

Content Delivery Network

Advanced Tools

Product Introduction



Tencent
Cloud

Copyright Notice

©2013-2017 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

 Tencent Cloud

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

Documentation Legal Notice 2

Advanced Tools..... 4

 Manage Certificates..... 4

 Manage Traffic Packages 11

Advanced Tools

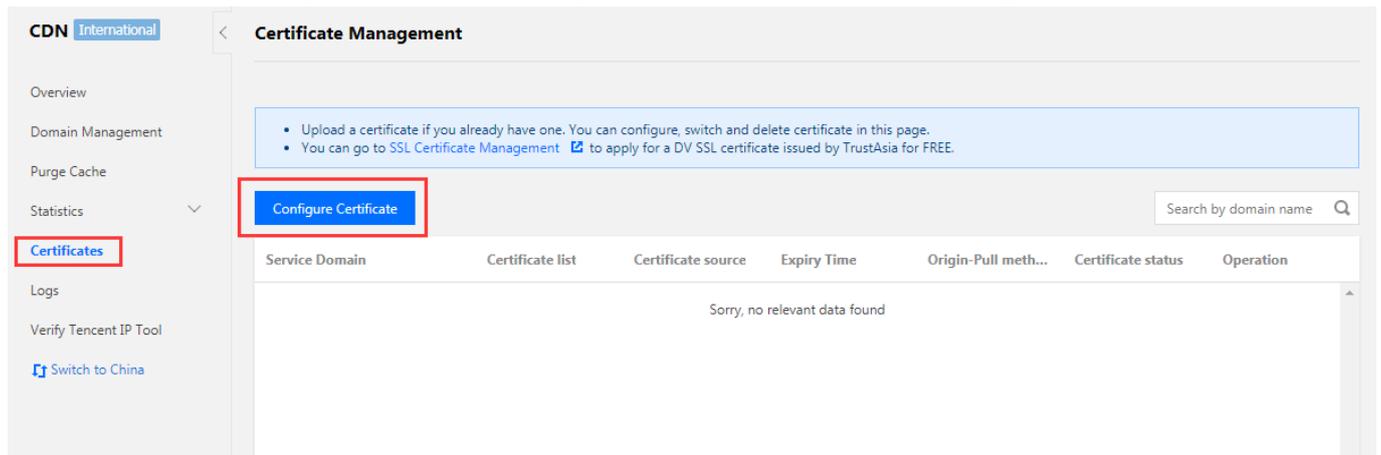
Manage Certificates

You can configure HTTPS certificate for a domain that has been connected to CDN. You can upload your existing certificate for deployment, or directly deploy the certificate hosted or issued by SSL Certificate Management platform.

You can apply for a free third party certificate from TrustAsia on SSL Certificate Management page.

Configuring Certificate

If you already have a certificate, you can upload it directly to the CDN page for configuration. Log in to [CDN Console](#), and go to Certificates page in Advanced and click "Configure Certificate":



1. Selecting a Domain

Select the accelerated domain for which you want to configure a certificate. Note:

- The domain is required to be connected to CDN with a status of Deploying or Activated. For a deactivated domain, certificate deployment is not allowed;
- When CDN acceleration has been activated for COS or Cloud Image, certificate cannot be deployed for domain

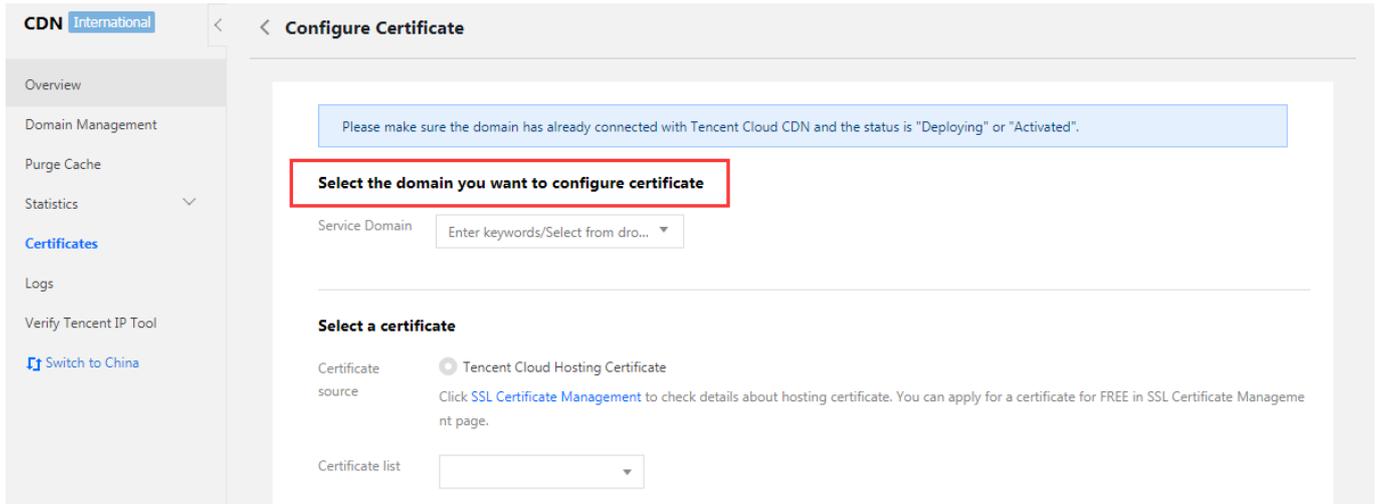
.file.myqcloud.com

or

.image.myqcloud.com

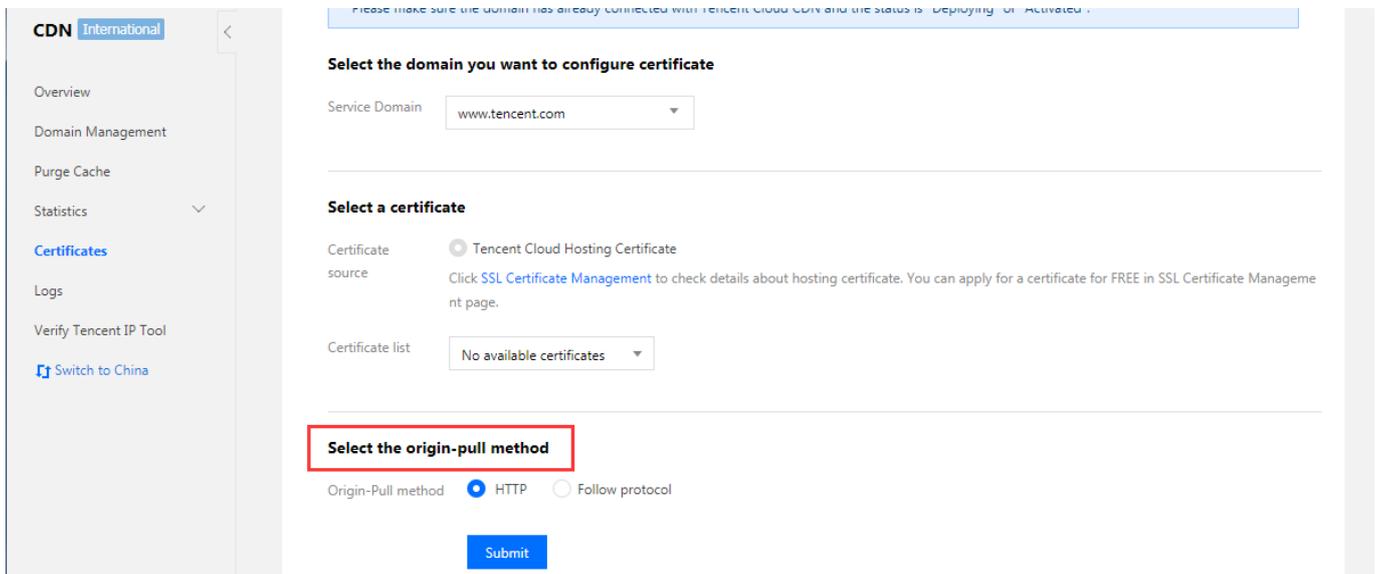
by default;

- Certificate cannot be deployed for SVN hosted origin currently.



2. Origin-Pull Method

After the certificate is configured, you can select the back-to-origin method by which CDN nodes get resources from origin server:



- If HTTP is selected, the requests sent from users to CDN nodes support HTTPS/HTTP, and the

requests sent from CDN nodes to origin server all use HTTP;

- If HTTPS is selected, the origin server is required to be already configured with a certificate, otherwise back-to-origin failure may occur. When this is checked, if the requests sent from users to CDN nodes use HTTP, the requests sent from CDN nodes to origin server also use HTTP; if the requests sent from users to CDN nodes use HTTPS, the requests sent from CDN nodes to origin server also use HTTPS;
- Currently, domains connected with COS origin or FTP origin do not support using HTTPS as the back-to-origin method;
- For the configuration of HTTPS, your origin server is required to have no port constraint or to be configured with port 443, otherwise the configuration may fail.

3. Finishing Configuration

Once the configuration is finished, you can see the domain and certificate that have been configured successfully on "Certificate Management" page.

Editing Certificate

For certificates that have been configured successfully, you can seamlessly update the certificates with "Edit" button.

- Seamless switching between self-owned certificate and Tencent Cloud hosted certificate is supported;
- Once the edited certificate is submitted, it will be deployed by seamlessly overwriting the original one without affecting your use of service.

PEM Certificate Format

The certificate issued by Root CA agency has a PEM format as show below:

Rules for certificate chain:

- No blank line is allowed between certificates;
- Each certificate shall comply with the certificate format rules described above;

PEM Private Key Format

RSA private key can include all private keys (RSA and DSA), public keys (RSA and DSA), and (x509) certificates. It stores DER data encoded with Base64 and is enclosed by ascii header, being suitable for textual transfer between systems. Example:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAziSSSChH67bmT8mFykAxQ1tKCYukwBiWZwk0StFEbTWHy8K
tTHSFD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMjclva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfz8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjin957ZEPHjtUpVZuhS3409DDM/tJ3T18aaNYWhrPBc0
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8a1L7UHDHPI4AYsatdG
z5TMPnmE f8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHRFi
laF6+Wen8ZvNqkm0hAMQwIjh1Vp1fL74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93T424WGpCwUshSfxewfbAYGF3ur8W0xq0uJ07BAxaKHNcmNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYLKGHjoiEys11ahLAJvICVgTc3+LzG2pIpM7I+K0nHC5eswM
i5x9h/OT/ujZsyX9POPpAyE2bqy0t080tGexM076Ssv0KVhKfVWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqqHu0edU
ZXIHRJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X141ox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwwNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzFEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTad1BW4led0Sa/uKRa04UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAERmtJf2yS
ICRkQaB3gPSe/lCgzy1nhtaFOUbNxxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoehkbYkAUtq038Y04EKH6S/IzMzB0frXiPKg9s8UKQzku+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn
R3kV10GMZCfAdqirAjiQWApkh9Bxbp2eHCrB81MFAWLRQSlOk79b/jVmTZMC3upd
EJ/iSWjZKpbw7hCFaERtPhxyNTJ5idEiu9U8EQid8111giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnzE9y0ZWWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKhl93HHF1joNM81LHFyGRFEWrrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

RSA private key rules:

- [---BEGIN RSA PRIVATE KEY---, ---END RSA PRIVATE KEY---] are the beginning and end, which should be uploaded with the content;
- Each line contains 64 characters, but the last line can contain less than 64 characters;

If the private key is generated using other methods than the one described above and has a format of [--- BEGIN PRIVATE KEY ---, --- END PRIVATE KEY ---], you can convert the format as follows:

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

Then upload the content of new_server_key.pem and the certificate.

PEM Format Conversion

Currently, CDN only supports the certificate with a PEM format. Any non-PEM certificates are required to be converted to PEM format before being uploaded to Cloud Load Balance. It is recommended to use openssl tool for the conversion. Here are some common methods for converting the certificate format to PEM format.

Converting DER to PEM

DER format generally occurs in Java platform.

Certificate conversion:

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

Private key conversion:

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

Converting P7B to PEM

P7B format generally occurs in Windows Server and Tomcat.

Certificate conversion:

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

Obtain [--- BEGIN CERTIFICATE ---, --- END CERTIFICATE ---] content in outcertificat.cer as a certificate for upload.

Private key conversion: no private key

Converting PFX to PEM

PFX format generally occurs in Windows Server.

Certificate conversion:

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

Private key conversion:

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

Completion of Certificate Chain

CA agency mainly provide the following three certificates: Apache, IIS, Nginx.

CDN uses Nginx. Select the certificates with an extension of .crt or .key under Nginx folder. A certificate of PEM format can be directly opened in text editor. You just need to copy and upload it.

You can also complete the certificate chain by pasting the content of CA certificate (PEM format) to the bottom of domain certificate (PEM format).

Manage Traffic Packages

If your billing method is Pay by Traffic, you can purchase a traffic package for cost saving. You can check the usage of traffic package in CDN Console to keep track of the balance of traffic package in real time and top it up in time so that your use of CDN services will not be affected.

Log in to [CDN Console](#) and select Advanced page. You'll see the Traffic Package Management feature provided by CDN:

The screenshot displays the 'Traffic Pack Management' page. On the left is a navigation sidebar with 'Data Packages' selected. The main content area shows a table of traffic packs under the 'Available Traffic Packs' tab. The table has the following data:

Type	Usage	Obtained time	Expiry Time	Source
undefined	Used: NaNTB(Total: NaNTB)			WeChat Official Account
FREE data pack	Used: 0B(Total: 10.00GB)	2017-05-01 05:35	2017-06-01	Tencent Cloud
Newbie data pack	Used: 9.90KB(Total: 50.00GB)	2017-05-01 00:00	2017-06-01	WeChat Official Account
Newbie data pack	Used: 0B(Total: 50.00GB)	2017-06-01 00:00	2017-07-01	WeChat Official Account
Newbie data pack	Used: 0B(Total: 50.00GB)	2017-07-01 00:00	2017-08-01	WeChat Official Account

At the bottom of the table, it indicates 'Total 5 items' and 'Lines per page: 10'. Navigation controls for the table are also visible.

This page provides the history of purchase and usage of traffic packages.