

# Content Delivery Network Advanced Tools Product Introduction



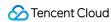


#### Copyright Notice

©2013-2018 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**

Advanced Tools

Manage Certificates

Manage Traffic Packages



# Advanced Tools Manage Certificates

Last updated: 2017-12-12 17:04:30

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

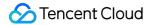
Select the accelerated domain for which you want to configure a certificate. Note:

- 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 backto-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:



-BEGIN CERTIFICATE-MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL ExZWZXJpU2lnbiBUcnVzdCB0ZXR3b3JrMTsw0QYDVQQLEzJUZXJtcyBvZiB1c2Ug YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykw0TEvMC0GA1UEAxMm VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4 MDAwMDAwWhcNMTMxMDA3MjM10TU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN 3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC AwEAAa0CAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT ZWN1cmVHMi5jcmwwRAYDVR0gBD0w0zA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19 RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq30P4y/Bi ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ 3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2L1DWGJ0GrNI NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn 1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas= ---END CERTIFICATE----

- [--- BEGIN CERTIFICATE ---, --- END CERTIFICATE ---] 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;

The certificate chain issued by intermediate agency:

```
---BEGIN CERTIFICATE---
---END CERTIFICATE---
---BEGIN CERTIFICATE---
---END CERTIFICATE---
---BEGIN CERTIFICATE---
---BEGIN CERTIFICATE---
```

#### 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--MIIEpAIBAAKCAQEAvZiSSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEbTWHy8K tTHSfD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A Xw95grqFJMJcLva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ fD0XXyuWoqaIePZtK9Qnjn957ZEPhjtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBc0/ jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8alL7UHDHHPI4AYsatdGz5TMPnmEf8yZPUYudTlxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHrFilaF6+Wen8ZvNqkm0hAMQwIJh1Vplfl74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35 cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8W0xq0uU07BAxaKHNcmNG7dGyolUowRu S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2 06W/zHZ4YAxwkTYlKGHjoieYs111ahlAJvICVgTc3+LzG2pIpM7I+K0nHC5eswvM i5x9h/OT/ujZsyX9POPaAyE2bqy0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqgHu0edUZXIHrJ9u6BlXE1arpijVs/WHmFhYSTm6DbdD7SltLy0BY4cPTRhziFTKt8AkIXMK605u0UiWsq0Z8hn1Xl4lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4ledOSa/uKRaO4UzVgnYp2aJKxtuWffvVbU +kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAErMtJf2yS ICRKbQaB3gPSe/lCgzy1nhtaF0UbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of QhGLITyoehkbYkAUtqO38YO4EKh6S/IzMzBOfrXiPKg9s8UKQzkU+GSE7ootli+a R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn R3kVl06MZCfAdqirAjiQWaPkh9Bxbp2eHCrb8lMFAWLRQSlok79b/jVmTZMC3upd EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEIu9U8EQid81l1giPgn0p3sE0HpDI89qZX aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9 BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z NTKh193HHF1joNM81LHFyGRfEWWrroW5gfBudR6USRnR/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).

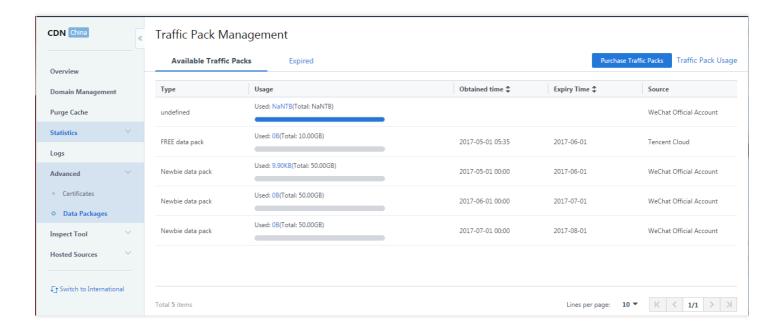


# Manage Traffic Packages

Last updated: 2018-04-03 16:34:50

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:



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