

# Secure Content Delivery Network

## User Guide

### Product Documentation



## Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

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

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

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

# Contents

## User Guide

Domain Name Connection

Domain Name Operations

Configuration Management

Event Logs

# User Guide

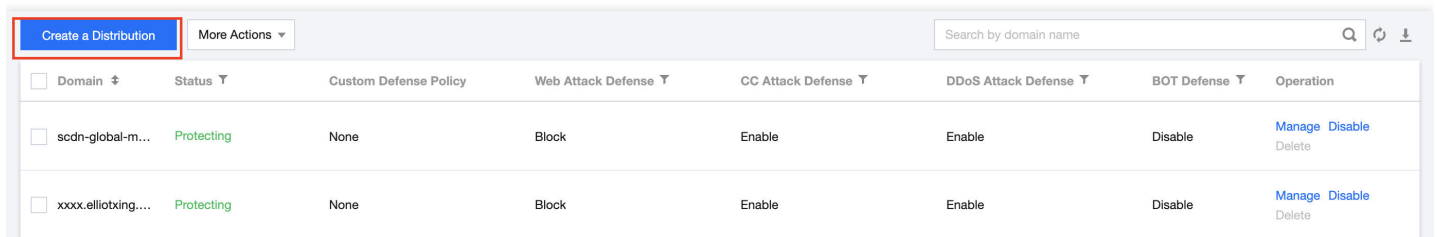
## Domain Name Connection

Last updated : 2021-11-25 12:09:53

After purchasing an SCDN package, log in to the [SCDN Console](#) to add and configure your domain name. Your defense configurations for the domain name will be deployed to all SCDN nodes, which does not affect your business.

## Creating a Distribution

On the **Defense Settings** page, click **Create a Distribution**.



<input type="checkbox"/> Domain	Status	Custom Defense Policy	Web Attack Defense	CC Attack Defense	DDoS Attack Defense	BOT Defense	Operation
<input type="checkbox"/> scdn-global-m...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <a href="#">Delete</a>
<input type="checkbox"/> xxx.elliotxing...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <a href="#">Delete</a>

The distribution creation page consists of two parts:

- Basic defense configuration
- Custom defense policy

### Basic defense configuration

This feature allows you to configure the web attack defense, CC attack defense, and DDoS attack defense settings for your domain name.

### Basic Defense Configuration

Protected Domain

Web Attack Defense

CC Attack Defense

DDoS Attack Defense

Elastic defense is disabled by default

Submit

- Protected domain name
  - Select one or more domain names to connect to SCDN (wildcard domain names are not supported).
  - The domain name you select must be already connected to CDN and the CDN service is enabled.
  - Up to 10 domain names can be added at a time. The total number of domain names connected to SCDN cannot exceed the limit of your SCDN package.
- Web attack defense

Web Attack Defense

Defense Level  Loose  General  Strict

Defense Mode  Block  Observe

Blocking Page  Default Page  Custom Block Page

- You can enable web attack defense as needed.
- Defense mode: supports **Block** and **Observe** modes. The **Block** mode enables SCDN nodes to detect web attack requests and block them based on your setting, returning the default blocking page and a 403 status code, or redirecting the requests to your custom blocking page.
- Custom page address: the user-defined page to which SCDN nodes redirect the web attack requests.

- Redirect status code: supports status codes 301 and 302.
- CC and DDoS attack defense
  - CC attack defense and DDoS attack defense are enabled by default.
  - Elastic defense will be enabled by default if your package includes the service. Otherwise, it is disabled by default. For more details, see [Billing](#).

## Custom defense policy

SCDN allows you to create complex access control rules by specifying fields, such as IP, URI, Referer, User-Agent and Params, to filter requests. You can also create and combine multiple conditions with the condition logic in a single rule depending on the business scenario.

### Custom Defense Policy

You can configure custom blocking rules by specifying the client IP, access path, parameters, Referer, User-Agent header, etc.

[Add Rule](#) [Adjust Priority](#)

Rule Name	Match Condition	Action	Rule Status	Operation
No data yet				

)

**Add Custom Defense Rule**

Rule Name

Match Condition

Match Field	Logical Operator	Matching Value ⓘ	Operation
Params ▼	Include ▼	<input type="text"/>	Delete
<a href="#">Add Condition</a>			

Action

Blocking Page

Default Page [Preview](#)

Rule Status

**Confirm**

Cancel

## • Defense rule

- A maximum of five custom rules can be created and each rule can have up to five matching conditions. These rules and conditions are combined with OR and run in order from top to bottom. **If any of these conditions is met, the access is blocked.**
- Match field: supports Params, URL (only limited to path, such as `/test/1.jpg`, excluding parameters after "?"), IP (client IP), Referer, and User-Agent.
- Match condition: supports Include, Exclude, Equal to, Not equal to, Length shorter than, Length equal to, and Length longer than.
- Match value: supports only **one** match, and does not support regular expressions. It is left blank by default if not specified.

**Submitting configuration**

Click "Submit" to submit your completed domain name configuration, which takes about five minutes to be effective. In the pop-up window, click **Back to Defense Configuration** if you want to return to view or modify your configuration; click **Continue** if you want to add domain names.

# Domain Name Operations

Last updated : 2021-11-25 12:09:53

If you want to delete a domain name connected to SCDN service, you can delete it on the [SCDN console](#). You can also manage its configuration on the console.

## Deleting a Domain Name

Only an SCDN domain name with its SCDN service disabled can be deleted. After the deletion, its configuration will also be removed. The steps are as follows:

Note :

- Click **Disable** to disable the SCDN service for the domain name you want to remove, which will not affect its CDN acceleration service.
- Click **Delete** on the right of the domain name.

Domain	Status	Custom Defense Policy	Web Attack Defense	CC Attack Defense	DDoS Attack Defense	BOT Defense	Operation
<input type="checkbox"/> scdn-global-m...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <a href="#">Delete</a>
<input type="checkbox"/> xxxx.elliotxing...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <a href="#">Delete</a>

Total items: 2

20 / page

1 / 1 page

## Managing Configuration

You can view and modify the configuration for a domain name as follows:

- Click **Manage** on the right of the domain name you want on the SCDN console.
- For more details, see [Configuration Management](#).



Create a Distribution More Actions Search by domain name

Domain	Status	Custom Defense Policy	Web Attack Defense	CC Attack Defense	DDoS Attack Defense	BOT Defense	Operation
<input type="checkbox"/> scdn-global-m...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <small>Delete</small>
<input type="checkbox"/> xxx.elliotxing...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <small>Delete</small>

Total items: 2 20 / page 1 / 1 page

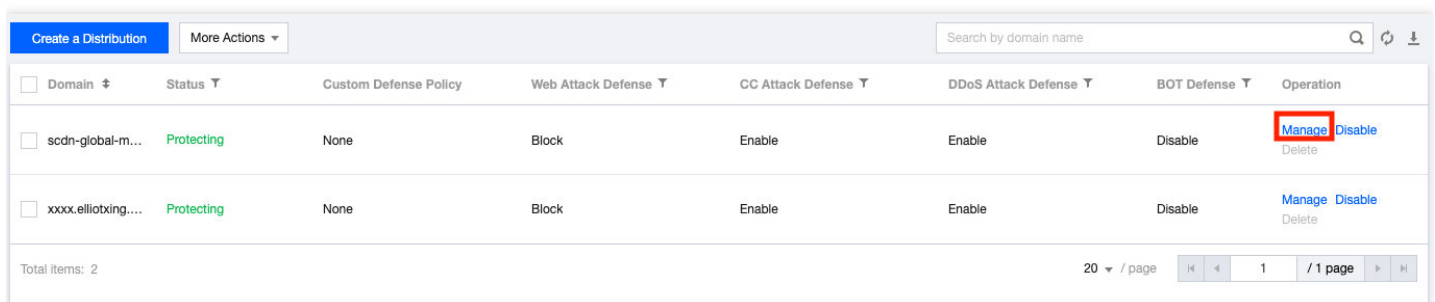
# Configuration Management

Last updated : 2021-11-25 12:14:16

On the [SCDN console](#), you can view and modify your SCDN configurations such as web attack defense and custom defense policies. Your modification will take effect in about 5 minutes once submitted.

## Configuring a Domain Name

Log in to the [SCDN Console](#), locate the domain name to check or modify its configuration, and click **Manage**.

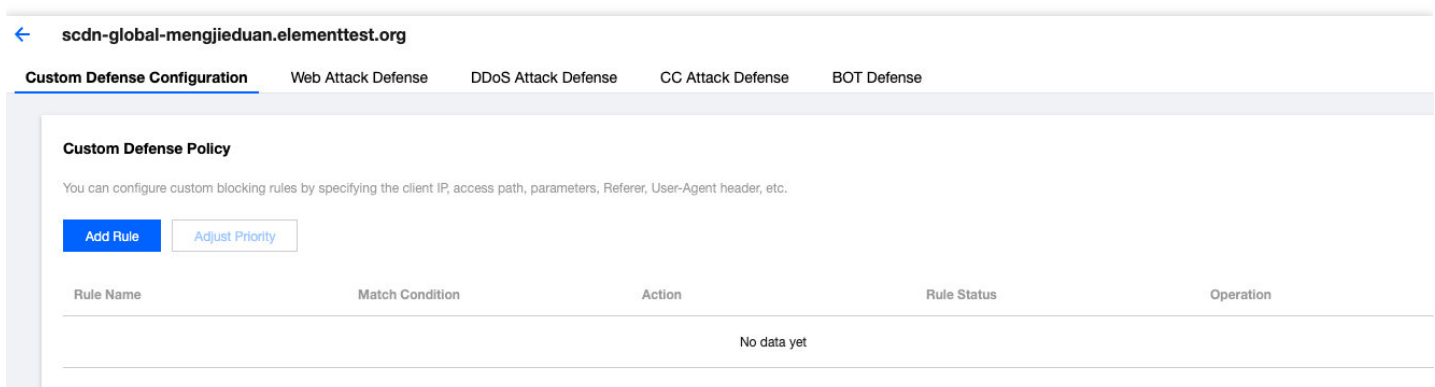


Domain	Status	Custom Defense Policy	Web Attack Defense	CC Attack Defense	DDoS Attack Defense	BOT Defense	Operation
<input type="checkbox"/> scdn-global-m...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <small>Delete</small>
<input type="checkbox"/> xxxx.elliotxing...	Protecting	None	Block	Enable	Enable	Disable	<a href="#">Manage</a> <a href="#">Disable</a> <small>Delete</small>

Total items: 2

20 / page

The domain name configuration page will display the security configuration details, including the web attack defense, DDoS attack defense and CC attack defense settings as well as custom defense policies.



← scdn-global-mengjieduan.elementtest.org

**Custom Defense Configuration** | Web Attack Defense | DDoS Attack Defense | CC Attack Defense | BOT Defense

**Custom Defense Policy**

You can configure custom blocking rules by specifying the client IP, access path, parameters, Referer, User-Agent header, etc.

[Add Rule](#) [Adjust Priority](#)

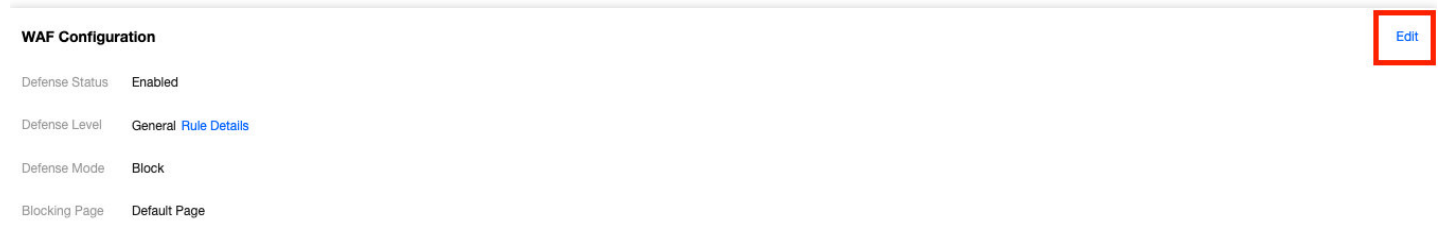
Rule Name	Match Condition	Action	Rule Status	Operation
No data yet				

## Modifying the Configuration

On the domain name configuration page, you can modify the following defense settings based on your business needs.

## Web attack defense

Based on Tencent's massive web attack samples, SCDN supports identifying good access requests from bad ones and protecting your origin server against web attacks including SQL injection, XSS attacks and local file inclusion in real time.



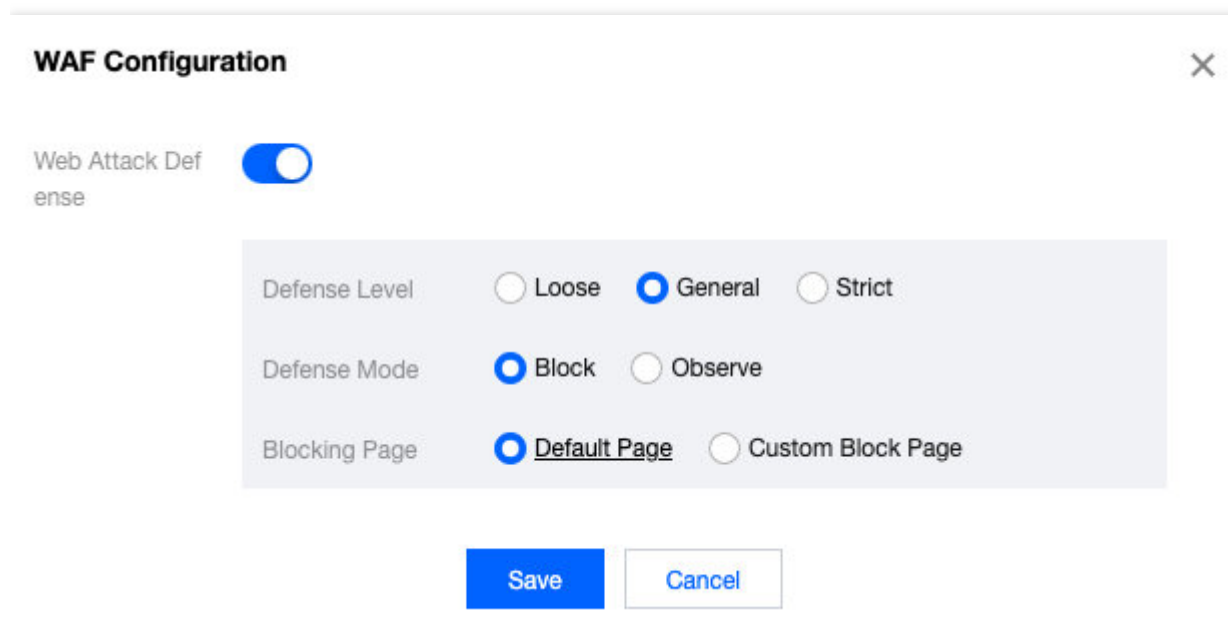
**WAF Configuration** Edit

Defense Status: Enabled

Defense Level: General [Rule Details](#)

Defense Mode: Block

Blocking Page: Default Page



**WAF Configuration** ×

Web Attack Defense

Defense Level:  Loose  General  Strict

Defense Mode:  Block  Observe

Blocking Page:  Default Page  Custom Block Page

**Save** **Cancel**

- You can enable web attack defense and set defense levels as needed.
- Defense mode: supports **Block** and **Observe** modes. The **Block** mode enables SCDN nodes to detect web attack requests and block them based on your setting, returning the default blocking page and a 403 status code, or redirecting the requests to your custom blocking page.
- Custom page address: the user-defined page to which SCDN nodes redirect the web attack requests.
- Redirect status code: supports status codes 301 and 302.

## Custom defense policy

SCDN allows you to create complex access control rules by specifying fields, such as IP, URI, Referer, User-Agent and Params, to filter requests. You can also create and combine multiple conditions with the condition logic in a single rule depending on the business scenario.

**Custom Defense Policy**

You can configure custom blocking rules by specifying the client IP, access path, parameters, Referer, User-Agent header, etc.

[Add Rule](#)
[Adjust Priority](#)

Rule Name	Match Condition	Action	Rule Status	Operation
No data yet				

**Add Custom Defense Rule**

Rule Name

Match Condition

Match Field	Logical Operator	Matching Value ⓘ	Operation
<input type="text" value="Params"/>	<input type="text" value="Include"/>	<input type="text"/>	Delete
<a href="#">Add Condition</a>			

Action

Blocking Page  [Preview](#)

Rule Status

[Confirm](#)
[Cancel](#)
**1. Adding and modifying defense rules**

- A maximum of five custom rules can be created and each rule can have up to five matching conditions. These rules and conditions are combined with OR and run in order from top to bottom. **If any of these conditions is met, the access is blocked.**
- Match field: supports Params, URL (only limited to path, such as `/test/1.jpg`, excluding parameters after "?"), IP (client IP), Referer, and User-Agent.
- Match condition: supports Include, Exclude, Equal to, Not equal to, Length shorter than, Length equal to, and Length longer than.
- Match value: supports only **one** match, and does not support regular expressions. It is left blank by default if not specified.

**2. Disabling and deleting rules**

- By clicking **Enable/Disable**, you can enable/disable rules as needed.
- By clicking **Delete**, you can delete rules as needed. The rules that you deleted cannot be restored.

### 3. Adjusting priority

- By clicking **Adjust Priority**, you can adjust the rule order, without affecting blocking requests.

## DDoS and CC attack defense

With advanced feature recognition algorithms, SCDN delivers a precise cleansing of attack traffic and an all-round protection against DDoS attacks including SYN floods, TCP floods and ICMP floods. Meanwhile, it can analyze and block malicious CC attacks using self-designed intelligent CC attack identification and blocking technologies, recommended policies, and multi-dimensional, custom rules.

- CC attack defense and DDoS attack defense are enabled by default.
- Custom IP access limit rules are supported.

**CC Attack Defense** [Edit](#)

Defense Status **Enabled**

Elastic Defense **Disabled**

---

**Custom Access Limit Rule**

Custom access limit rules can defend against CC attacks by limiting the number of requests to certain domain name paths, file extensions, full-path files, and homepages on a single node in a specified time period.

[Add Rule](#) [Adjust Priority](#)

Type	Content	Detection Granularity	Single-Node Access Limit	Action	IP Penalty	Operation
No data yet						

- Elastic defense will be enabled by default if your package includes the service. Otherwise, it is disabled by default. For more details, see [Billing](#).

# Event Logs

Last updated : 2021-11-25 12:09:54

## Overview

SCDN supports logging web attack information, including the time that SCDN received the attack request, attacker IP address, attack type, and content at which the attack targeted. It also allows you to output logs you need by setting download filters and creating log tasks.

## Downloading Logs

Log in to the SCDN console, select **Event Logs** on the left sidebar, and then create log tasks as follows:

The screenshot shows the 'Log Query' interface in the SCDN console. It features a 'Download Task' section with the following elements:

- Time range selection: Last 1 Hour, Last 6 Hours, **Today**, Yesterday, Last 7 Days, and a date range selector (2021-10-11 00:00:00 ~ 2021-10-11 19:53:45).
- Domain selection: All Domain Names, **Chinese Mainland**, and Overseas.
- Attack type selection: Web Attack, All Attack Types, and All Actions.
- Filters: A dropdown menu for Filters.
- Buttons: Query and Create Log Task (with an information icon).

Below the filters is a table with the following columns: No, Attack Time, Domain, Path Parameter, Attack Source IP, Attack Type, Attack Location, Attack Content, Action, and Operation. The table currently displays 'No data yet'.

- Click **Create Log Task**. Select the domain name you want, attack type (which can be set to all attack types or a specific one), action (which can be set to all actions or a specific one), and time period.
- Attack logs for the last seven days can be downloaded.
- A maximum of 100 log tasks can be created per day and each log task can contain up to 1,000 logs.

Attack Type	Defense Type	Domain	Protected Region	Task Details	Time Period ⌵	Creation Time ⌵	Status ⌵	Operation
Web Attack	All Attack Types	All Domain Names	Chinese Mainland	All Attack Types; All Actions;	2021-10-11 00:00:00 to 2021-10-11 19:53:45	2021-10-11 19:55:01	No logs ⓘ	Download

- After the log task is created, log files will be generated in about one minute. Click **Download**.
- Downloaded log files can be retained for seven days.