

# Alibaba Cloud

SSL Certificates

FAQ

Document Version: 20220601











# 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
 <b>Danger</b>	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.
 <b>Warning</b>	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.
 <b>Notice</b>	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.
 <b>Note</b>	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</b> > <b>Network</b> > <b>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.
<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.How do I enter domains to be added to a certificate? .....	05
2.Install SSL certificates on JBoss servers .....	06
3.How do I deploy a certificate to an Alibaba Cloud service? .....	09
4.What are the advantages of SSL certificates? .....	10
5.How do OSS users apply for SSL certificates? .....	11
6.How do I handle certificate order exceptions? .....	12
7.What do I need to do after I submit a certificate application? .....	13



# 1. 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, `*.aliundoc.com` is a correct wildcard domain, however, `*.*.aliundoc.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.aliundoc.com` or `aliundoc.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 `learn.example.com` or `demo.learn.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.



## 2. Install SSL certificates on JBoss servers

Alibaba Cloud SSL Certificates Service allows you to download an SSL certificate and install it on a JBoss server so that HTTPS can be enabled on the JBoss server. This topic describes how to install an SSL certificate.

1. Check the version of your JBoss server. We recommend that you deploy the SSL certificate on JBoss 7.1.1 or later.
2. Modify service configurations. Go to the *standalone/configuration* directory in the JBoss home directory and modify the *standalone.xml* file.

```
<interfaces>
  <interface name="management">
    <inet-address value="${jboss.bind.address.management:127.0.0.1}"></inet>
  </interface>
  <!-- Enable remote access -->
  <interface name="public">
    <inet-address value="${jboss.bind.address:0.0.0.0}"></inet>
  </interface>
  <interface name="unsecure">
    <inet-address value="${jboss.bind.address.unsecure:127.0.0.1}"></inet>
  </interface>
</interfaces>

<socket-binding-group name="standard-sockets" default-interface="public" port-offse
t="${jboss.socket.binding.port-offset:0}">
  <socket-binding name="management-native" interface="management" port="${jboss.m
anagement.native.port:9999}"></socket>
  <socket-binding name="management-http" interface="management" port="${jboss.man
agement.http.port:9990}"></socket>
  <socket-binding name="management-https" interface="management" port="${jboss.ma
nagement.https.port:9443}"></socket>
  <socket-binding name="ajp" port="8009"></socket>
  <!-- Modify the HTTP port -->
  <socket-binding name="http" port="80"></socket>
  <!-- Modify the HTTPS port -->
  <socket-binding name="https" port="443"></socket>
  <socket-binding name="osgi-http" interface="management" port="8090"></socket>
  <socket-binding name="remoting" port="4447"></socket>
  <socket-binding name="txn-recovery-environment" port="4712"></socket>
  <socket-binding name="txn-status-manager" port="4713"></socket>
  <outbound-socket-binding name="mail-smtp">
    <remote-destination host="localhost" port="25"></remote>
  </outbound-socket-binding>
</socket-binding-group>
```

3. Go to the *bin* directory of the JBoss installation directory and run the `standalone.sh` script to ensure normal application access.
4. Obtain the SSL certificate and convert it to the *JKS* format.



Download an SSL certificate in *Tomcat* format from Alibaba Cloud. If you manually generate a *CSR* file, generate a *PFX* certificate key pair file. The following files are extracted:

- *214362464370691.key*
- *214362464370691.pem*
- *214362464370691.pfx*
- *pfx-password.txt*

For a manually generated *CSR* file, convert the *PFX* certificate key pair file to the *JKS* format. In Windows systems, run the command in the `%JAVA_HOME%/jdk/bin` directory. The following code shows an example on how to convert the format:

```
openssl pkcs12 -export -out 214362464370691.pfx -inkey 214362464370691.key -in 214362464370691.pem
```

Press Enter, enter the password of the *JKS* certificate twice, and then enter the password of the *PFX* certificate once. The passwords that you entered must be recorded in the *pfx-password.txt* file.

#### 5. Deploy the certificate.

- i. Go to the *standalone/configuration* directory in the JBoss home directory, create a *cer* file, and then place the *JKS* certificate into the *standalone/configuration* folder.

```
# cd /opt/jboss711/standalone/configuration
#mkdir cert
# pwd
/opt/jboss711/standalone/configuration/cert
#cp -rf /opt/keys/jboss.jks .
```

- ii. Modify the *standalone.xml* file and add certificate-related configurations.

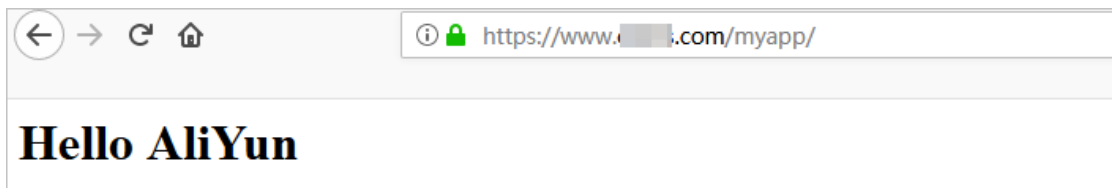
```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
    <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
    <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
        <ssl name="https" password="214362464370691" certificate-key-file="
        ../standalone/configuration/cert/jboss.jks" cipher-suite="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA" protocol="TLSv1,TLSv1.1,TLSv1.2"/>
    </connector>
    <virtual-server name="default-host" enable-welcome-root="true">
        <alias name="localhost"/>
        <alias name="example.com"/>
    </virtual-server>
</subsystem>
```

- iii. Restart the JBoss server. Go to the *bin* directory in the JBoss directory and run the *standalone.sh* script.

```
#pwd
/opt/jboss711/bin
#sh standalone.sh &
```



- iv. Verify whether the SSL certificate is deployed.





## 3. How do I deploy a certificate to an Alibaba Cloud service?

This topic is no longer maintained and will be removed due to documentation adjustment.

For more information about how to install an SSL certificate, see [Installation overview](#).



## 4. What are the advantages of SSL certificates?

This topic describes the advantages of SSL certificates compared with traditional encryption methods.

- **Quick deployment** : You need only to apply for an SSL certificate and deploy it on your server.
- **Intuitive display** : After you deploy an SSL certificate on your server and access your website over HTTPS, a lock icon appears in the address bar or on the right of the address bar. This icon indicates that the website is encrypted. If you deploy an Extended Validation (EV) certificate, the enterprise name also appears in the address bar.
- **Identity authentication** : This feature is unavailable in other encryption methods. You can view the owner enterprise of the website in the SSL certificate information, and then check whether the website is valid and authentic. This prevents you from phishing attacks.
- **Quick issuance** : Certificate application is easy and efficient. You can purchase SSL certificates of different brands in the Alibaba Cloud SSL Certificates Service console at a time. Alibaba Cloud can accelerate the review and issuance of SSL certificates.
- **Easy deployment** : You can deploy SSL certificates to your Alibaba Cloud services, such as Server Load Balancer (SLB), Alibaba Cloud CDN, Secure CDN (SCDN), and Dynamic Route for CDN (DCDN). This way, you can use the certificates in the cloud at minimal cost.



## 5. How do OSS users apply for SSL certificates?

This topic is no longer maintained and will be removed.

For more information about how Object Storage Service (OSS) users configure certificates, see [Host SSL certificates](#).



## 6. How do I handle certificate order exceptions?

This topic is no longer maintained and will be removed due to documentation adjustment.



## 7. What do I need to do after I submit a certificate application?

This topic is no longer maintained and will be removed.

For more information about the operations that need to be performed after a certificate application is submitted, see [Cooperation with the CA to complete the verification process](#).