ALIBABA CLOUD

# Alibaba Cloud

## SSL Certificates
## Product pricing

Document Version: 20201230

Alibaba Cloud

# Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

# Document conventions

| Style | Description | Example |
|---|---|---|
| ⚠ **Danger** | A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. | ⚠ **Danger:**<br>Resetting will result in the loss of user configuration data. |
| 🔔 **Warning** | A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. | 🔔 **Warning:**<br>Restarting will cause business interruption. About 10 minutes are required to restart an instance. |
| 📢 **Notice** | A caution notice indicates warning information, supplementary instructions, and other content that the user must understand. | 📢 **Notice:**<br>If the weight is set to 0, the server no longer receives new requests. |
| ⓘ **Note** | A note indicates supplemental instructions, best practices, tips, and other content. | ⓘ **Note:**<br>You can use Ctrl + A to select all files. |
| > | Closing angle brackets are used to indicate a multi-level menu cascade. | Click **Settings**> **Network**> **Set network type**. |
| **Bold** | Bold formatting is used for buttons , menus, page names, and other UI elements. | Click **OK**. |
| `Courier font` | Courier font is used for commands | Run the `cd /d C:/window` command to enter the Windows system folder. |
| *Italic* | Italic formatting is used for parameters and variables. | `bae log list --instanceid`<br>*Instance_ID* |
| [] or [a\|b] | This format is used for an optional value, where only one item can be selected. | `ipconfig [-all\|-t]` |
| {} or {a\|b} | This format is used for a required value, where only one item can be selected. | `switch {active\|stand}` |

# Table of Contents

# 1.Billing

SSL Certificates Service allows you to purchase SSL certificates that are billed on a subscription basis. This topic describes the billing of SSL Certificates Service.

## Subscription SSL certificates

If you purchase a subscription SSL certificate in the SSL Certificates Service console, you can select one year as the subscription duration.

For more information about certificate prices, visit SSL Certificates Service buy page.

## Expiration

If your purchased SSL certificates or value-added services expire, they are automatically stopped.

- You are notified by emails or text messages seven days before expiration. If you do not renew the certificates or services before they expire, your website can no longer provide HTTPS-encrypted data transmission.
- After expiration, the system retains the settings of your SSL certificates and value-added services for seven days. If you renew the certificates and services within the seven days, you can directly use the original settings. If you do not renew the certificates and services within the seven days, the settings are cleared. If this happens, you must configure the settings again when you purchase SSL certificates or value-added services.

## References

Select and purchase certificates

Renewal upon expiration

What is the price of SSL certificates?

"Failed to open" error when purchasing a certificate

What should I do when my SSL certificate expires?

# 2.Renewal upon expiration

You must renew your SSL certificate before it expires. Otherwise, you cannot continue to use the SSL certificate, which may cause your website to be marked as not secure. Alibaba Cloud SSL Certificates Service allows you to renew your certificate upon expiration. For early renewals, the remaining validity of your certificate will be added to the validity period of the renewed certificate.

## Prerequisites

You have purchased a GlobalSign certificate.

> ? **Note** Renewal is supported only for GlobalSign certificates, but not for Entrust certificates.

## Context

Post-payment is not accepted. You must pay first to use an SSL certificate.

The SSL Certificates Service console will notify you of upcoming expiration 60 days in advance. You must renew your certificate 3 to 10 business days before it expires to ensure that the certificate renewal can be approved before your certificate expires.

If you renew your certificate before it expires, Alibaba Cloud automatically adds the remaining validity of the old certificate to the validity period of the renewed certificate. However, this rule does not apply to free Domain Validation (DV) certificates and Digicert DV wildcard certificates.

For example, an issued certificate with one-year validity will expire on May 1, 2021. If you renew the certificate on April 25, 2021, the renewed certificate will be valid for one year plus six days starting from April 25, 2021. This means that your renewed certificate will expire on May 1, 2022. Alibaba Cloud has added the remaining validity of your old certificate to the validity period of the renewed certificate.

> ? **Note** If your existing certificate is about to expire and you purchase a new certificate instead of renewing the existing certificate upon expiration, the remaining validity of the existing certificate cannot be added to the validity period of your newly purchased certificate.

A renewed certificate is issued faster than a newly purchased certificate.

## Limits

Make sure that the certificate you want to renew is a GlobalSign certificate.

> ? **Note** Renewal is supported only for GlobalSign certificates, but not for Entrust certificates.

The renewed certificate must be consistent with the existing certificate in terms of certificate type, certification authority (CA), and applicant information. Otherwise, the renewed certificate will be identified as a newly purchased certificate, and the remaining validity of your existing certificate will not be counted.

## Step 1: View certificates that are about to expire

1.
2. View **Will Expire** certificates.
3. (Optional)View the notes about certificate renewal before you renew a certificate.In the certificate

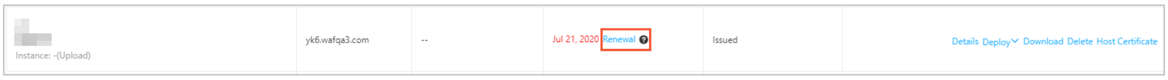
list of the Pending Expiration section, move the pointer over ? in the **Expire On** column to view the renewal notes.

- After you renew a certificate, log on to the SSL Certificates Service console and apply for certificate renewal as instructed.
- The console stores your previous application information. Therefore, you do not need to enter the information again during the application.
- Wait for the CA to approve your application. After the renewal is completed, you will obtain a renewed certificate.
- After the renewed certificate is issued, replace your expiring certificate with the renewed certificate.

Alternatively, click **Renew Now** above the certificate list to obtain the certificate renewal procedure.

## Step 2: Renew a certificate

1. In the certificate list of the **Pending Expiration** section, find the target certificate and click **Renewal** in the **Expire On** column.



| | | | | | |
|---|---|---|---|---|---|
| Instance: -(Upload) | yk6.wafqa3.com | -- | Jul 21, 2020 Renewal ? | Issued | Details Deploy Download Delete Host Certificate |

2. On the certificate buy page, select the type and configuration of your certificate.

> Note
>
> - After the renewal is completed, you will receive a new certificate order. You must apply for the certificate, so that the CA can issue it.
> - The brand and type of the certificate after renewal are the same as those of the certificate that you purchase.

3. Click **Buy Now**.
4. Select **I agree to the Alibaba Cloud certificates service (subscription) agreement of service**, and click **Pay** to complete the renewal.
5. Log on to the SSL Certificates Service console. In the **Confirm that the renewal has been completed?** dialog box, click **OK**.
6. In the certificate list of the **Pending Expiration** section, find the certificate that has been renewed and click **Certificate Application** in the **Actions** column to submit the information for verification.For more information, see Apply for and validate certificates.

> Note When you apply for a certificate, Alibaba Cloud SSL Certificates Service automatically synchronizes the application information and data that you submitted last time.

7. Click **Submit**.
8. Wait for the CA to approve and issue the certificate.The issuance of a DV certificate takes about 5 to 10 minutes, and the issuance of an OV or EV certificate takes at least two business days.
9. Install the renewed certificate on your server to replace the certificate that is about to expire.

> Note If you do not install the renewed certificate on your server, the HTTPS service will become unavailable after the existing certificate expires.

## Step 3: Check whether the certificate has been updated

After you install the renewed certificate on your server, click the security lock in the address bar of your browser to check whether the certificate validity period has been updated. If a new validity period is displayed, your certificate has been updated.

- View the validity period of the renewed certificate on a Linux server

```
echo | openssl s_client -servername www.yourwebsite.com -connect www.yourwebsite.com:443 2>/dev/
null | openssl x509 -noout -dates
```

- View the validity period of the renewed certificate on a Windows server

## References

- Install SSL certificates on Tomcat servers
- Install SSL certificates on Apache servers
- Deploy SSL certificate on Ubuntu Apache2
- How do I deploy the issued certificate in Apache server
- Install an SSL certificate on an NGINX or Tengine server
- Install SSL certificates in IIS servers
- Deploy SSL certificates in CentOS Tomcat 8.5 or Tomcat 9.0
- An SSL certificate is configured by the jetty server

# 3.Refund instructions

You can request a full refund for a purchased SSL certificate when specific conditions are met. This topic describes the conditions and steps on how to request a refund in the SSL Certificates Service console.

## Refund conditions

You can request a refund for a purchased SSL certificate in the SSL Certificates Service console when specific conditions are met.

Notice

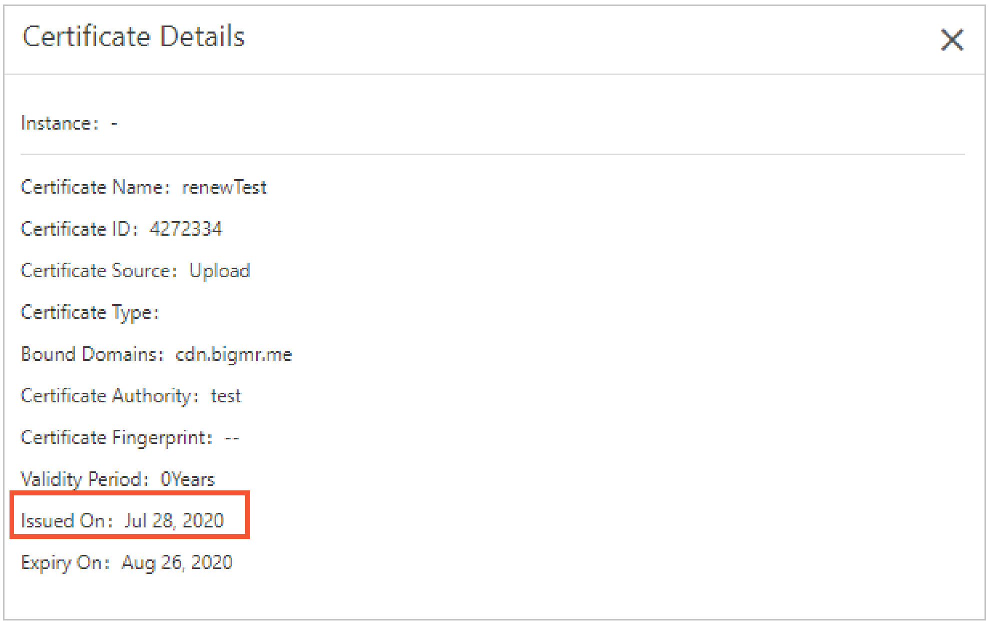
- You must submit a refund request at least 15 business days before the SSL certificate expires. Otherwise, you may fail to complete the refund process and receive the refund before the SSL certificate expires.
- If you purchased an SSL certificate by using a voucher, you cannot request a refund for the voucher.
- If the refund for an unissued SSL certificate fails, you can continue to use the certificate.
- You cannot request a refund for a free DV SSL certificate no matter whether it is valid.

The following table describes specific conditions for refunds.

| Whether an SSL certificate is issued | Duration | Whether the SSL certificate is submitted for validation | Refund | Refund amount | Remarks |
|---|---|---|---|---|---|
| Unissued | No more than 5 calendar days after purchase | **Not submitted** or submitted but **not validated** | Supported | Full refund | Manual validation is not required. You can immediately receive the refund after you submit the refund request. |
| Unissued | More than 5 calendar days after purchase to 15 calendar days before expiration | **Not submitted** or submitted but **not validated** | Supported | Full refund | Manual validation is required. The validation process requires up to 15 business days, but it is usually completed within 5 business days. You can immediately receive the refund after validation. For more information about how to view the expiration time of an SSL certificate, see What to do next. |
| Unissued | Within 15 calendar days before expiration | No matter whether the SSL certificate is validated | Not supported | None | If you submit a refund request within 15 business days before the SSL certificate expires, the request may not be validated before the expiration, and therefore the refund fails. |

| Whether an SSL certificate is issued | Duration | Whether the SSL certificate is submitted for validation | Refund | Refund amount | Remarks |
|---|---|---|---|---|---|
| Issued | Revocation completed within 28 calendar days after issuance | Validated | Supported | Full refund | Manual validation is required. The validation process requires up to 15 business days, but it is usually completed within 5 business days. You can immediately receive the refund after validation. |
| Issued (more than 28 calendar days after issuance) | Not expired | Validated | Not supported | None | None |
| Issued or unissued | Expired | No matter whether the SSL certificate is validated | Not supported | None | None |

In the certificate list, you can filter SSL certificates in the **Issued** state. Then, find an SSL certificate and click **Details** in the **Operate** column. In the **Certificate Details** panel, you can view the date when the SSL certificate was issued.



Certificate Details

Instance: -

Certificate Name: renewTest

Certificate ID: 4272334

Certificate Source: Upload

Certificate Type:

Bound Domains: cdn.bigmr.me

Certificate Authority: test

Certificate Fingerprint: --

Validity Period: 0Years

Issued On: Jul 28, 2020

Expiry On: Aug 26, 2020

## Refund procedure

1.
2. On the **Overview** page, find the SSL certificate for which you want to request a refund, and click

**Refund**.

> **Note** You can find the SSL certificate in the certificate list. If an SSL certificate is in the **Issued** state and has been issued for more than 30 calendar days, the system does not display the **Refund** button for this certificate.

3. In the **Refund Application** panel, specify **Refund Reasons**.

   The following reasons are supported.

| Reason | Operation |
|---|---|
| I failed to apply for or install the certificate, and do not know where to get help. | Click **Next** to determine whether to seek technical support. If you require technical support, enter your DingTalk information or mobile number in the **Refund Application** panel. Alibaba Cloud technical support will contact you in a timely manner.<br>**Note** Make sure that the DingTalk information and mobile number you enter are valid. |
| The certificate application process is stuck in the Verifying or Verification Failed state. This affects my business. | Click **Next** to determine whether to seek technical support. If you require technical support, enter your DingTalk information or mobile number in the **Refund Application** panel. Alibaba Cloud technical support will contact you in a timely manner.<br>**Note** Make sure that the DingTalk information and mobile number you enter are valid. |
| The type of the renewed certificate is inconsistent with that of the original certificate. I want to claim a refund and purchase a new certificate. | Go to Step 4. |
| I no longer need the certificate. | Go to Step 4. |
| Other | Enter your feedback or suggestions. |

4. Click **OK**.

   After you submit the refund request, the state of the SSL certificate on the **Overview** page in the SSL Certificates Service console changes to **Validating Application**.

> **Note** The validation process requires up to 15 business days, but it is usually completed within 5 business days. The refund is returned to the Alipay account, online bank account, or Alibaba Cloud account that you used to pay for the purchase order.

After you submit a refund request, you can cancel the refund request, view the refund progress, or check the validity period of the SSL certificate. For more information, see What to do next.

## What to do next

- ### Cancel a refund request

  If you want to cancel a refund request, find the SSL certificate on the **Overview** page and click **Cancel refund**.

  > Note You can cancel the refund request only for an SSL certificate in the **Validating Application** state.

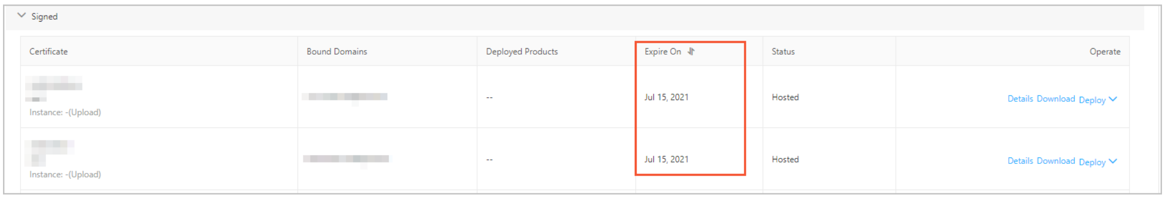
- ### View the refund progress

  If you want to view the refund progress, filter the SSL certificates in the **Refunded** state in the SSL Certificates Service console. If the refund request is rejected, the system provides further details.

- ### Check the validity period of an SSL certificate

  - #### Issued

    If the SSL certificate is issued, filter SSL certificates in the **Issued** state in the certificate list. Then, find the SSL certificate and check the value of **Expire On**.



Signed

| Certificate | Bound Domains | Deployed Products | Expire On | Status | Operate |
|---|---|---|---|---|---|
| [redacted]<br>Instance: -(Upload) | [redacted] | -- | Jul 15, 2021 | Hosted | Details Download Deploy |
| [redacted]<br>Instance: -(Upload) | [redacted] | -- | Jul 15, 2021 | Hosted | Details Download Deploy |

  - #### Unissued

    The validity period of an SSL certificate starts from the date when the certificate was issued. If an SSL certificate is not issued, it does not expire. In this case, the SSL certificate is in a state other than **Issued**, such as in the **Paid** or **Validating Application** state.

## References

Billing

# 4.SSL certificate billing and activation

## 4.1. What is the price of SSL certificates?

The price of SSL certificates depends on the factors such as the number of domains, years, and servers you need these SSL certificates for, please see Billing.

## 4.2. What should I do when my SSL certificate expires?

When your SSL certificate expires, it becomes unavailable. You must purchase another one. After purchasing a new certificate, you need to re-bind the domain name and submit materials for review.

Once the review process is complete, a new certificate is issued. To replace the expired certificate, you must install the new SSL certificate on your server.

> ⓘ **Note** Purchase the replacement certificate three to ten working days before certificate expiration so that the new certificate can be reviewed before the existing certificate expires.

For more information, see New purchase upon expiration.

## 4.3. How do I renew my certificate?

Alibaba Cloud SSL Certificates Service allows you to renew a certificate before it expires. The remaining validity period of the original certificate is added to the validity period of the renewed certificate. To comply with the requirements of CAs, SSL Certificates Service does not support auto-renewal. You must manually renew certificates.

A renewed certificate must be consistent with the original certificate in terms of the certificate type, brand, and enterprise information. Otherwise, the renewed certificate is identified as a purchased certificate. In this case, the remaining validity period of the original certificate is not added.

You must renew a certificate in the SSL Certificates Service console. For more information, see Renewal upon expiration.

> ⓘ **Note** If your existing certificate is about to expire and you purchase a new certificate instead of renewing the existing certificate upon expiration, the remaining validity of the existing certificate cannot be added to the validity period of your newly purchased certificate.