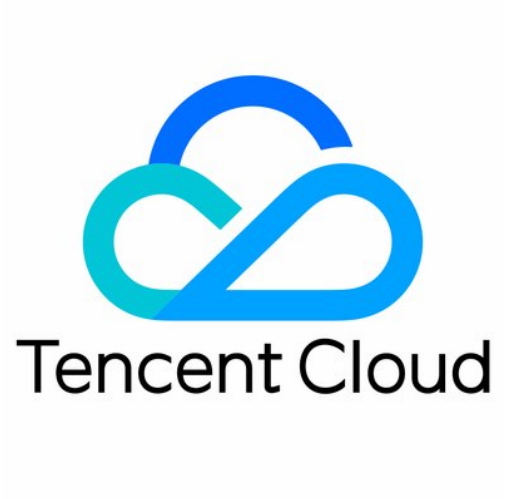
SSL Certificate Service

Announcements

Product Documentation



Contents

Announcements

Price Change to DigiCert SSL Certificates

Last updated：2024-03-06 15:40:28

Dear user,

In accordance with DigiCert’s price increase notice, we will increase the price of DigiCert SSL certificates starting January 5, 2023 (Beijing time). This price change involves GeoTrust, SecureSite, and code signing certificates. For more information, visit .

TrustAsia Root Certificate Update

Last updated：2024-03-06 15:40:28

TrustAsia Root Certificate Update

As notified by TrustAsia, TrustAsia root certificates have changed from DigiCert root certificates to Sectigo root certificates since **March 3, 2022 22:00:00**. That is, the root certificates of TrustAsia SSL certificates applied before **March 3, 2022 22:00:00** were issued by DigiCert, and those applied after **March 3, 2022 22:00:00** are issued by Sectigo.

Sectigo root certificates support Online Certificate Status Protocol (OCSP) nodes in the Chinese mainland. Therefore, the TrustAsia root certificate update greatly improves the HTTPS access speed of websites in the Chinese mainland.

Note:

This update has no effect on the SSL certificates already issued for use.

After the update, the original product features and services remain unchanged.

Domain Validation Policy Update

Last updated：2024-03-06 15:40:28

In order to comply with the requirements of CA/Browser Forum, the following changes will be introduced to domain validation policies, which take effect from **December 1, 2021**.

From December 1, 2021, file validation supports only issuing the SSL certificate for the current validated domain, but not wildcard SSL certificates as well as its subdomains.

Currently, Tencent Cloud's SSL Certificate Service only requires validating the primary domain (e.g., `dnspod.cn`), and will also issue SSL certificates for wildcard certificates (e.g., `*.dnspod.cn` or `*.sub.dnspod.cn`) and its subdomains (e.g., `sub.dnspod.cn` or `sub2.sub1.dnspod.cn`).

But from December 1, 2021, if a domain is validated using file validation, the certificate can only be issued for the domain validated. For example, if the domain `dnspod.cn` is validated using file validation, an SSL certificate can be issued only for the `dnspod.cn` domain, but not `*.dnspod.cn` or `sub.dnspod.cn`.

Note:

Please be informed that Tencent Cloud discontinued the file validation mode for wildcard certificates on **November 21, 2021**.

SSL Certificate Service Console

Last updated：2024-03-06 15:40:28

To offer a better experience, the SSL Certificate Service console has been fully upgraded through feature combination and optimization. New feature modules are added, including certificate overview, operation history, and quick start. The new console works with SSLPod to provide more comprehensive and convenient configuration and management. This document describes how to quickly get started in the console.
If you have any questions, suggestions, or comments, contact us.

Feature overview

Module	Description
Certificate Overview	The **Certificate Overview** page displays the SSL certificate application status and monitoring status and allows for other operations. Specifically: **Application Status** : You can quickly view SSL certificates in **Pending Submission , Validating , Issued** , and **Rejected** statuses and manipulate them. **Monitoring Status** : You can quickly view SSL certificate monitoring information such as Normal Access , Access Exception , and **Expiration Alert** and view the corresponding SSLPod monitoring report.
My Certificates	The **My Certificates** page allows you to view and manage SSL certificates that are being applied for as well as issued and expired SSL certificates. Specifically: View the information of certificates that are being applied for as well as issued and expired certificates. Purchase a certificate. Apply for a free certificate. Upload an existing certificate. Manage a certificate, for example, submit the application information, reissue a certificate, and renew it.
Operation History	The operation history allows you to view the operation records of existing SSL certificates. Specifically: Export operation records in CSV or JSON format. Filter operation records.
Certificate Monitoring	This feature enables the collaboration between SSL Certificate Service and SSLPod, facilitating management and use.

Multi-Year SSL Certificate and Automatic Review

Last updated：2024-03-06 15:40:28

This document describes multi-year certificate purchase and automatic profile review, two features newly added to the SSL Certificate Service console to enhance your experience when applying for a certificate and reapplying for one during renewal.

If you have any questions, suggestions, or comments, contact us.

Feature overview

Note:

The specific operations are as displayed in the console.

Module	Description
My Profile	On the **My Profile** page, you can add the organization, administrator, and domain information for review. Specifically: Organization information management: Manage organization information, for example, add, modify, and delete an organization. Domain information management: Manage a domain of an organization, for example, add, modify, and delete a domain, and verify the domain ownership.
Multi-Year Certificate	You can log in to the SSL certificate purchase page to purchase a multi-year certificate of a certain brand. Tencent Cloud will issue a new certificate before the current one expires, relieving you of the concern that CAs may shorten the validity period of a certificate.

Notice on Stopping the Issuance of 2-Year SSL Certificates by CAs Starting from September 1, 2020

Last updated：2024-03-06 15:40:28

Due to the changes in Apple and Google's root store policies, as of September 1, 2020, newly issued SSL/TLS certificates with a validity period greater than 13 months (397 days) will be prohibited by policy and will not be trusted. Starting from September 1, 2020, global CAs will no longer issue 2-year SSL certificates. Tencent Cloud will also stop providing the 2-year SSL certificate purchase service from August 25, 2020. To purchase a 2-year SSL certificate, ensure that it is requested and issued before August 25, 2020.
FAQs:

What changes will the policy changes bring?

Due to the root store policy changes of Apple and Google, as of September 1, 2020, the validity periods of newly issued SSL/TLS certificates cannot exceed 13 months.

When will the policy changes take effect?

September 1, 2020.

I just bought a 2-year SSL certificate. Will it still be trusted after September 1, 2020?

Certificates issued before September 1, 2020 with a validity period longer than 397 days will not be affected by the policy changes.

What happens if I reprocess a 2-year certificate after the policy changes take effect?

If you reprocess a 2-year certificate after September 1, 2020, the validity period of the reissued certificate will be limited to 397 days.

Note:

Thank you for your support for Tencent Cloud. We will, as always, continue to provide you with professional HTTPS services.
If you encounter any problems while using our services, contact us for assistance by submitting a ticket.

Announcement on Stop Using the Symantec SSL Certificate Name After 30 April 2020

Last updated：2024-03-06 15:40:28

DigiCert (formerly Symantec) noted that the Symantec logo would not be used on its SSL certificate after 30 April 2020.

Updates

1. The Symantec SSL Certificate is renamed as DigiCert Secure Site SSL Certificate, as shown in the following figure.

2. Norton Secured Seal is also updated, as shown in the following figure.

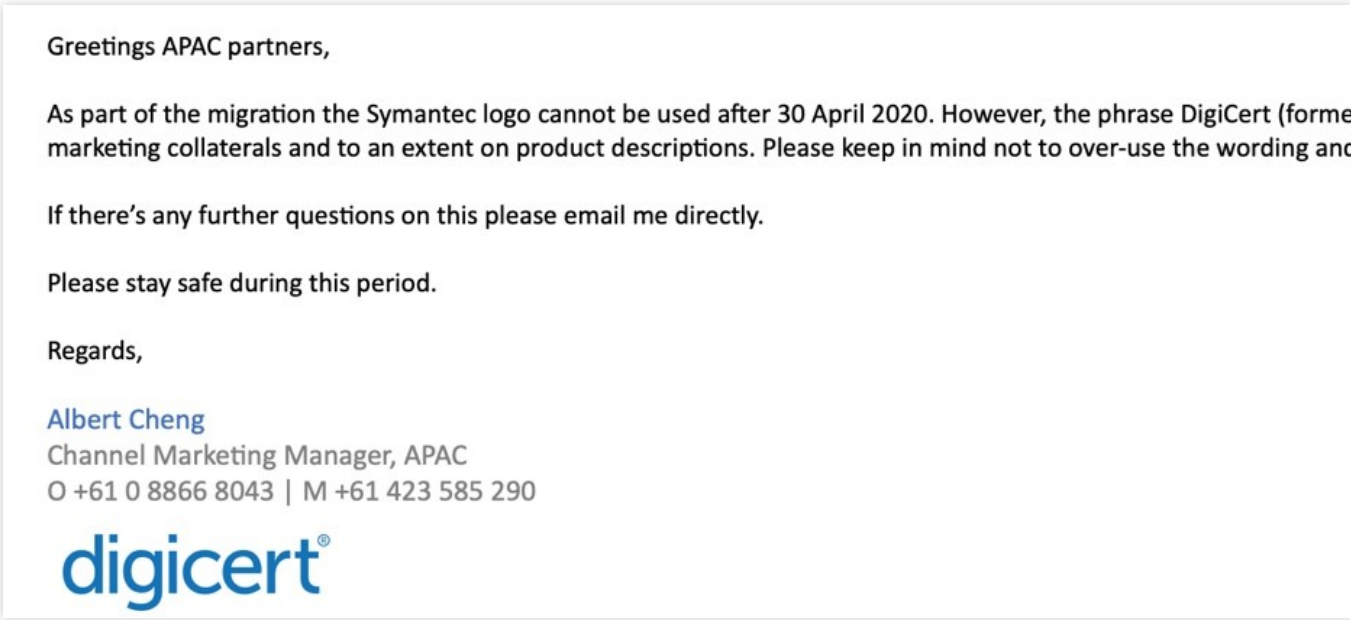
Note：

Renaming exerts no influence on certificate delivery and use.

After renaming, the original product features and services remain unchanged. Moreover, DigiCert provides Secure Site Pro to support the post-quantum algorithm feature.

DigiCert Announcement

The following figure shows the announcement from DigiCert:



Greetings APAC partners,

As part of the migration the Symantec logo cannot be used after 30 April 2020. However, the phrase DigiCert (forme
marketing collaterals and to an extent on product descriptions. Please keep in mind not to over-use the wording and

If there's any further questions on this please email me directly.

Please stay safe during this period.

Regards,

Albert Cheng
Channel Marketing Manager, APAC
O +61 0 8866 8043 | M +61 423 585 290

digicert®

Note：

Thank you for your support for Tencent Cloud. We will, as always, continue to provide you with professional HTTPS service.

If you have any problems when using our services, contact us by submitting a ticket.

Notice on Certificate Revocation Due to Private Key Compromises

Last updated：2024-03-06 15:40:28

Certificate Authorities (CAs) automatically detect private key compromises on project code hosting platforms such as GitHub and SourceForge. When detecting compromised private keys, they will notify subscribers and revoke the corresponding certificates 24 hours later.

To protect your website and information security, please keep your certificate's private key safe. Do not upload your private key to public networks to avoid incidents such as certificate revocation or information leakage.

Note:

Thank you for your support for Tencent Cloud. We will continue to provide you with professional HTTPS services.

If you have problems when using the product, please feel free to contact us.

Notice on Application Limits for DV SSL Certificates

Last updated：2024-03-06 15:40:28

Due to the policy adjustments of CAs and certificate agents, from January 1, 2018, you can apply for 20 free TrustAsia DV SSL certificates at most for one primary domain (the second-level domain and its subdomains, such as `tencent.com`, `ssl.tencent.com`, and `ssl.ssl.tencent.com`, belong to the same primary domain). Issued certificates will continue to be valid within their validity periods. If your business is affected by the adjustments, we recommend you purchase wildcard SSL certificates.

Note:

From September 1, 2022, the quota for one Tencent Cloud UIN account to apply for a free certificate will be reduced from 50 to 20.

Thank you for your support for Tencent Cloud. We will continue to provide you with professional HTTPS services.

If you have problems when using the product, please feel free to contact us.

Notice on Adjustment of Free SSL Certificates Policy

Last updated：2024-06-24 14:50:29

Dear Tencent Cloud user,
To provide better service, **Tencent Cloud SSL Certificates will adjust the free certificates policy at 00:00 on April 25, 2024 (Thursday) (UTC+8)**.

The validity period of free SSL certificates will be shortened from 12 months to 3 months.

We have received a notification from the vendors about The Adjustment of the Validity Period of Free SSL Certificates. **The validity period of free SSL certificates will be adjusted from 12 months to 3 months**. Starting from 00:00 on April 25, 2024 (UTC+8), the validity period of free SSL certificates applied on Tencent Cloud will be shortened from 12 months to 3 months. This change will not affect certificates issued before April 25, 2024.
Note：
1. Certificates applied before 00:00 on April 25, 2024, which are still under review, will still have a validity period of 12 months after the review is passed. If the certificate review fails, the validity period will be changed to 3 months after the application is resubmitted.
2. The certificate validity period is counted from the date of certificate issuance.

The quota of free SSL certificates will be uniformly increased to 50.

To facilitate organization users to better manage certificates and meet the needs of more usage, after 00:00 on April 25, 2024, **the quota of free certificates for enterprise accounts will be increased from 10 to 50, and the quota of free certificates for individual accounts will remain unchanged at 50.**

Free SSL certificates will no longer be restricted by Tencent Cloud domain name quota and domain name quota across the entire internet.

After 00:00 on April 25, 2024, **Tencent Cloud free SSL certificates can be bound to any domain name, and there will be no distinction between Tencent Cloud domain name quota and domain name quota across the entire internet**, which will bring you greater flexibility and convenience when using Tencent Cloud SSL certificates.

Free SSL certificates will no longer be restricted by the domain name quota.

Before April 25, 2024, the same parent domain name could bind up to 20 subdomain names, and no more applications could be made after exceeding the limit. After 00:00 on April 25, 2024, **there will be no parent domain quota limit for free SSL certificates**.

Let's Encrypt Root Certificate Expired on September 30, 2021

Last updated：2024-03-06 15:40:28

The old Let's Encrypt SSL root certificate (Root CA) was disused on **September 30, 2021**. If deployed with Let's Encrypt SSL certificates not updated before expiration, your websites may not be trusted by PCs, devices, or web browsers, the compatibility may be compromised, and certain websites may even become inaccessible, affecting your normal use.

To avoid affecting your business, you can check your Let's Encrypt SSL certificates for these issues through SSLPod and view the report details.

Note:

If the above issues exist, we recommend that you update to SSL certificates of other brands as soon as possible, thereby preventing the consequences of the Let's Encrypt root certificate expiration at the source.

Tencent Cloud does not sell or issue Let's Encrypt certificates, so you can ignore this notice if your SSL certificates are issued by Tencent Cloud.