

Alibaba Cloud

SSL Certificates
Manage the certificates

Document Version: 20201230

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: 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: 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: 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: 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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Select and purchase certificates	05
2. Revoke certificates	06
3. Upload certificates	08
4. FAQ	10
4.1. How do I set the TLS version of my certificate?	10

1. Select and purchase certificates

On the Alibaba Cloud SSL certificate purchase page, you can select and purchase a certificate.

Procedure

1. Go to the [Alibaba Cloud SSL Certificate](#) purchase page.
2. Select the target certificate configuration.

Basic

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, 5, 10

1 Domain(Sans/Subdomain/FQDN/Wildcard)

For information about the certificate brand, type, and other items, see [SSL certificate configuration table](#) in this document.

3. Select the quantity and validity period of certificates.

Note For all certificate types, the validity period is up to two years.

4. After making the payment, you can apply for the certificate.

SSL certificate configuration table

There are two types of SSL certificates:

- OV SSL
- EV SSL

According to quantity demand of protected domain, SSL certificate is classified into:


- One domain name: One SSL certificate protects one domain, such as www.abc.com or login.abc.com.
- Multiple domain names: One SSL certificate protects multiple domain names, such as protect www.abc.com, www.bcd.com and pay.efg.com at the same time.

2.Revoke certificates

You can revoke the certificates that you no longer need or that pose security risks in the SSL Certificates Service console.

Context

Revoke Certificate allows you to deregister an issued certificate from the CA. After a certificate is revoked, it is no longer valid for encryption or trustworthy for browsers. Alibaba Cloud SSL Certificates Service allows you to revoke the certificates issued by Alibaba Cloud. Third-party certificates that are uploaded to the SSL Certificates Service console cannot be revoked.

 **Notice** After you submit a certificate revocation request, you cannot view or download the certificate in the SSL Certificates Service console.

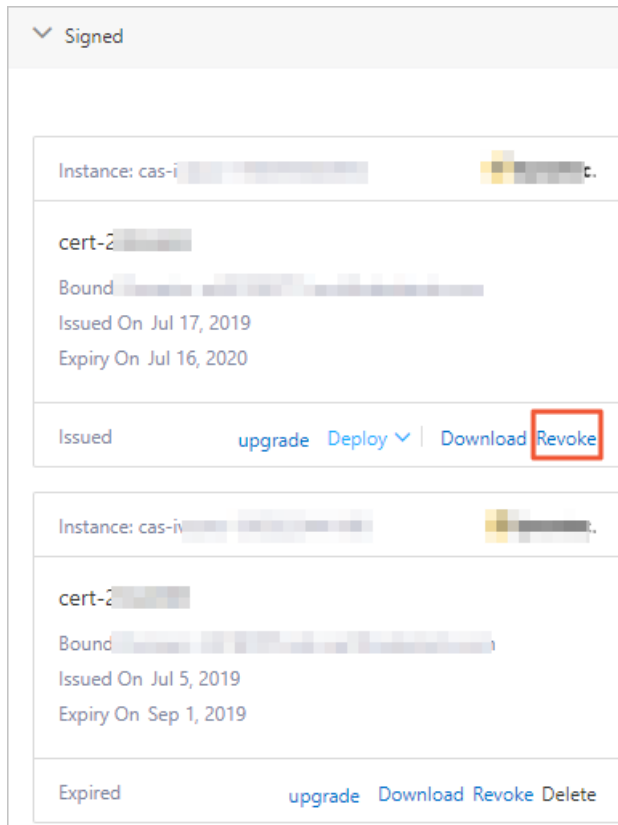
You can delete revoked certificates from the SSL Certificates Service console. You cannot delete issued certificates that are not revoked. For more information about the differences between revocation and deletion, see [吊销、删除证书分别有什么限制条件?](#)

Note


- If you want to claim a refund for an issued certificate, you must request revocation for the certificate and complete the revocation process within 28 calendar days after the certificate is issued. Otherwise, the refund cannot be claimed. You cannot claim a refund for a certificate 28 calendar days after it is issued or for a certificate that is not revoked within 28 calendar days after it is issued.
- Certificate authorities (CAs) can process a certificate revocation request within a maximum of 5 business days. If you want to revoke a certificate and claim a refund, you must submit the certificate revocation request in the Alibaba Cloud SSL Certificates console 28 calendar days the 28 calendar days elapse. Otherwise, the revocation request may fail to be approved in time, and the refund request will be rejected.

Procedure

- 1.
- 2.
3. On the **Overview** page, find the certificate that you want to revoke and click **Revoke**.



4. In the **Revoke Certificate** panel, specify Revocation Cause and click **OK**.
5. In the message that appears, click **OK**.
6. Complete the email confirmation. After you submit the revocation request, the CA sends a confirmation email to the address that you specified for **Applicant's Email Address**. You must check for the email and confirm the revocation activity promptly.

 **Note** CAs send confirmation emails only for OV and EV certificates. If you want to revoke DV certificates, the CAs do not send confirmation emails.

After you complete the email confirmation, the certificate is revoked.

References

[Refund instructions](#)


[Renewal upon expiration](#)

3.Upload certificates

You can upload third-party certificates to the SSL Certificates Service console for centralized management.

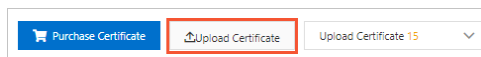
Background

In the SSL Certificates Service console, you can upload only the **PEM**-encoded CA certificate files and private key files. If your CA certificate files or private key files are not PEM-encoded, convert them to **PEM**-encoded files before you upload the files. The CA certificate files support the PEM and CRT formats. The private key files support the KEY format. For more information about how to convert files, see [Certificate format conversion](#).

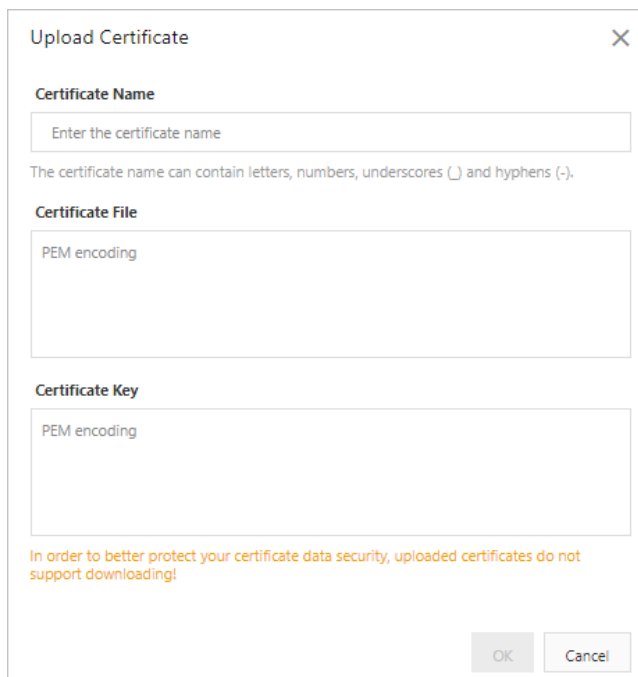
 **Note** The certificates that you upload in the SSL Certificates Service console cannot be downloaded.

Procedure



- 1.
2. On the **SSL Certificates** page, click **Upload Certificate** above the certificate list.



3. In the **Upload Certificate** dialog box, specify the following parameters.





A screenshot of the 'Upload Certificate' dialog box. It has a title bar with a close button (X). The dialog contains three input fields: 'Certificate Name' with a placeholder 'Enter the certificate name' and a note below it stating 'The certificate name can contain letters, numbers, underscores (_) and hyphens (-)'; 'Certificate File' with a placeholder 'PEM encoding'; and 'Certificate Key' with a placeholder 'PEM encoding'. At the bottom, there is a note: 'In order to better protect your certificate data security, uploaded certificates do not support downloading!' and two buttons: 'OK' and 'Cancel'.




Parameter	Description
Certificate Name	Enter a name for the certificate that you want to upload. The name can contain letters, digits, underscores (_), and hyphens (-).

Parameter	Description
Certificate File	<p>Enter the content of the CA certificate file that is encoded in the PEM format. You can copy the content from your PEM or CRT file to this field.</p> <p> Note We recommend that you use a text editor, such as Notepad or Notepad++, to open your CA certificate file and private key file.</p>
Certificate Key	<p>Enter the content of the private key file that is encoded in the PEM format. You can copy the content from your KEY file to this field.</p> <p> Note We recommend that you use a text editor, such as Notepad or Notepad++, to open your CA certificate file and private key file.</p>

4. Click **OK**.

After the certificate is uploaded, you can click the number in the **Upload Certificate** section on the **SSL Certificates** page to view the uploaded certificate.

All Status 	To be applied/Application review/Verification Failed	Issued 	Pending Expiration 	Upload Certificate	Expired 
0	0 / 0 / 0	0	0	3	1

Purchase Certificate	Upload Certificate	Upload Certificate 3	All Brands	Certificate Domain	<input type="text"/>	<input type="button" value="Q"/>
Certificate	Bound Domains	Deployed Products	Expire On	Status	Operate	
 DigiCert Instance: --		--	Aug 7, 2021	Upload Certificate	Deploy Download Renew 	

What's next

You can deploy the uploaded certificate to Alibaba Cloud services. For more information, see [Deploy certificates on Alibaba Cloud services](#).

4.FAQ

4.1. How do I set the TLS version of my certificate?

Supported TLS versions are TLSv1.0, TLSv1.1, and TLSv1.2. You can set the TLS version on your Alibaba Cloud services and web servers as required.

If your certificate is installed on the following Alibaba Cloud services, set the TLS version by referring to the respective links:

- SLB: [Manage TLS security policies](#)
- CDN: [Configure TLS](#)
- DCDN: [Configure TLS](#)

If your certificate is installed on a web server, find `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` in the certificate configuration file and modify the settings as required. For example, if you want to use TLSv1.1 and TLSv1.2 in your certificate, remove `TLSv1` from `ssl_protocols TLSv1 TLSv1.1 TLSv1.2`.