

# Alibaba Cloud SSL Certificates

Procedure of certificate applying and  
verifying

Issue: 20200709

# 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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 contact Alibaba Cloud directly if you discover any errors in this document.



# Document conventions

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

---

<b>Style</b>	<b>Description</b>	<b>Example</b>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	switch {active stand}



# Contents

---

<b>Legal disclaimer.....</b>	<b>I</b>
<b>Document conventions.....</b>	<b>I</b>
<b>1 FAQ.....</b>	<b>1</b>
1.1 Domain name certificate application note.....	1
1.2 Notes on completing information for fee-based certificate requests.....	1
1.3 Guidelines for OSS users applying for SSL certificates.....	2
1.4 How do I select: certificate type-certificate brand-number of protected domain names?.....	3
1.5 How do I enter domains to be added to a certificate?.....	4
1.6 How do I request certificates for multiple wildcard and hybrid domains?.....	5
1.7 What do I need to do after I submit a certificate verification request?.....	7
1.8 Can an already-in-use SSL certificate be used if the IP of a server is changed?.....	7
1.9 Why does my certificate order status remain unchanged even after receiving a notification from the CA?.....	8
1.10 What can I do if my order is accidentally closed or some information is incorrect?.....	8

# 1 FAQ

---

## 1.1 Domain name certificate application note

When the domain name console automatically issues a domain name association certificate, it can be automatically issued without requiring the user to apply for the certificate, there are the following prerequisites for the configuration of the relevant subsequent certificate issuance and verification file:

- Domain name in ALI cloud WAN network
- Cloud analytics in ALI cloud

If cloud resolution is not in ALI cloud, the autoissue cannot be completed after the certificate application. If the user does not have the ability to configure DNS resolution, it is recommended that DNS resolution be transferred to Ali cloud, authorization is automatically configured for DNS authentication parsing records in the background so that the issue can be completed.

When there is a large number of certificate-issuing requirements, it is recommended that you transfer DNS resolution to Ali cloud, certificate Application and management work can be greatly simplified.

- Domain Name certified by real name
- Domain name within the effective period

## 1.2 Notes on completing information for fee-based certificate requests

When completing information for fee-based certificate requests, make sure that the following information is entered correctly so that the certificate can be issued more quickly.

### **Company Name**

The company name must be exactly the same as that written in the business license.

### **Company Phone**

We strongly recommend that you provide a phone number that is available on a third-party public information platform or one that is on file with an administration for handling

industry and commerce queries. The reviewing staff may attempt to contact you for additional operations.

### Confirmation email

- Make sure that this email address belongs to the requester contact.
- For any need to verify domain information in the certificate request, make sure that you provide a administrator email ID so that a verification email can be sent.
- If the domain administrator's phone number is specified as the requester contact number, we recommend that you provide the domain administrator's email ID as the email for request confirmation (any change to, and confirmation of, the request information can be sent to this email ID). All these factors make the certificate issuance process smooth and easy.
- To request an EV certificate, the email must be a business or a fee-based email ID, that is , not a free email ID.
- Domain protection must be disabled so that the issuing staff can find the administrator email ID for your domains. Privacy Protection close mode, please refer to setting up domain name privacy protection.

## 1.3 Guidelines for OSS users applying for SSL certificates

This topic provides guidelines for Alibaba Cloud OSS users to apply for SSL certificates.

You can manage your SSL certificates in the OSS console as follows:

1. Apply for a new SSL certificate.
2. Upload an existing SSL certificate for management.

Procedure: choose **Bucket > Domain Name > Certificates Service**.

### Paid version of EntrustOV or EntrustEV SSL certificates

Your domain name must be hosted on Alibaba Cloud so that Alibaba Cloud can automatically issue the certificate that you have applied for.

If the DNS record is not hosted on Alibaba Cloud, the certificate you applied for cannot be automatically issued. You must check the certificate **Status** in SSL Certificates console and configure the DNS record as instructed.



#### Note:

If you are not authorized to configure DNS records, we recommend you authorize Alibaba Cloud to configure the DNS record for you. If you are authorized to configure DNS records, purchase a DV SSL certificate in the [Alibaba Cloud SSL Certificates console](#). After you purchase the certificate, follow the DNS verification requirements shown in the console to configure a TXT DNS record on the third-party DNS resolution platform. This demonstrates your ownership to the domain name, so that your SSL certificate can be issued.

If a large number of SSL certificates need to be issued, we recommend that you authorize Alibaba Cloud to configure the DNS record for you. This simplifies the procedure of certificate application and management.

## 1.4 How do I select: certificate type-certificate brand-number of protected domain names?

### Certificate Type Selection

- For general businesses, it is recommended to purchase digital certificates of Type OV and above. For financial and payment enterprises, it is recommended to purchase EV certificate.
- If the mobile site or interface is called, it is recommended that you use certificates of Type OV and above.



#### Note:

Symantec-branded ev-type certificates have Server IP restrictions. If your domain name has multiple hosts IP, and it is recommended that you purchase multiple digital certificates. If you also use one of Alibaba Cloud's other cloud products, select one of the certificates to upload to the corresponding cloud product.

### Brand Selection

- The order of digital certificate brand compatibility from strong to weak: Symantec> geotrust> CFCA.
- The mobile Web site or interface calls related apps, and it is recommended that you select the Symantec brand.

### Number of protected domain names

- One domain name: this digital certificate can only be configured with one specific domain name.

- **Multiple Domain Names:** this digital certificate can configure multiple specific domain names. These domain names can be either a top-level domain name or a non-top-level domain name, such as p1.taobao.com, p1.aliyun.com Etc.
- **Wildcard Domain Name:** this digital certificate can be configured with a wildcard domain name. The wildcard domain name is typically in the form \*.aliyun.com.

Wildcard domain names only support peer-to-peer matching, such as binding \*.aliyun.com A digital certificate for a wildcard domain name that supports, but does not support . If you need any support For the wildcard domain name digital certificate, you also need to purchase a \* wildcard Domain Name Certificate.

**Note:**

- In the digital certificate for the wildcard domain name, only the root domain name contains the domain name principal itself. For example:
  - \*. Aliyun.com's wildcard domain name digital certificate contains aliyun.com.
  - \* The wildcard domain name digital certificate for .p1.aliyun.com does not contain.
- If the specific domain name is completed with the WWW domain name, the main domain name itself is included. For example:
  - The digital certificate bound by the www.aliyun.com domain name contains aliyun.com.
  - The digital certificate that is bound by the domain name does not contain the certificate.
- Once your digital certificate is issued, you will not be able to modify domain name information, and so on.

## 1.5 How do I enter domains to be added to a certificate?

After you have placed an order for a digital certificate, go to the certificate service console to complete the information for certificate review. Through the console, you can enter the information about the domains. The certificate is issued with HTTPS service availability only if the domains have been entered correctly.

The certificate services console then prompts you with the type of domains to enter based on the certificate you have purchased.

## What is a wildcard domain?

A wildcard domain is a domain that begins with “\*”. For example, \*.a.com is a correct wildcard domain, however, \*.\*.a.com is incorrect.



### Note:

In this scenario, a wildcard domain counts as one domain. For information about how a wildcard works for domains, see [What domains are supported by an “all-subdomains” wildcard certificate](#).

## What is a common domain?

A common domain is a specific domain, and is not a wildcard domain. For example, www.a.com or a.com is a common domain. The numbers of common domains can be added to a certificate depends on the number of domains specified in your certificate order.



### Note:

A specific subdomain such as buy.example.com or next.buy.example.com is regarded as separate domains.

## How domain information relates to CSR

- If you choose to manually create the CSR file, then the domain (CN attribute) in the CSR file must be one of the domains added to your certificate. When both wildcard and common domains are included in the domain information, use a common domain as the CN attribute of the CSR file. For more information about the CSR file, see [How to create a CSR file](#).
- If you choose to use the CSR generated by system function, the system automatically selects the first domain you entered as the CN attribute value in the CSR file. When both wildcard and common domains are included in the domain information, place a common domain as the first domain.

## 1.6 How do I request certificates for multiple wildcard and hybrid domains?

To request a certificate containing one or more wildcard domains and one or more common domains, follow these steps: For more information about domain types, see [How to enter domains to be added to a certificate](#).

1. This function supports only OV SSL Professional certificates.
2. Identify the domains, including how many common domains and how many wildcard domains, to be added to the certificate. At least one common domain is required for this certificate.

For more information about how a wildcard works for domains, see [What domains are supported by an "all-subdomains" wildcard certificate](#).

**Note:**

Make sure to purchase certificates of the same brand (and with the same validity, for example, one year). Otherwise, they cannot be merged.

**Example**

Here, an Entrust OV SSL Professional certificate for two wildcard domains and three common domains is used as an example.

1. Purchase two wildcard certificates and one multi-domain certificate (Select 3 for the number of domains). Make sure that the total number of domains specified in the orders is the same as that of the domains to be added to the certificate.
2. After the purchase is complete, do not perform any action on the orders.
3. Submit a ticket as follows:
  - Ticket title: Merge a certificate for multiple domains.
  - Ticket details: Screenshots of the orders to be merged. Provide the domains to be merged. For example, the primary domain a.com (which indicates that this certificate is issued to a.com) and additional domains b.com, a.com, \*.p.a.com, \*.p.b.com.
  - Ticket type: urgent ticket.
4. After the ticket is reviewed, only one of the merging orders is retained. The other orders are closed and cannot be opened. Click the editable order to add domains. The numbers of common and wildcard domains to be added are displayed next to the respective fields.

**Note:**

The first domain must be a common domain. For more information about domain types, see [How to enter domains to be added to a certificate](#).

Create the CSR file using the CSR generated by system function. Or, if you manually create the CSR file, enter the first domain in the domain list, (it must be a common

domain) as the Common Name attribute of the CSR file. For more information about how to generate a CSR file, see [How to generate a CSR file](#).

5. Submit the required materials for review.
6. Allow up to five business days for the CA to process your request, during which time they may attempt to contact you for additional operations.

## 1.7 What do I need to do after I submit a certificate verification request?

After purchasing an SSL certificate, you must apply for the certificate and submit it for verification. You can use the certificate only after it is approved.

After submitting a certificate verification request, you can view the status and subsequent procedures of your certificate on the **Order** page in the SSL Certificates console.

- **Verifying:** when the certificate application is in the Verifying state, you have to wait until it is approved . For more information about the [OV and EV certificates verification duration](#).
- **Failed:** if the verification fails, you must modify the certificate application information .

Move the pointer to the certificate page to view the reason for the failure. You can modify the application information according to the prompt reason .

### OV and EV certificates

If you purchased an OV or EV certificate, you need to wait 3 to 7 business days. The CA will verify your certificate order within 3 to 7 business days.

If the CA has any questions about the verification, the customer service of the CA will call you and guide you through the process. Make sure that your contacts are available .

## 1.8 Can an already-in-use SSL certificate be used if the IP of a server is changed?

Yes, as SSL certificates are associated with domains. Changing the IP address of a server does not affect the usage of the certificate if the domains stay the same and are resolved to a new IP address.

## 1.9 Why does my certificate order status remain unchanged even after receiving a notification from the CA?

The reason can be, the CA may first try to contact you (may send email updates to you (the requester)) before pushing review updates to Alibaba Cloud, resulting into a delay in updating your certificate status.

## 1.10 What can I do if my order is accidentally closed or some information is incorrect?

### If your certificate order is accidentally closed before completion

You can open a ticket to Alibaba Cloud technical support and request it be re-opened.

### If your certificate has incorrect information

- If this information does not affect the review, issuance, or utilization of the certificate, you may leave it as is.
- If modification is necessary, you can open a ticket to Alibaba Cloud technical support and request it be re-opened for modification.

**Note:**

Make sure your input is correct before submitting the application.