

腾讯云Dynamic Site Accelerator

Operation Guide

产品文档



腾讯云

## 【版权声明】

©2015-2016 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

## 【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

## 【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

文档声明.....	2
Manage Certificates.....	4

## 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;

#### ← 证书管理 | 配置证书

您配置证书的域名需要已接入腾讯云CDN，且域名状态需要处于部署中或已启动。

#### 选择要配置证书的域名

域名  ^

### 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.

### < 证书管理 | 配置证书

#### 选择要配置证书的域名

域名

#### 选择证书

证书来源  自有证书  腾讯云托管证书

证书内容

[查看样例](#)

私钥内容

[查看样例](#)

备注(选填)

#### 选择回源方式

回源方式  HTTP  协议跟随

**提交**

- 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:

← 证书管理 | 配置证书

您配置证书的域名需要已接入腾讯云CDN，且域名状态需要处于部署中或已启动。

**选择要配置证书的域名**

域名

**选择证书**

证书来源  自有证书  腾讯云托管证书

[点击 SSL 证书管理](#) 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书列表

**选择回源方式**

回源方式  HTTP  协议跟随

- 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:

#### 证书管理

- 若您已有证书，可直接上传进行配置，同时可以在本页面对证书进行无缝切换、删除等操作；
- 您可以前往 [SSL证书管理](#) 免费申请由亚洲诚信提供的DV SSL证书。

+ 配置证书
批量配置
删除

🔍

<input type="checkbox"/>	域名	证书备注	证书来源	到期时间	回源方式	证书状态	操作
<input type="checkbox"/>	www.██.com	CDN SSL Cert	腾讯云托管证书	2017-09-21	协议跟随	配置成功	<a href="#">编辑</a>   <a href="#">删除</a>

## Editing Certificate

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

[< 证书管理](#) | **配置证书**

您配置证书的域名需要已接入腾讯云CDN，且域名状态需要处于部署中或已启动。

**选择要配置证书的域名**

域名

**选择证书**

证书来源  自有证书  腾讯云托管证书

[点击 SSL 证书管理](#) 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书列表

**选择回源方式**

回源方式  HTTP  协议跟随

**提交**

- 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-----
MIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTElMAkGA1UEBhMCVVMxZjZlbnVBAoTD1Z1cm1TaWduLzBjbmMuMR8wHQYDVQQL
ExZW7Y1nI1Z1nbiBUcnVzdCB0ZXR3b3JrMTswOQYDVQQL EzJUZXJtcyBvZiB1c2Ug

bSBjbmMuMR0wGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAObjQAwYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xcvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNgh0dHA6Ly9TVLJTZW1cm1UzRzI+Y3JsLnZ1cm1zaWduLmNvbS9TVLJT
ZWN1cmVHMi5jcmwwRAYDVVR0gBD0wOzA5BAtahkaBhvFA0cXAZAqMCgGCCsGAQUF

RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZ1cm1z
aWduLmNvbTBABggrBgEFBQcAwAoY0aHR0cDovL1NWU1N1Y3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWU1N1Y3VyZUcyLmN1cjBuBggrBgEFBQcBDARiMGChXqBcMFow

1vCNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrs13dWK1dFiq30P4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmp7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeZaCxfqBiLdEIodNwzcvGJ+2L1DWGJ0GrNI

R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnc1S5vas=
-----END CERTIFICATE-----

```

- [--- 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:

```
-----BEGIN RSA PRIVATE KEY-----
Xw95grqFJMjclva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9QnJn957ZEPHjtUpVZuhS3409DDM/tJ3T18aaNYWWhrPBc0
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8a1L7UHDHPI4AYsatdG
z5TMPnmEf8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQABoIBAG168Z/nnFyRHRFi
LaF6+Wen8ZvNqkm0hAMQwIJh1Vp1fL74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
ZXIHrJ9ub8lXE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X141ox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwwNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTad1BW41ed0Sa/uKRa04UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAERMtJf2yS
R3kV10GMZCFAdqirAjiQWaPkh9BxbpZeHCrb8LMFAWLRQSlOk79b/jVmTZMC3upd
-----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, 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:

名称	修改日期	类型	大小
Apache	2016/11/8 15:07	文件夹	
IIS	2016/11/8 15:07	文件夹	
Nginx	2016/11/8 15:07	文件夹	

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:

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

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