

Alibaba Cloud SSL Certificates Service

User Guide

Issue: 20190920

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
{} or {a b}	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 Overview.....	1
2 Select and purchase certificates.....	5
3 Apply for and validate certificates.....	6
4 Deploy issued certificates to Alibaba Cloud products.....	10
5 Upload certificates.....	12
6 Download and install SSL certificates.....	14
6.1 Download certificates.....	14
6.2 Install SSL certificates in Tomcat servers.....	14
6.2.1 Install .pfx SSL certificates.....	15
6.2.2 Install .jks SSL certificates.....	17
6.3 Install SSL certificates in Apache servers.....	19
6.4 Install SSL certificates in Nginx/Tengine servers.....	22
6.5 Install SSL certificates in IIS servers.....	25
6.6 Install SSL certificates in GlassFish servers.....	31
7 Revoke certificates.....	33

1 Overview

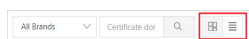
This document provides an overview of operations on Alibaba Cloud SSL Certificates Service and the main modules of its console.

You can manage and perform operations on certificates in the Alibaba Cloud SSL Certificates console as follows:

- Purchase SSL certificates
- View SSL certificate status
- Manage certificates:
 - [#unique_4](#) to the console for unified management
 - [Apply for certificates](#) and withdraw certificate applications
 - [#unique_6](#)
 - Download issued certificates and [Install them in other types of servers](#)
 - [Delete/#unique_8](#)
- Renew the certificates that will expire

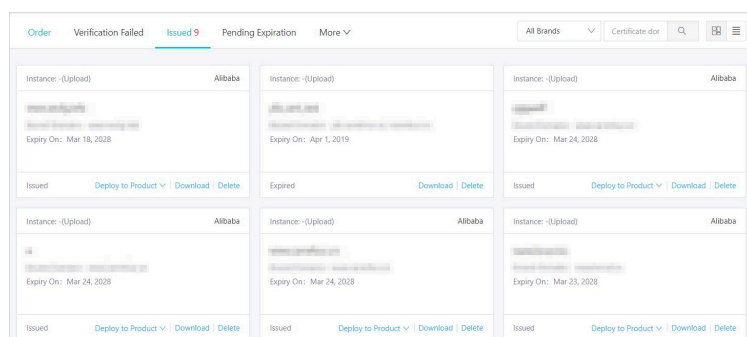
Console layout mode

The Alibaba Cloud SSL Certificates console supports two layout modes. You can click either of the layout icons at the top of the console to select the desired layout mode.



All operations in this document are based on the card view.

- Card view

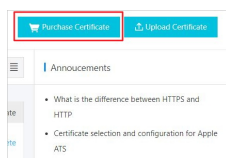


• List view

Certificate	Status	Bound Domains	Validity Period	Expiry On	Deployed Products	Operate
www.secfp.info	Issued	www.secfp.info	10 Year(s)	Mar 18, 2028	--	Details Deploy to Product Download Delete
www.secfp.info	Expired	www.secfp.info	1 Year(s)	Apr 1, 2019	--	Details Download Delete
www.secfp.info	Issued	www.secfp.info	10 Year(s)	Mar 24, 2028	--	Details Deploy to Product Download Delete
www.secfp.info	Issued	www.secfp.info	10 Year(s)	Mar 24, 2028	--	Details Deploy to Product Download Delete
www.secfp.info	Issued	www.secfp.info	10 Year(s)	Mar 23, 2028	--	Details Deploy to Product Download Delete
www.secfp.info	Issued	www.secfp.info	10 Year(s)	Mar 18, 2028	--	Details Deploy to Product Download Delete

Purchase SSL certificates

On the SSL Certificates page, click **Purchase Certificate** in the upper-right corner. For more information, see [Select and purchase certificates](#).



Multiple types of SSL certificates are available. For more information, see [Features](#).

View SSL certificate status

You can view the status of your certificate on the SSL Certificates page.

Certificate	Status	Bound Domains	More
www.secfp.info (Instance: (Upload))	Issued	www.secfp.info	Paid Verifying Expired 1 Revoked Refund
yib.cert.test (Instance: (Upload))	Expired	yib.carrefour.cn, carrefour.cn	

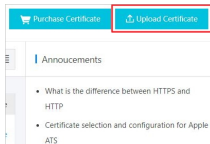
The certificate statuses are as follows:

- **Ordered:** The certificate has been paid for and can be used upon application and review.
 - Paid
 - Pending Verification
 - Revoked
- **Issued:** The certificate has been issued upon payment, application, and review. You can deploy the certificate to the target Alibaba Cloud product or download or delete it.
 - **Expired:** The certificate has expired and you need to purchase and apply for a new one to ensure website security.

Manage certificates

You can manage certificates and deploy them to Alibaba Cloud products on the SSL Certificates page. You can view certificate status and validity, upload other certificates to the SSL certificate console, and delete/revoke SSL certificates.

- **Upload certificates to the console for unified management:** You can upload other types of certificates to the console for deployment to Alibaba Cloud products or unified management.



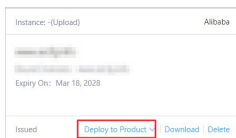
- **Apply for certificates and withdraw certificate applications:** You can apply for a purchased certificate or withdraw certificate applications.



Note:

Applications cannot be withdrawn after the certificate is issued.

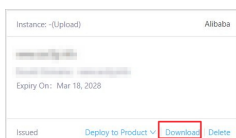
- **Deploy to cloud products:** You can deploy issued certificates to Alibaba Cloud products.



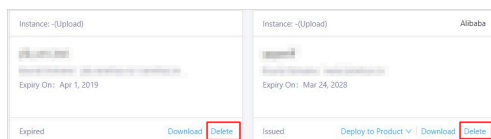
Note:

At present, your certificates can be deployed to CDN and SLB.

- **Download certificates:** You can download issued certificates and install them in your web server.



- **Delete/revoke certificates:** You can delete or revoke certificates that have been issued and are no longer in use.

**Note:**

Deleted certificates cannot be restored, so proceed with caution.

**Note:**

We will refund full payment to you if you revoke a certificate within 30 days after it is issued. However, any revocation after 30 days is non-refundable.

2 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.

The screenshot shows the configuration interface for purchasing an SSL certificate. A red box highlights the following sections:

- Region:** Asia Pacific 01, EU Central 1, Middle East 1
- Category:** OV SSL (Description: OV SSL offers encryption to implement strict identity verification for applicants. It certifies trusted identity.)
- Select Brand:** F5 (Description: F5 SSL offers the most stringent organization validation certificate.)
- Type of Domain:** Wildcard Domain, Single Domain, Multiple Domain (Description: 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 *.example.com, *.example.com.cn, *.example.com and so on, but does not support *.example.com, *.example.com.cn and so on.)
- Domains:** A table with columns for quantity (1, 2, 3, 4, 5, 10) and price (20, 50, 100, 100, 100, 100). Below the table, it says "1 Domain(Same/Subdomain/T DNS/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.

3 Apply for and validate certificates

After purchasing a certificate, you need to go through the certificate application, verification, and review process. The certificate takes effect after being validated.

Step 1: Fill in the certificate application information

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. Click Apply in the lower-right corner of the certificate you purchased and pending for application.
3. On the Apply for Certificate page, enter the certificate application information on the Enter Application tab page.
 - Domains to Bind: Click the question mark of this parameter to view the tips and enter a correct domain name.



Note:

- Application information varies with certificate types. For free and standard SSL certificates, you need to enter personal information. For professional SSL certificates, you need to enter personal information and company details.

- Limitations on bound domain names vary with certificate types. Enter the domain name based on the tips.

- **Company Name:** Enter actual information as required.
- **Type of Company:** Select the type of your company.
- **Company Phone:** Enter contact phone number. The certificate authority will call you on this number to confirm the certificate verification.
- **Company/Organization ID:** Enter actual information as required.
- **Location:** Select the location as appropriate.
- **Detailed Address:** Enter the detailed address of your company.
- **Zip Code:** Enter the zip code.
- **Applicant's Phone:** Enter your contact telephone number. The certificate authority will call you on this number to confirm certificate verification.
- **Applicant's Email Address:** Enter your email address. After the certificate is submitted for review, the certificate authority will send a verification email to your email address. Check your email promptly.
- **Applicant ID Number:** Enter your ID number.

4. Select CSR Generation.

- **Automatic:** Your CSR file is automatically generated by the system. Once your certificate application is completed, you can download your certificate and private key directly on the certificate management page.



Note:

We recommend that you select Automatic for CSR Generation. If not, your certificate may fail to be pushed to the specified Alibaba Cloud product.

- **Manual:** Your CSR file is manually generated and you need to copy its content to the CSR File dialog box. For more information, see [../DNcas1816450/EN-US_TP_13600.dita#concept_b4f_mrp_ydb](#).



Note:

The manually generated CSR file cannot be pushed to the specified Alibaba Cloud product with one click.

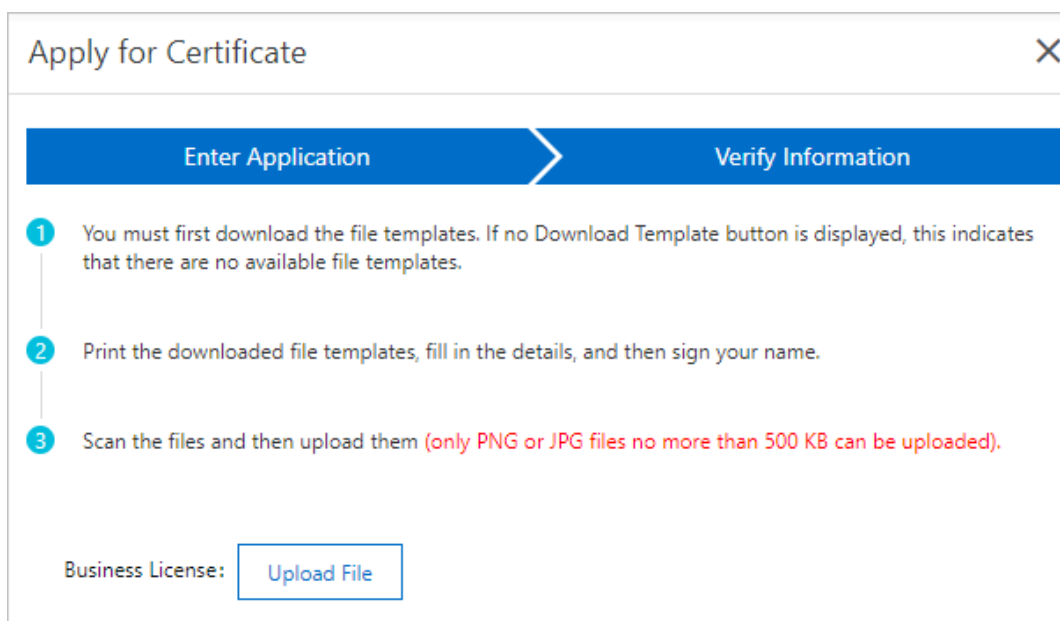
- Your CSR file format must be correct in order ensure secure certificate application.

- You must store your private key securely when generating a CSR file. One certificate file maps a key file. Your digital certificate becomes useless if the private key is lost. Alibaba Cloud is not responsible for storing your private key. If your private key is lost, you have to re-purchase a digital certificate to replace the original one.

5. Click Next to go to the Verify Information tab page.

Step 2: Verify the application information and submit it for review

After entering all the required certificate application information, you need to upload the verification file.



1. Follow the instructions on the Apply for Certificate page. Verification information varies with certificate types.



Note:

- To download the verification template, fill in it, and stamp it, follow the tips on the Verify Information tab page.
- If uploading an image, make sure that the image is in PNG or JPEG format and its size does not exceed 500 KB.
- The certificate has a validity period. You can save the application information for subsequent use.

2. Click Upload File and upload the qualification documents as required.

3. Click Submit in the lower-right corner of the page. The system displays this prompt: This application request has been submitted to the certificate authority. Keep your phone on and check for the email from the certificate authority in your mailbox.

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

In the Unissued Certificates area of the SSL Certificates page, you can see the expected issuance time, type, bound domain, and validity period of the certificate you applied for.

**Note:**

To modify your application information, you must withdraw the application and modify the information before the certificate is issued. The application cannot be withdrawn after the certificate is issued.

Related

[#unique_13](#)

[#unique_14](#)

4 Deploy issued certificates to Alibaba Cloud products

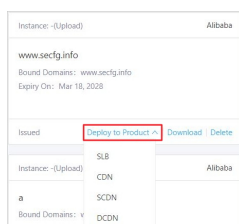
You can deploy the issued certificates to Alibaba Cloud products in one click.

SSL certificates are available for the following Alibaba Cloud products:

- Server Load Balancer (SLB)
- Content Delivery Network (CDN)
- SCDN
- DCDN

Procedure

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. Open the Issued Certificates page, click Deploy to Product for the target certificate.



3. Select the target Alibaba Cloud product from the drop-down list.
4. In the Deploy Certificate to CDN/SLB pane on the right, select the region where you want to deploy the certificate.



Multiple regions can be selected.

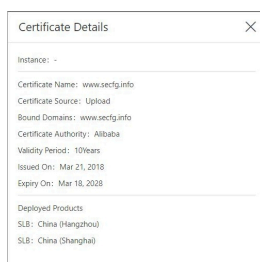


Note:

To deploy a certificate in your SLB instance, you need to select the region where the SLB instance is located.

5. Click OK. The certificate is deployed to the Alibaba Cloud product you selected.

After deploying the certificate to the Alibaba Cloud product, click the certificate card. On the displayed Certificate Details page, you can view the details about the certificate and the information about the Alibaba Cloud product.



5 Upload certificates

Alibaba Cloud SSL Certificates Service allows you to upload other types of certificates and manage them centrally in the SSL Certificates console.

PEM certificate files can be directly uploaded while the other formats of certificate files must **be converted to** PEM files before uploading.

A PEM file can have either of the following extensions:

- .pem
- .crt

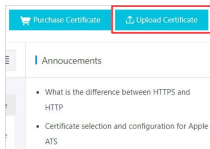


Note:

Uploaded certificates cannot be downloaded.

Procedure

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, click Upload Certificate in the upper-right corner.



3. In the Upload Certificate dialog box, enter Certificate Name. In Certificate File, paste the content in your certificate file (suffixed with .pem or .crt, or of .pem or .crt file format). In Certificate Key, paste the content in your key file (suffixed with .key or of .key file format).

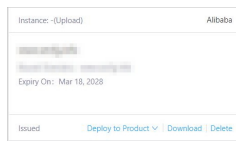


Note:

Use a text tool (Notepad or Notepad++) to open your certificate file and private key file.

4. Click OK.

You can locate the certificate you uploaded on the Issued tab page. You can also deploy the uploaded certificate to Alibaba Cloud products.



6 Download and install SSL certificates

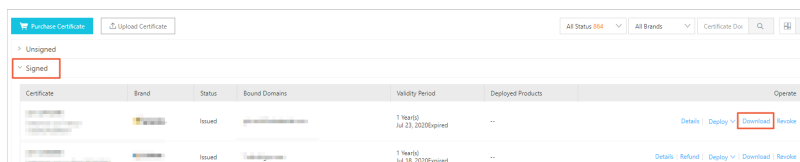
6.1 Download certificates

SSL Certificates Service allows you to download SSL certificates and install them in your web server. With an SSL certificate, your web server can support SSL communication, ensuring high security.

Only the issued and expired SSL certificates can be downloaded.

Procedure

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, locate the target SSL certificate and click Download in the lower-right corner.



3. Locate the row that contains the certificate with the desired Server Type and click Download in the Actions column to download the package to your local host.
4. Decompress the package and install the certificate in your web server.

Alibaba Cloud SSL certificates can be installed in the following types of web servers:

- [Tomcat](#)
- [Apache](#)
- [Nginx](#)
- [IIS](#)
- Other

6.2 Install SSL certificates in Tomcat servers

6.2.1 Install .pfx SSL certificates

This topic describes how to install the downloaded SSL certificate in your Tomcat server. Tomcat supports both .pfx and .jks certificates. You can install a .pfx or .jks certificate based on your Tomcat version.

Prerequisites

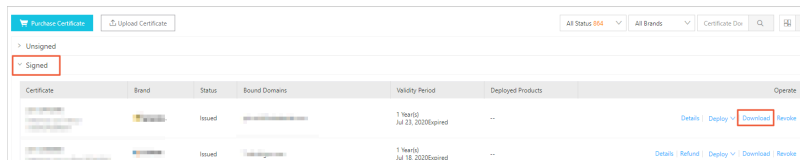
You selected Automatic for CSR Generation when applying for the certificate.

If you selected Manual for CSR Generation when applying for the certificate, no certificate file is generated. You have to download the .crt certificate whose Server Type is Other, and then run the OpenSSL command to convert the certificate to .pfx format.

In this example, the certificate name is domain name, and the certificate file is named domain name.pfx.

Procedure

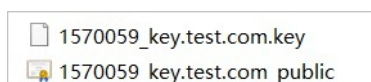
1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, locate the target SSL certificate and click Download in the lower-right corner.



3. In the Download Certificate dialog box, locate the row that contains the certificate whose Server Type is Tomcat, and click Download in the Actions column to download the package to your local host.
4. Decompress the package.

The following two files are extracted:

- Certificate file (suffixed with .pfx or of .pfx file format)
- Key file (suffixed with .txt or of .txt file format)



Note:

Each time the certificate is downloaded, a new password is generated, which is valid only for the current certificate. To update the certificate file, you also need to update the matching key file.

5. In the Tomcat directory, create cert directory. Copy the downloaded certificate and password file to the cert directory.
6. Open Tomcat installation directory > conf > server.xml. In the server.xml file, add the following attributes (you can modify the port attribute as needed):

```
< Connector port = " 8443 "
  protocol = " HTTP / 1 . 1 "
  SSLEnabled = " true "
  scheme = " https "
  secure = " true "
  keystoreFile = " domain . pfx " # keystoreFile
  le indicates the path of your certificate file
  . Replace domain name with the name of your
  certificate file .
  keystoreType = " PKCS12 "
  keystorePassword = " Certificate password " # Replace the
  certificate password with the content in your key
  file .
  clientAuth = " false "
  SSLProtocol = " TLSv1 + TLSv1 . 1 + TLSv1 . 2 "
  ciphers = " TLS_RSA_WITH_AES_128_CBC_SHA , TLS_RSA_WITH_
  AES_256_CBC_SHA , TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  , TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 , TLS_RSA_WITH_
  AES_128_CBC_SHA256 , TLS_RSA_WITH_AES_256_CBC_SHA256 "
/>
```

7. Save the configuration in the server.xml file.
8. (optional) Configure web . xml file to force HTTP jump to HTTPS.

```
# All the following content behind </ welcome - file - list
>:
< login - config >
  <!-- Authorization setting for SSL -->
  < auth - method > CLIENT - CERT </ auth - method >
  < realm - name > Client Cert Users - only Area </ realm -
  name >
</ login - config >
< security - constraint >
  <!-- Authorization setting for SSL -->
  < web - resource - collection >
    < web - resource - name > SSL </ web - resource - name >
    < url - pattern > /* </ url - pattern >
  </ web - resource - collection >
  < user - data - constraint >
    < transport - guarantee > CONFIDENTIAL </ transport -
  guarantee >
  </ user - data - constraint >
</ security - constraint >
```

9. Restart Tomcat.

References:

- [#unique_20](#)
- [#unique_25](#)
- [#unique_26](#)
- [#unique_21](#)
- [#unique_22](#)
- [#unique_27](#)
- [#unique_28](#)

6.2.2 Install .jks SSL certificates

This topic describes how to install the downloaded SSL certificate in your Tomcat server. Tomcat supports both .pfx and .jks certificates. You can install a .pfx or .jks certificate based on your Tomcat version.

Prerequisites

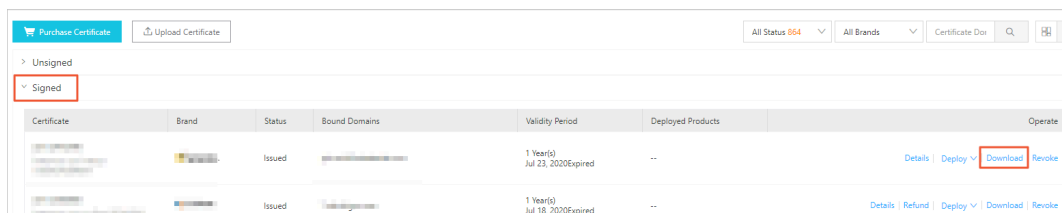
You selected Automatic for CSR Generation when applying for the certificate.

If you selected Manual for CSR Generation when applying for the certificate, no certificate file is generated. You have to download the .crt certificate whose Server Type is Other, and then run the OpenSSL command to convert the certificate to .pfx format.

In this example, the certificate name is domain name, and the certificate file is named domain name.pfx.



Procedure

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, locate the target SSL certificate and click Download in the lower-right corner.



3. In the Download Certificate dialog box, locate the row that contains the certificate whose Server Type is Tomcat, and click Download in the Actions column to download the package to your local host.

- Decompress the package. You will obtain a certificate file (suffixed with .pfx or of .pfx file format) and a key file (suffixed with .txt or of .txt file format).

 1570059_key.test.com.key
 1570059_key.test.com_public
**Note:**

Each time the certificate is downloaded, a new password is generated, which is valid only for the current certificate. To update the certificate file, you also need to update the matching key file.

- Run the following Java JDK command to convert the .pfx certificate file to a .jks file:

```
keytool -importkeys -storename domain_name.pfx
-destkeystore domain_name.jks -srcstoretype PKCS12
-deststoretype JKS
```

**Note:**

In Windows systems, you must run the preceding command in the % JAVA_HOME %/ jdk / bin directory.

- Press Enter and enter the passwords in the .pfx certificate file and .jks certificate file respectively.

**Note:**

The password in the .jks certificate file must be the same as that in the .pfx certificate file. If the two passwords are different, Tomcat may fail to restart.

- In the Tomcat directory, create cert directory. Copy the downloaded certificate and password file to the cert directory.
- Open Tomcat installation directory > conf > server.xml. In the server.xml file, locate the < Connection port = " 8443 " sheet and add the following parameters:

```
# keystoreFile indicates the path of your certificate
file. Replace the content after cert / with the
name of your certificate file.
keystoreFile="cert / domain_name.jks"
keystoreType="PKCS12"
# Replace the certificate password with the content
in your key file.
```

```
keystorePassword="certificatepassword"
```

The complete configuration is as follows (you can modify the port attribute as needed):

```
< Connector port="8443"
  protocol="HTTP/1.1"
  SSLEnabled="true"
  scheme="https"
  secure="true"
  keystoreFile="cert/domainname.jks"
  keystoreType="PKCS12"
  keystorePassword="certificatepassword"
  clientAuth="false"
  SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
  ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256"
/>
```

9. Save the configuration in the `server.xml` file.

10. (optional) Configure `web.xml` file to force HTTP to jump to HTTPS.

```
# Add the following after </welcome-file-list>:
<login-config>
  <!-- Authorization setting for SSL -->
  <auth-method>CLIENT-CERT</auth-method>
  <realm-name>ClientCertUsers-onlyArea</realm-name>
</login-config>
<security-constraint>
  <!-- Authorization setting for SSL -->
  <web-resource-collection>
    <web-resource-name>SSL</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

11. Restart Tomcat.

6.3 Install SSL certificates in Apache servers

This topic describes how to download an SSL certificate from the Alibaba Cloud SSL Certificates console and install it in your Apache server.

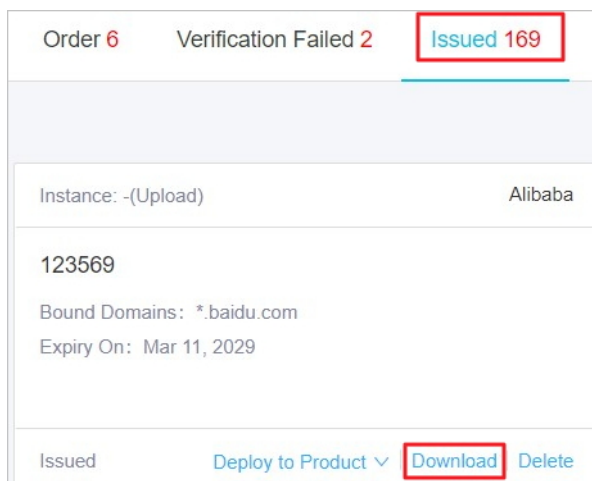
Prerequisites

Select Automatic for CSR Generation when applying for the certificate.

In this example, domain name is the certificate name, domain name_public.cert is the certificate file name, domain name_chain.cert is the certificate chain file, and domain name.key is the certificate ket file.

Procedure

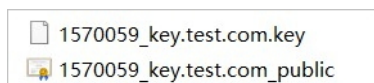
1. Log on to [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, locate the target SSL certificate and click Download in the lower-right corner.



3. In the Download Certificate dialog box, locate the row that contains the certificate whose Server Type is Apache, and click Download in the Actions column to download the package to your local host.
4. Decompress the certificate package.

The following three files are extracted:

- Certificate file (suffixed with . crt or of . crt file format)
- Certificate chain file (suffixed with . crt or of . crt file format)
- Key file (suffixed with .key or of . key file format)



Note:

The .crt certificate file is a Base64-encoded text file and you can modify its extension to .pem as needed.

For more information about the certificate format, see [What are the formats of mainstream digital certificates?](#)

5. Create a `/cert` directory in the Apache installation directory, and copy the downloaded certificate file, certificate chain file, and key file to the `/cert` directory.

**Note:**

If you have selected Manual for CSR Generation when applying for the certificate, save the key file you created manually to the `/cert` directory.

6. Open `Apache installation directory / conf / httpd . conf`. In the `httpd . conf` file, find the following parameters and configure them:

```
# LoadModule ssl_module modules / mod_ssl . so
# Delete the configuration statement annotator "#" at
the beginning of the line . If it is not found ,
check if the OpenSSL plug - in has been compiled .
# Include conf / extra / httpd - ssl . conf
# Delete the configuration statement annotator "#" at
the beginning of the line .
```

7. Save the `httpd . conf` file and exit.
8. Open `Apache installation directory / conf / extra / httpd - ssl . conf`. In the `httpd - ssl . conf` file, find the following parameters and configure them:

**Note:**

Depending on the operating system, the `http - ssl . conf` file may be stored in the `conf . d / ssl . conf` directory.

```
SSLProtoco l all - SSLv2 - SSLv3
# Add supported SSL protocols and remove the insecure
ones .
SSLCipherS uite HIGH :! RC4 :! MD5 :! aNULL :! eNULL :!
NULL :! DH :! EDH :! EXP :+ MEDIUM
# Use this cipher suite .
SSLHonorCi pherOrder on
SSLCertifi cateFile cert / domain name_publi c . crt
# Replace domain name_publi c . crt with the name of
your certificat e .
SSLCertifi cateKeyFil e cert / domain name . key
# Replace domain name . key with the name of your
private key file .
SSLCertifi cateChainF ile cert / domain name_chain . crt
# Delete the annotator "#" ( if any ) at the beginning
of the certificat e chain .
```

9. Save the configuration in the `httpd - ssl . conf` file.

10. Go to the `/ bin` directory in the Apache installation directory to restart the Apache server.

- a. In Apache `/ bin` directory, execute the following command to stop Apache server:

```
apachectl -k stop
```

- b. In Apache `bin` directory, execute the following command to start Apache server:

```
apachectl -k start
```

References:

- [Install SSL certificates in Tomcat servers](#)
- [#unique_25](#)
- [#unique_26](#)
- [#unique_21](#)
- [#unique_22](#)
- [#unique_27](#)
- [#unique_28](#)

6.4 Install SSL certificates in Nginx/Tengine servers

This topic describes how to download an SSL certificate from the Alibaba Cloud SSL Certificates console and install it in your Nginx/Tengine server.

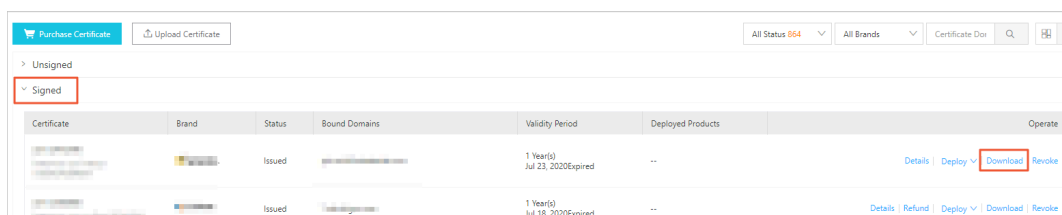
Prerequisites

You selected Automatic for CSR Generation when applying for the certificate.

In this example, the certificate name is domain name, the certificate file is named domain name.pem and the key file is named domain name.key.

Procedure

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, locate the target SSL certificate and click Download in the lower-right corner.



3. In the Download Certificate dialog box, locate the row that contains the certificate whose Server Type is Nginx/Tengine, and click Download in the Actions column to download the package to your local host.
4. Decompress the package.

The following two files are extracted:

- Certificate file (suffixed with .pem or of .pem file format)
- Key file (suffixed with .key or of .key file format)



Note:

The .pem certificate file is a Base64-encoded text file and you can modify its extension as needed.

For more information about the certificate format, see [What are the formats of mainstream digital certificates?](#)

5. Create a cert directory in the Nginx installation directory, and copy the downloaded certificate file and key file to the cert directory.



Note:

If you have selected Manual for CSR Generation when applying for the certificate, place the private key file in the cert directory.

6. Open Nginx installation directory > conf > nginx.conf. In the nginx.conf file, locate the following attributes:

```
# HTTPS  server
server {
    listen 443 ;
    server_name localhost ;
    ssl on ;
    ssl_certificate cert . pem ;
    ssl_certificate_key cert . key ;
    ssl_session_timeout 5m ;
    ssl_protocols SSLv2 SSLv3 TLSv1 ;
    ssl_ciphers ALL :! ADH :! EXPORT56 : RC4 + RSA :+ HIGH :+
    MEDIUM :+ LOW :+ SSLv2 :+ EXP ;
    ssl_prefer_server_ciphers on ;
    location / {
```

Modify the `nginx.conf` file as follows:

```
The attributes that start with "ssl" are related to
certificat e configurat ions , while the others can
be configured as needed .
server {
listen 443 ;
server_nam e localhost ; # Replace localhost with the
domain name bound to your certificat e .
ssl on ; # Set this attribute to On to enable the
SSL function .
root html ;
index index . html index . htm ;
ssl_certif icate cert / domain name . pem ; # Replace
domain name . pem with the name of your certificat e
file .
ssl_certif icate_key cert / domain name . key ; # Replace
domain name . key with the name of your private key
file .
ssl_sessio n_timeout 5m ;
ssl_cipher s ECDHE - RSA - AES128 - GCM - SHA256 : ECDHE : ECDH
: AES : HIGH :! NULL :! aNULL :! MD5 :! ADH :! RC4 ; # Use
this cipher suite .
ssl_protoc ols TLSv1 TLSv1 . 1 TLSv1 . 2 ; # Change
protocols .
ssl_prefer _server_ci phers on ;
location / {
root html ; # Set the site directory .
index index . html index . htm ; # Add an attribute .
}
}
```

7. (optional) Configurec http request to force to jump to https, and you can access via use http protocol. Modify `nginx.conf` file as follows:

```
server {
listen 80 ;
server_nam e localhost ; # replace localhost with
domain name bound by the certificat e .
return 301 https :// $ server_nam e $ request_ur i ;
}
server {
listen 443 ssl ;
server_nam e localhost ; # replace localhost with
domain name bound by the certificat e .
}
```

8. Save the `nginx.conf` file and exit.

9. Restart the Nginx server.

References:

- [Install SSL certificates in Tomcat servers](#)
- [#unique_20](#)

- [#unique_25](#)
- [#unique_26](#)
- [#unique_22](#)
- [#unique_27](#)
- [#unique_28](#)

6.5 Install SSL certificates in IIS servers

This topic describes how to install a downloaded Alibaba Cloud SSL certificate in an (Internet Information Services) IIS server.

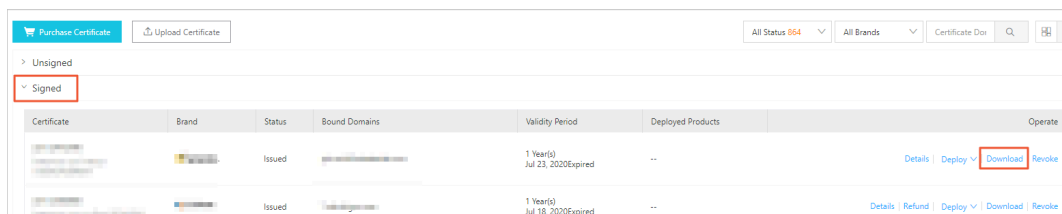
Prerequisites

You selected Automatic for CSR Generation when applying for the certificate.

If you selected Manual for CSR Generation when applying for the certificate, no certificate file is generated. You have to download the .crt certificate whose Server Type is Other, and then run the OpenSSL command to convert the certificate to .pfx format.

Procedure

1. Log on to the [Alibaba Cloud SSL Certificates console](#).
2. On the SSL Certificates page, locate the target SSL certificate and click Download in the lower-right corner.



3. In the Download Certificate dialog box, locate the row that contains the certificate whose Server Type is IIS, and click Download in the Actions column to download the package to your local host.
4. Decompress the package. You will obtain a certificate file (suffixed with .pfx or of .pfx file format) and a key file (suffixed with .txt or of .txt file format).

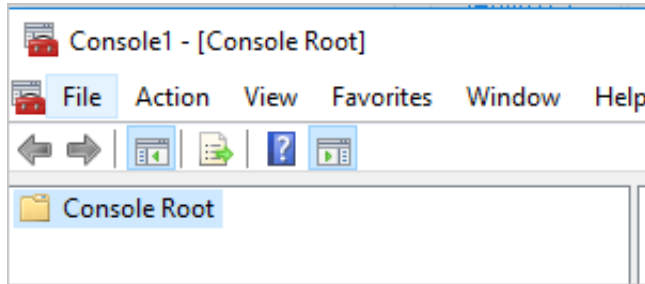


Note:

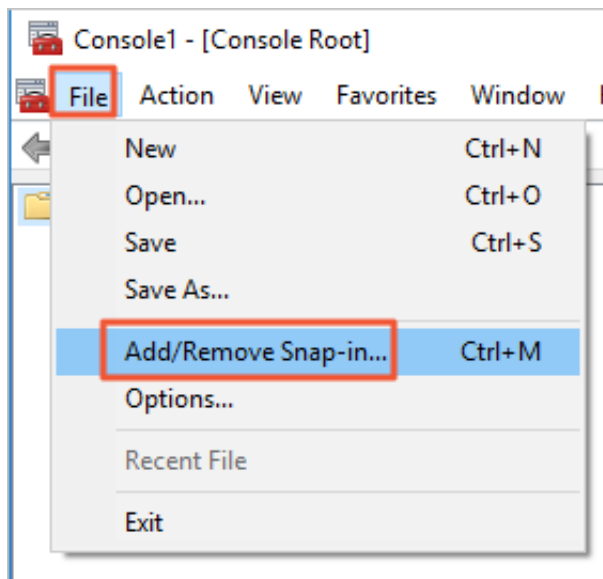
Each time the certificate is downloaded, a new password is generated, which is valid only for the current certificate. To update the certificate file, you also need to update the matching key file.

5. In the Console of your operating system, import your IIS server certificate file.

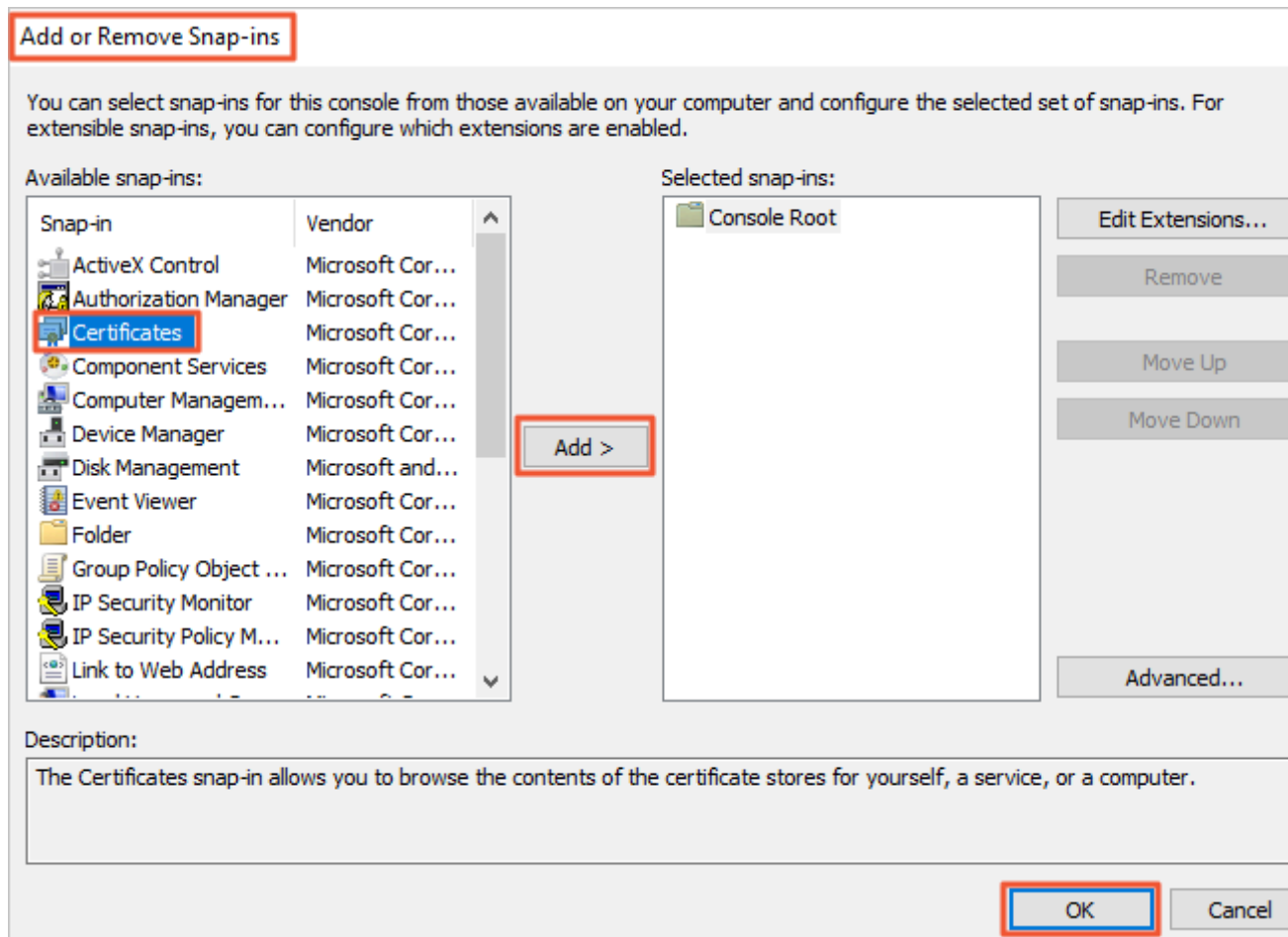
a. Choose Start > Run > MMC to open the console.



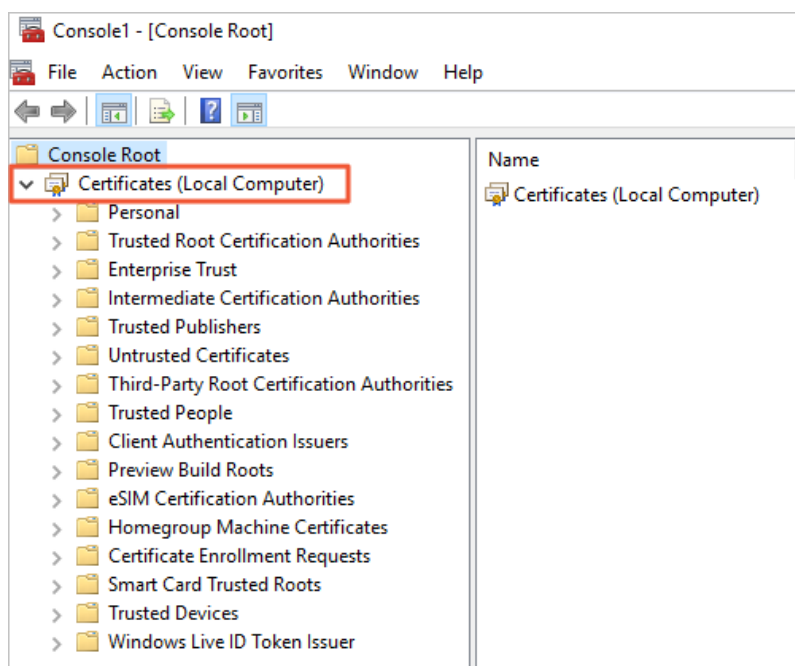
b. Choose File > Add/Remove Snap-in.



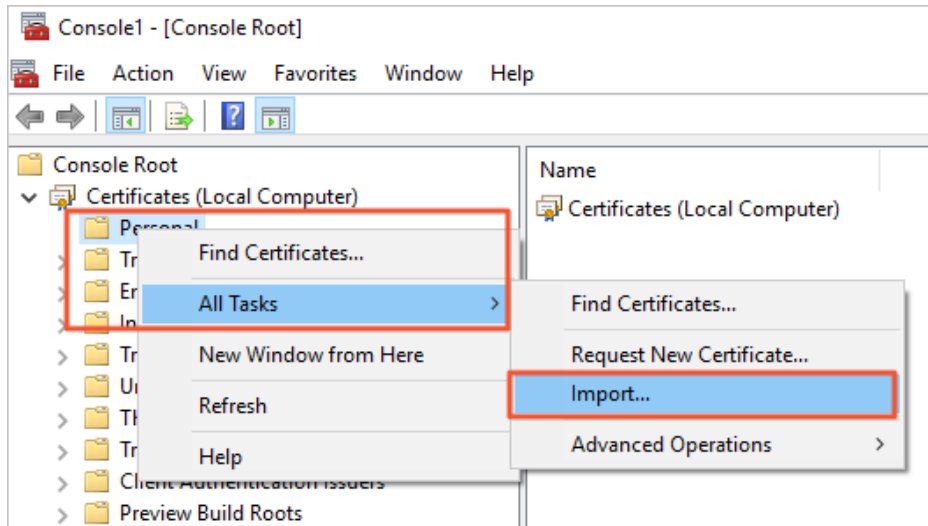
c. In the Add or Remove Snap-ins dialog box, choose Certificates > Add > Computer account > Next > Local computer: (the computer this console is running on) > Finish.



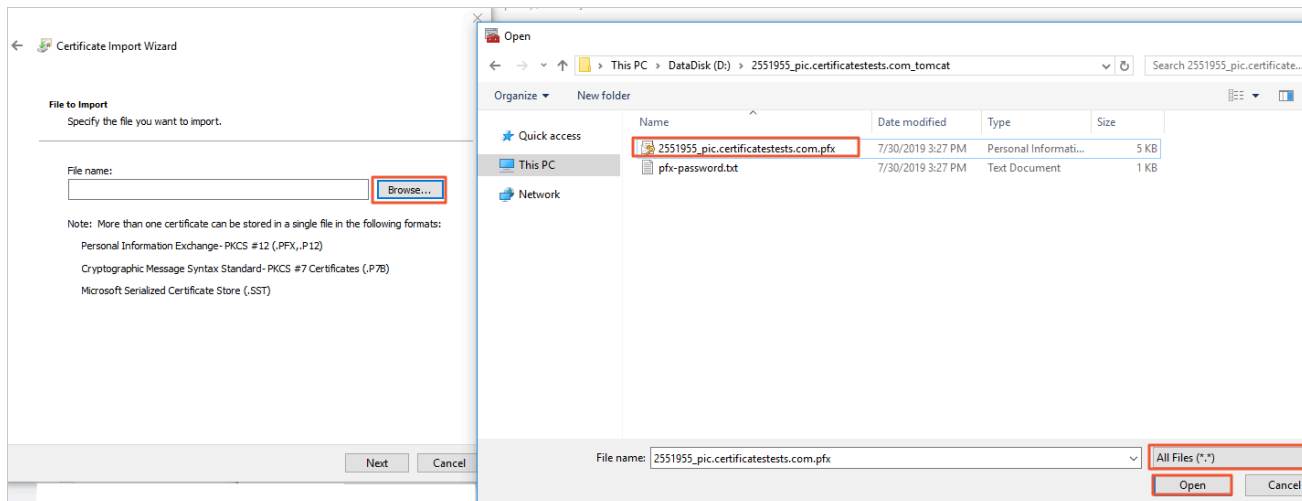
- d. In the left-side navigation pane of the console, click Certificates under Console Root to expand the certificate list.



- e. Choose Personal > All Tasks > Import.



- f. In the Certificate Import Wizard dialog box, click Browse. In the Open dialog box, select the downloaded .pfx certificate file and click Open to import it.

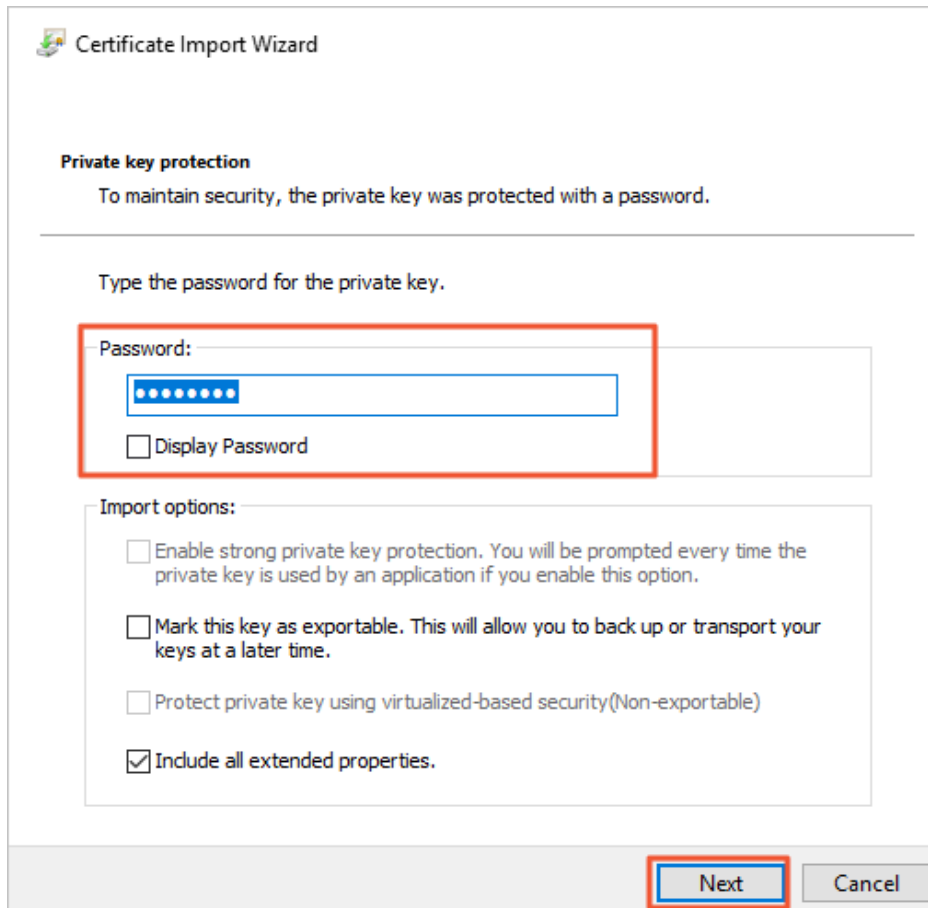


Note:

In the Open dialog box, select All Files (*.*) from the file type drop-down list on the right of File Name.

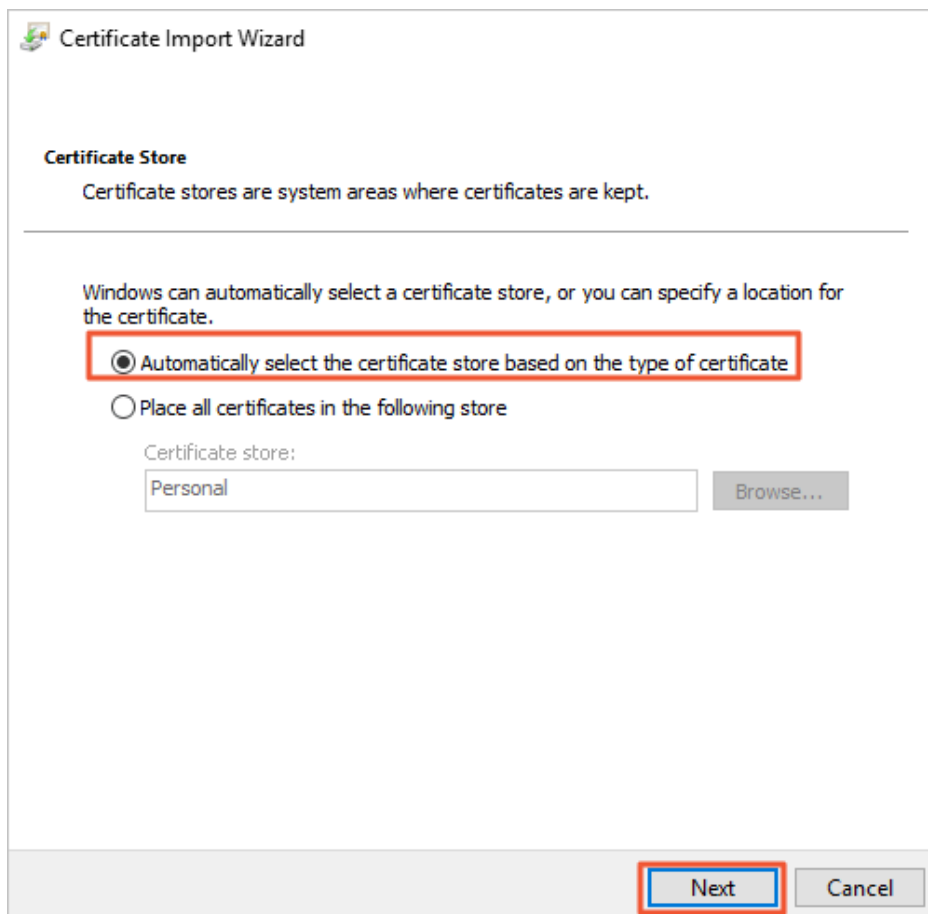
- g. Enter the password in the key file.

You can open the pfx-password .txt file in the downloaded IIS server certificate files to retrieve the password.



The image shows the 'Certificate Import Wizard' dialog box. The title bar says 'Certificate Import Wizard'. The main section is titled 'Private key protection' and contains the text 'To maintain security, the private key was protected with a password.' Below this, it says 'Type the password for the private key.' There is a 'Password:' label followed by a text box containing several dots. A red rectangle highlights the 'Password:' label and the text box. Below the text box is a checkbox labeled 'Display Password'. Below the password section is a section titled 'Import options:' with four checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.', 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.', 'Protect private key using virtualized-based security(Non-exportable)', and 'Include all extended properties.' The 'Include all extended properties.' checkbox is checked. At the bottom right, there are 'Next' and 'Cancel' buttons. A red rectangle highlights the 'Next' button.

- h. Select Automatically select the certificate store based on the type of certificate and click Next to complete the import.



6. Assign a certificate for the server.

- a. Go to the IIS8.0 manager, locate the website where the certificate is to be deployed, and click Bind.
- b. In the Site Bindings dialog box, choose Add > https > 443 > SSL certificate > OK.



Note:

The default port for SSL is port 443, and we recommend this not be changed. If other ports are used, such as 8443, enter `https :// www . domain . com : 8443` to visit the website.

6.6 Install SSL certificates in GlassFish servers

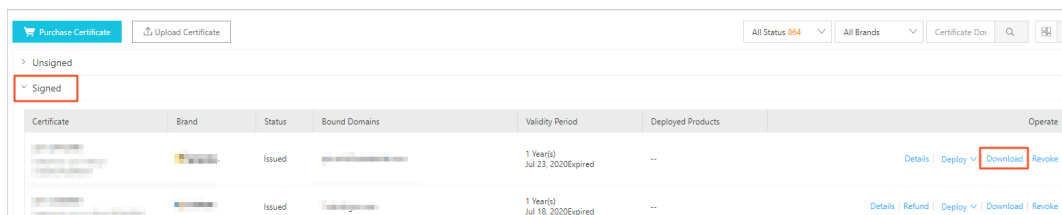
This topic describes how to install your SSL certificate in a GlassFish server.

Procedure

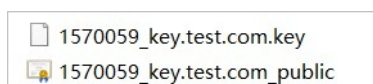
In this example, the SSL certificate name is cer01, the certificate file is named cer01.pem and the key file is named cer01.key.

1. Log on to the [Alibaba Cloud SSL Certificates console](#).

2. On the SSL Certificates page, locate the target SSL certificate and click Download in the lower-right corner.



3. In the Download Certificate dialog box, locate the row that contains the SSL certificate whose Server Type is Other, and click Download in the Actions column to download the package to your local host.
4. Decompress the package. You will obtain a certificate file (suffixed with .pem or of .pem file format) and a key file (suffixed with .txt or of .txt file format).



5. Run the following commands to convert the certificate file and key file to .jks files:

```
openssl pkcs12 - export - in cer01 . pem - inkey cer01
. key - out temp . p12 - passout pass : changeit - name
slas
# Replace cer01 . pem with the name of your
certificat e file , and replace cer01 . key with the
name of your key file . The password that you
set when converting the certificat e format must
be the same as the certificat e password on the
GlassFish server . The default password is changeit .
```

```
keytool - importkeys tore - srckeystor e temp . p12 -
srcstorety pe PKCS12 - srcstorepa ss changeit - deststoret
ype JKS - destkeysto re ./ glassfish5 / glassfish / domains /
domain1 / config / keystore . jks - deststorep ass changeit -
alias slas
# The password that you set when converting the
certificat e format must be the same as the
certificat e password on the GlassFish server . The
default password is changeit .
```

6. Restart the domain.

```
./ glassfish5 / bin / asadmin restart - domain
```

7. Check whether the domain name bound to your Alibaba Cloud SSL certificate is valid.

```
wget https :// 127 . 0 . 0 . 1 : 8181
```


7 Revoke certificates

Alibaba Cloud SSL Certificates Service allows you to revoke issued SSL certificates.

You can request to revoke a certificate when you no longer need it or for security purposes.

A full refund will be made when revocation is completed within 30 days after the issuance of the certificate. No refund will be made for revocation that is completed over 30 days after the issuance of the certificate.



Note:

Uploaded certificates cannot be revoked.

You can delete revoked certificates. For differences between revoking and deleting, please see [#unique_35](#)

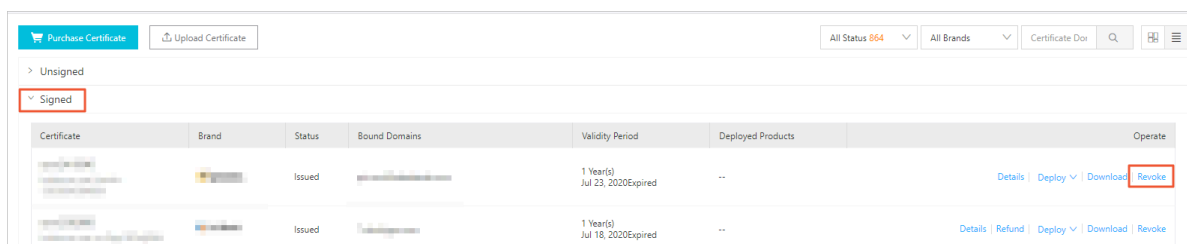
Procedure



Notice:

The certificate cannot be viewed or downloaded after it is submitted for revocation. Therefore, submit an application for certificate revocation with caution.

1. Log on to the Alibaba Cloud [SSL Certificates console](#).
2. Go to the Issued page.
3. Select the certificate to revoke and click Revoke.



4. Fill in the revocation application and click Next to submit the application.
5. Verify the information and click Submit.

The certificate is revoked after your application has been reviewed and approved. Alibaba Cloud completes the revocation application review for an OV or EV certificate within three to five work days after the application is submitted.