

Alibaba Cloud Certificates Service

Quick Start

Issue: 20190425

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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Limits.....	1
2 Overview.....	2
3 Step 1: Select a certificate.....	4
4 Step 2: Enter the information.....	7
5 View and manage purchased SSL certificates.....	11
6 Deploy to other cloud products.....	12

1 Limits

Alibaba Cloud Certificates Service is subject to the following limits:

- Only two types of server certificates (Professional and Advanced) are available. Different Certificate Authorities (CAs) provide different products (or do not have the specified type of certificates available) for you to choose from.
- As required by the CA, you must provide genuine and legitimate materials of your organization. Alibaba Cloud submits the materials provided by you to the CA for review. The CA can contact you for verification purpose.
- When generating a CSR file, the minimum bit length of the encryption key is RSA 2048 and SHA 256 for hash algorithm.
- Certificates provided by Alibaba Cloud Certificates Service are in the PEM format.

2 Overview

This article describes how to purchase digital certificates, enter the information for review, and deploy certificates to Alibaba Cloud products.

Audience

This article is useful to the users who want to:

- Learn how to purchase a digital certificate and compare the different types of digital certificates.
- Purchase a digital certificate and submit review materials.
- Deploy a digital certificate in cloud products.

Procedure

The flowchart for how to purchase and manage a digital certificate is as follows:



Generally, you can use Alibaba Cloud Certificates Service by following these steps:

1. *Select a certificate.*
2. *Enter request information and submit for review.*
3. *Manage the certificate.*
4. *Deploy the certificate to other Alibaba Cloud products.*

3 Step 1: Select a certificate

This article describes how to choose and purchase SSL certificate, and the features among different certificates.

1. Log on to the [Alibaba Cloud Certificates purchase page](#) to purchase an SSL certificate.

Alibaba Cloud Certificates Service

Basic Configuration

Region: Asia Pacific SE 2 EU Central 1 Middle East 1

Category: OV SSL
OV SSL offers encryption to implement strict identity verification for applicants. It certifies trusted identity.

Select Brand: Entrust
Entrust Datacard provides the most stringent organization validation certificate

Type of Domain: Wildcard Domain Single Domain Multiple Domain
Protection of one domain name with a wildcard (covering all the domain names at the same level as the "*" wildcard). When you apply for a certificate for a domain name such as *.example.com, the certificate issued will support a.example.com, a1.example.com, a2.example.com and so on, but does not support b.a.example.com, b1.a.example.com and so on

Domains:

1	2	3	4	<input checked="" type="radio"/> 5	10
20	50	100			

5 Domain(Sans/Subdomain/FQDN/Wildcard)

Purchase Plan

Quantity:

Duration: 1 Year 2 Years 3 Years
Expired after one year

2. Select the digital certificate and make the payment to enter the certificate configuration process.

Select a region.

We recommend that you select the region according to location of your website server that your certificate to be installed on.

Certificate brand (CA provider)

Alibaba Cloud works with the following CA to issue digital certificates:

Entrust: Entrust is the world's leading public key infrastructure provider. It has built a trusted virtual environment that facilitates communication, around the world. Entrust provides trust services to web sites, software developers, and individuals, this includes issuing SSL server certificates that specifically respond to web site authentication and encryption, more than 83% of the world's top 500 enterprises use the Entrust SSL server certificate.

Certificate type

In conjunction with qualified Certificate Authorities (CAs), Alibaba Cloud provides the following options to configure your digital certificates:

- **OV SSL:** A type of OV SSL (Organization Validation SSL) certificate. Details of an SSL Professional certificate include:
 - The CA verifies domain ownership and organization identity.
 - The requester's business name is displayed in the certificate.
 - The certificate provides strong encryption for communication links.
 - The certificate supports up to 100 domains, and supports wildcard domains.
- **EV SSL:** A type of EV SSL (Extended Validation SSL) certificate. Details of an SSL Advanced certificate include:
 - The CA strictly verifies domain ownership and organization identity.
 - A green address bar is displayed for this certificate in most browsers (the Safari browser has some exceptions).
 - The requester's organization identity details are displayed in the certificate.
 - The certificate provides strong encryption for communication links.
 - The certificate supports up to 100 domains.

Domain protection

Before purchasing a digital certificate, you must determine the type and number of domains you want to secure with the certificate. You can secure single or multiple domains, or wildcard domains.

- **Single domain:** Your digital certificate can only protect one domain (for example, buy.example.com) and does not support wildcards.
- **Multiple domains:** Your digital certificate can protect multiple domains (for example, buy1.example.com and buy2.example.com) though the maximum number of domains varies according to the certificate type. Generally, up to 100

domains can be secured. You can select on the basis of the number of Domains option. However, the wildcard domains are not supported.

- **Wildcard domains:** Your digital certificate can protect an extensive domain with a wildcard. Certificates for securing multiple wildcard subdomains are currently unavailable. For example, with the wildcard domain, *.example.com, you can protect domains such as a1.example.com and a2.example.com, but not a1.sport.example.com or a2.thanks.example.com.



Note:

Alibaba Cloud verifies the number and type of domains you select when you enter the domain information. If you select to protect multiple domains, you must submit all selected domains at the same time.

Certificate validity period

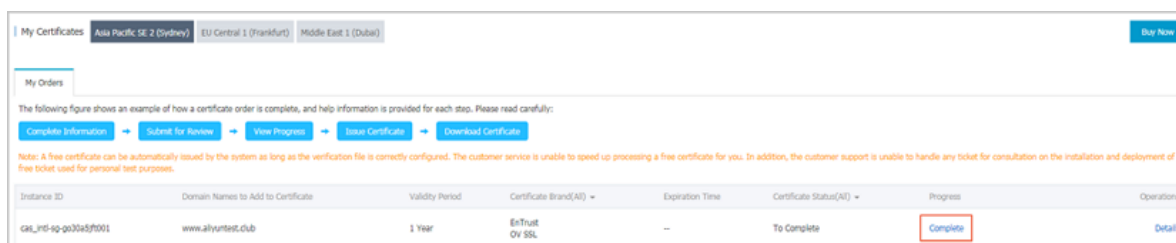
Every digital certificate has a validity period. The validity period of the digital certificate is calculated after the certificate is issued. You can select one or two years for the certificate validity period.

4 Step 2: Enter the information

After you have purchased a digital certificate, you must enter the certificate details and submit it for review. This step is needed to complete the certificate application request.

Follow these steps to enter the information:

1. Log in to the [Certificate Services Management console](#).
2. Select the Region where you have the certificate purchased.
3. In the My Orders list, select the certificate instance and click Complete to go to the Complete Information page to enter certificate details.



4. Click Submit for Review to submit the certificate application request.

Enter domain information

Enter the domain information based on the type and number of domains you have selected while purchasing the certificate. For example, if you want to secure multiple domains and have specified the number of domains to protect as five, enter all five domains (one per line) at this step.

Alibaba Cloud then verifies your entered domain information.



Note:

The CA must confirm the ownership of the submitted domains. You may receive an email from the CA that prompts you to verify your domain ownership. You must periodically check the designated mailbox after you submit the details for verification purpose. After you submit your information, check your inbox (applicant inbox) promptly and verify it. If the verification is not performed, you may fail the certificate review. If your domain name ownership verification fails, your certificate review will fail.

The screenshot shows a progress bar with three steps: 'Fill in domain name information' (active), 'Fill in organization information', and 'Submit'. Below the progress bar, a yellow banner states: 'The SSL certificate service provider will verify the email of the administrator for your domain name (example.com)'. The main form area contains a label '* Domain Names to Add to Certificate:' followed by an empty text input field. Below the input field, there is a note: 'Add up to 5 common domain names and 0 wildcard domain names.' and a tip: 'Tip: If the Alibaba Cloud Security Certificate System is used to create the CSR, the first domain name will be taken as the primary domain name.'

Enter request information

To purchase an SSL Professional or Advanced certificate, you have to enter detail information of your organization.

Enter organization information

Enter the organization information as needed. These details are further used to verify the authenticity of your organization.

The screenshot shows a progress bar with three steps: 'Fill in domain name information', 'Fill in organization information' (active), and 'Submit'. The main form area contains several fields with labels and values:

- * Organization Name: xxxx Co., Ltd.
Use the company name in the business license
- * Country: CHINA
- * Organization Province(State): Shanghai
- * Organization City: Shanghai
- * Organization Address: Organization address
Use the company domicile in the business license
- * ZIP Code: 200000
- * Requester Name: John Smith
- * Requester Mobile Phone: +86 12345678901
Very important. The issuing staff will call this phone number to confirm matters associated with certificate verification.
- * Email for Request Confirmation: John.smith@zhangsan.com
Very important. Make sure that you can send and receive emails using the provided email address. Any confirmation on and change to the certificate information confirmation will be sent to this email address.
- * Requester Title: IT
- * Applicant Department: IT

At the bottom, there are two radio buttons: CAS Generated by System and CSR Generated by Yourself.

Upload the relevant information

We strongly recommend you use the CSR Generated by System method to generate a CSR file.

- As a result, your private key is automatically generated by the system. Once your certificate request is completed, you can download your certificate and private key directly from the Certificate Management list.
- You can also generate a CSR (Certificate Signing Request) certificate request file on your own and upload it manually. For more information about how to generate a CSR file, see [How to generate a CSR file](#).



Note:

- Your CSR file format must be correct in order for your certificate application to succeed.
- You must keep your private key safe when generating a CSR file. The private key develops a one-to-one correspondence with the certificate. Your digital certificate becomes useless, if the private key is lost. Alibaba Cloud is not responsible for managing or keeping your private key. Additionally, if the private key is lost or forgotten, you must buy a new digital certificate to replace the original one.

Submit for Review

After submission,

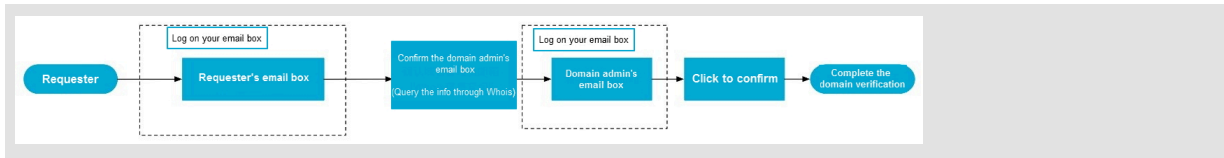
Alibaba Cloud verifies your certificate qualification. The time required for this process varies according to the individual requirements of each CA. Thus, we recommend that you must periodically check your email and phone for the notifications.

If the verification fails, you can revise and update the request information (especially the organization qualification review) and resubmit for another review.



Note:

After receiving your submission, the CA sends a verification email asking you to verify the domain information. If domain verification is not performed, you cannot pass the certificate review, and your certificate remains in the Under Review status until the verification is completed.

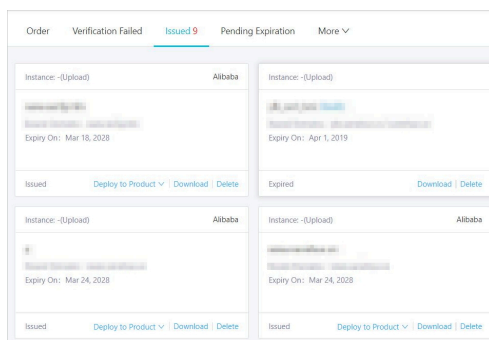


5 View and manage purchased SSL certificates

After your SSL certificates are approved, you can manage all of them centrally in the Alibaba Cloud SSL Certificates console. For example, you can upload your own certificates, modify certificate names, check the certificate validity period, and revoke or delete certificates.

Procedure

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, view and manage your SSL certificates.



- **Manage the certificate lifecycle:** Check the validity period of your certificate, and [purchase the certificate again](#) before it expires.
- **Check the status of your certificate:** Check whether your certificate has been issued, whether it is approved, or whether it is about to expire.
- **Modify the name of your certificate:** Modify the name of your certificate for easy identification.
- **Upload existing certificates:** Upload other certificates to the Alibaba Cloud SSL Certificates console to manage them centrally. For example, download certificates, view certificate information, or modify certificate names.

6 Deploy to other cloud products

You can push approved digital certificates to other Alibaba Cloud products like CDN, SCDN, DCDN, and Server Load Balance.

You must upload your private key before you can push a digital certificate to any cloud product. If you select “CSR generated by system” when submitting the certificate request, the private key is saved by the system and does not need to be uploaded again.



Note:

The private key is in a one-to-one correspondence with the certificate, so you must make sure you upload the correct private key. For more information on private keys, see [What is a public key and a private key](#).



Note:

Your digital certificate becomes useless, if the private key is lost. Alibaba Cloud is not responsible for managing or keeping your private key. Additionally, if the private key is lost or forgotten, you must buy a new digital certificate to replace the original one. You cannot re-download a private key once it has been uploaded. So, make sure you save and secure your original private key.