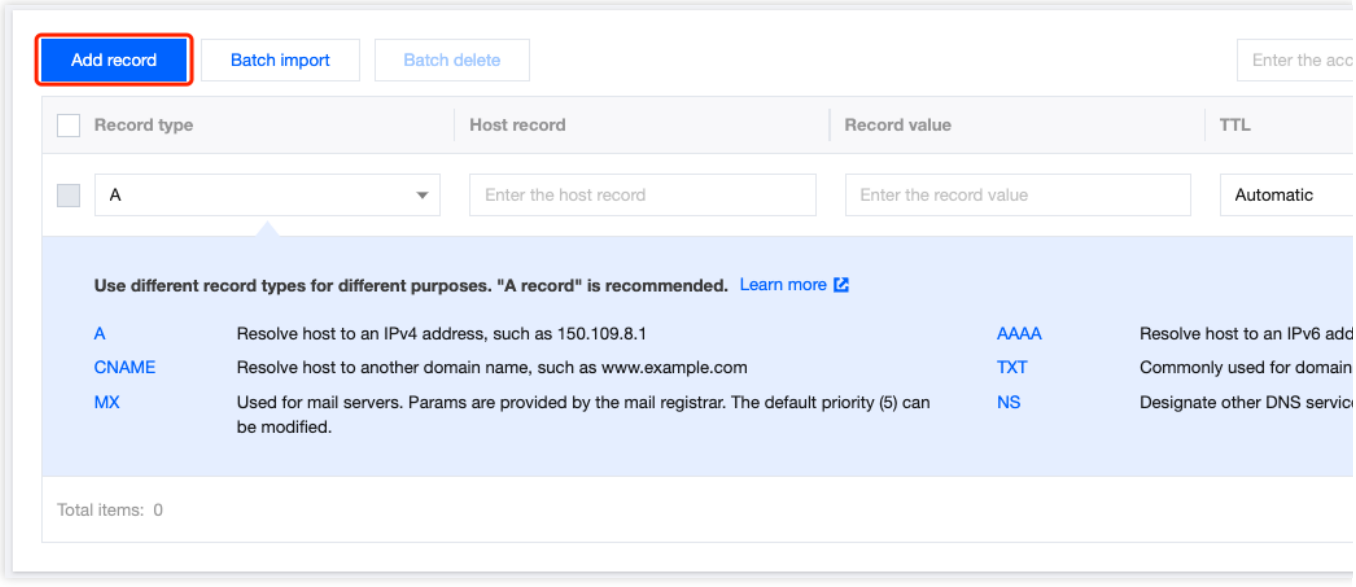
Prerequisite

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**.



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 ususally 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.

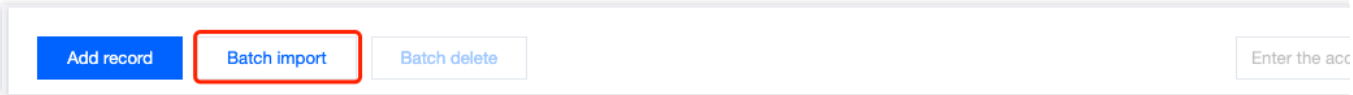
Note:

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.

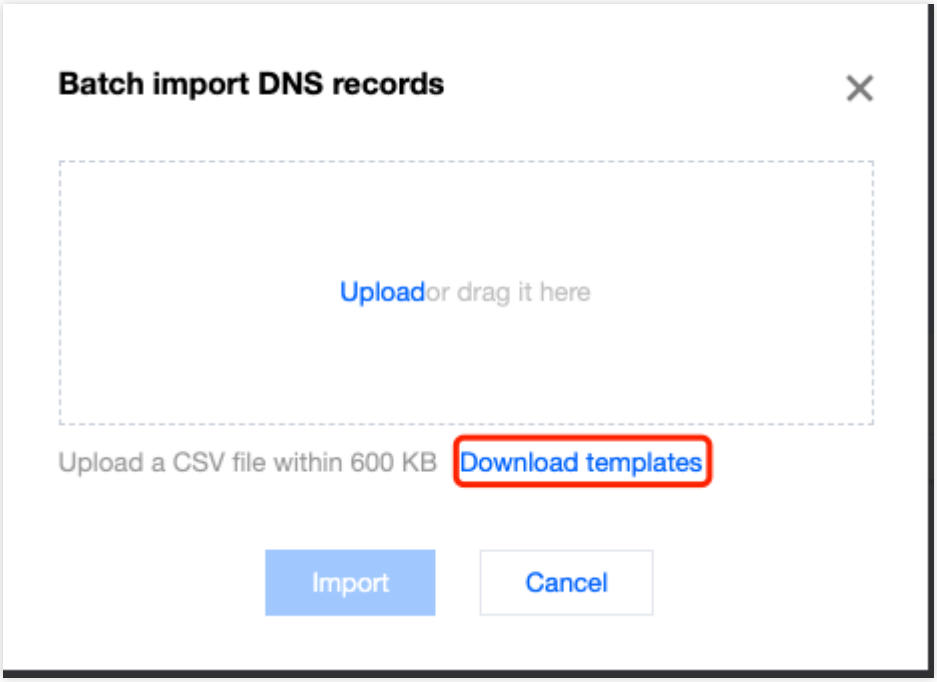
2. When you enable acceleration for a domain name, it is moved to **Acceleration**. You can also check it in the **DNS records** page.
3. If you want to configure multiple origins, or set a COS bucket as the origin, please see Adding Acceleration Domain Name.

Scenario 2: Batch Importing DNS Records

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 records page, click **Batch Import**.



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



5. 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.

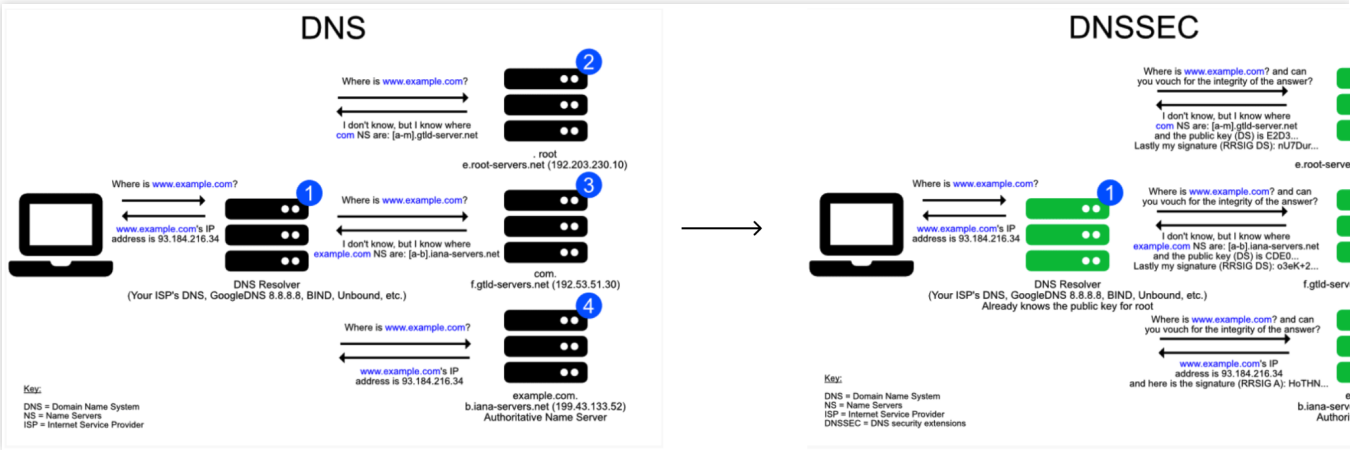
DNSSEC

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.

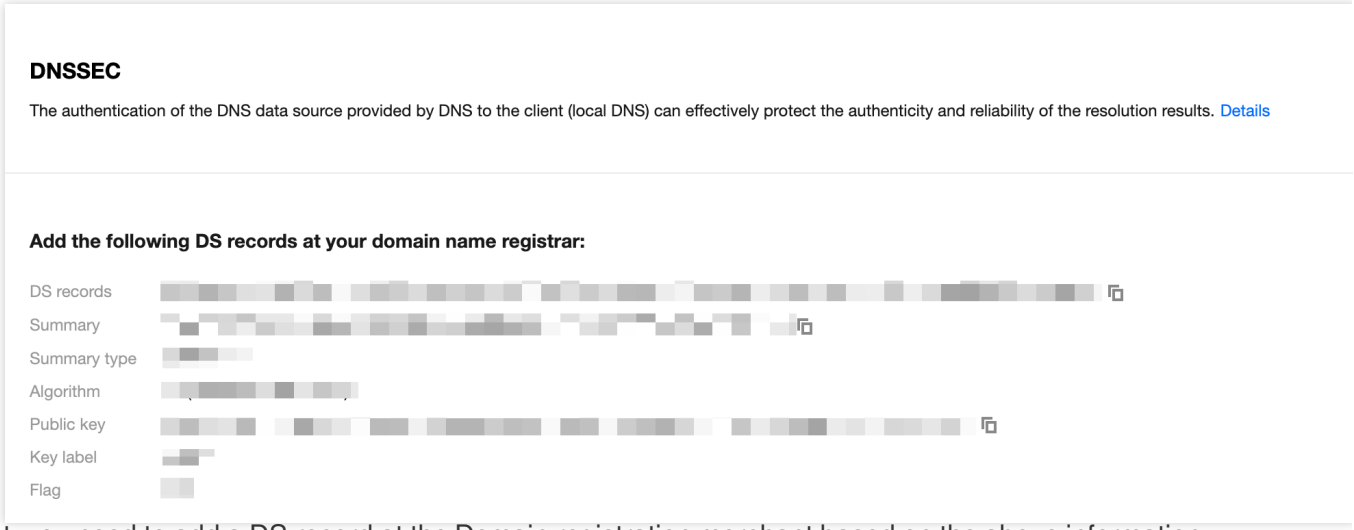


Directions

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.



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`.

Record type	Host record	Record value	TTL
A	loopone	1.2.3.4	Automatic
CNAME	looptwo	loopone.example.com	Automatic
CNAME	loopthree	looptwo.example.com	Automatic

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

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

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

```
;; ANSWER SECTION:
loopthree.[redacted]  272     IN      A       1.2.
```

Domain Connection
Adding A Domain Name for Acceleration

Last updated：2024-04-01 10:04:18

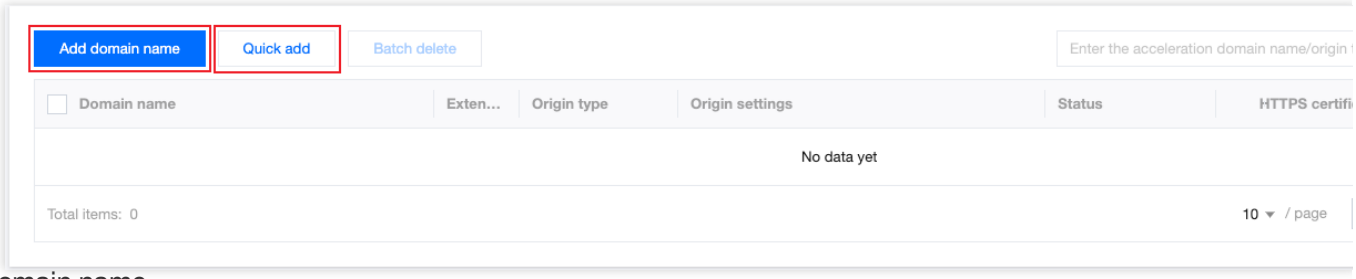
This document describes how to connect your domain name to EdgeOne and enable domain acceleration.

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.

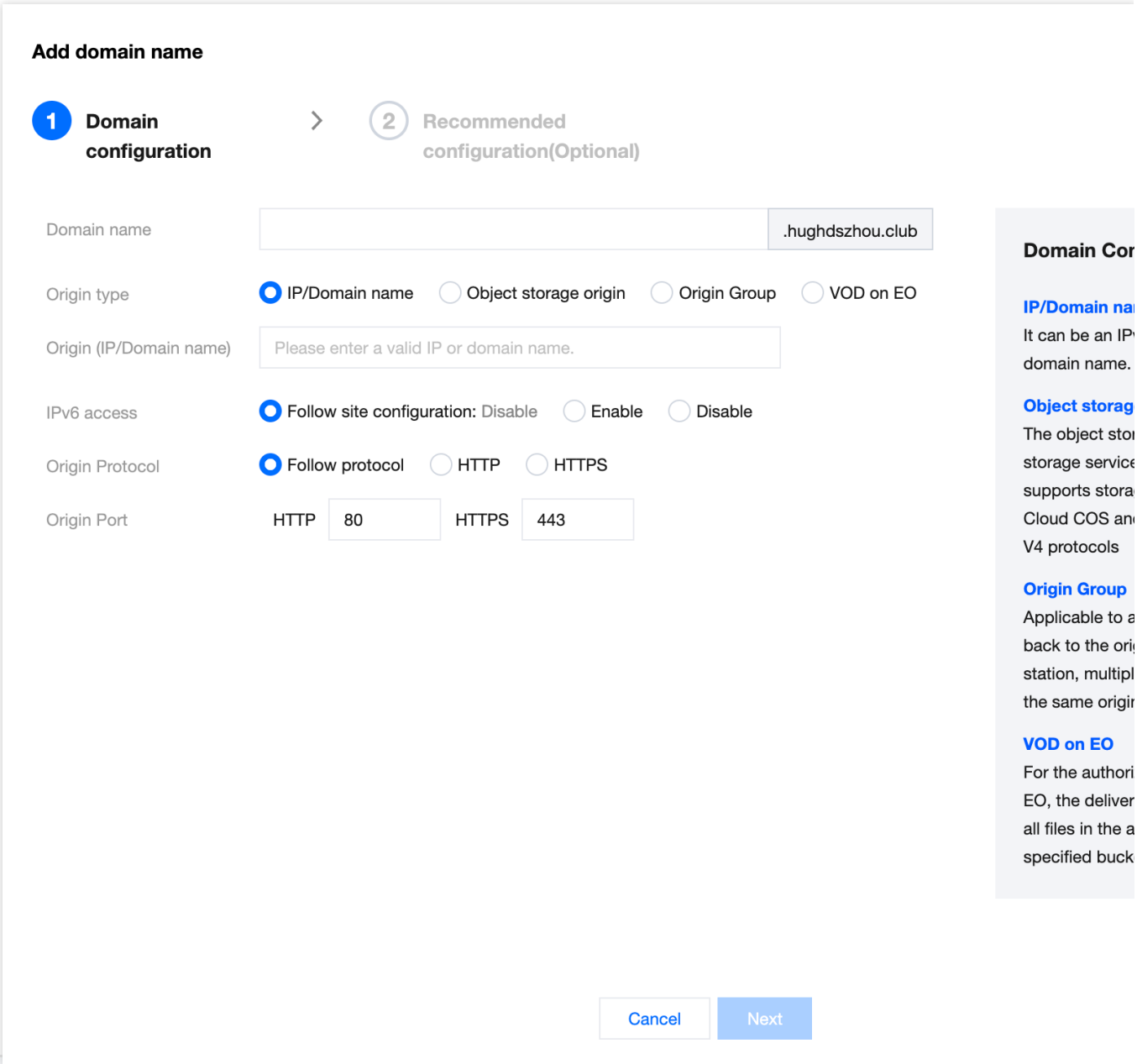
Directions

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.

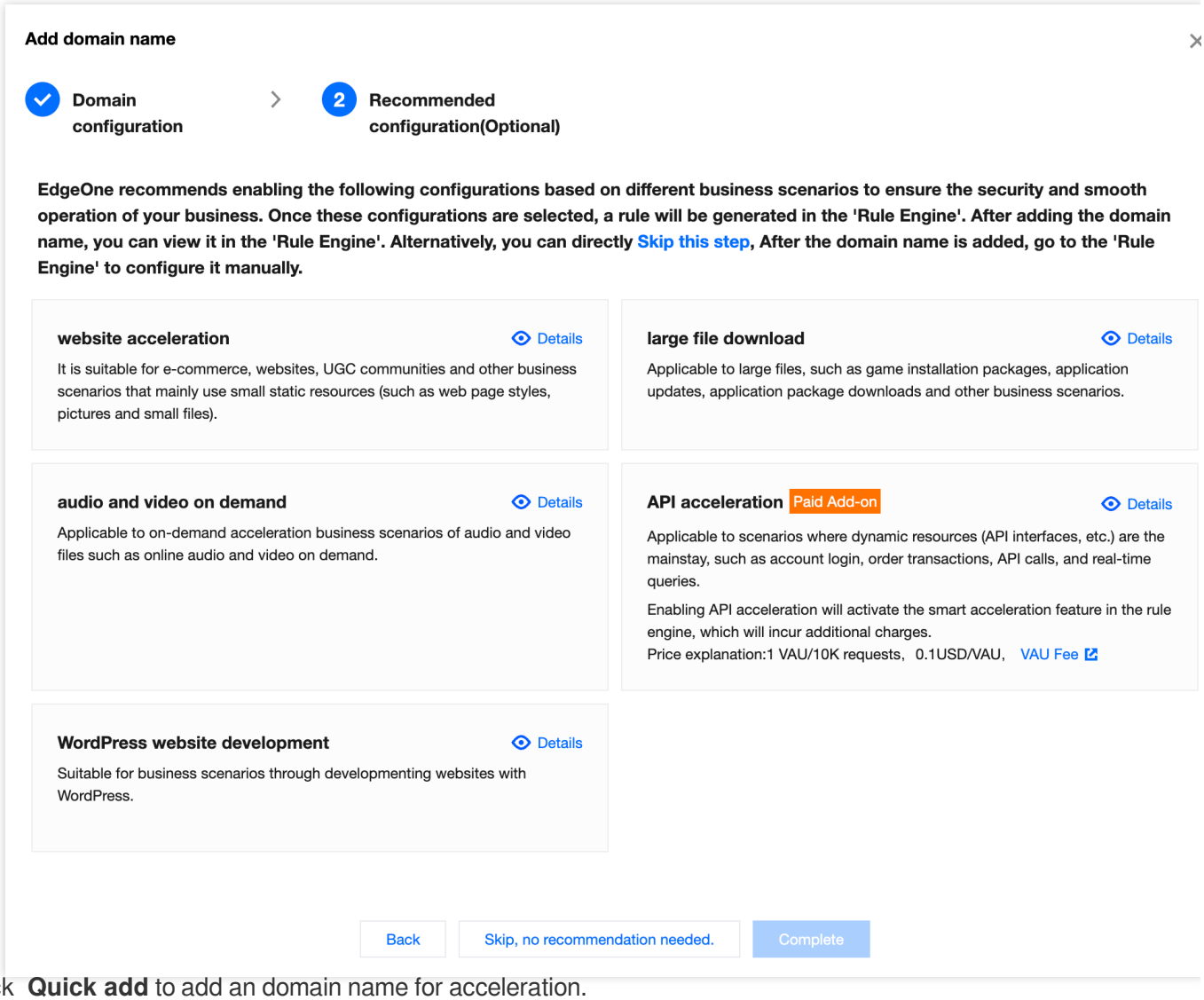
2. Specify the domain name to be connected to EdgeOne and specify the information of the corresponding origin. Then, click **Next**.



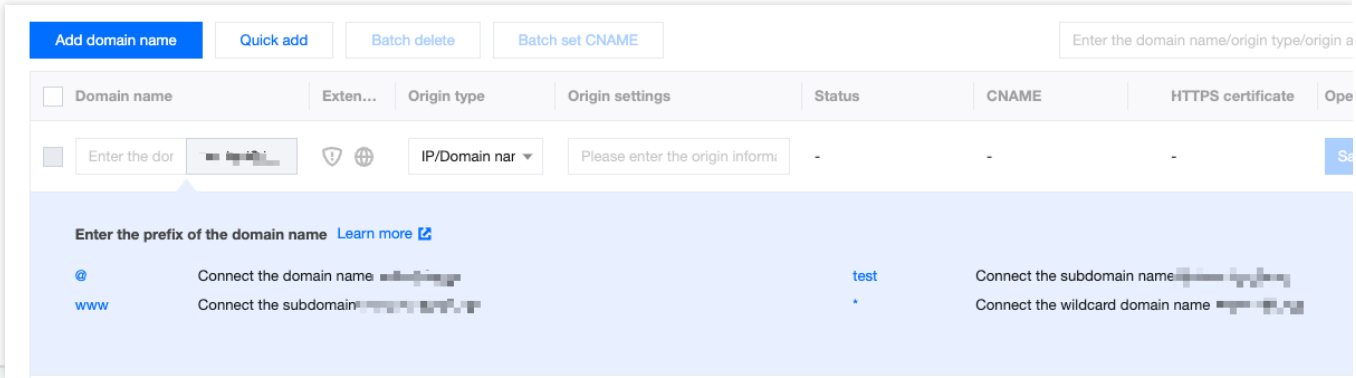
Item	Description
Domain name for acceleration	The domain name accessible to the client. You can enter the value of the host record. EdgeOne supports connecting wildcard domain names. If you want to access the root domain, enter `@`. For example, if the domain name is `www.example.com`, enter `www`.
Origin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

	Object storage origin: 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. **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.
IPv6 access	Select whether to enable support for access via IPv6. Refer to the document: IPv6 Access.
Origin-pull protocol	Choose the access protocol supported by your origin. Options include: **Follow protocol:** The protocol used during origin-pull is identical to the user's access request protocol. **HTTP**: The HTTP protocol is used for origin-pull. **HTTPS**: The HTTPS protocol is used for origin-pull.
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**.



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.

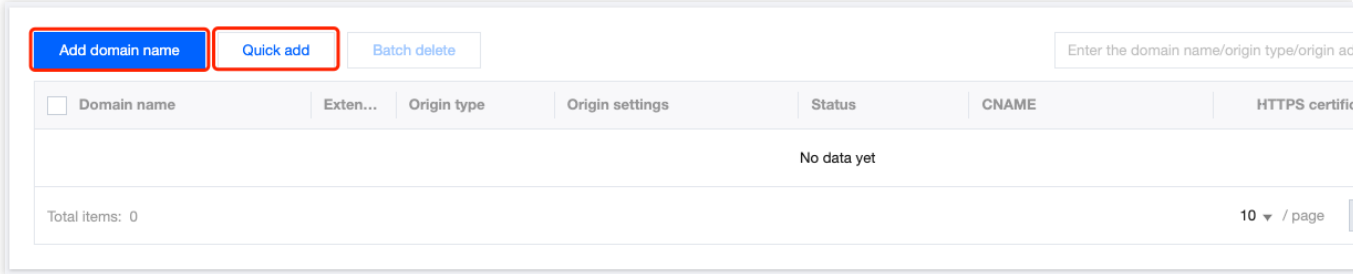


Item	Description
Domain name for acceleration	The domain name accessible to the client. You can enter the value of the host record. EdgeOne supports connecting wildcard domain names. If you want to access the root domain, enter `@` . For example, if the domain name is `www.example.com` , enter `www`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

Origin settings	Origin is the address of the resource that is accessed when the client initiates a request. Options: **IP/Domain name**, **Object storage origin**, and **Origin group**. **IP/Domain name**: 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. 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**.

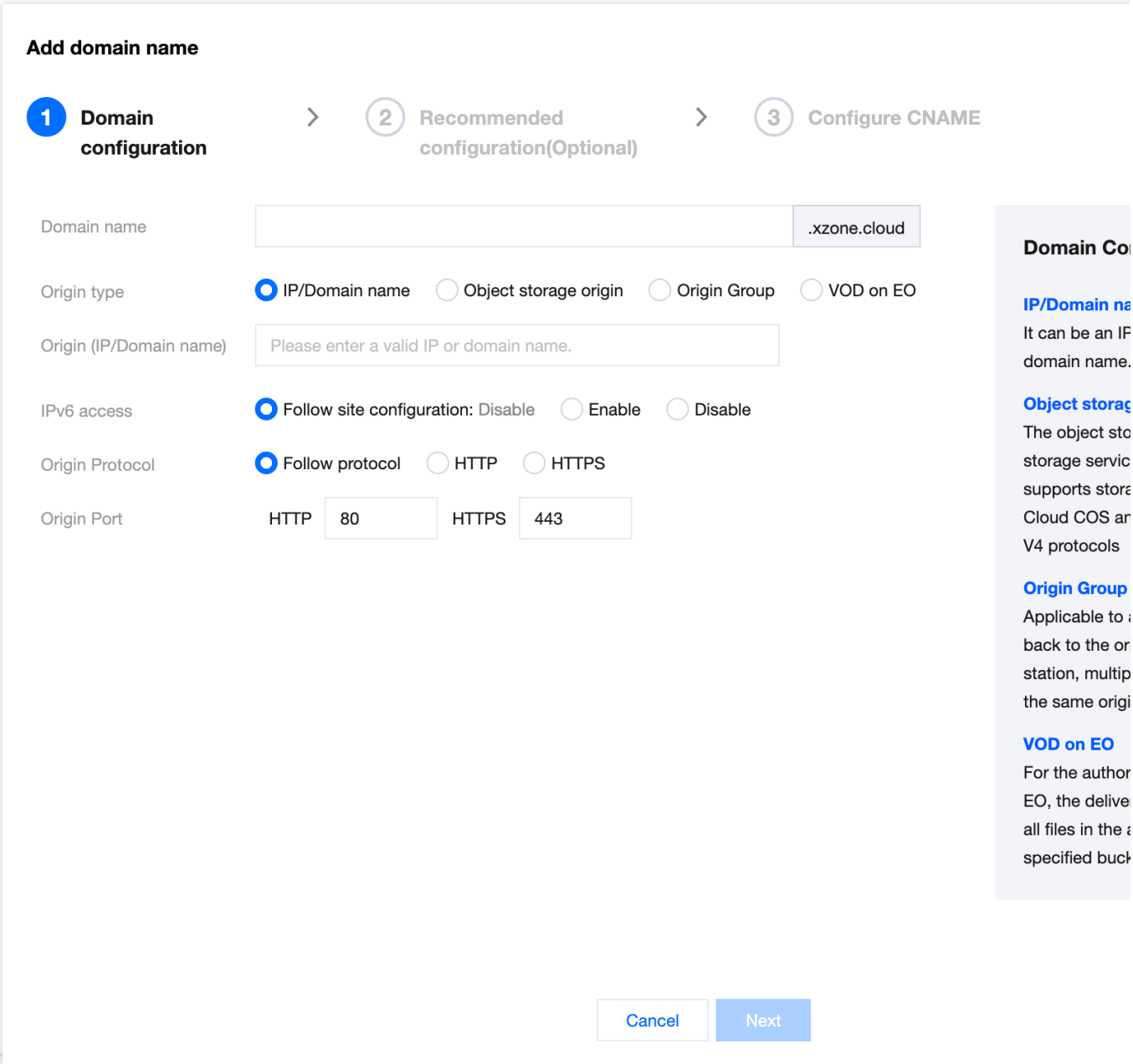


Add domain name

Quick add

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

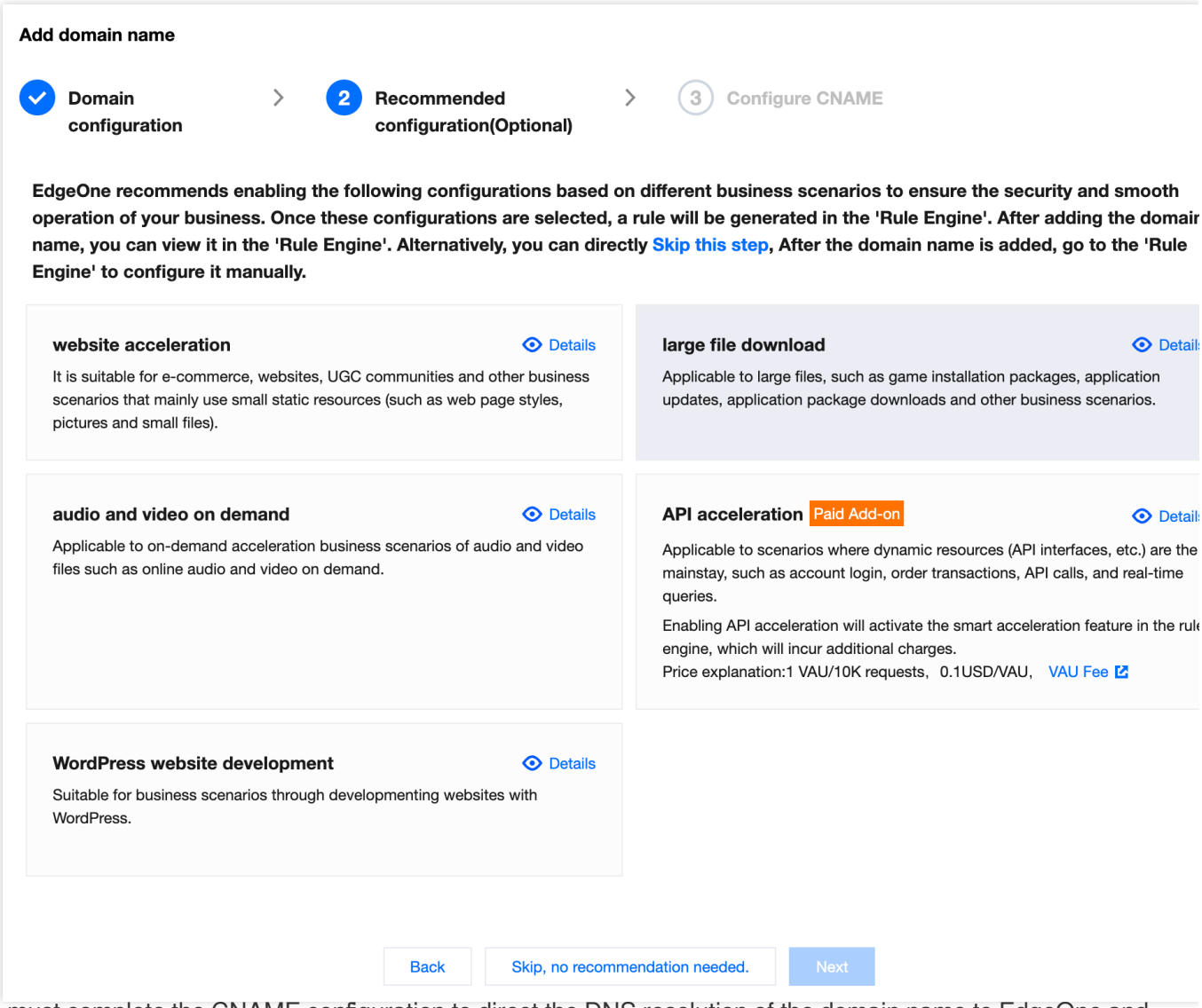
2. Specify the domain name to be connected to EdgeOne and specify the information of the corresponding origin. Then, click **Next**.



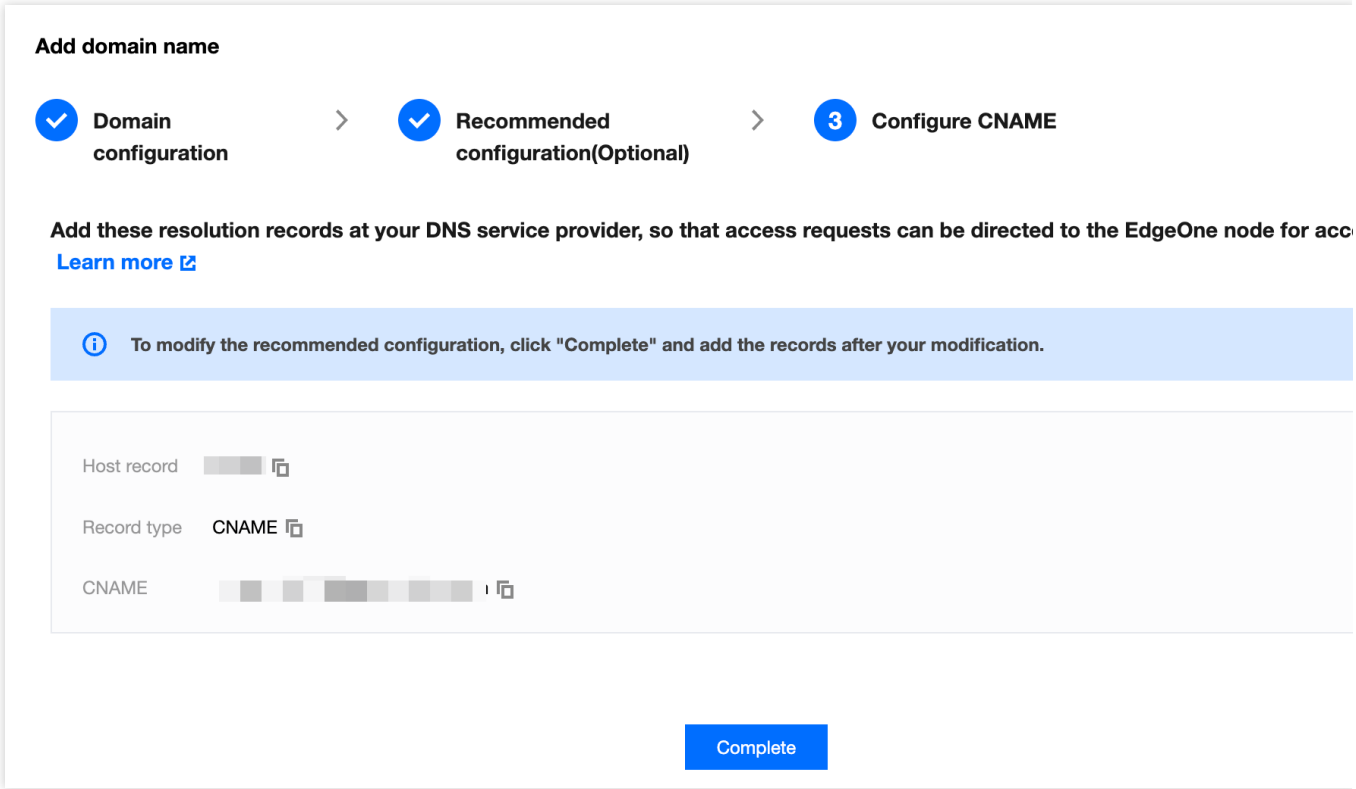
Item	Description
Domain name for acceleration	The domain name accessible to the client. You can enter the value of the host record. EdgeOne supports connecting wildcard domain names. If you want to access the root domain, enter `@`. For example, if the domain name is `www.example.com`, enter `www`.
Origin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

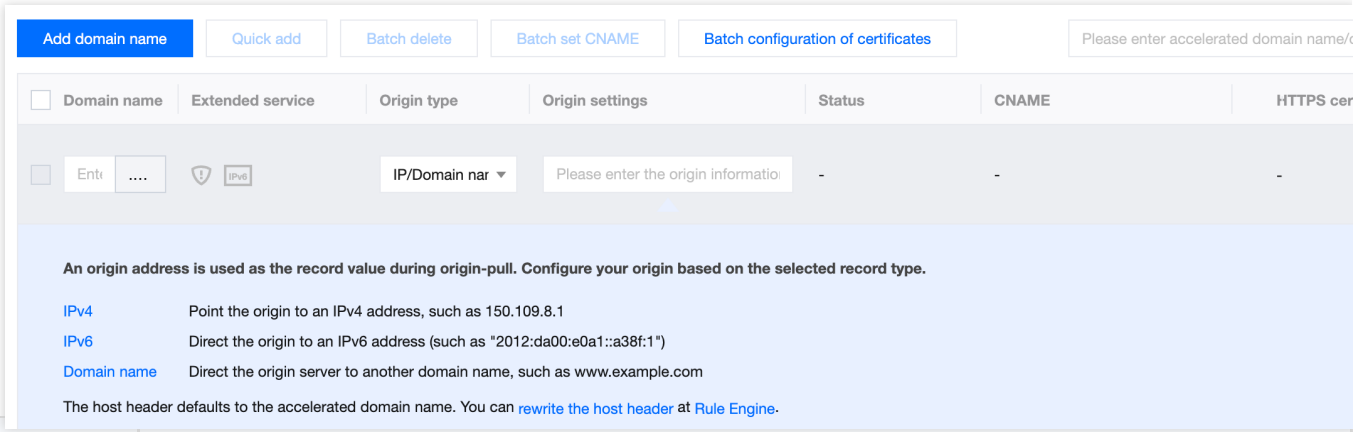


4. You must complete the CNAME configuration to direct the DNS resolution of the domain name to EdgeOne and then enable domain acceleration. EdgeOne will assign a CNAME address to the domain name. Please visit the DNS provider and configure CNAME records for the domain name.



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

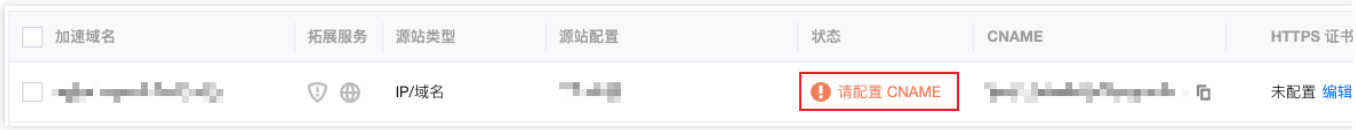
1. Click **Quick add** to add an domain name for acceleration.
2. Specify the domain name to be connected to EdgeOne and specify the information of the corresponding origin.



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: **IP/Domain name**, **Object storage origin**, and **Origin group**. **IP/Domain name**: 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.

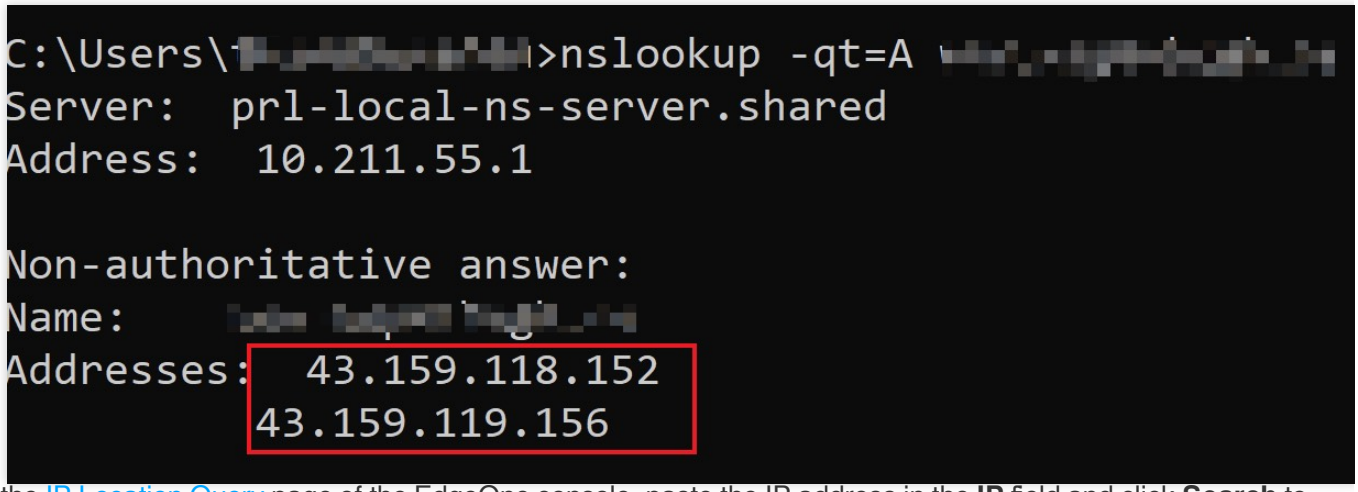
3. Click **Save**.
4. You must complete the CNAME configuration to direct the DNS resolution of the domain name to EdgeOne and then enable domain acceleration. EdgeOne will assign a CNAME address to the domain name. Please visit the DNS provider and configure CNAME records for the domain name.



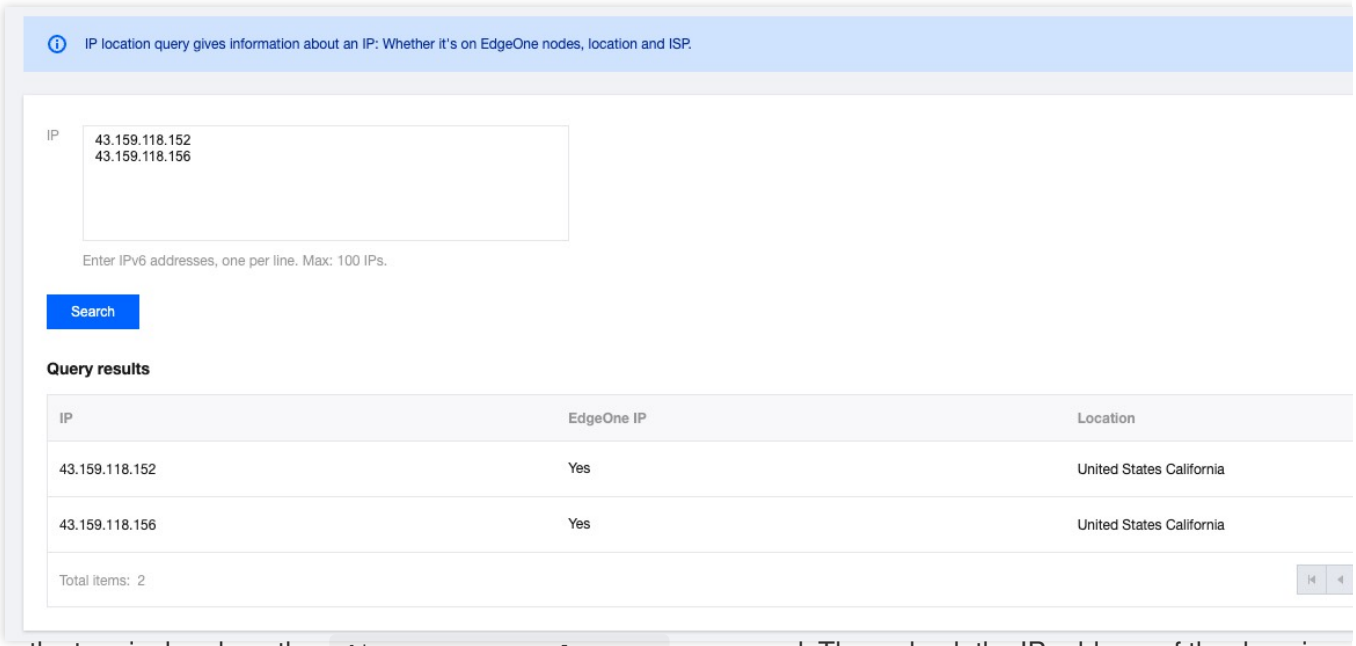
Verifying Domain Name Acceleration

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

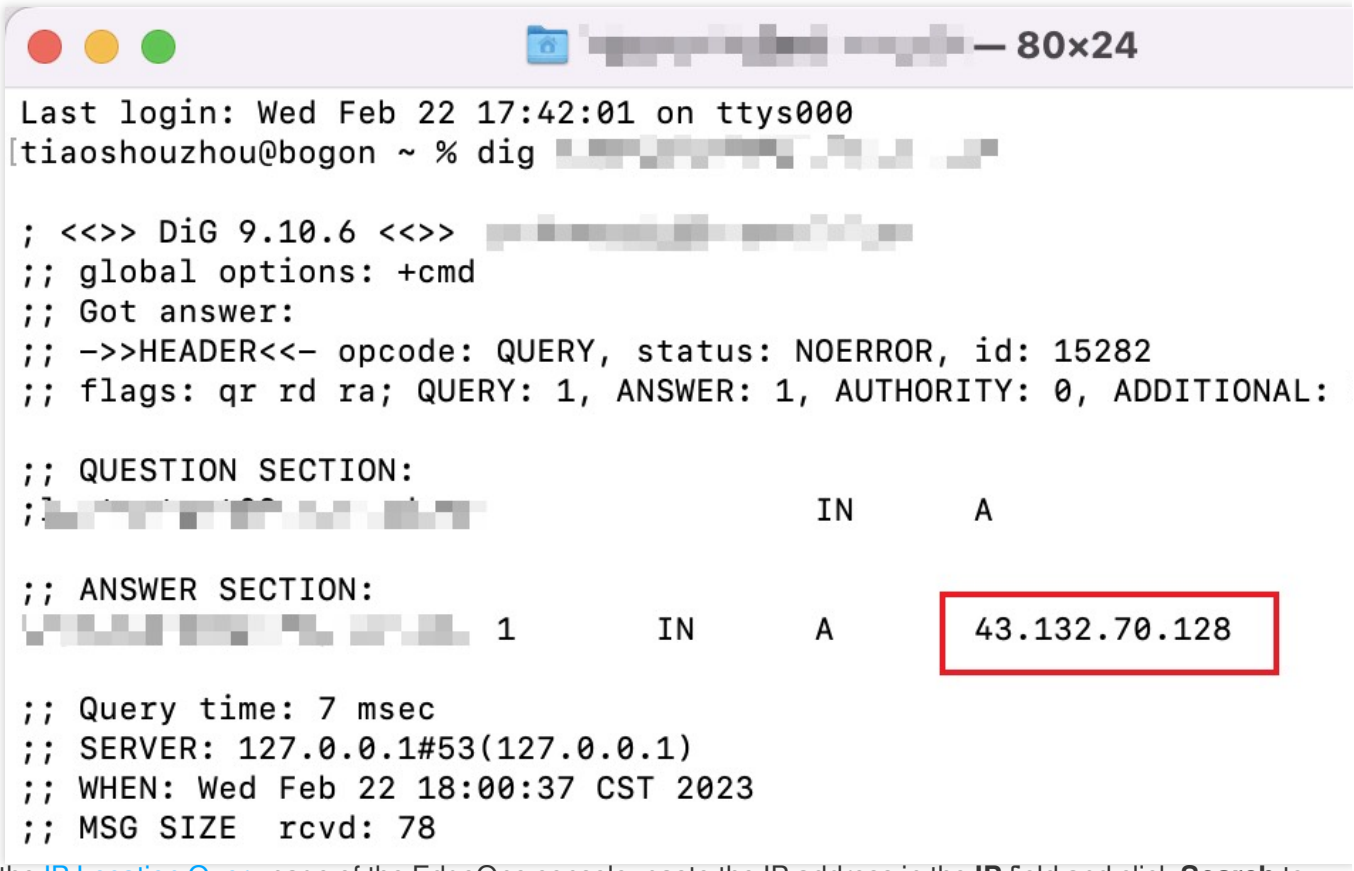
1. Open the command prompt and run the `nslookup -qt=A www.example.com` command. Then, check the IP address of the domain obtained by the A record resolution.



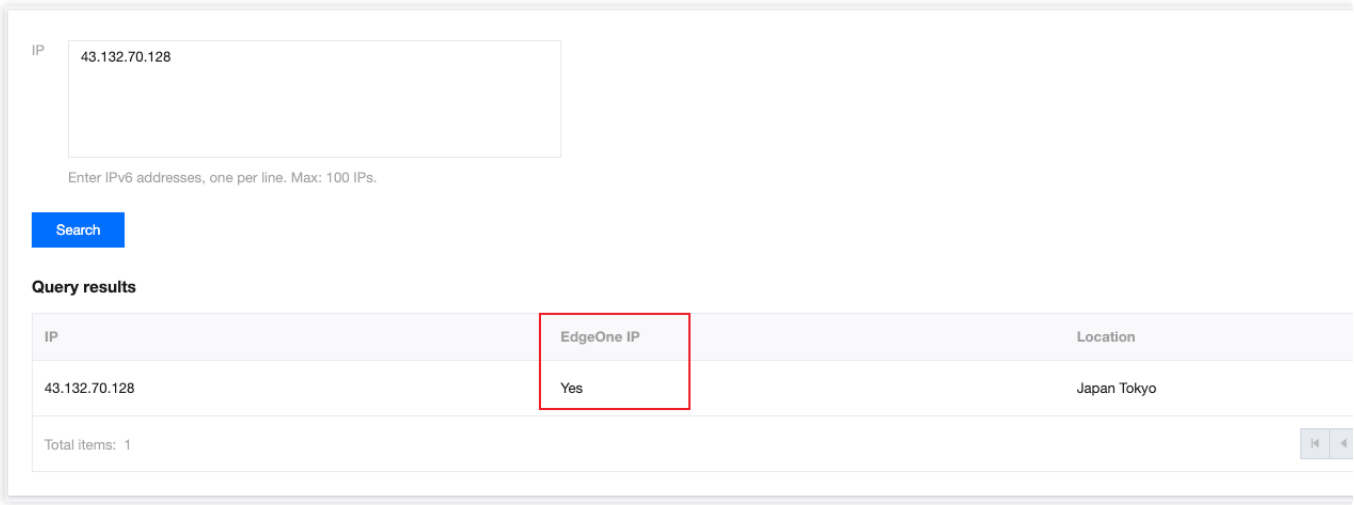
2. On the IP Location Query page of the EdgeOne console, paste the IP address in the **IP** field and click **Search** to check whether the IP address is on EdgeOne. If yes, DNS of the accelerated domain has been switched to EdgeOne.



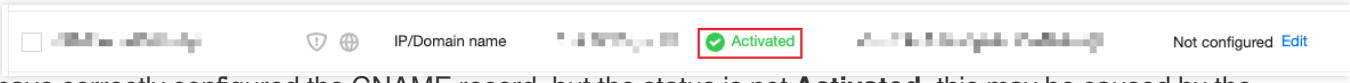
1. Open the terminal and run the `dig www.example.com` command. Then, check the IP address of the domain obtained by the A record resolution.



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



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

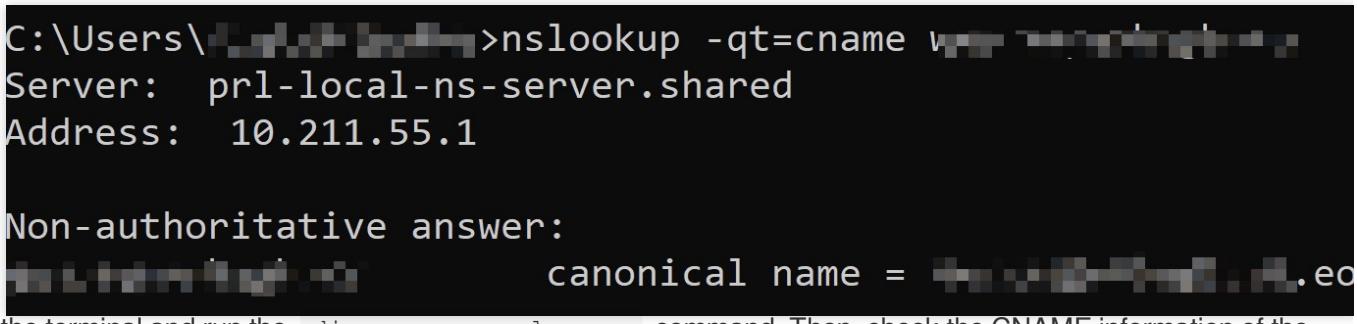


If you have correctly configured the CNAME record, but the status is not **Activated**, this may be caused by the CNAME resolution latency of the DNS provider. In this case, you can manually verify the connection as instructed below.

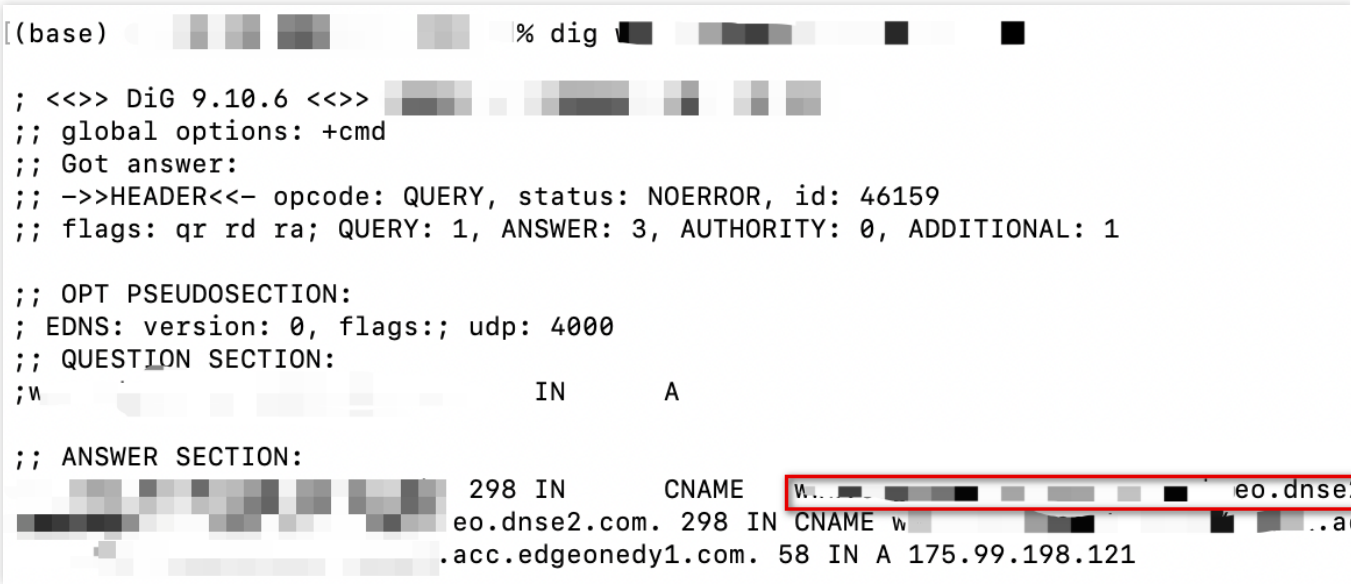
Windows

Mac/Linux

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



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



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 yourownership 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 yourownership 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.

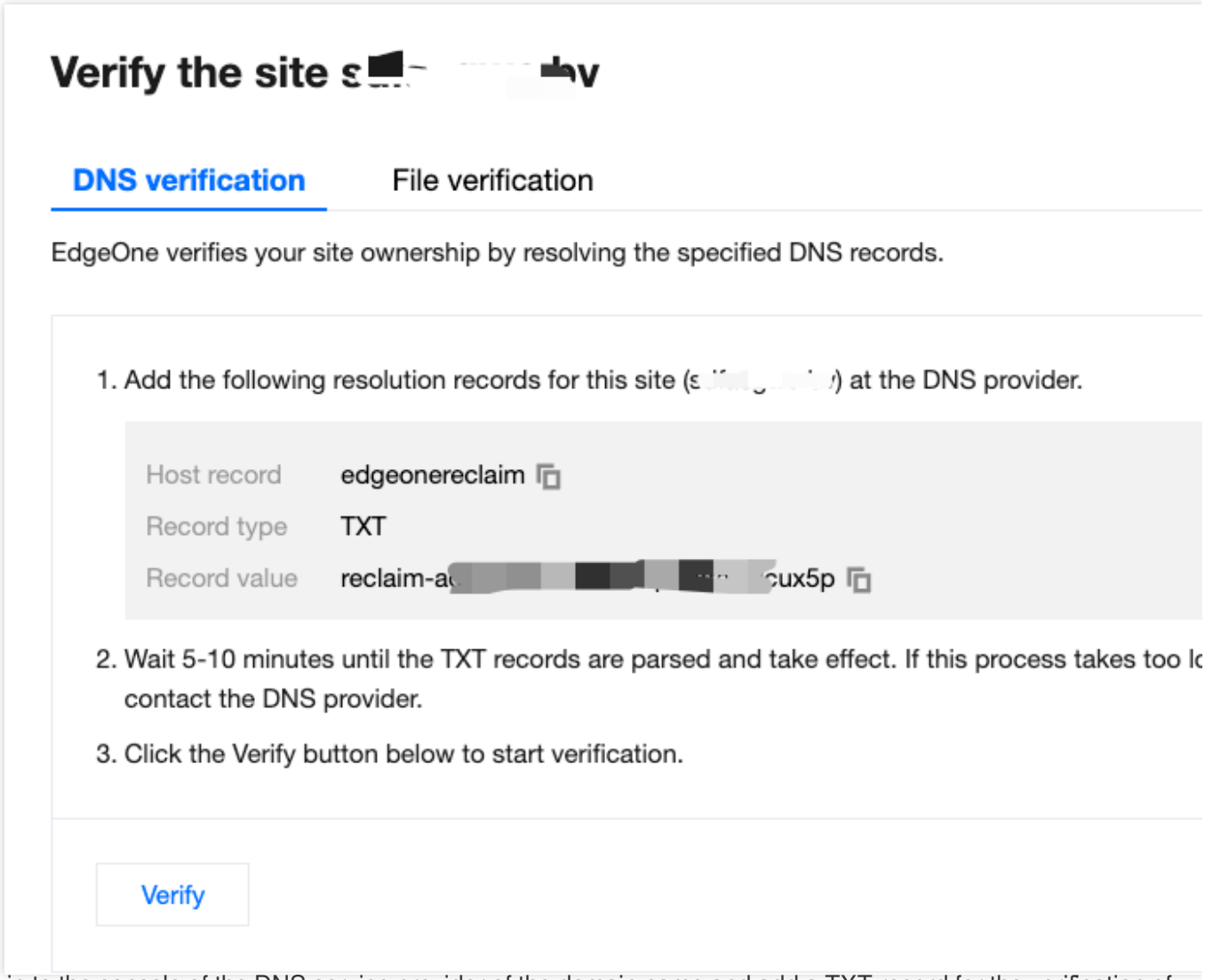
Steps to Verify the Site or Domain Name Ownership

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.



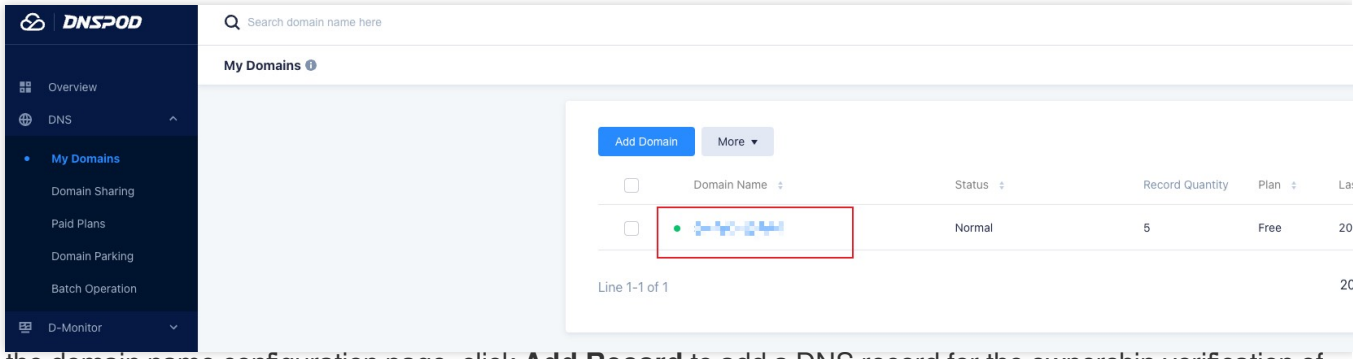
2. Log in to the console of the DNS service provider of the domain name and add a TXT record for the verification of the site ownership. The following examples describe how to add the TXT record in the console of different DNS service providers.

Tencent Cloud DNSPod

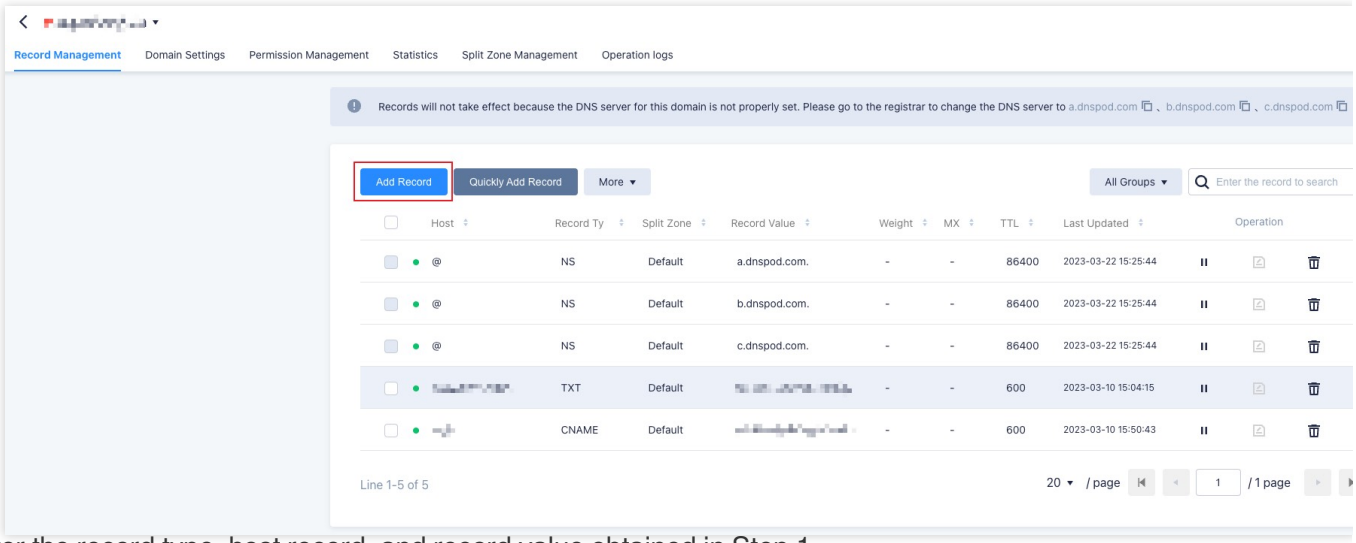
Alibaba Cloud DNS

Godaddy

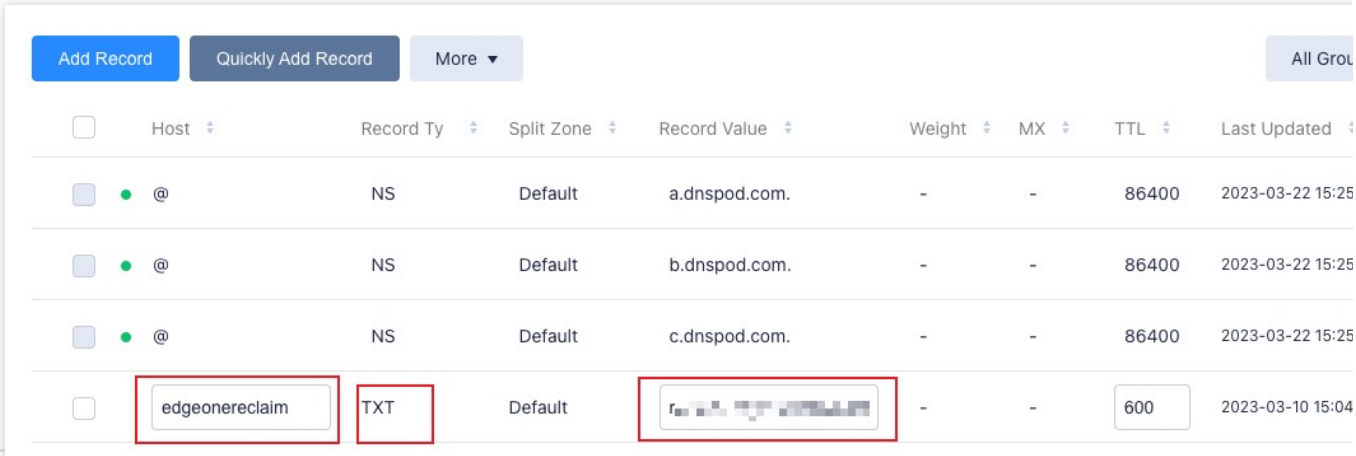
a. Log in to the DNSPod console and click **My Domains** in the left sidebar. On the page that appears, click the target domain name to enter its configuration page.



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



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



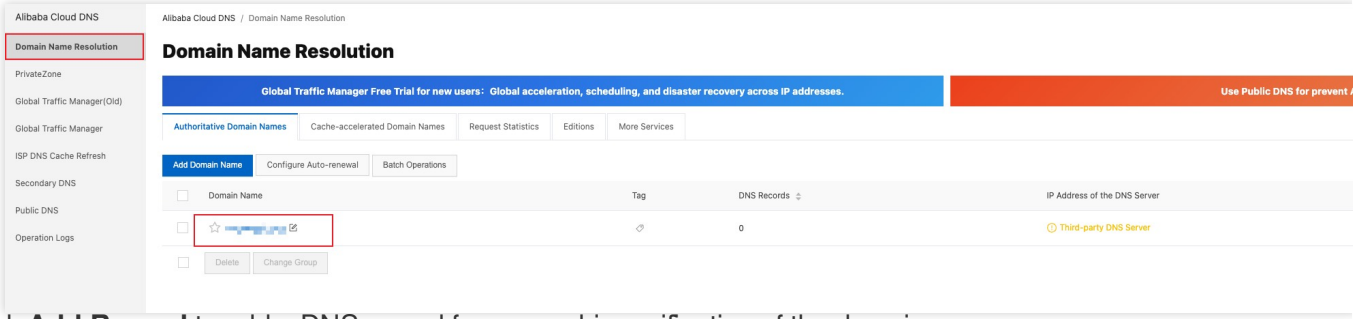
Parameter	Description
Record Type	TXT
Host	edgeonereclaim
Split Zone	Default

Text content	Enter the record value provided by EdgeOne
TTL	600

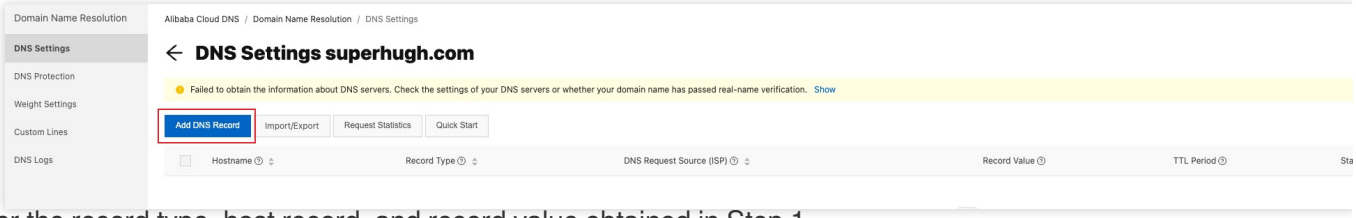
d. Click **OK**.

a. Log in to the Alibaba Cloud DNS console.

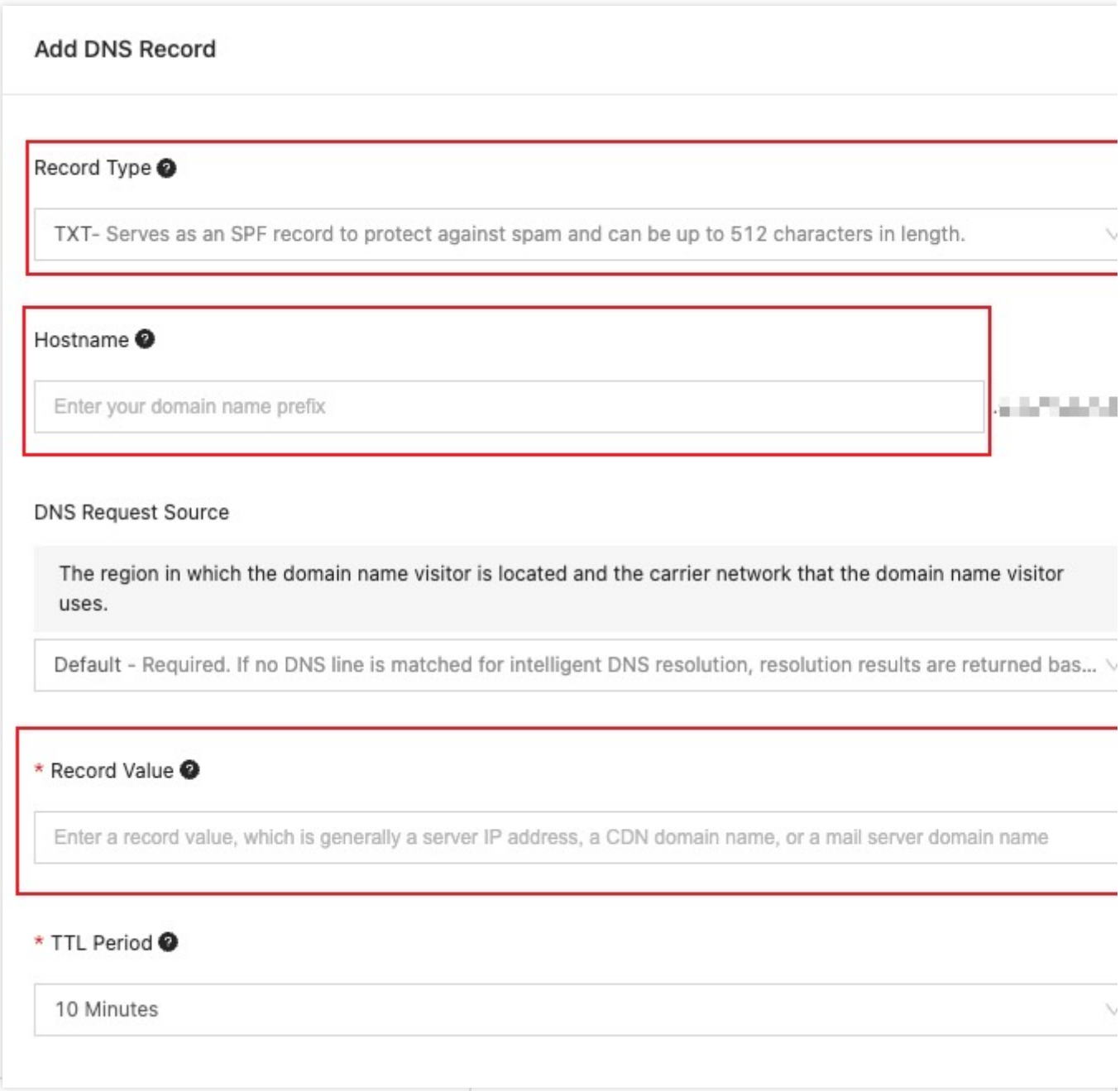
b. On the **Manage DNS** page, find the target domain name, and click **Configure** in the **Actions** column to go to the **DNS Settings** page.



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



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

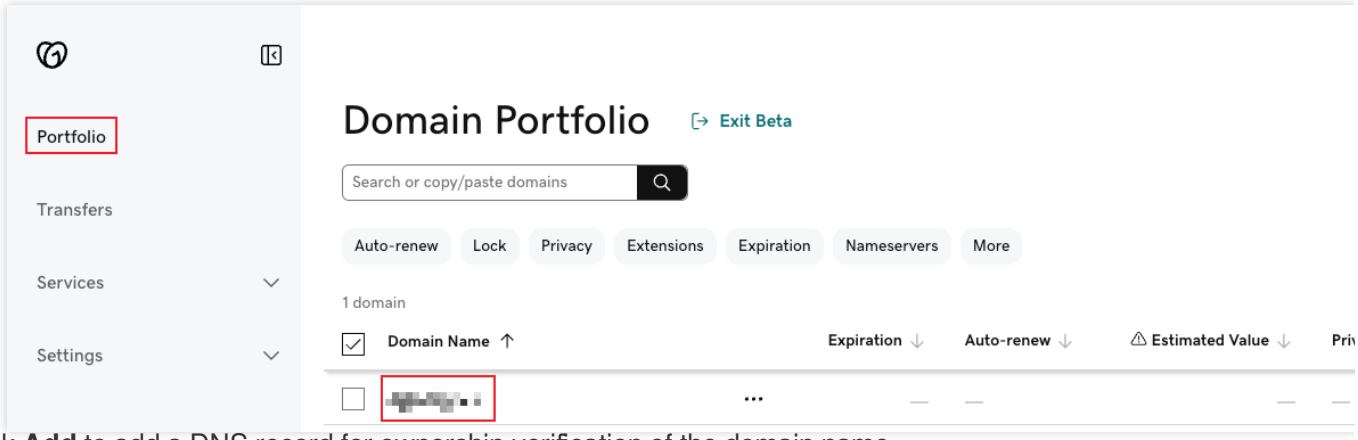


Parameter	Description
Type	TXT
Host	edgeonereclaim
ISP Line	Default
Value	Enter the record value provided by EdgeOne
TTL	10 minutes

d. Click **OK**.

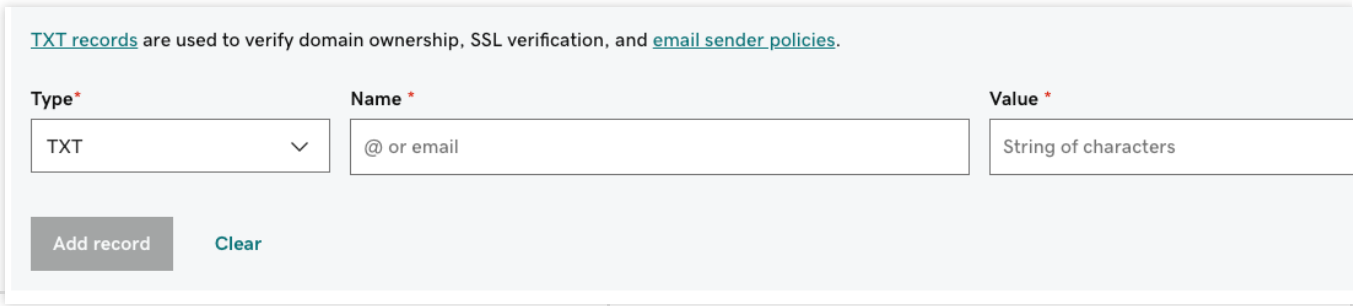
a. Log in to the Godaddy Domain Portfolio console.

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



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

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



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

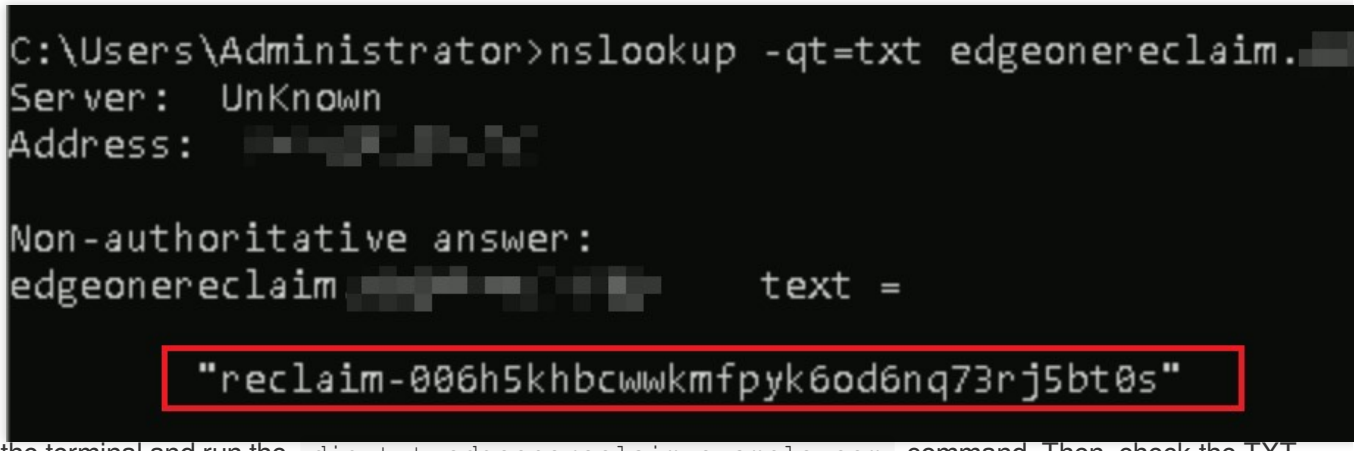
d. Click **Add Record**.

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

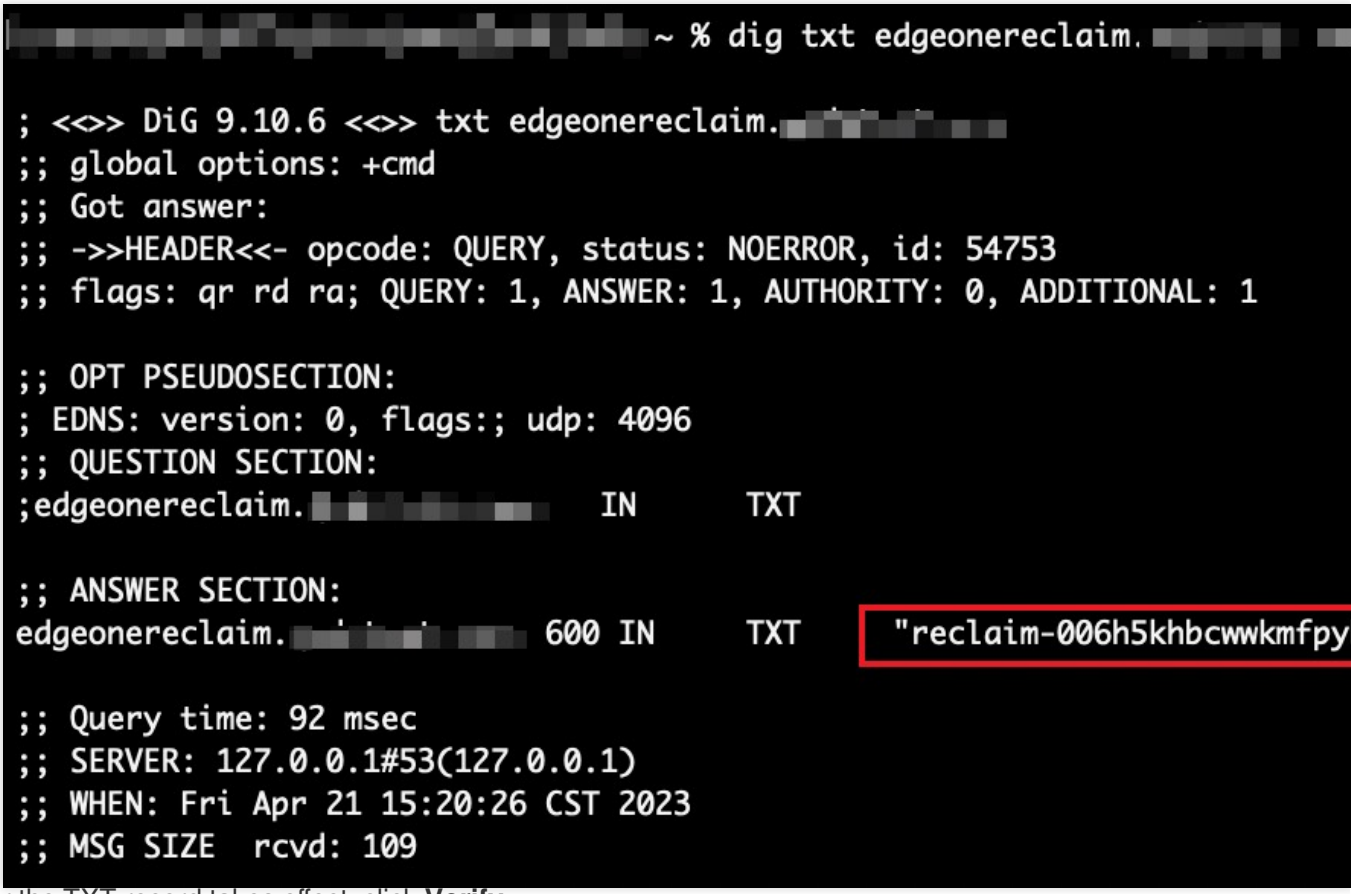
Windows

Mac/Linux

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

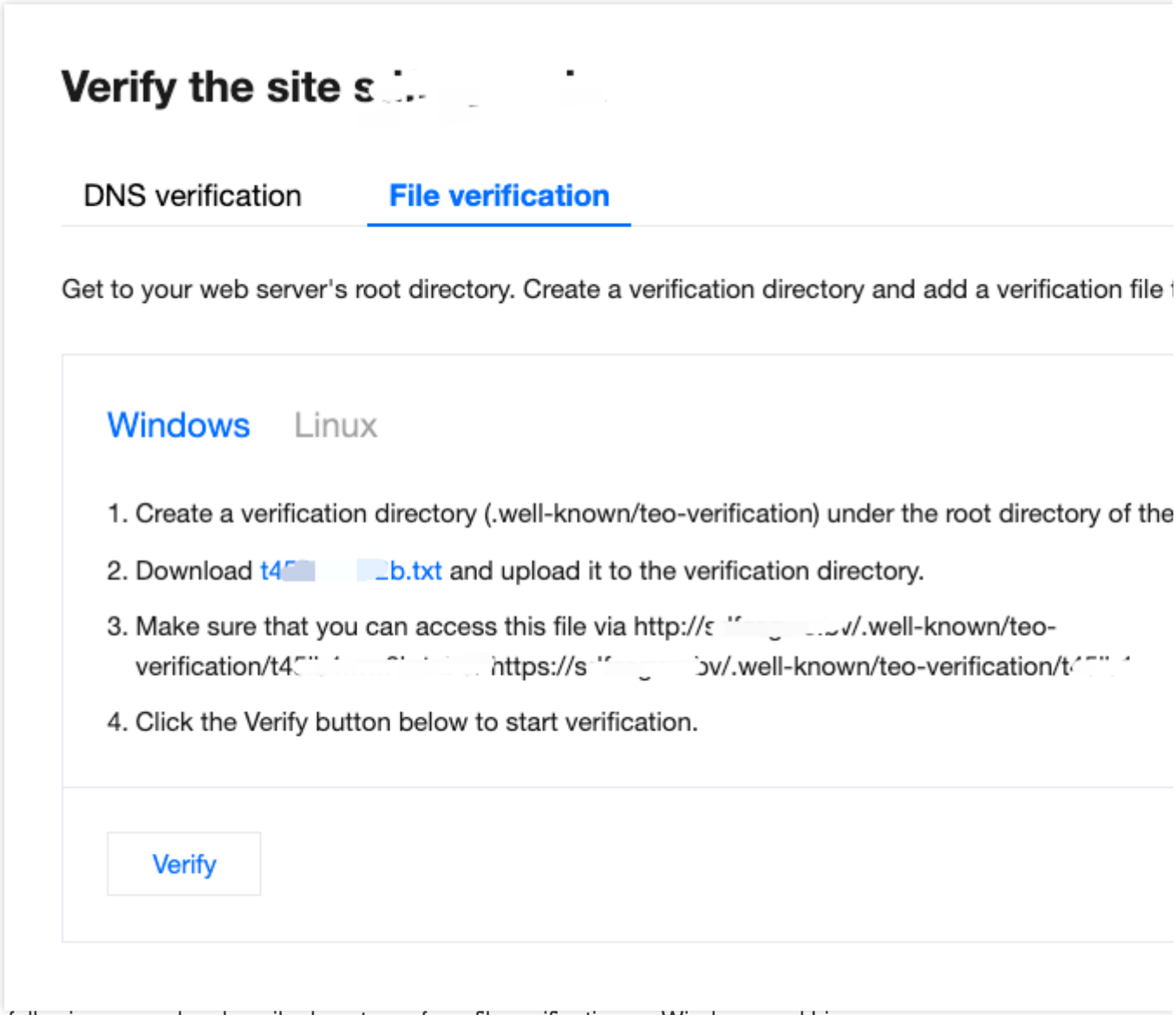


Open the terminal and run the `dig txt edgeonereclaim.example.com` command. Then, check the TXT record information of the domain. If the TXT record is the same as that provided by Step 1, the TXT record is effective.



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

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



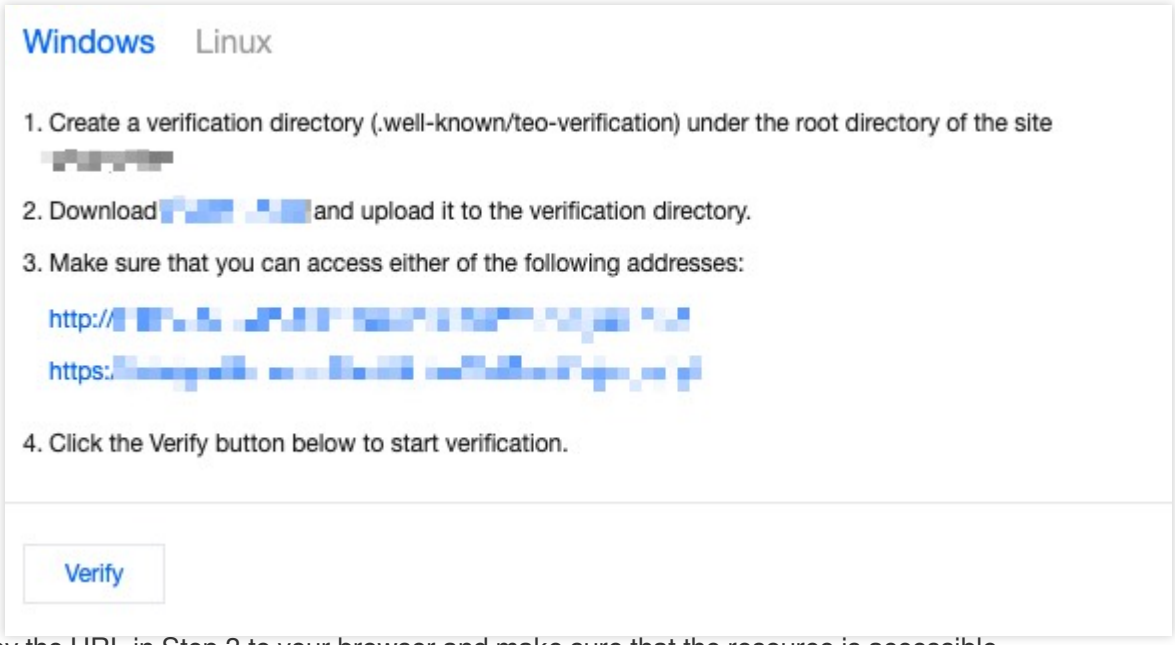
2. The following examples describe how to perform file verification on Windows and Linux.

Windows

Linux

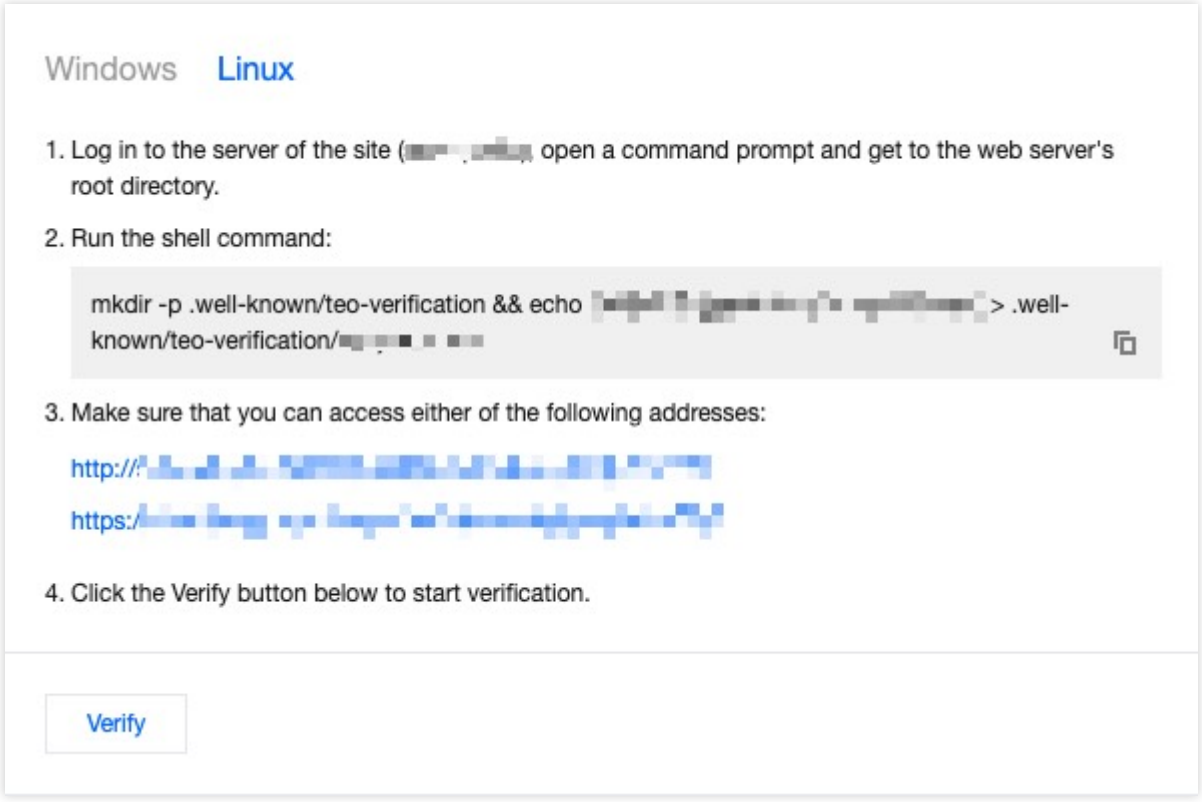
1. Go to the root directory of the server and create the verification directory `.well-known/teo-verification`.

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



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

1. Open a command window and get to the web server's root directory.
2. Copy the code in Step 2 to the command window and run it.



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

Modifying CNAME Records

Last updated：2023-07-06 16:24:53

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

Note:

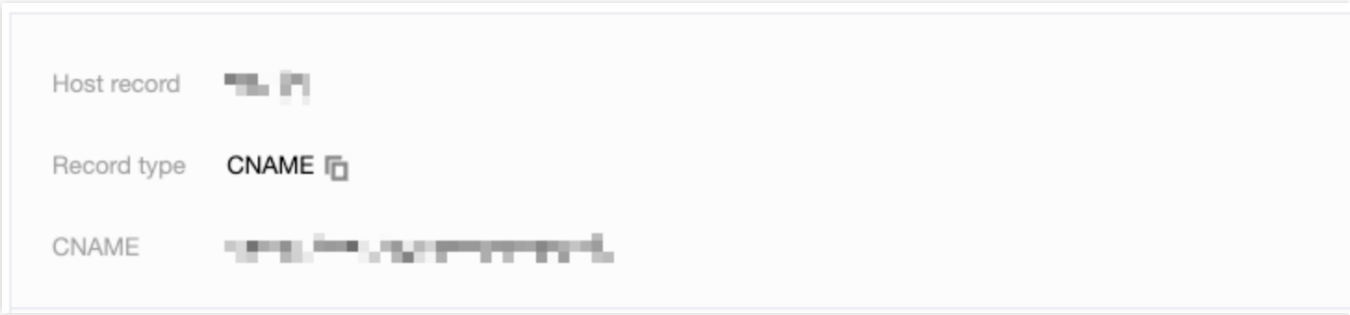
This is only required for sites connected via the CNAME. You don't need to do this for sites connected via the NS.

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.



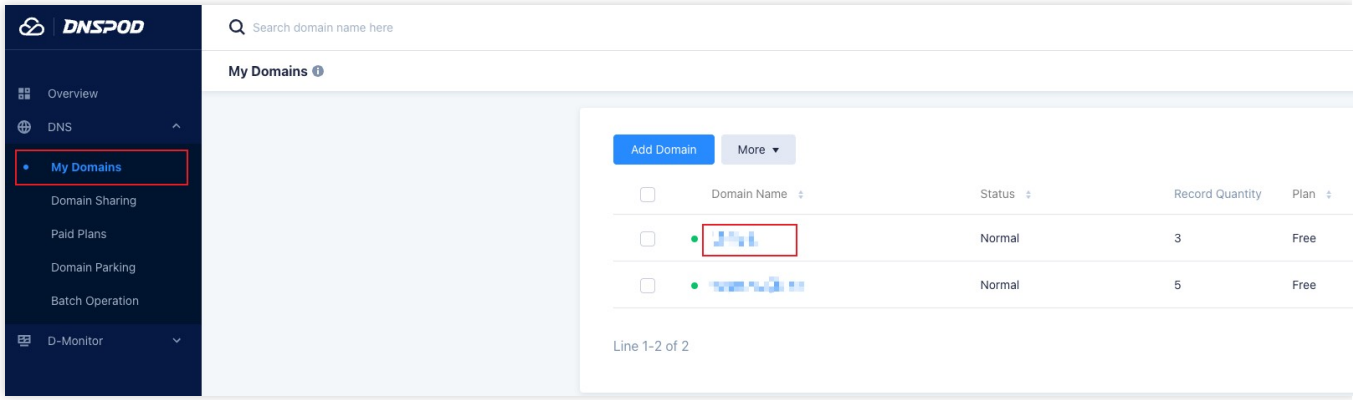
2. Go to the DNS service provider of the domain name and add a CNAME record. See below for examples for different DNS service providers.

Tencent Cloud DNSPod

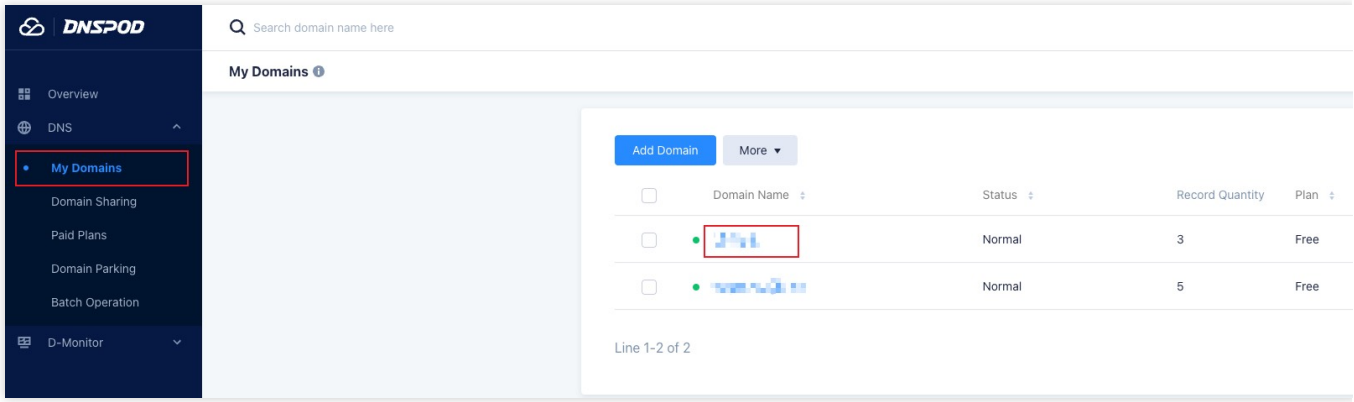
Alibaba Cloud DNS

Godaddy

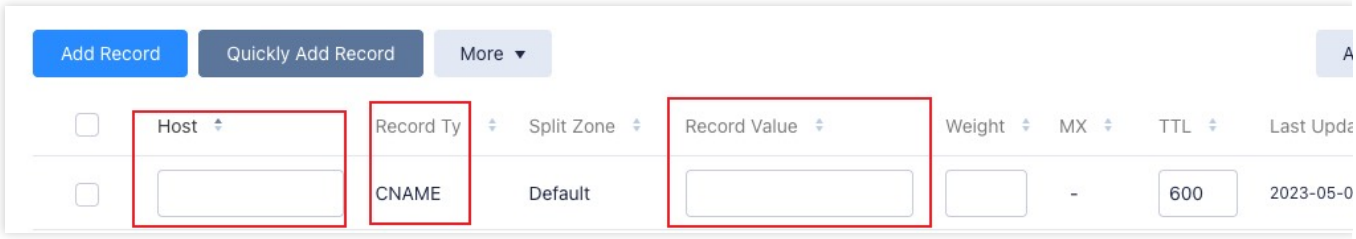
a. Log in to the DNSPod console. Find the domain to verify in **My Domains**. Click the domain to enter the domain name configuration page.



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.

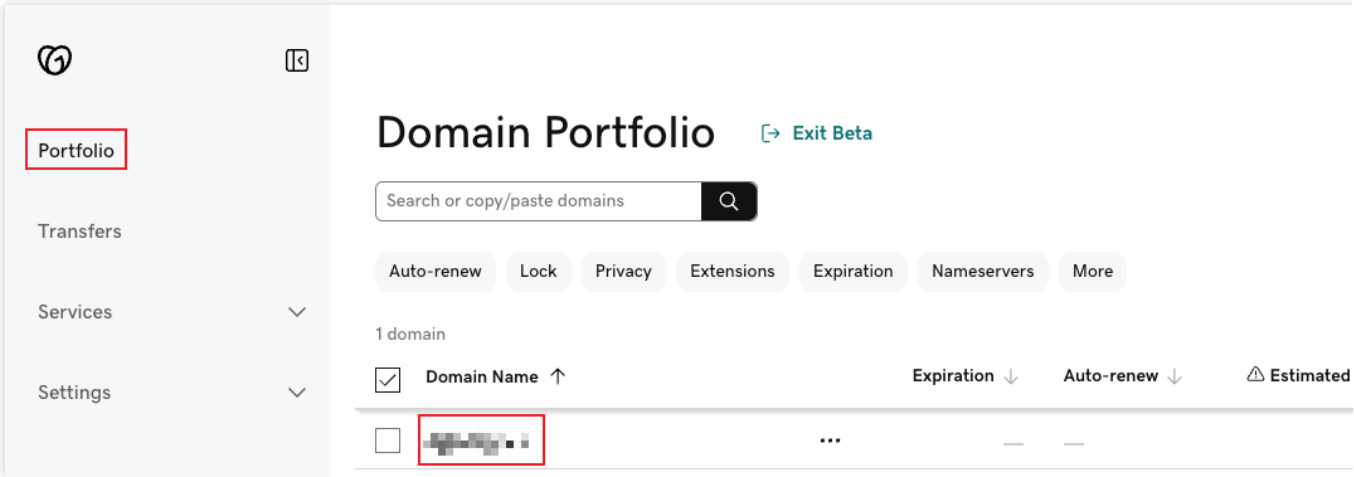
d. Enter the record type, host record, and record value obtained in Step 1.

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

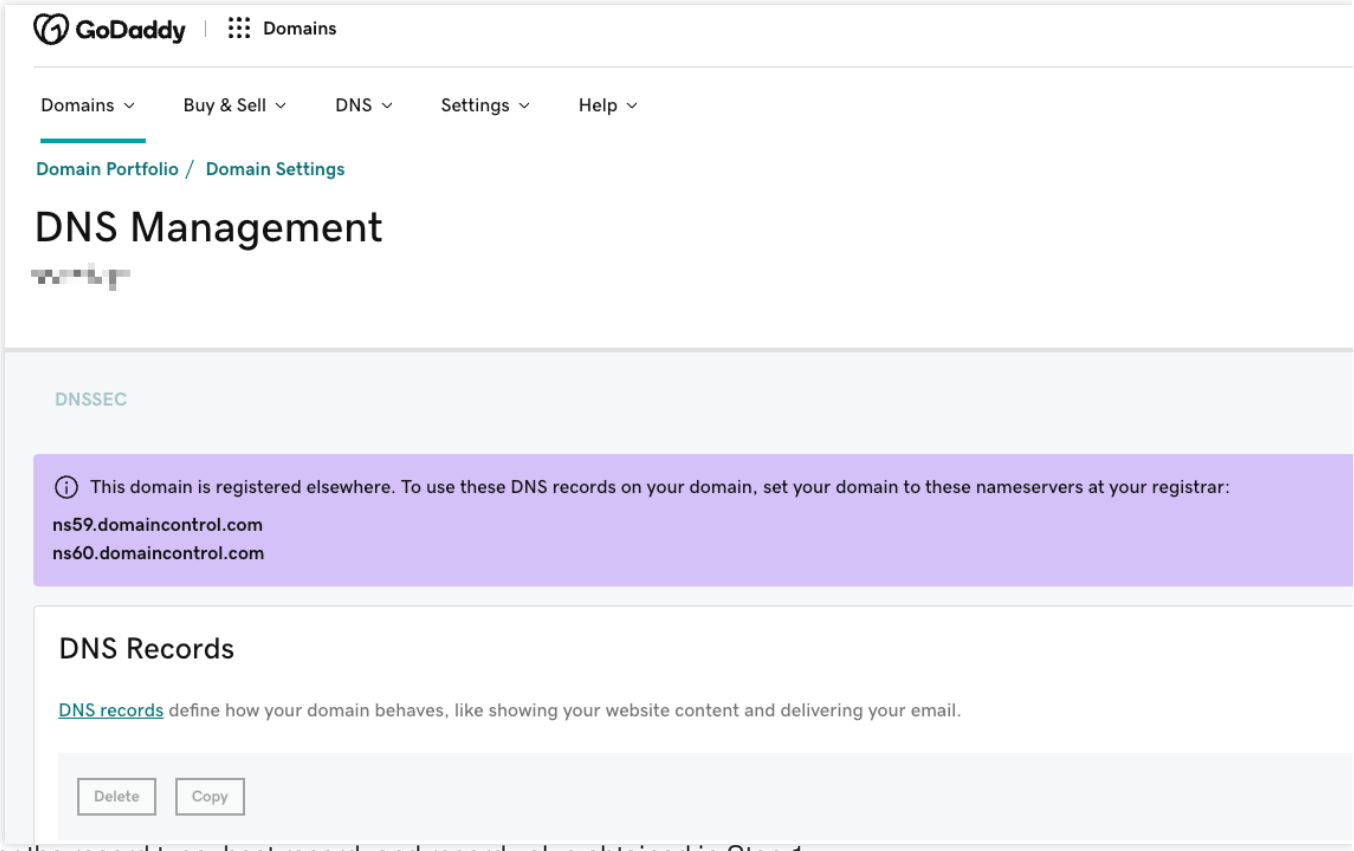
e. Click **OK**.

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.



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



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

Parameter 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**.

Verifying CNAME Records

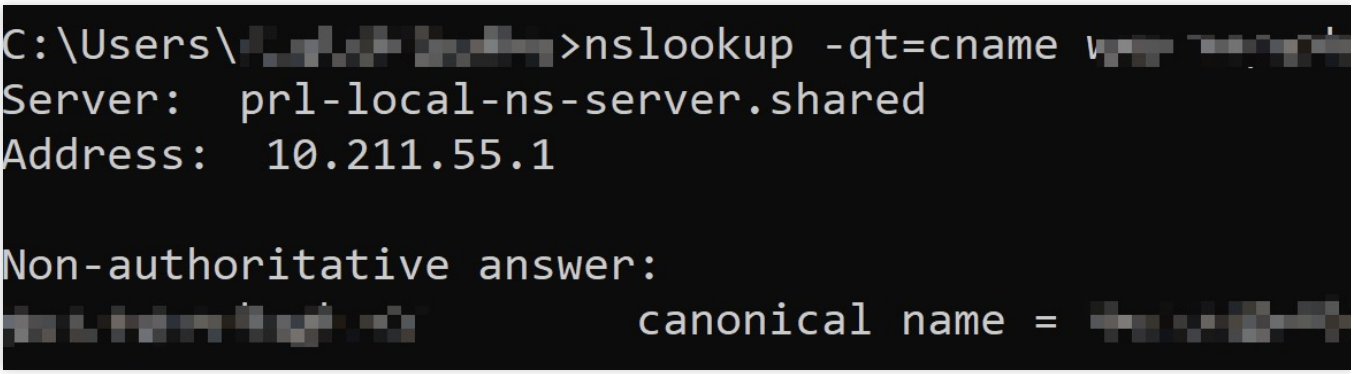
After you complete the CNAME configuration, EdgeOne automatically detects whether the CNAME configuration has taken effect. In the domain list, if the **Status** column of the accelerated domain is **Activated**, the domain is correctly configured and accelerated.

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:

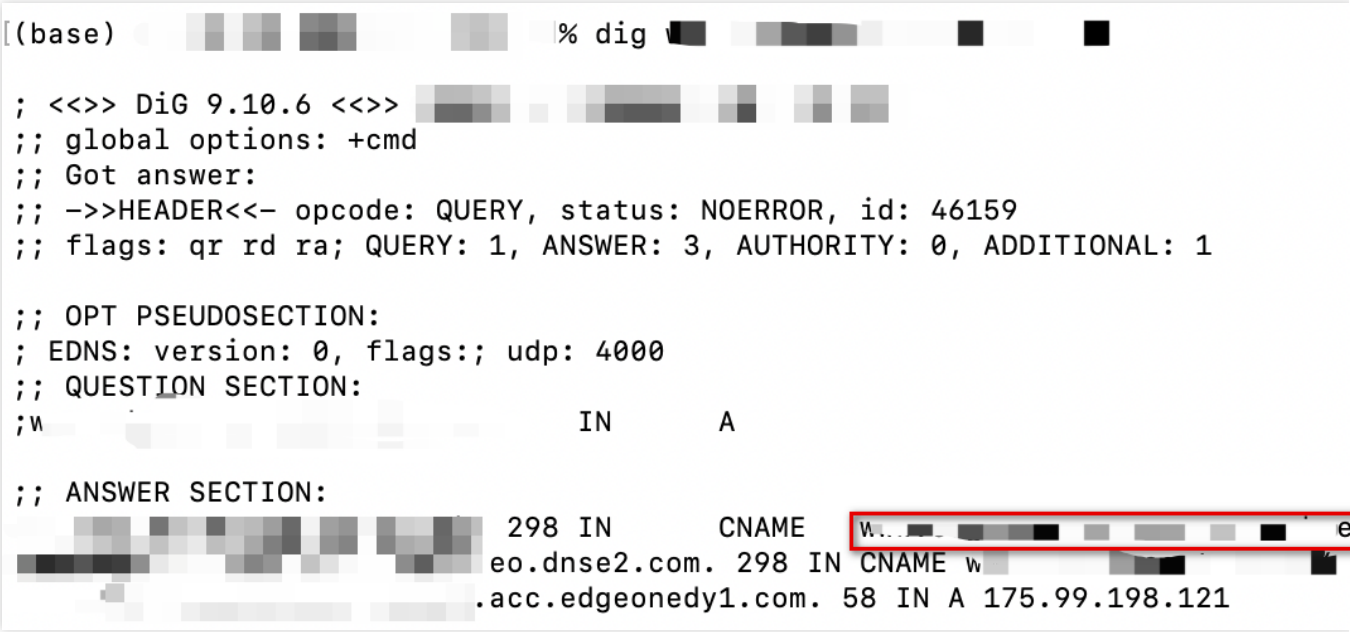
Windows

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.



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.



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.

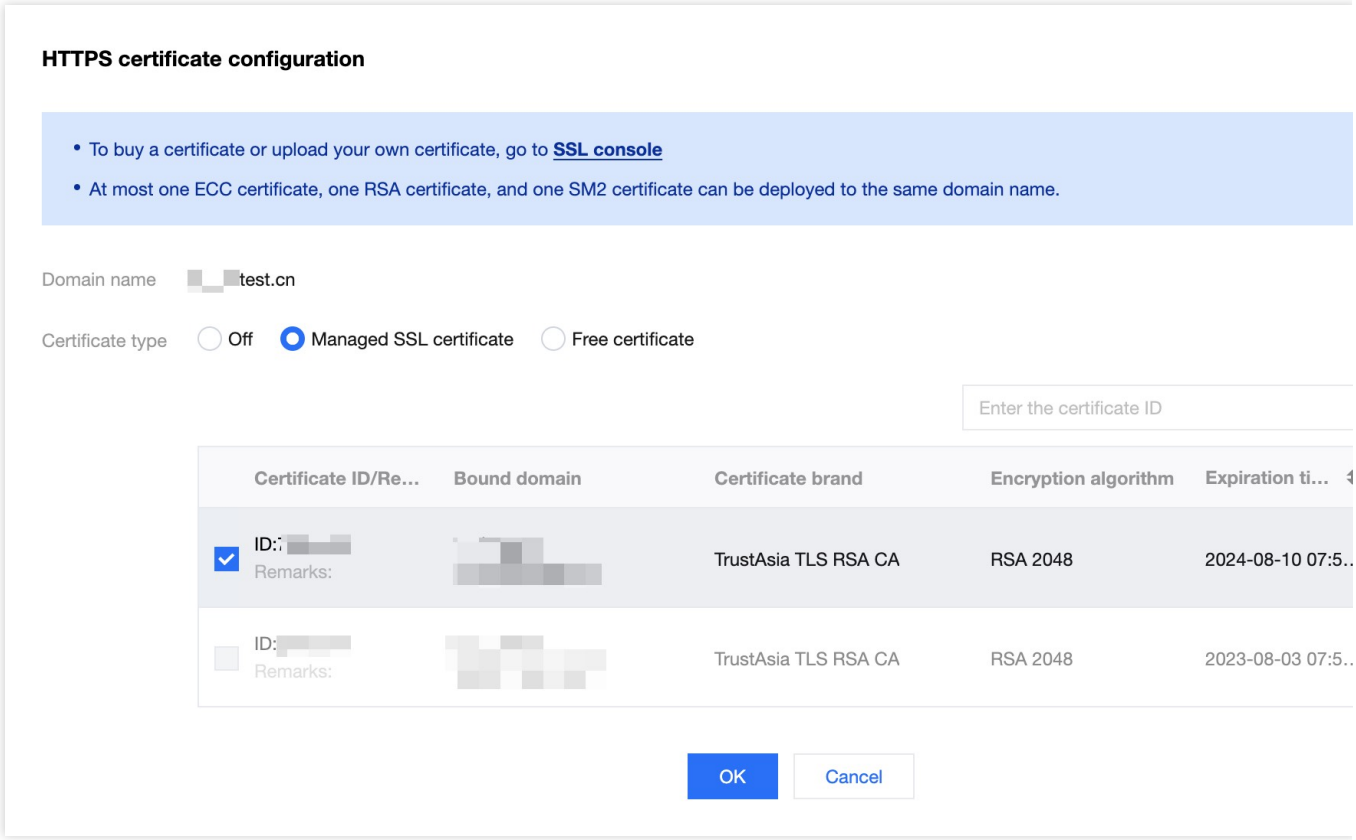
Deploying Certificate

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

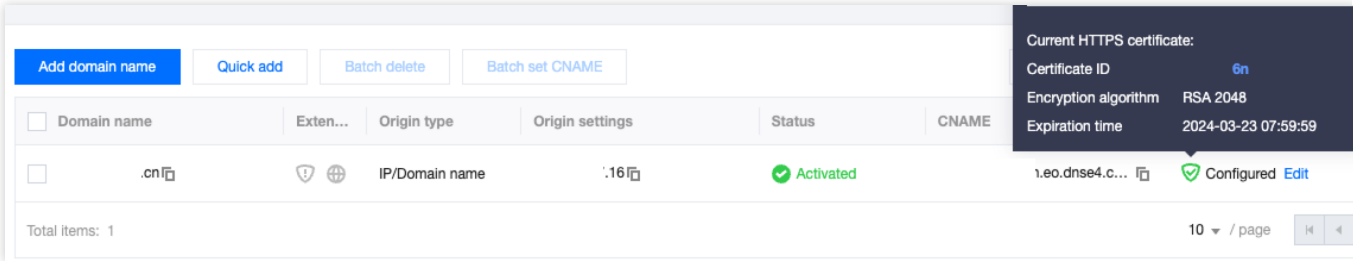
You can manage and use a self-owned certificate via the EdgeOne console as instructed below.
1. Log in to the EdgeOne console and click the target site in the site list to display second-level menus for site management.
2. In the left sidebar, click **Domain Name Service > Domain Management**.
3. In 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.



Note:

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

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

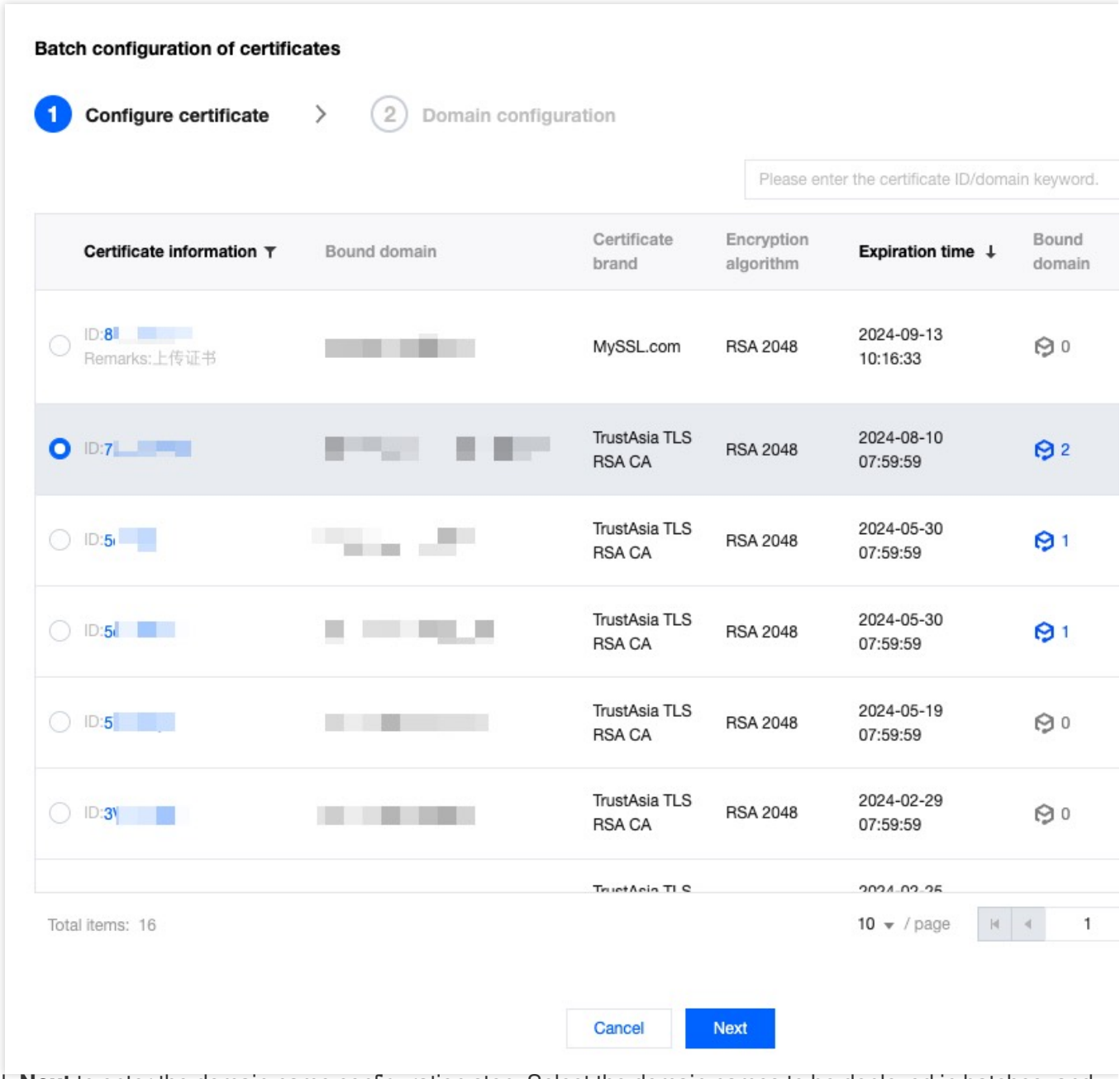


Scenario 2: Batch Certificate Configuration through EdgeOne console

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

1. Log in to the EdgeOne console, select the site to be configured through the site list, and enter the site management secondary menu.
2. In the left navigation bar, click **Domain Name Service > Domain Management.**

3. On the Domain Management page, click **Batch Configuration of Certificate**, and in the steps of batch configuration certificate, select the certificate to be configured.

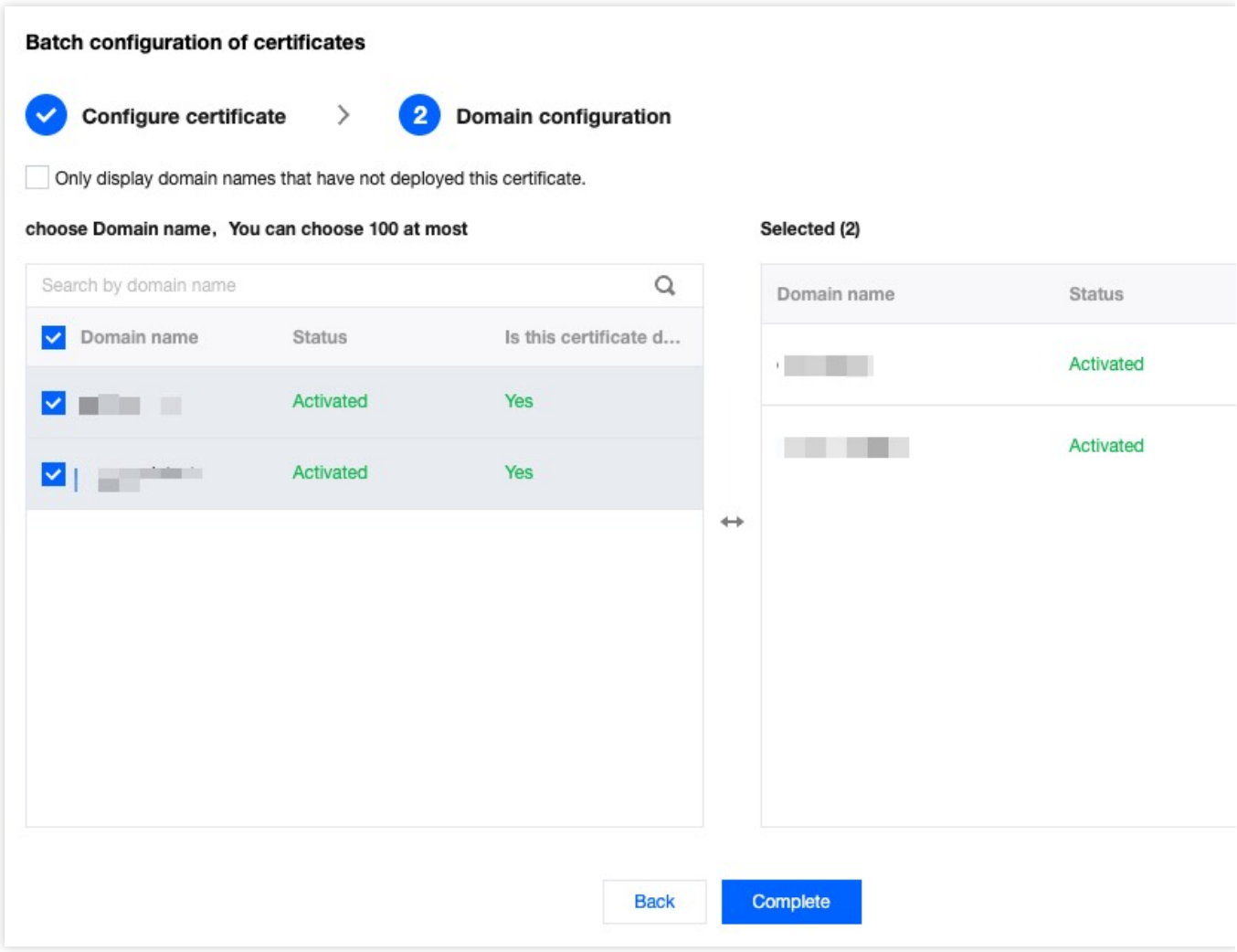


4. Click **Next** to enter the domain name configuration step. Select the domain names to be deployed in batches, and click Complete to issue the certificate deployment.

Note：

1. Up to 100 domain names can be selected at once. If the certificate needs to be deployed to more than 100 domain names, please operate in batches.

2. If you need to quickly filter out domain names that have already deployed this certificate, please check: Show only domain names that have not deployed this certificate.



Updating Certificate

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

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

Configuring A Free Certificate for A Domain Name

Last updated：2024-04-16 16:54:34

Overview

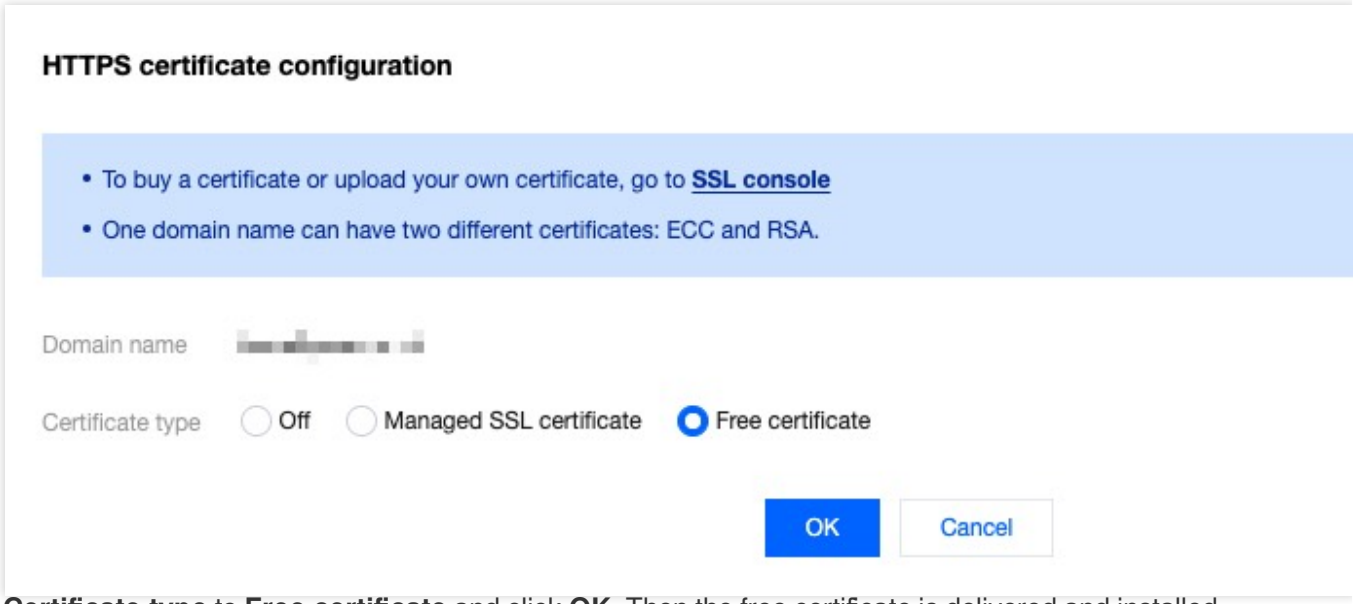
If you haven’t purchased an HTTPS certificate for the website, and the accelerated domain names do not contain any wildcard domain name, you can configure a free certificate.

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.

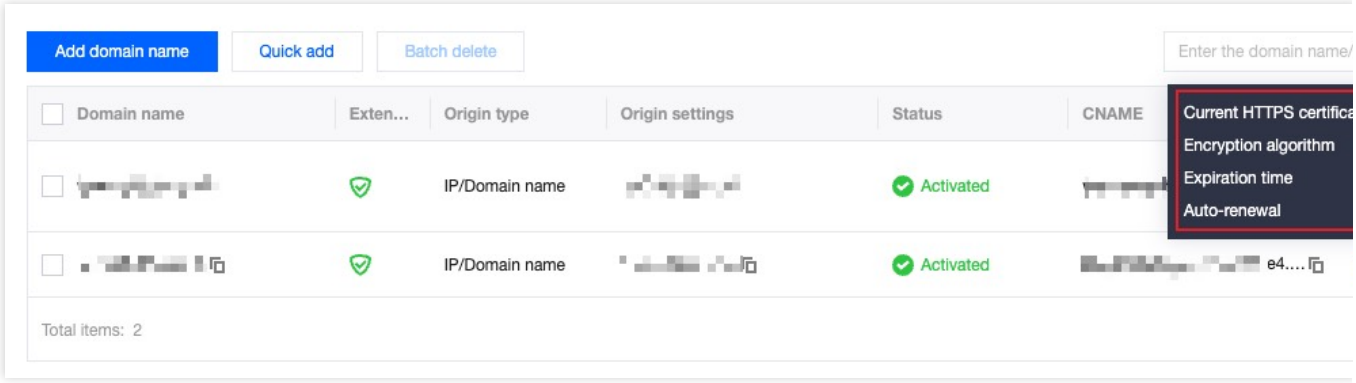
Directions

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.



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.

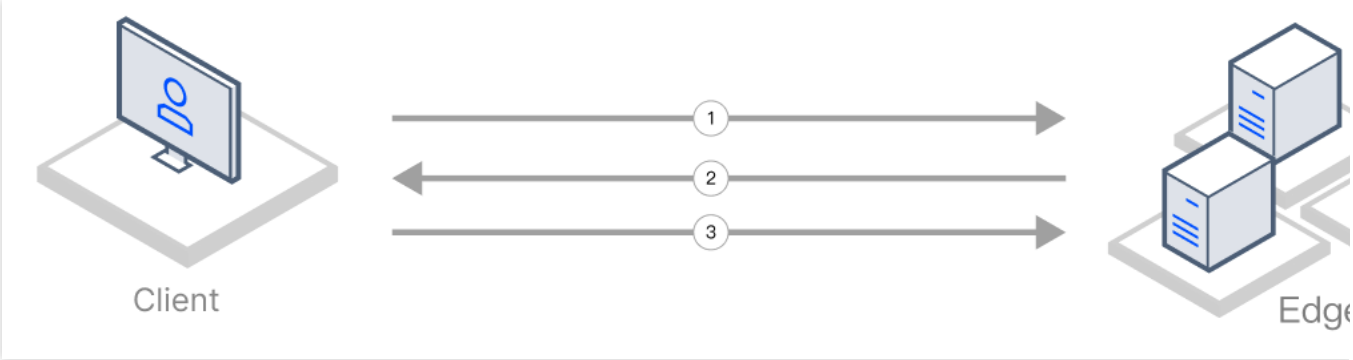


HTTPS Configuration
Forced HTTPS Access

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.

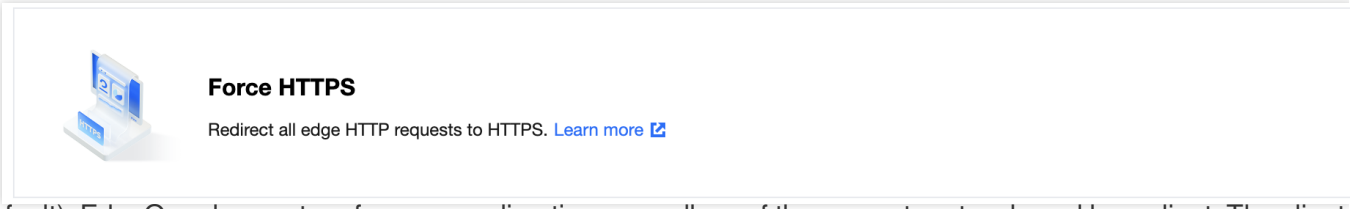
Prerequisites

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

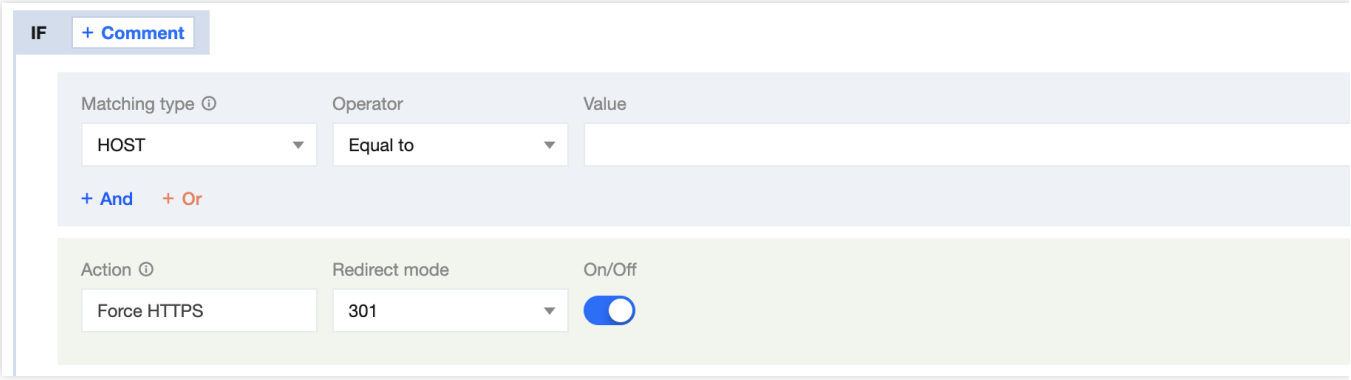
To enable forced HTTPS access for specified domain names used to access the current site, refer to the following information.

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.



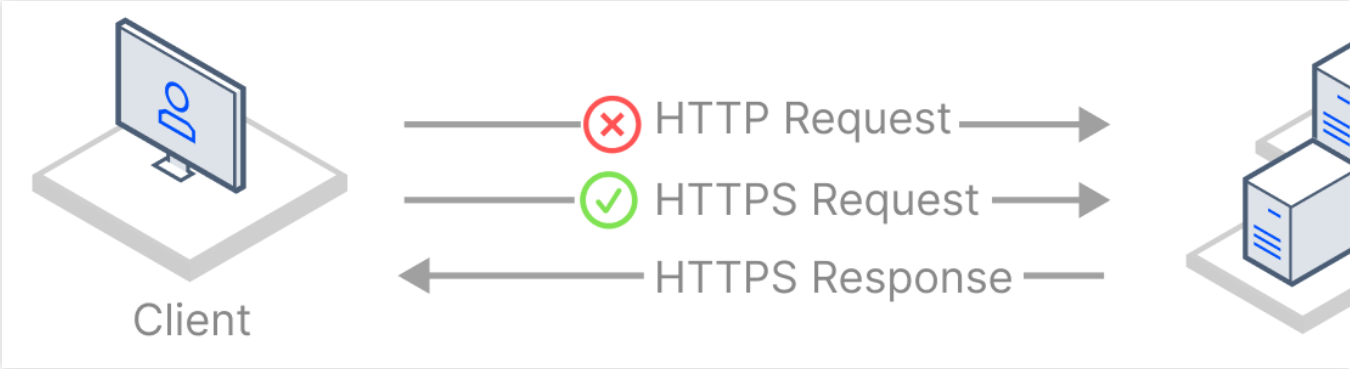
6. Click **Save and publish**.

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

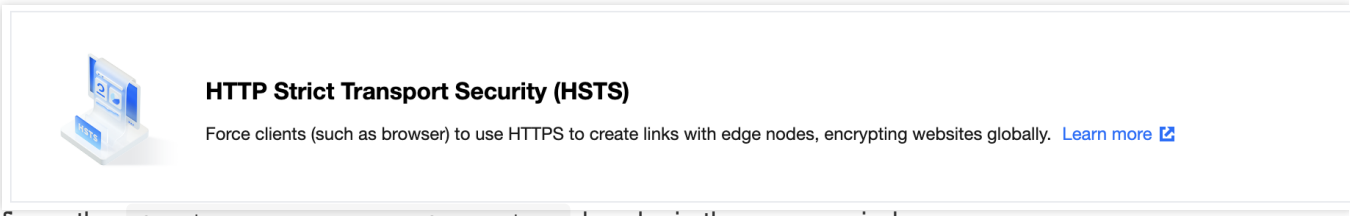
To enable HSTS for all domain names used to access the current site, refer to the following information.

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.



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

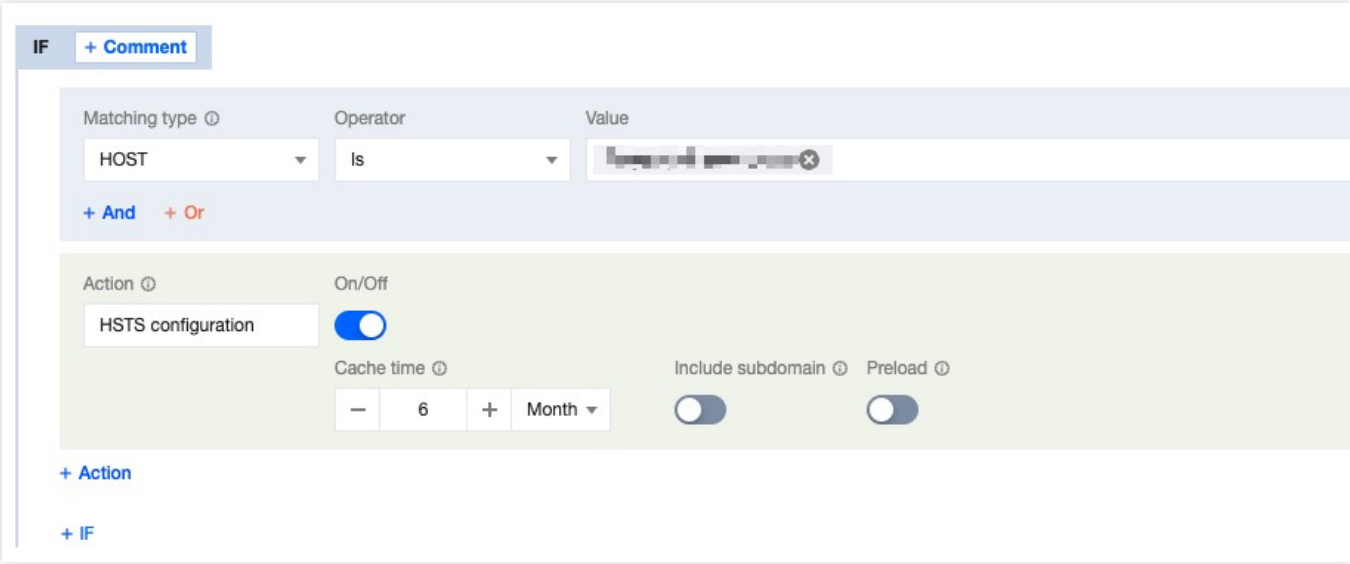
To enable HSTS for specified domain names or differentiate the HSTS configuration for different domain names, refer to the following information.

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
`max-age=<expire-time>`	The validity period of the HSTS header, measured in seconds. Within this period, browsers always send requests over HTTPS.
`includeSubDomains` (optional)	Enable HSTS for the current domain name and all of its subdomain names.
`preload` (optional)	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: `max-age` is no less than 31536000 (one year). `includeSubDomains` is contained. `preload` is contained. You can view the HSTS preload list 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.

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

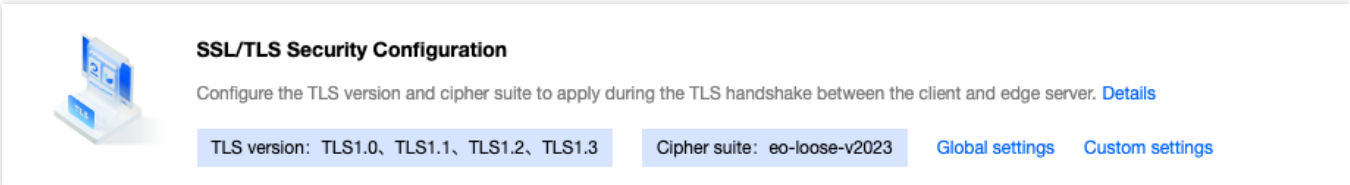
To configure required SSL/TLS versions for all domain names used to access a site, refer to the following information.

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.



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

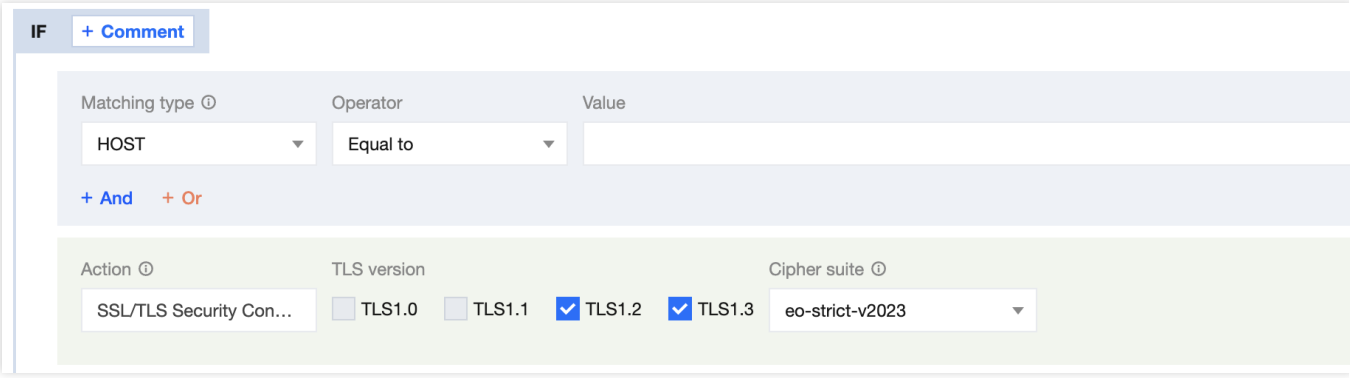
To configure required SSL/TLS versions for specified domain names, refer to the following information.

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.



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	`eo-loose-v2023`
A balanced approach is needed to ensure a moderate level of security and browser version compatibility.	TLS 1.2 and TLS 1.3	`eo-general-v2023`
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	`eo-strict-v2023`

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

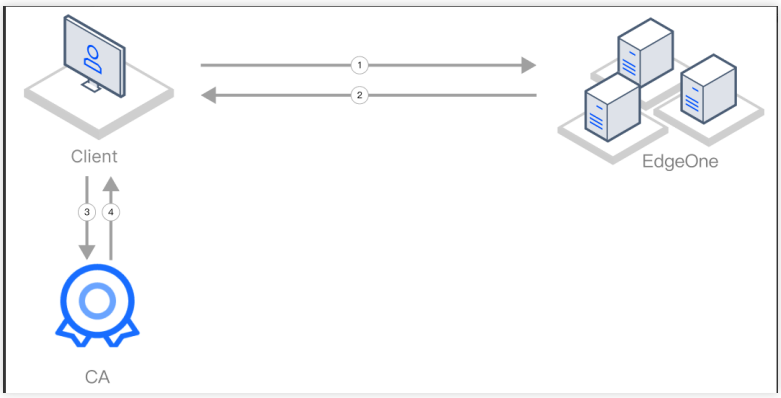
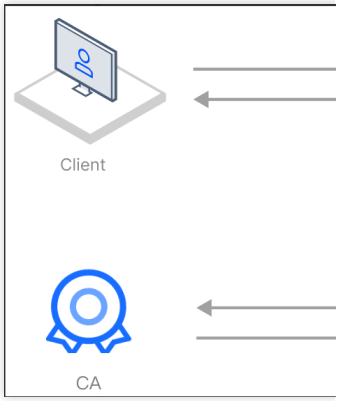
Last updated：2023-05-08 10:00:27

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
	
1. The client initiates a TLS handshake. 2. EdgeOne responds to the TLS handshake (by returning the certificate). 3. The client initiates an OCSP query. 4. The CA returns the result.	1. The client initiates a TLS hands 2. EdgeOne initiates an OCSP que 3. The CA returns the result, and E 4. EdgeOne responds to the TLS h OCSP information). Because OCSP information is cac respond to subsequent query requ

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**.

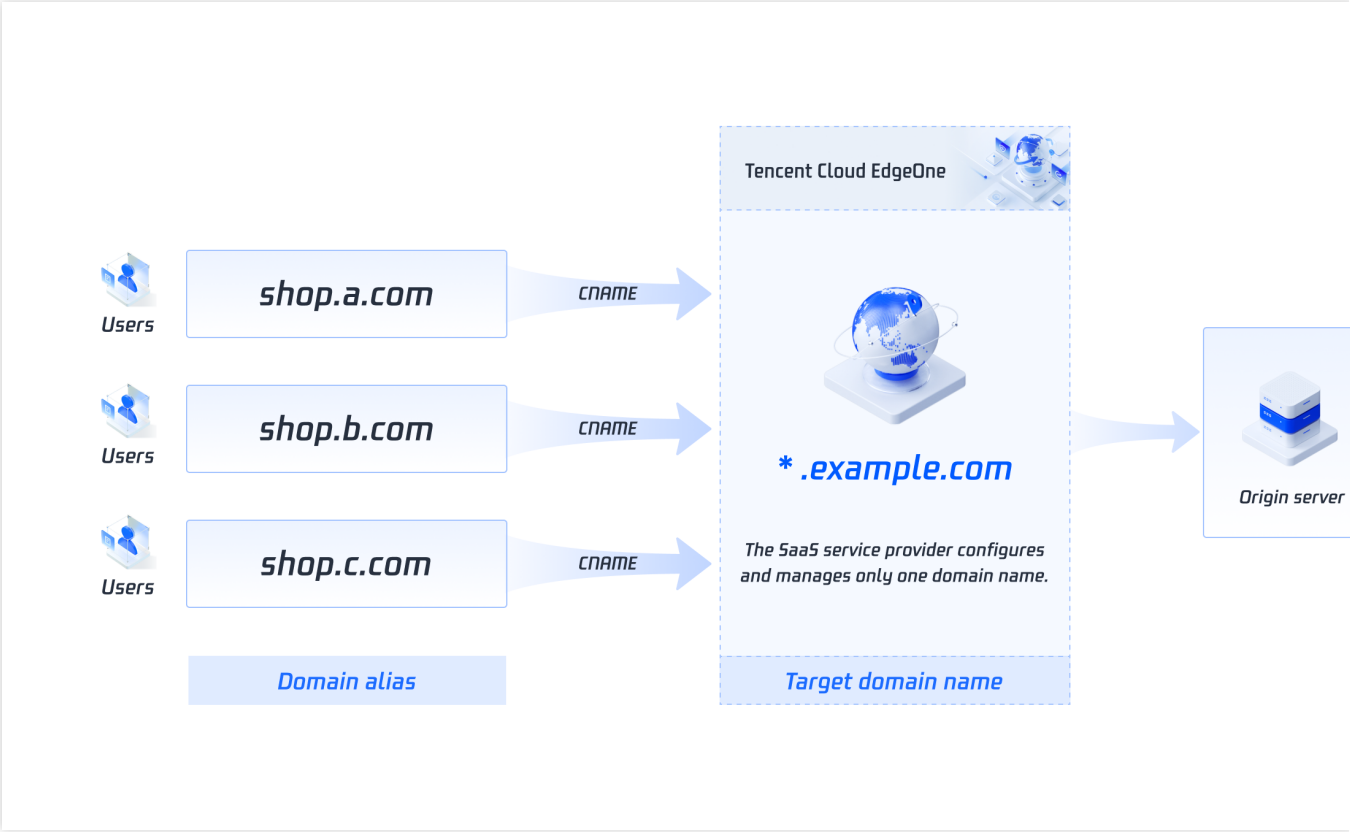
Domain alias Overview

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.

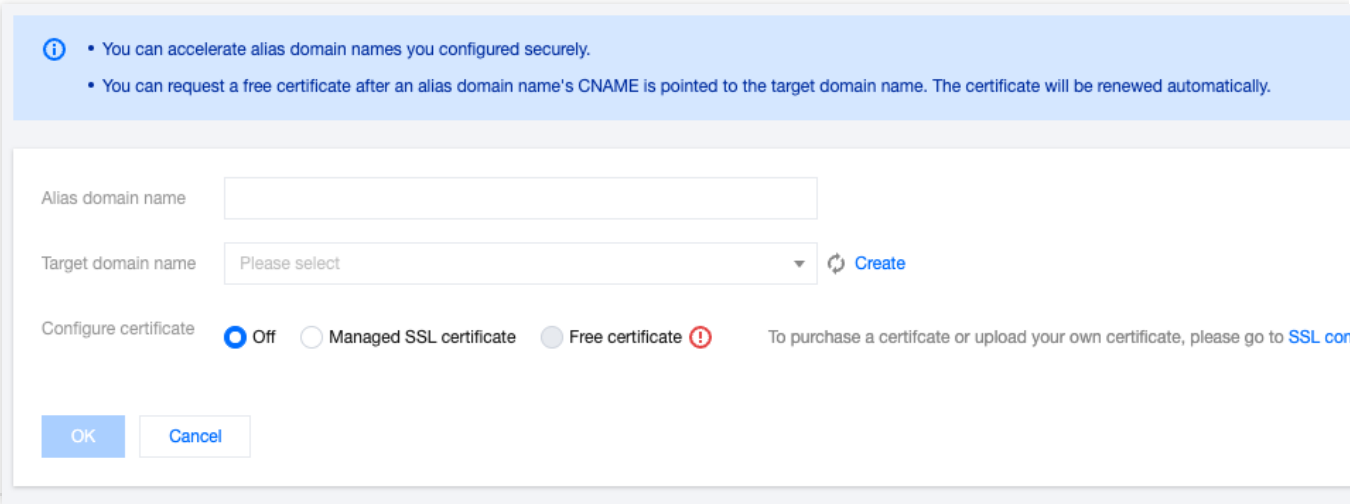
Prerequisites

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**.

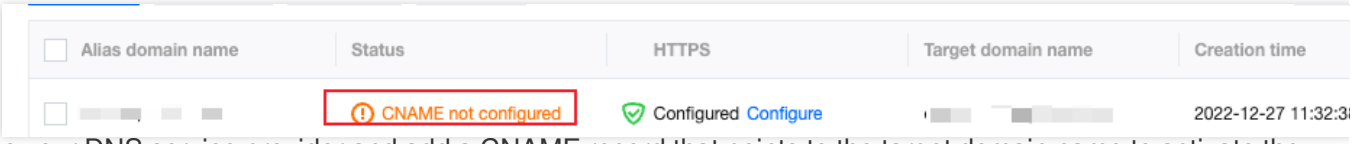


Parameter	Description
Alias domain name	It can contain up to 81 characters. Wildcard domain names such as `*.test.com` are not supported. If the acceleration region of your site is in the Chinese mainland, you must obtain an ICP filing number for your domain alias.
Target domain name	You can select a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

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.

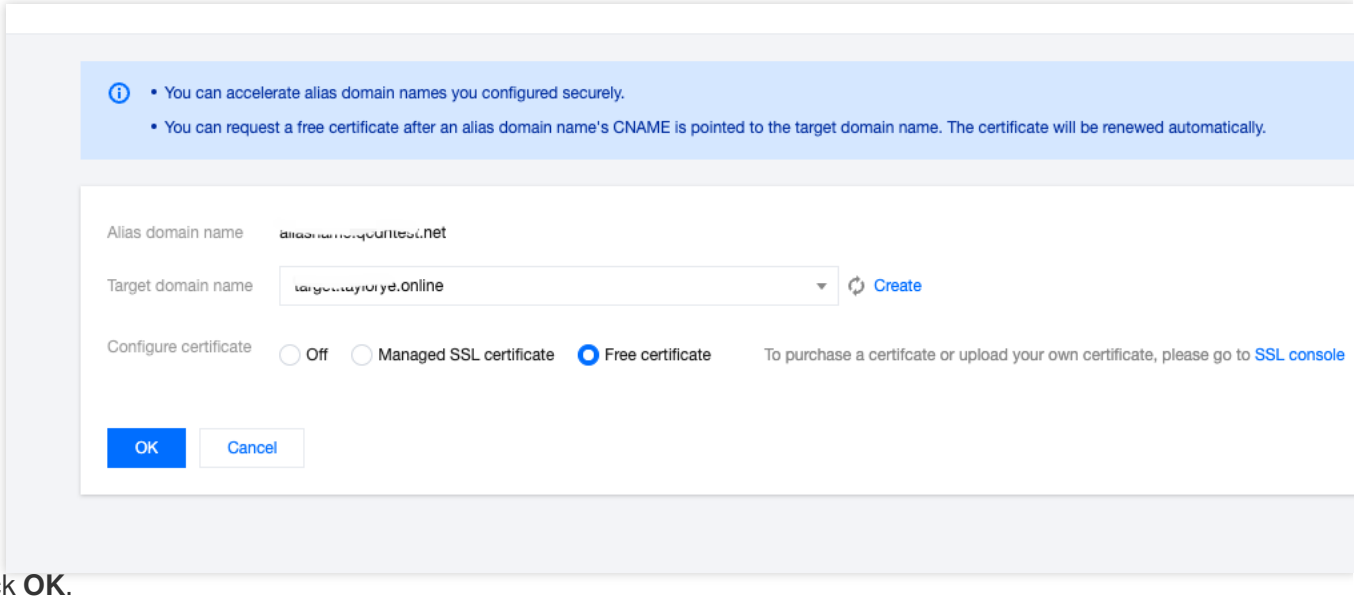


2. Go to your DNS service provider and add a CNAME record that points to the target domain name to activate the domain alias.
3. EdgeOne automatically checks for updates, and changes the status of the domain alias to **Activated**.

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**.



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**.

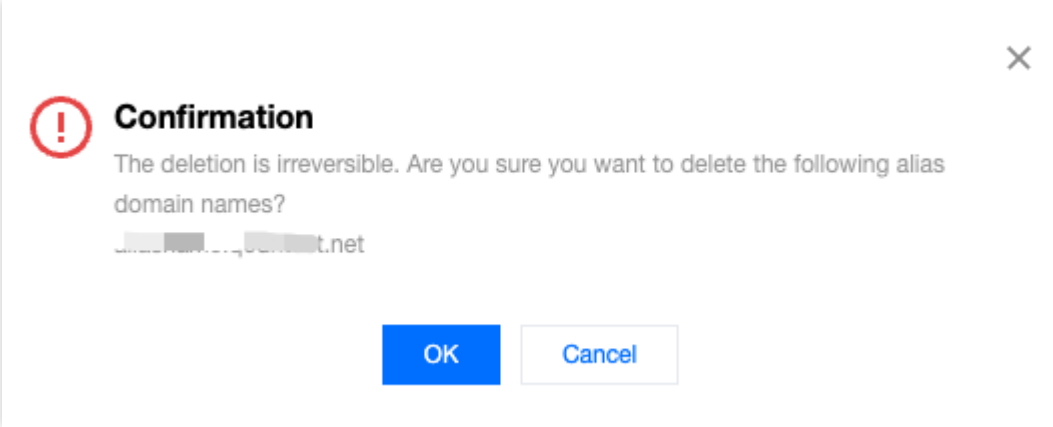
Deleting a Domain Alias

Note

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

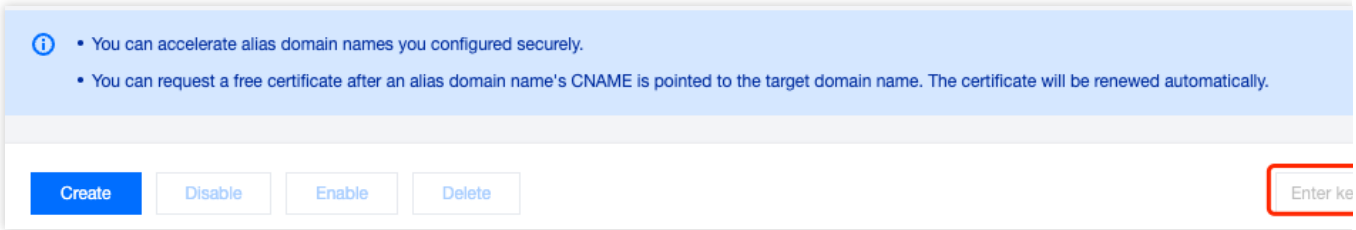
The data cannot be recovered once a domain alias is deleted.

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

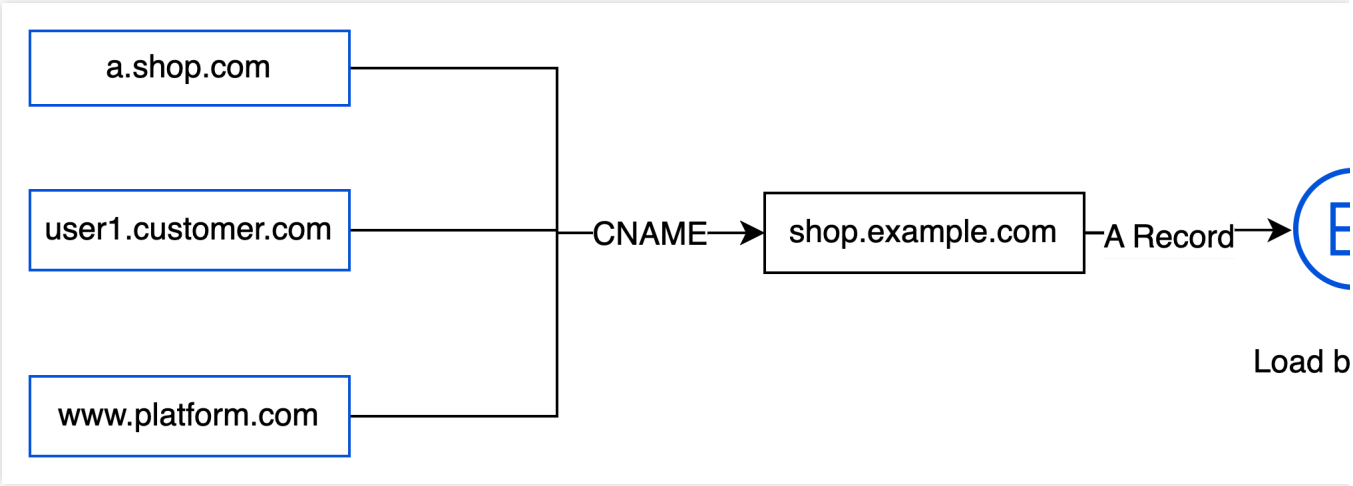
Reading this document may take 10 minutes, which helps you understand:
What challenges for SaaS business can be overcome with alias domain names.
How to use alias domain names to relieve the workload of maintaining multiple domain names for the same business.

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

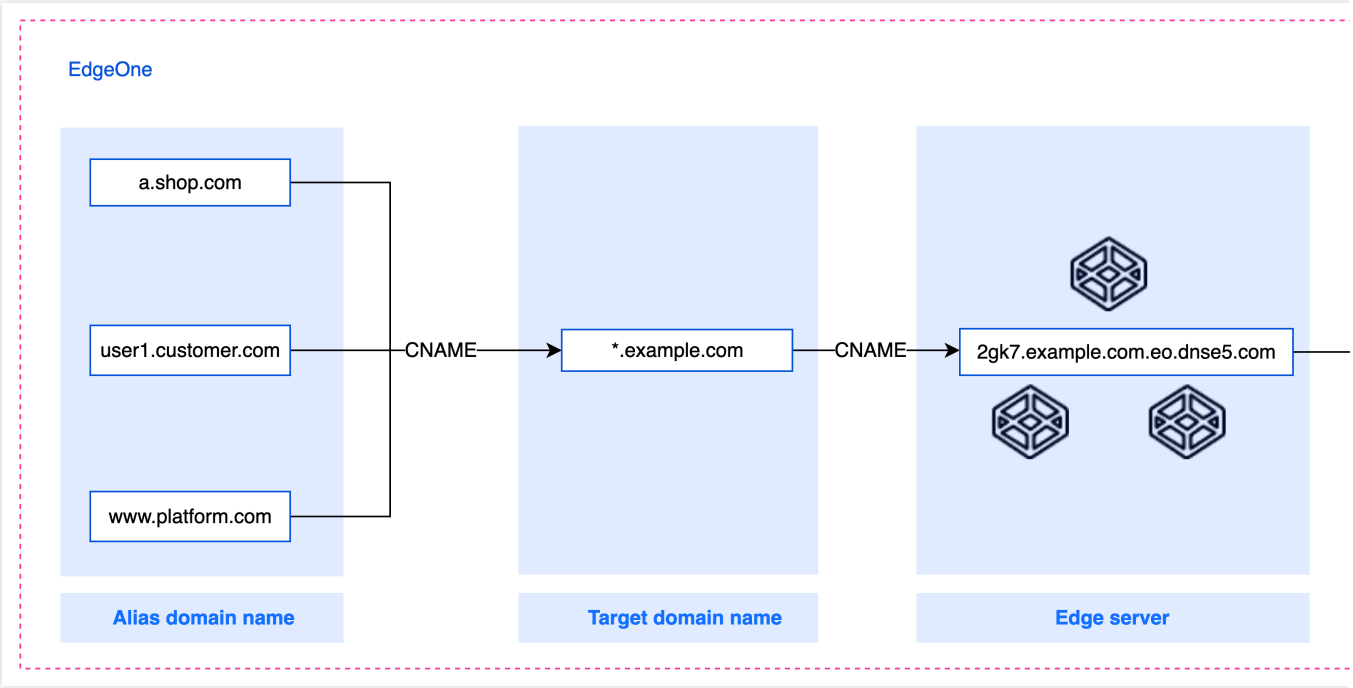
For SaaS providers, the support required by users is basically identical, except for the site content. Thus, an architecture that can facilitate operation and maintenance is used:



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:

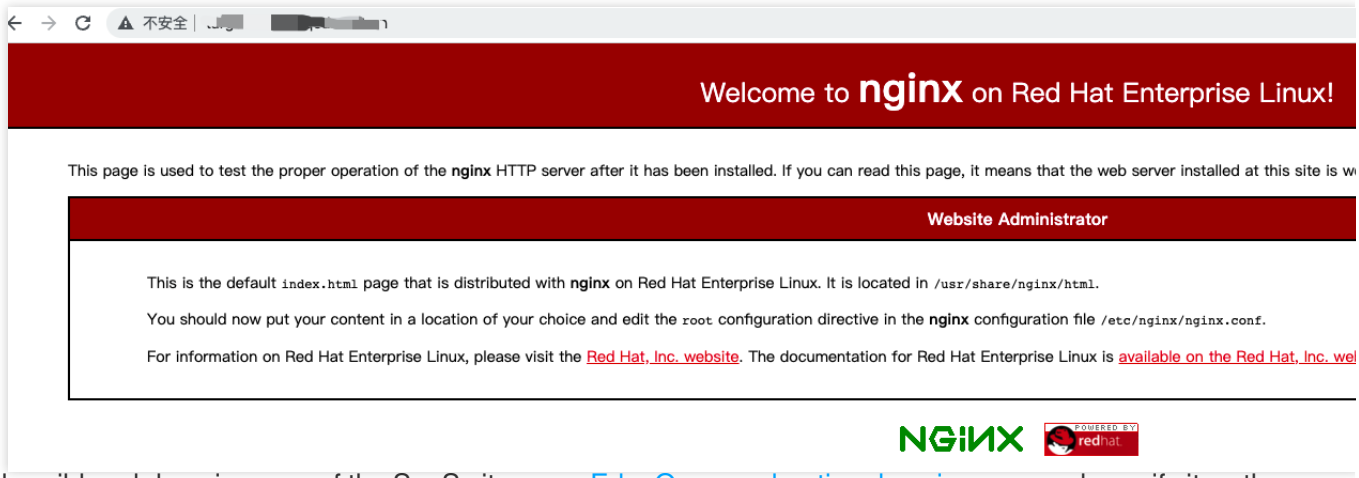
1. When the target domain name is added to EdgeOne, it can access security and content acceleration services, which are also reachable for the alias domain names.
2. SaaS website builders can greatly reduce costs as a result of maintaining target domain names only.
3. Customer-defined domain names can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

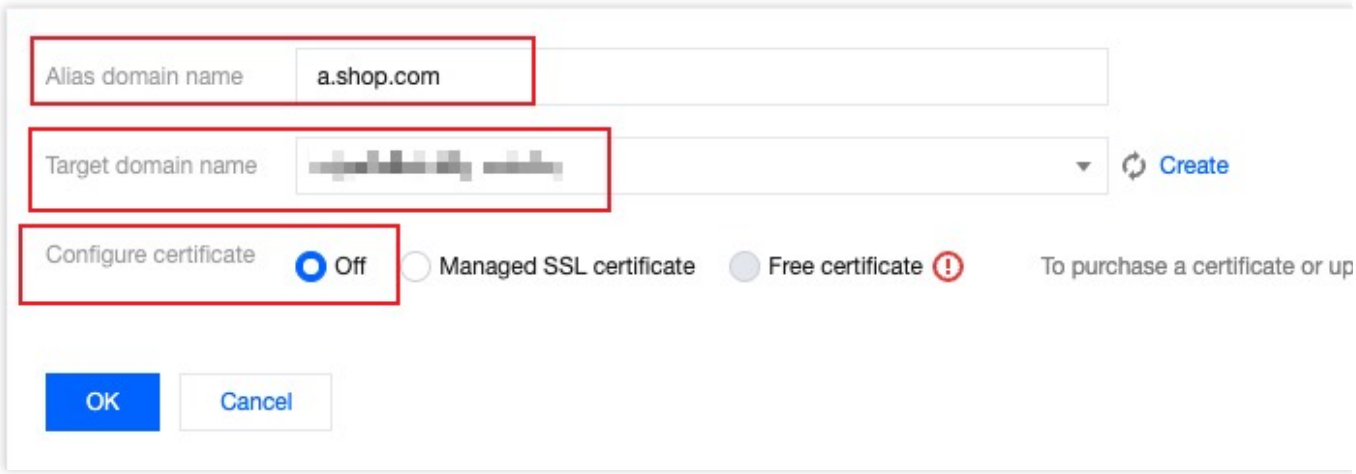
3. Add customer-defined domain names as alias domain names. See the table below:

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

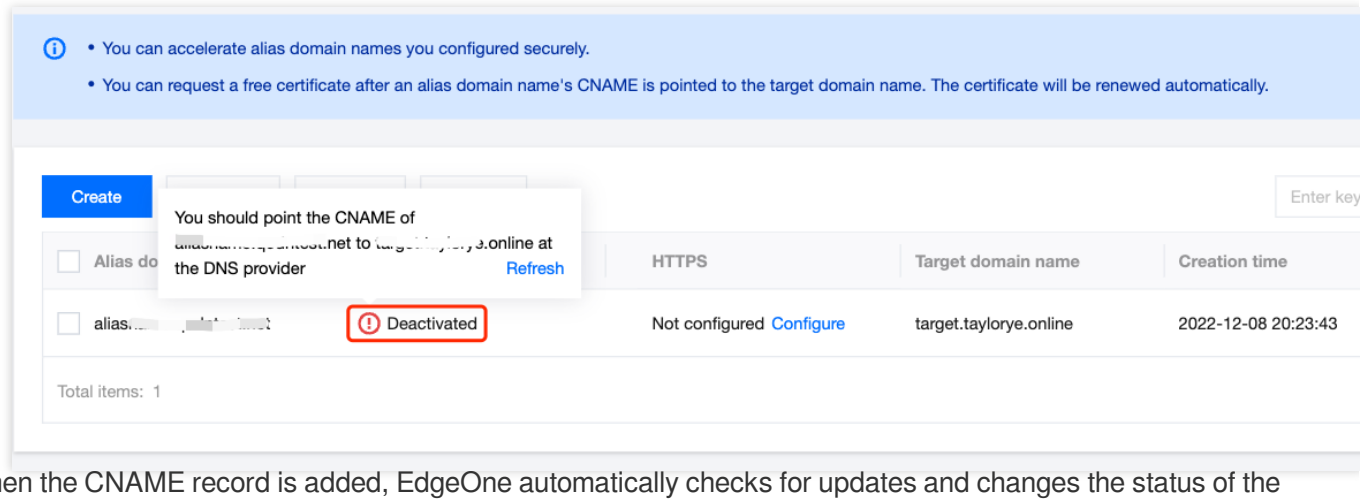
1. Log in to the EdgeOne console. Navigate to **Site List** and select a site for management.
2. In the left sidebar, click **Alias Domain Names**. On the page that appears, click **Create**.
3. Enter `a.shop.com` as the alias domain name, select `*.example.com` as the target domain name, and set **Off**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



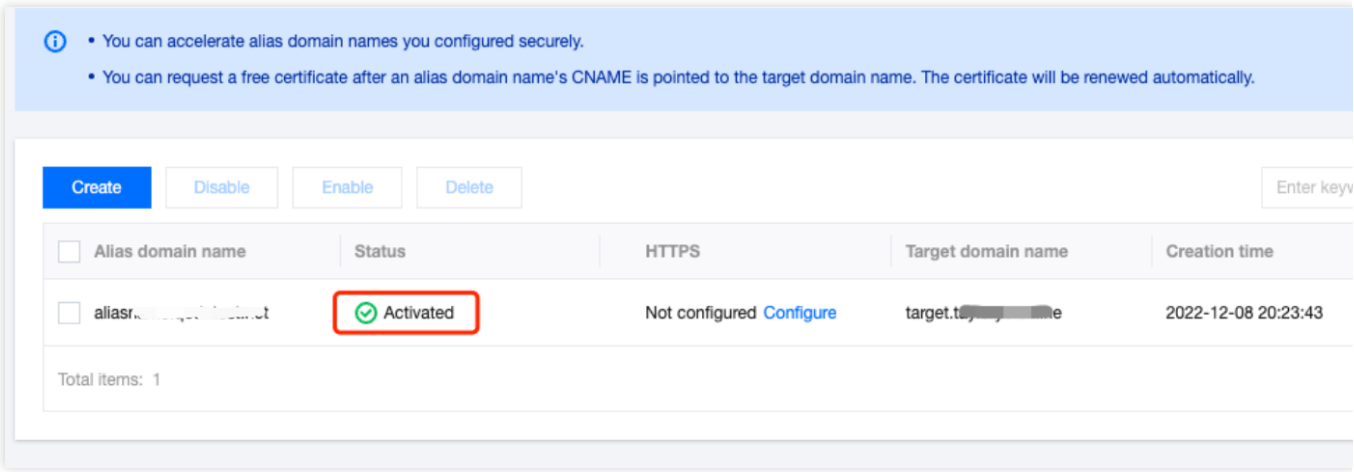
Step 2. Add a CNAME record that points to the target domain name

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.

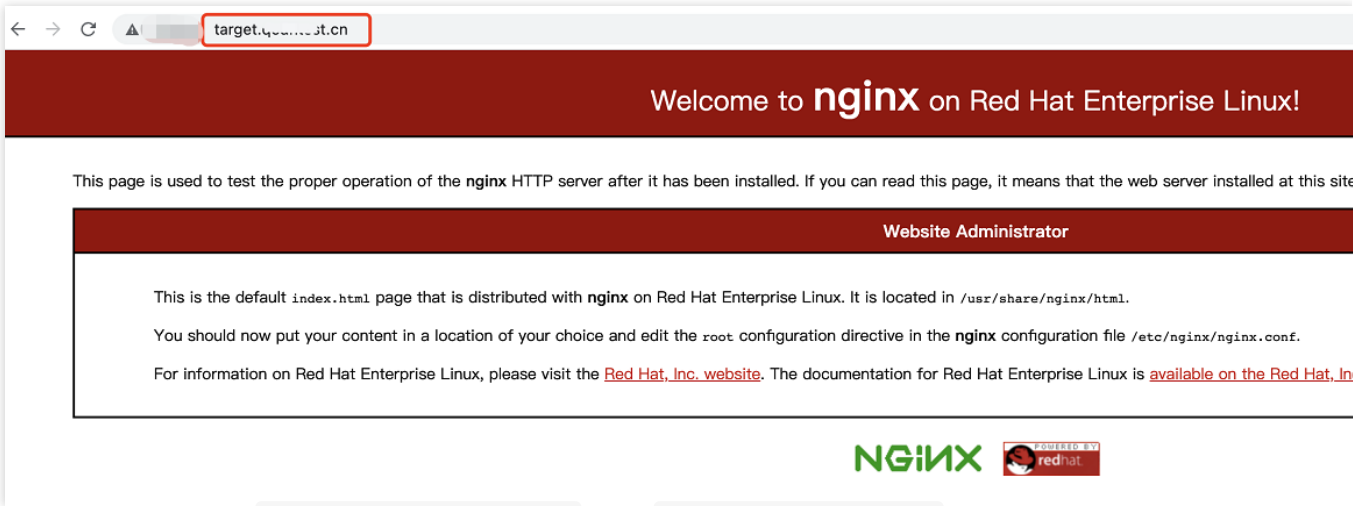


2. When the CNAME record is added, EdgeOne automatically checks for updates and changes the status of the domain alias to **Activated**.



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` .

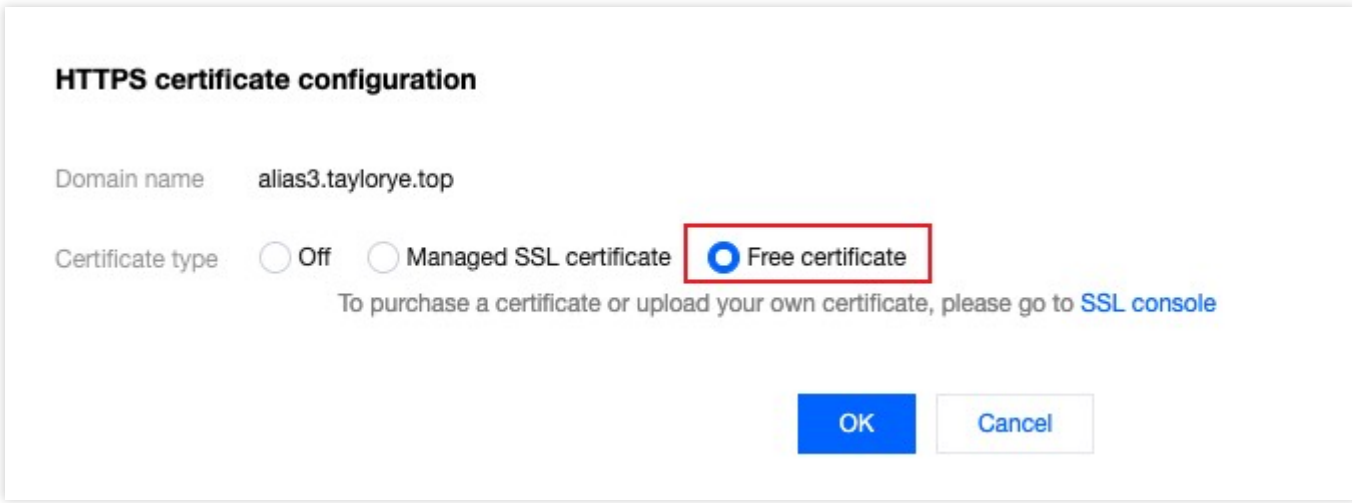


Other alias domain names `user1.customer.com` and `www.platform.com` can be verified in the same way.

Step 4. Apply for a free certificate (optional)

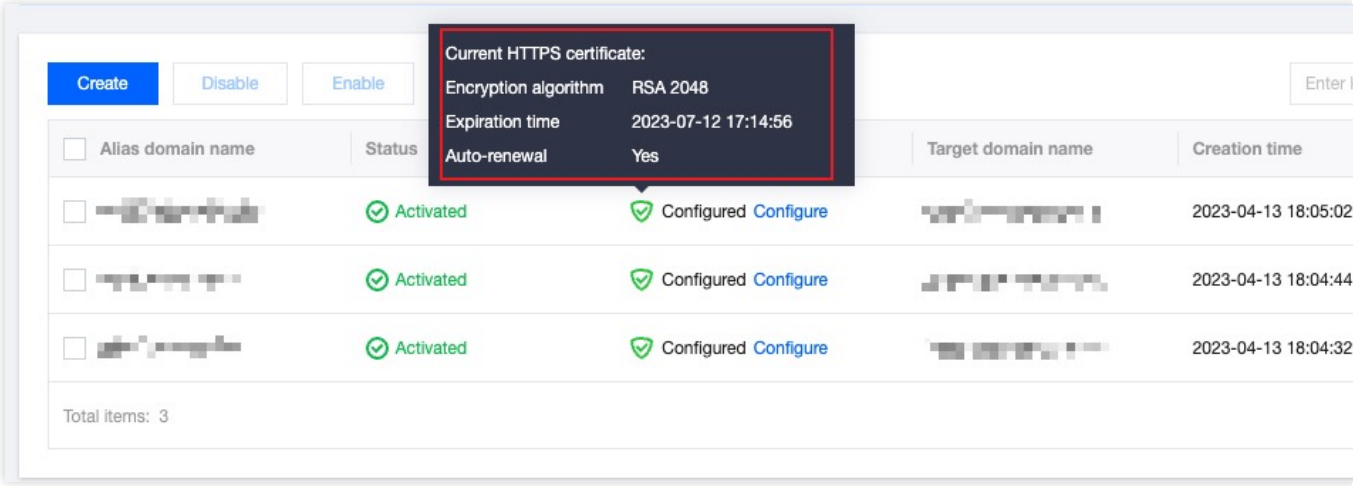
After you configure the CNAME record for the alias domain name by following Step 2, apply for a free HTTPS certificate as follows:

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**.



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

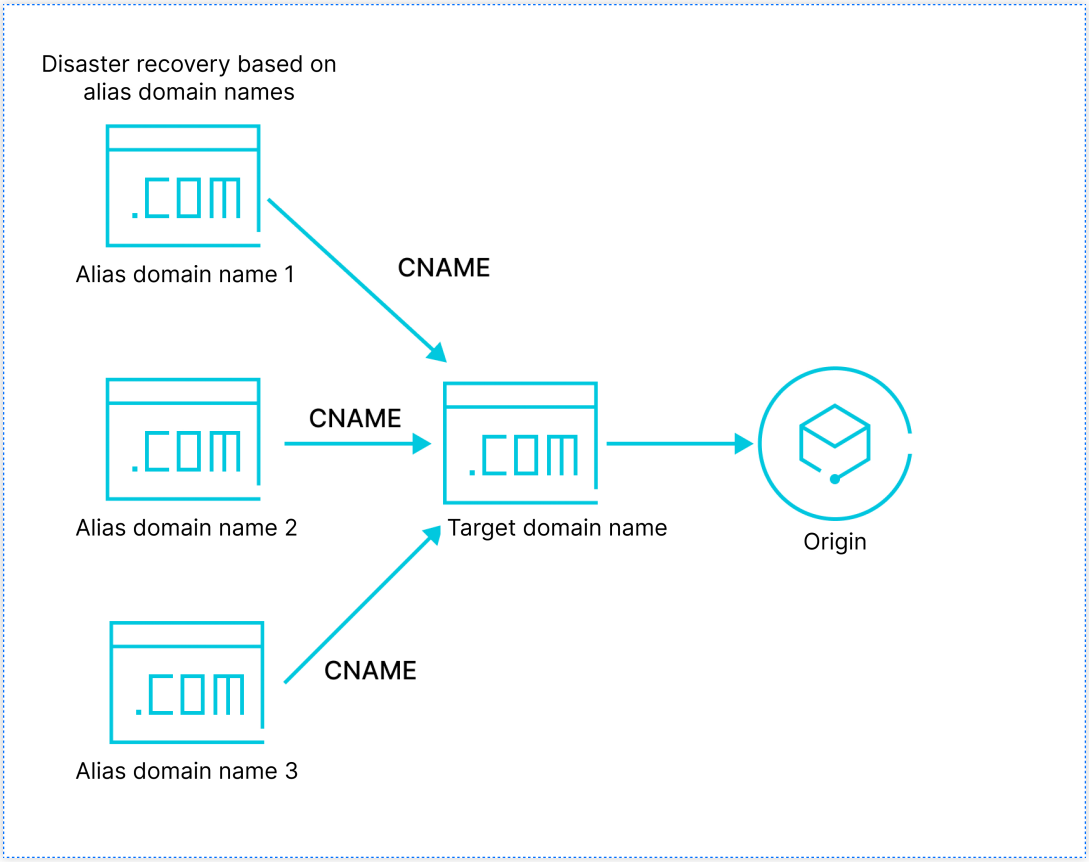
to view the information about the certificate:



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:

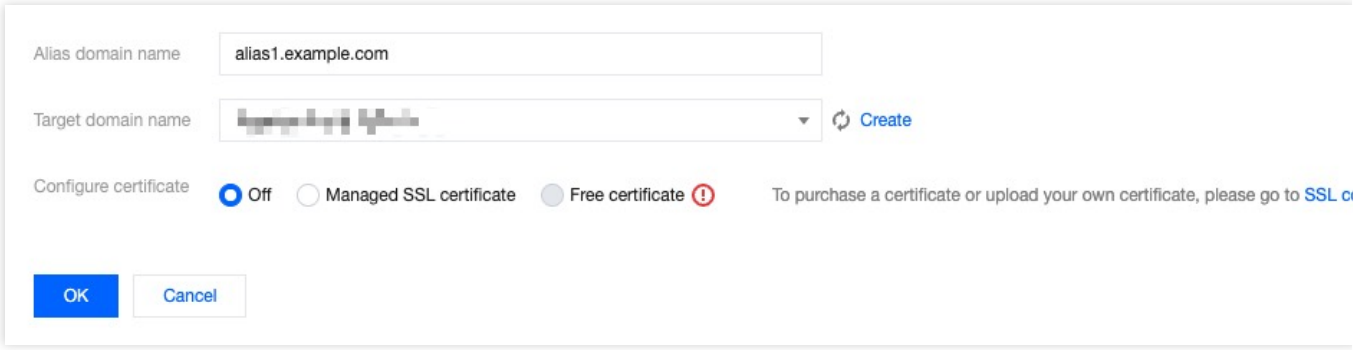
1. `alias1.site.com`
2. `www.shop.com`
3. `backup.website.com`

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

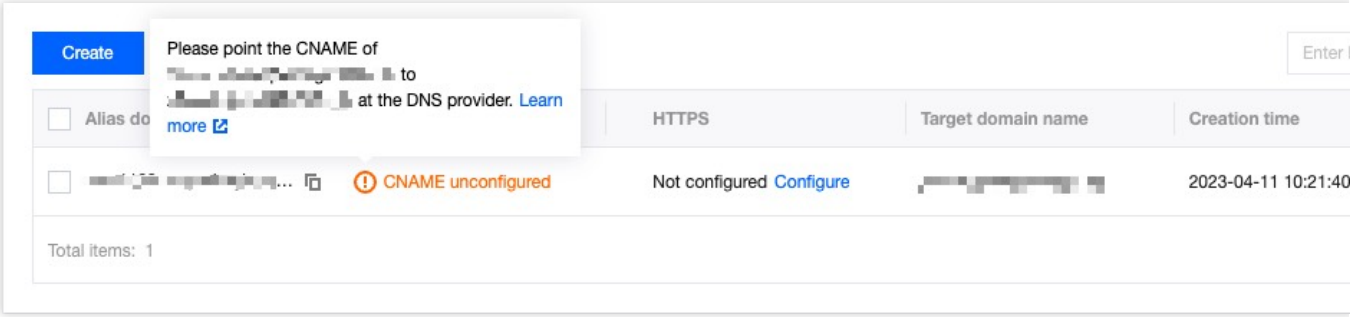
1. Log in to the EdgeOne console. Navigate to **Site List** and select a site for management.
2. In the left sidebar, click **Alias Domain Names**. On the page that appears, click **Create**.
3. Enter `alias1.site.com` as your alias domain name, select `target.example.com` as your target domain name,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

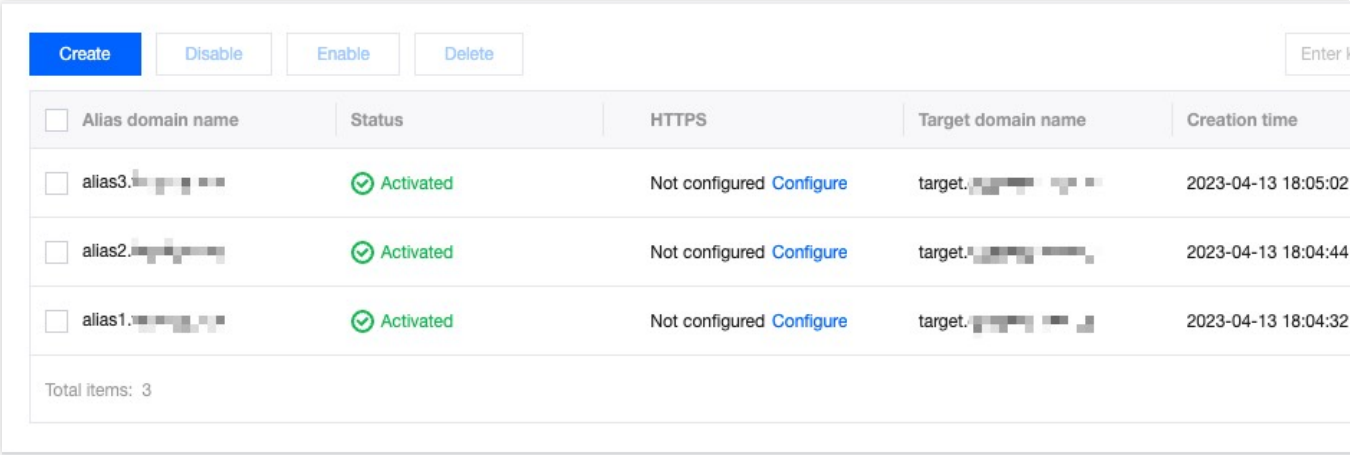
1. When your alias domain name is added, the status is default to **Not activated**, as shown in the figure below:



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.

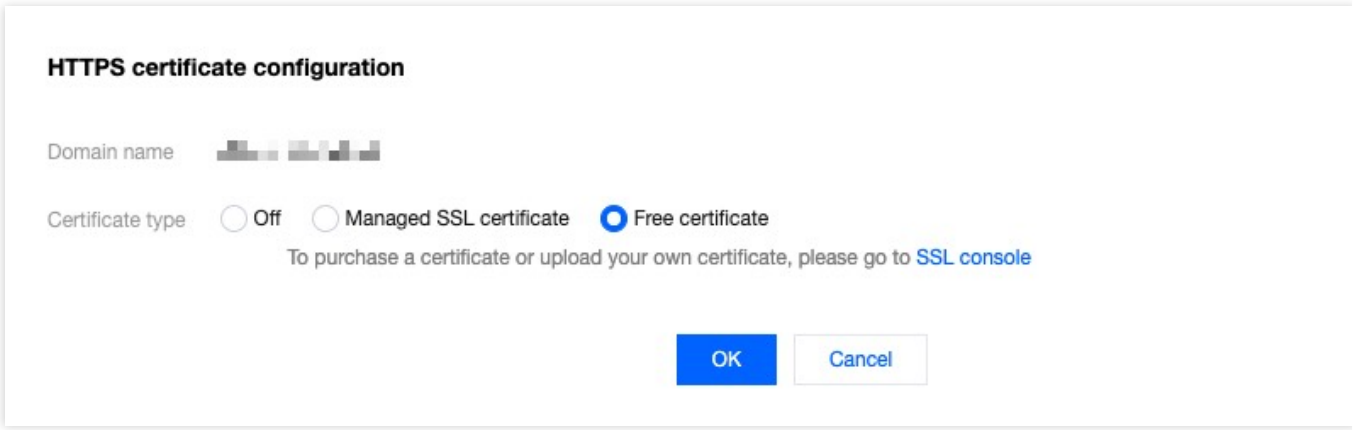
As shown above, the same response is obtained for the access requests to the alias domain names and target domain name. This indicates that the alias domain names have taken effect as expected.

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)

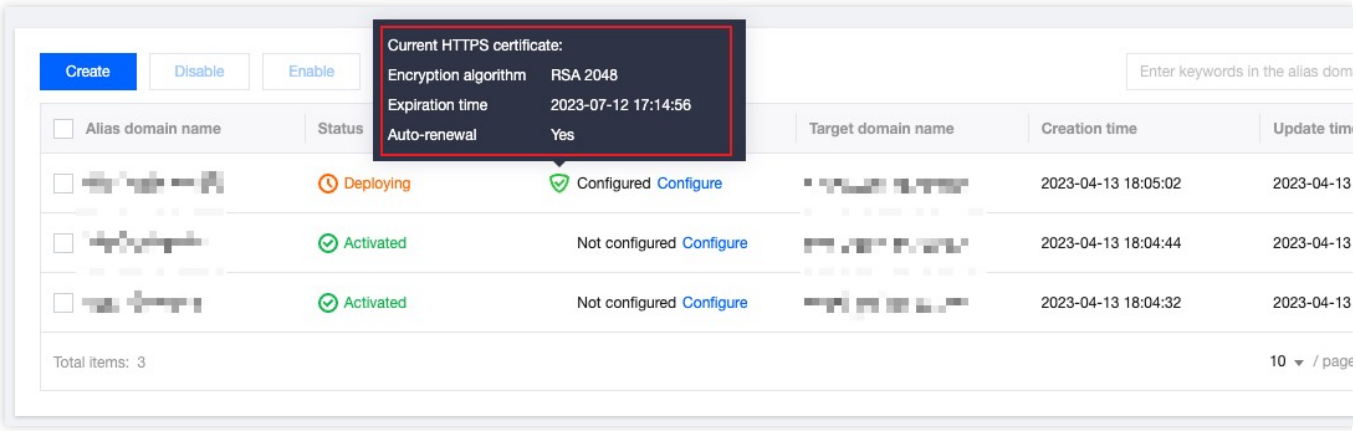
After you configure the CNAME record for your alias domain name by following Step 2, apply for a free HTTPS certificate as follows:

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:



Traffic Scheduling
Traffic Scheduling Management

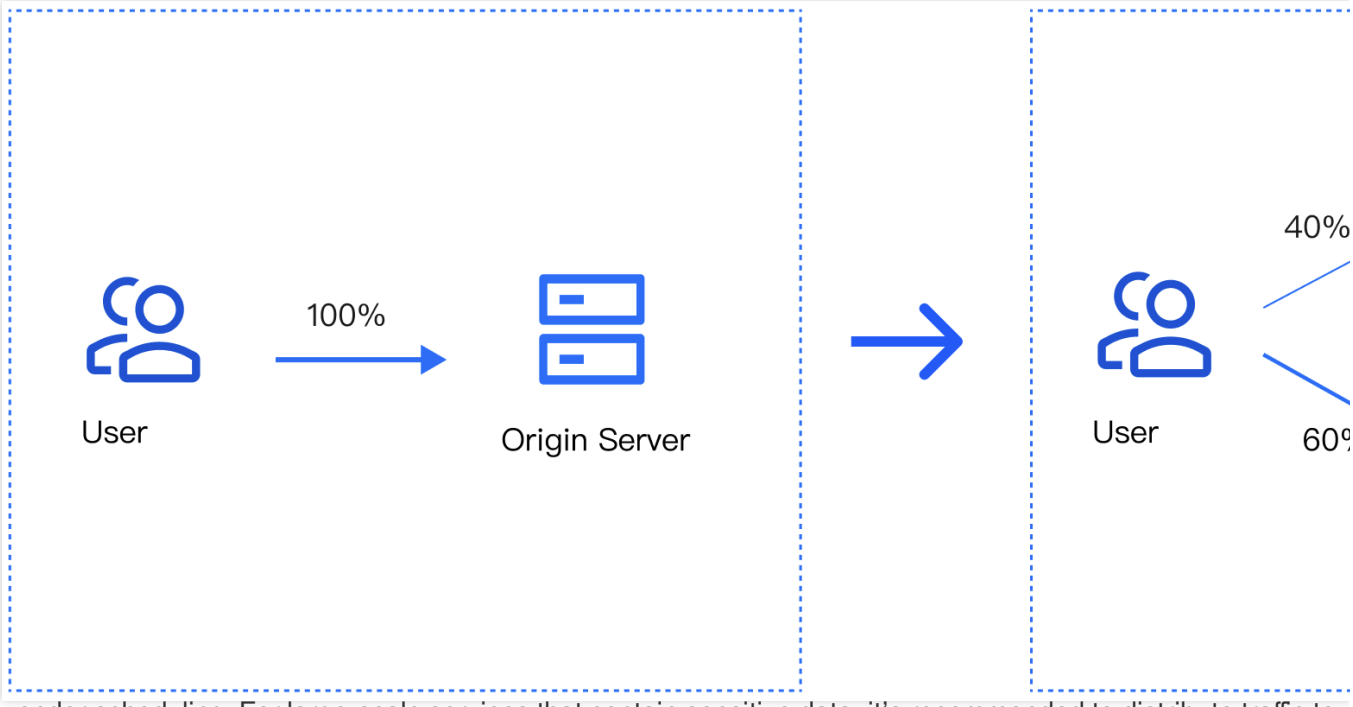
Last updated：2024-04-16 17:06:58

Overview

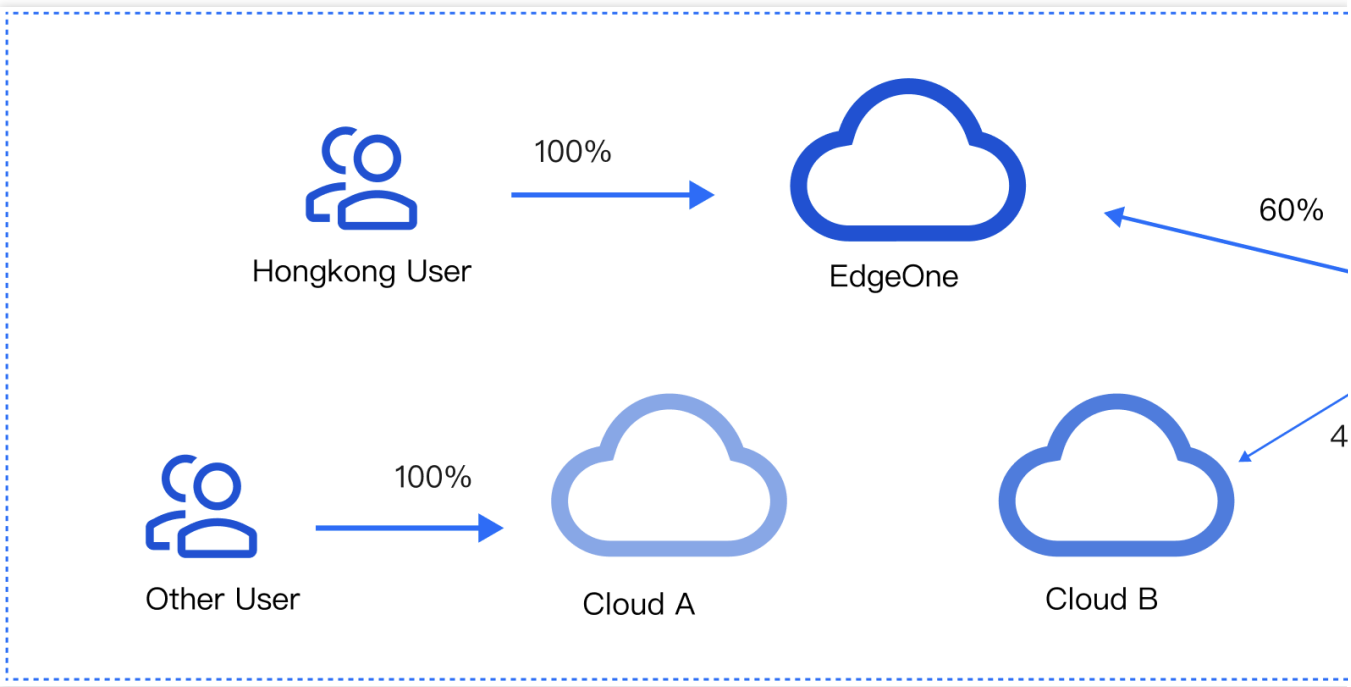
Traffic scheduling management is a multi-CDN smart resolution and scheduling tool provided by EdgeOne. It supports custom traffic scheduling policies between the origin and service providers to implement smooth canary migration of traffic and flexible allocation of services, thereby ensuring a high service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

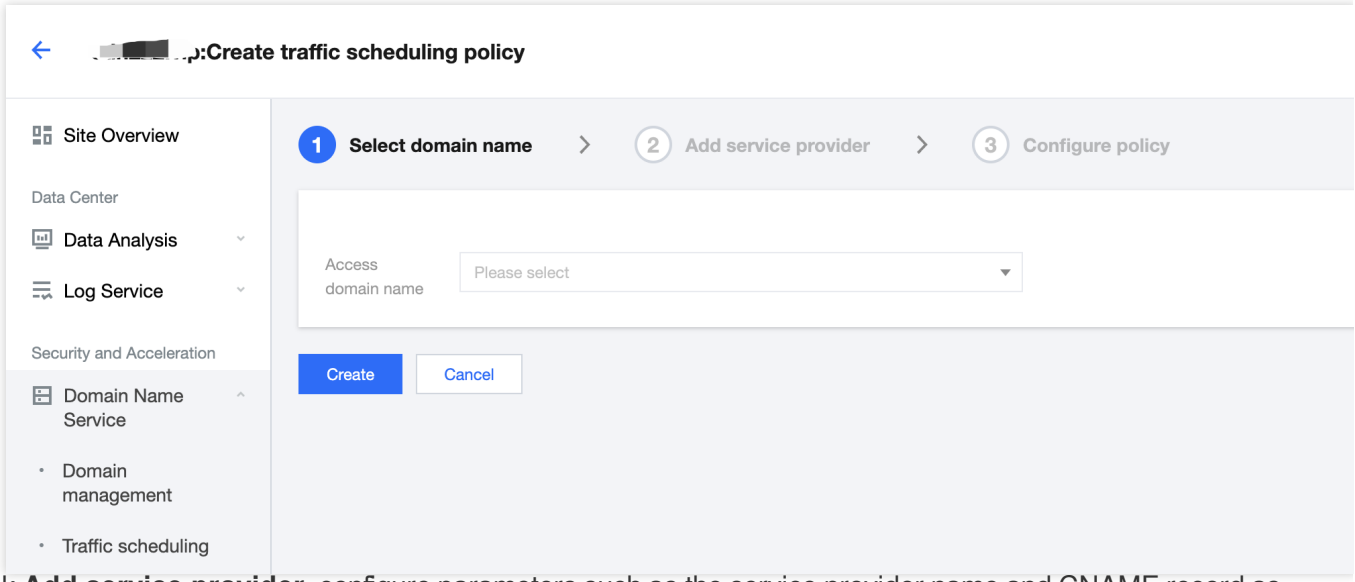
Simple management: Select a domain name, add service providers, and add scheduling policies.
Quick access: Add the CNAME record assigned by EdgeOne at your DNS service provider
Scheduling modes: Support ratio-based and region-based scheduling.
Multiple scenarios: You can use either the origin or services 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

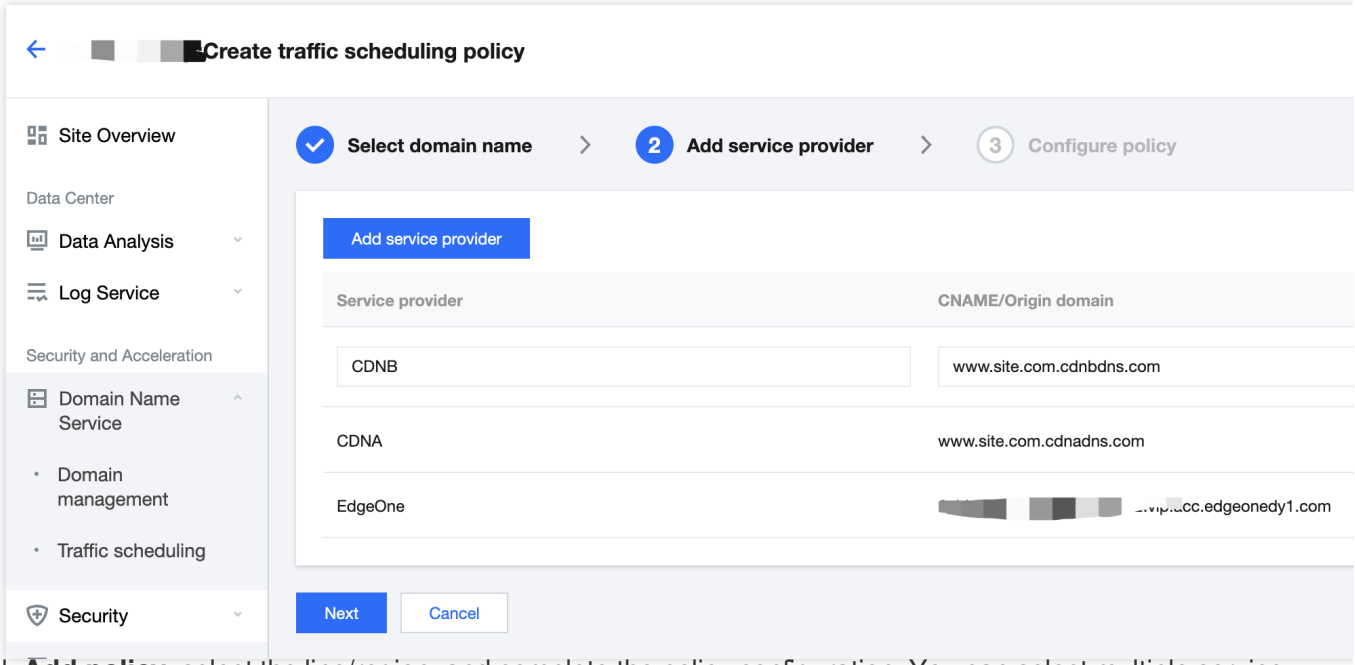
1. Log in to the EdgeOne console, and click Site List in the left sidebar. In the site list, click the target site to enter the site details page.
2. On the site details page, click **Domain Name Service** > **Traffic Management**.
3. On the **Traffic scheduling** tab, click **Add scheduling policy**. 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.



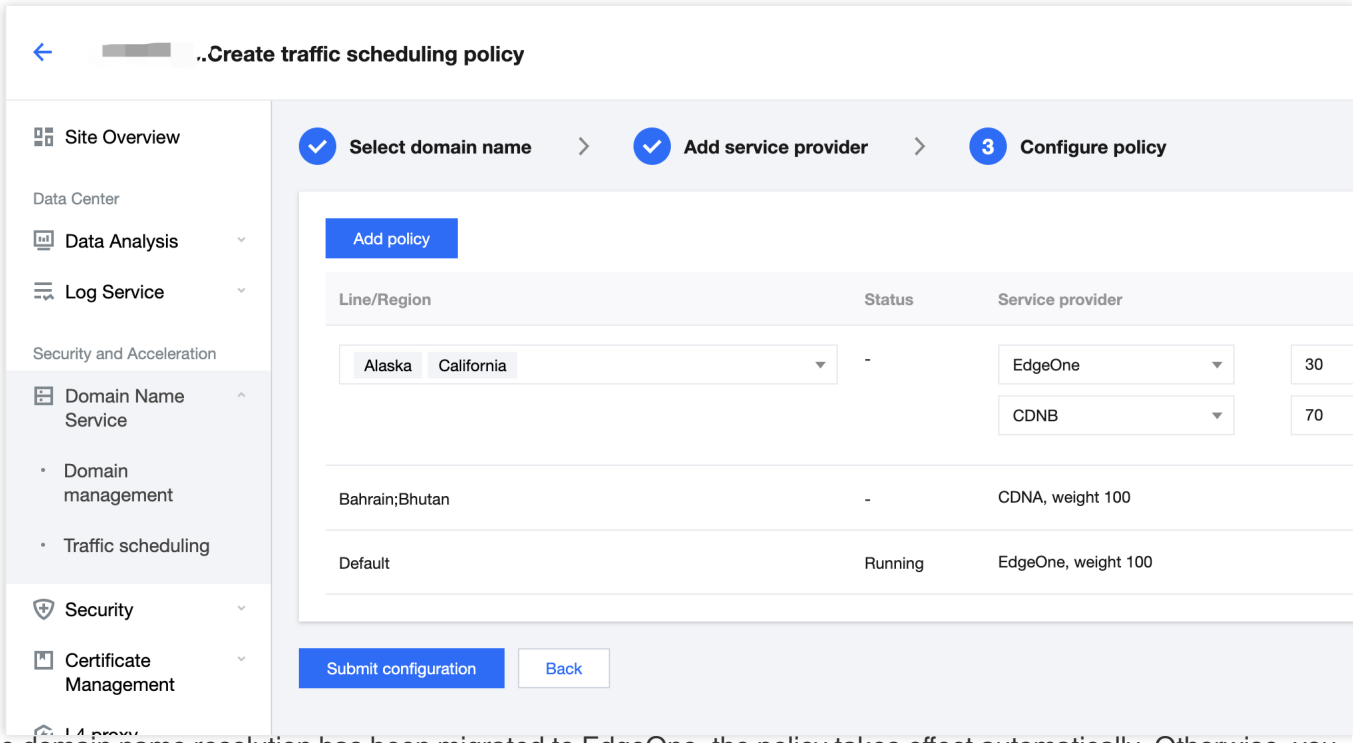
5. Click **Add policy**, select the line/region, and complete the policy configuration. You can select multiple service providers and specify their weights to configure a multi-service provider scheduling policy. After the configuration is complete, click **Submit configuration**.

Note:

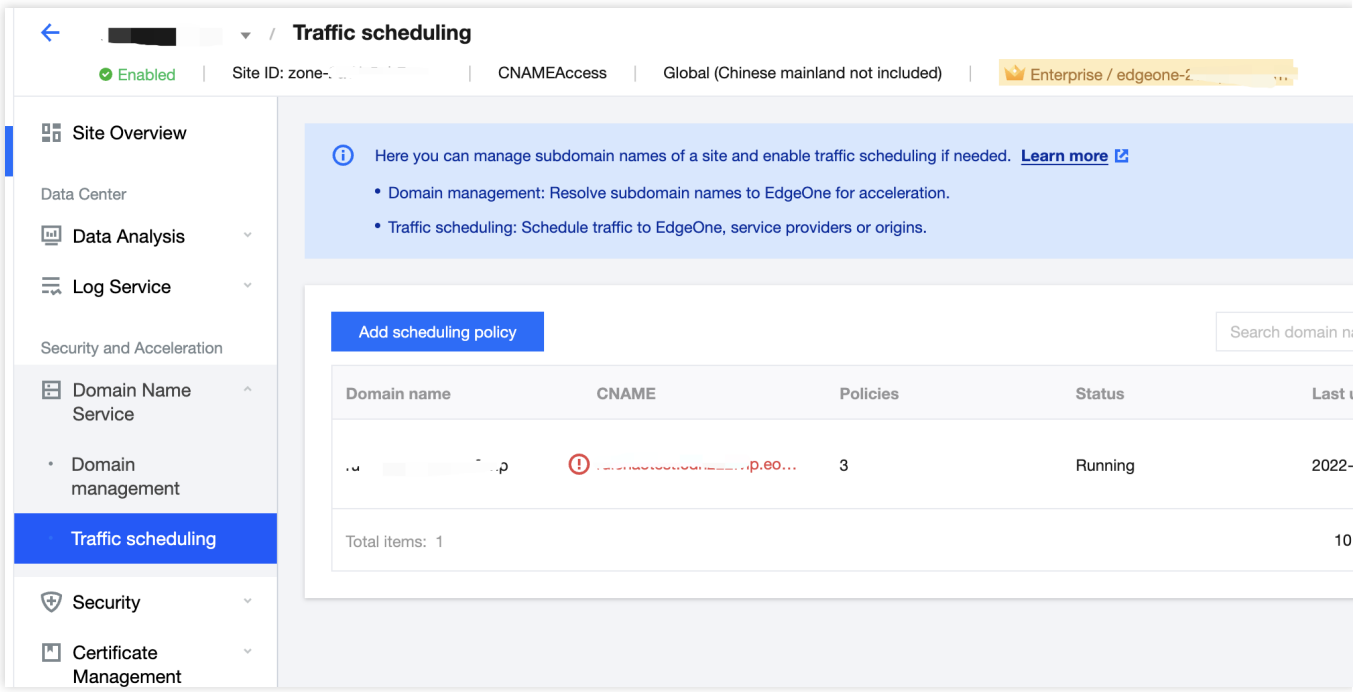
By default, all traffic passes EdgeOne. This is the base policy, which cannot be deleted but can be changed to another service provider.

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.