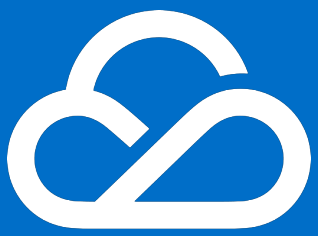
腾讯云Dynamic Site Accelerator

Operation Guide

产品文档



腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

Manage Certificates

You can configure HTTPS certificate for a domain name that has been connected to DSA. 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.

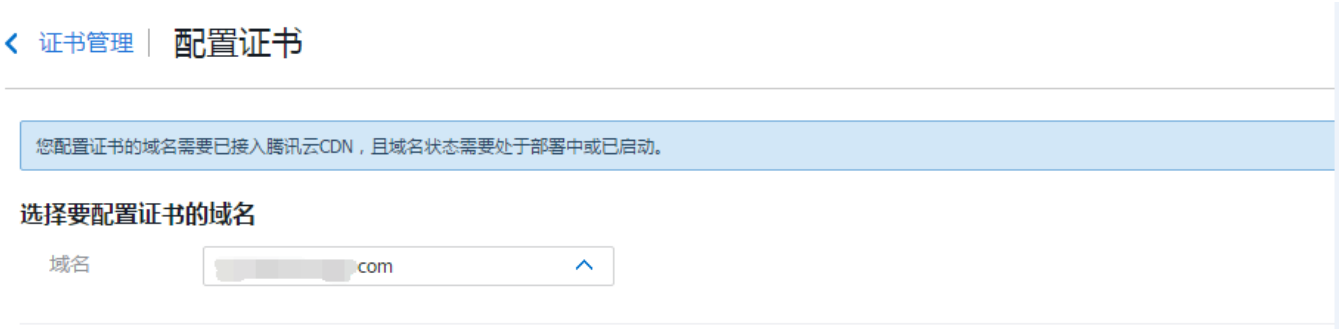
Configuring Certificate

If you already have a certificate, you can upload it directly to the DSA page for configuration. Log in to DSA Console and go to Certificate Management page, click "Configure Certificate":

1. Select a Domain Name

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

- The domain name is required to be connected to DSA and with a status of Deploying or Activated. You cannot deploy certificate for a domain name with the Deactivated status;



2. Select a Certificate

2.1 Use self-owned certificate

Select "Own Certificate", and paste the certificate content and private key to the corresponding text boxes. You can optionally add a remark for identifying the certificate.

- Certificate content must be in PEM format. For non-PEM certificates, please refer to the instructions below for format conversion;
- If your certificate has a certificate chain, please convert its content into PEM format, and

upload it with the certificate content. The instructions on completing certificate chain is described later in this document.

2.2 Use Tencent Cloud Hosted Certificate

You can apply for a free third-party certificate from TrustAsia on SSL Certificate Management page or trust an existing certificate to Tencent Cloud to use it for cloud products such as DSA, Cloud Load Balance.

Select "Tencent Cloud Hosted Certificate" to see the list of certificates available for the domain name in SSL Certificate Management:

- Select the certificate to use from the certificate list;
- The certificates are displayed as Certificate IDs (Remark) in the list . You can learn more about the certificates by going to SSL Certificate Management.

3. Origin-Pull Method

After the certificate is configured, you can select the origin-pull method by which DSA nodes acquire resources from the origin server:

- When HTTP origin-pull configuration is selected, requests sent from users to DSA nodes support HTTPS/HTTP, and requests sent from DSA nodes to the origin server all use HTTP;
- If protocol following is selected, the origin server is required to be already configured with a certificate, otherwise origin-pull may fail. If successfully configured, origin-pull requests from DSA nodes will be HTTP when requests sent from users to DSA nodes are HTTP. While origin-pull requests from DSA nodes will be HTTPS when requests sent from users to DSA nodes are HTTPS;
- 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.

4. Finish Configuration

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

Editing Certificate

For certificates that have been successfully configured, you can seamlessly update the certificates by using the "Edit" button:

- You can seamless switch between self-owned certificate and Tencent Cloud hosted certificate;
- Once the edited certificate is submitted, it will be deployed by seamlessly overwriting the original one without affecting your business.

PEM Certificate Format

The certificate issued by Root CA are in PEM format as shown below:

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

Certificate chain issued by intermediate CA:

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

Rules for certificate chain:

- No blank line is allowed between certificates;
- Each certificate shall comply with the certificate format rules described in Item 1;

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, thus it is suitable for textual transfer between systems. Example:

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, and the last line can contain less than 64 characters;

If the private key is not generated using the above method 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 along with the certificate.

PEM Format Conversion

Currently, CDN only supports certificates 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.

Converting DER to PEM

DER format usually appears on Java platforms.

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 usually appears 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 usually appears in Windows Server.

Certificate conversion:

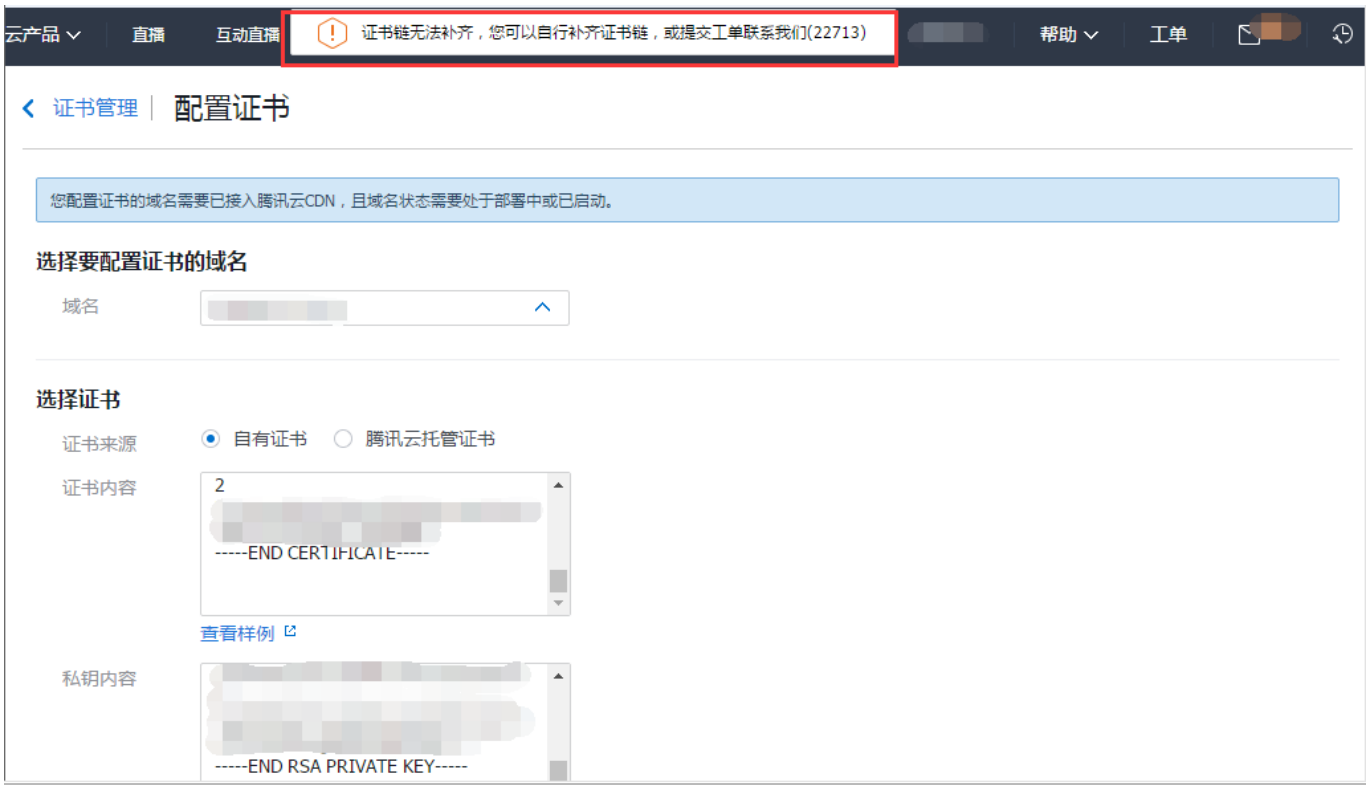
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem

Private key conversion:

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

Completing Certificate Chain

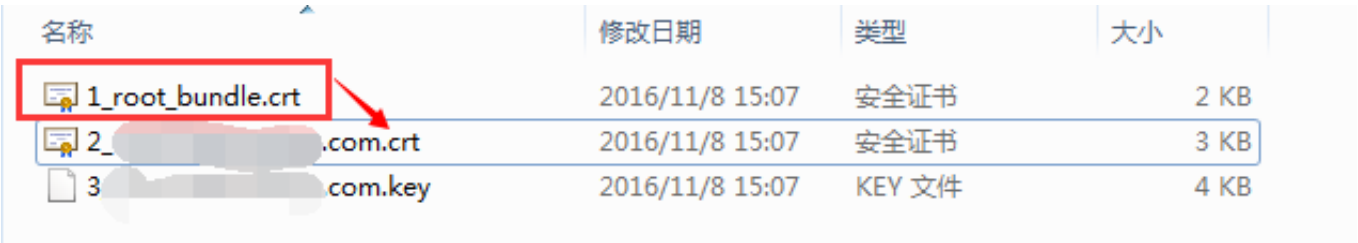
During configuration using self-owned certificate, if "Completion of Certificate Chain is Required" appears:



CA mainly provides the following three types of certificates:

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 with text editor. Simply 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):


名称
修改日期
类型
大小
1_root_bundle.crt
2016/11/8 15:07
安全证书
2 KB
2_ .com.crt
2016/11/8 15:07
安全证书
3 KB
3 com.key
2016/11/8 15:07
KEY 文件
4 KB