



# 证书管理服务

用户指南

天翼云科技有限公司

## 目录

1 产品概述.....	5
1.....	5
1.1 产品定义.....	5
1.2 产品优势.....	6
1.3 功能特性.....	7
1.4 权限管理.....	9
1.5 应用场景.....	9
1.6 术语解释.....	10
1.7 使用限制.....	14
1.8 个人数据保护机制.....	18
2 计费说明.....	19
2.1 计费说明.....	19
2.2 计费方式.....	20
2.3 产品续订.....	21
2.4 产品退订.....	21
3 快速入门.....	23
3.1 SSL 证书使用简介.....	23
4 实例.....	24
4.1 购买 SSL 证书.....	24
4.2 申请 SSL 证书.....	26
4.2.1 申请域名型 (DV) 型 SSL 证书.....	26
4.2.2 申请企业型 (OV) /增强型 (EV) SSL 证书.....	28
4.2.3 域名验证.....	31
4.3 安装 SSL 证书.....	34
4.3.1 <b>下载 SSL 证书</b> .....	34
4.3.2 <b>一键部署 SSL 证书</b> .....	37
4.3.3 <b>安装 SSL 证书至服务器</b> .....	38

4.4 管理 SSL 证书	50
4.4.1 上传证书	50
4.4.2 吊销证书	51
4.4.3 续订证书	52
4.4.4 删除证书	53
4.4.5 查看证书详情	53
4.4.6 证书检测	54
5 CSR 管理	55
5.1 创建 CSR	55
5.2 上传 CSR	56
6 信息管理	58
6.1 联系人管理	58
6.2 公司管理	60
7 常见问题	63
7.1 SSL 证书订购类	63
7.2 SSL 证书申请类	69
7.3 SSL 证书验证类	72
7.4 SSL 证书审核类	76
7.5 SSL 证书下载类	79
7.6 SSL 证书吊销类	79
7.7 SSL 证书有效期类	81
7.8 SSL 证书部署类	83

7.9 其他 SSL 证书问题.....	86
----------------------	----

# 1 产品概述

## 1.1 产品定义

证书管理服务定位云上安全基础 IT 设施，是一款集 SSL 证书购买申请、安全应用为一身的云上证书管家。产品支持国密、国际算法证书，帮助用户实现数据传输加密，保障数据安全。

### 域名型 (DV) SSL 证书

**场景特点：**不验证企业/组织身份，只验证域名控制权，可以快速签发。属于基础型产品，仅能实现 HTTPS，没有标示官网身份和反钓鱼的能力，价格便宜。

**适用场景：**个人博客、API 接口、微信小程序。

**解决问题：**只提供 HTTPS 协议，企业信息非必须项。

**签发周期：**1 个工作日。**资产运维**

### 企业型 (OV) SSL 证书

**场景特点：**在信息传输加密的功能上，增加了验证企业身份的功能。在证书内容中能显示中文或英文公司名称。标示官网身份，起到反钓鱼作用。

**适用场景：**公共部门、教育、医疗、制造、农业、卫生等行业。

**解决问题：**证书中包含了企业信息，标示网站身份，起到反钓鱼作用。

**签发周期：**1~3 个工作日

### 增强型 (EV) SSL 证书

**场景特点**：拥有独一无二的绿色地址栏及地址栏公司名称显示，也因此具有帮助网站提升形象以及增加网站体验度的功能。在功能和效果上较之企业型（OV）证书更强大更多样化。

**适用场景**：银行、金融、保险、证券、互联网金融等行业。

**解决问题**：企业型（OV）证书的升级版，在原有加密性及验证身份的基础上，加强了防假冒网站功能。证书中包含了企业信息，标示网站身份，起到反钓鱼作用。

## 产品功能

证书管理服务具备以下功能，帮助用户解决数据传输安全、身份认证、提高搜索排名、保证数据完整、提高访问速度问题。

**传输安全保护用户隐私**：SSL 证书将在网站和客户端之间建立一条安全的信息传输加密通道，保护用户隐私数据的传输。

**确认网站真实性**：SSL 证书能帮助确认网站的真实身份，如同网站在互联网世界中的身份证。

**提升搜索引擎排名**：知名搜索引擎已经优先收录对 HTTPS 支持的网站，可以帮助网站快速提高排名。

**确保数据完整性**：网站采用 HTTPS 加密通讯，防止数据在传送过程中被窃取、篡改，确保数据的完整性；同时有效抵挡中间人的攻击，提升安全性。

**提高网站访问速度**：SSL 证书全面兼容 HTTP2.0 协议，快速动态加载网页内容，为网站服务提速。

**高可用高可靠**：提供电信级服务高可用能力，为云上应用提供可靠的证书管理服务。

## 1.2 产品优势

**支持国际&国密算法**

全面支持国际主流的 RSA 和 ECC 标准加密算法，适配用户密钥加密长度，同时支持我国商用密码 SM2 及相关标准算法。

#### **证书颁发速度快**

DV 证书域名审核周期不多于 1 个工作日；OV、EV 证书域名审核周期不多于 5 个工作日。

#### **兼容性良好**

兼容性关系到用户访问时浏览器是否会正确给予网页安全的提示，支持目前 99%主流的浏览器和移动设备。

#### **生命周期管理**

支持 SSL 证书申请、域名验证、续订、下载、吊销等 SSL 证书全生命周期管理。

#### **与知名品牌合作，提供多种 SSL 证书类型**

与知名数字证书服务机构合作，确保数字证书认证可信力和加密强度，安全有保障。提供企业型（OV）、增强型（EV）、域名型（DV）多种 SSL 证书，便于企业根据自身业务场景灵活选择。

#### **身份认证**

身份认证是别的加密方式都不具备的，能在 SSL 证书信息里面看到网站所有者公司信息，进而确认网站的有效性和真实性，不会被钓鱼网站所欺骗。

## **1.3 功能特性**

#### **证书管理**

统一管理云上用户 SSL 证书申请使用，提供 SSL 证书申请、验证、安装、下载、续费、吊销、删除的全生命周期管理能力。

### **传输安全保护用户隐私**

SSL 证书将在网站和客户端之间建立一条安全的信息传输加密通道, 保护用户隐私数据的传输。

### **确认网站真实性**

SSL 证书能帮助确认网站的真实身份, 如同网站在互联网世界中的身份证。

### **提升搜索引擎排名**

知名搜索引擎已经优先收录对 HTTPS 支持的网站, 可以帮助网站快速提高排名。

### **确保数据完整性**

网站采用 HTTPS 加密通讯, 防止数据在传送过程中被窃取、篡改, 确保数据的完整性; 同时有效抵挡中间人的攻击, 提升安全性。

### **提高网站访问速度**

SSL 证书全面兼容 HTTP2.0 协议, 快速动态加载网页内容, 为网站服务提速。

### **国际可信签章**

SSL 证书含有国际可信签章, 将签章放置在您的网站中, 用户可以通过签章的链接, 了解您网站的安全以及可信状况。



## 1.4 权限管理

如果您需要对天翼云上购买的证书管理服务 (CCMS) 资源, 给企业中的员工设置不同的访问权限, 以达到不同员工之间的权限隔离, 您可以使用统一身份认证服务 (Identity and Access Management, 简称 IAM) 进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能, 可以帮助您安全的控制天翼云资源的访问。

通过 IAM, 您可以在天翼云帐号中给员工创建 IAM 用户, 并使用策略来控制他们对天翼云资源的访问范围。例如您的员工中有负责软件开发的人员, 您希望他们拥有证书管理服务 (CCMS) 的使用权限, 但是不希望他们拥有删除 CCMS 等高危操作的权限, 那么您可以使用 IAM 为开发人员创建用户, 通过授予仅能使用 CCMS, 但是不允许删除 CCMS 的权限策略, 控制他们对天翼云 CCMS 资源的使用范围。

如果天翼云帐号已经能满足您的要求, 不需要创建独立的 IAM 用户进行权限管理, 您可以跳过本章节, 不影响您使用 CCMS 服务的其它功能。IAM 是天翼云提供权限管理的基础服务, 无需付费即可使用, 您只需要为您帐号中的资源进行付费。关于 IAM 的详细介绍, 请参见《IAM 产品介绍》。

## 1.5 应用场景

### **公共服务类网站、小程序、APP 等满足安全技术要求**

适用客户：通过互联网向公众提供服务的政府、金融、中小企业等客户。

解决问题：面向公众提供服务的各类网站、小程序、APP, 验证企业身份, 满足行业安全

要求，确保站点安全，屏蔽钓鱼网站，提升搜索引擎收录排名，提高网站访问速度。

### 等保、密评等合规监管场景

适用场景：政府、医疗、央国企等领域需要通过密评的客户。

解决问题：满足合规监管机构要求，适用等保、密评场景，可通过国密证书实现传输机密性和完整性保护。

## 1.6 术语解释

### SSL 证书

SSL 证书是一种数字证书，用于在互联网上建立安全通信连接。SSL 代表安全套接层 (Secure Sockets Layer)，它在客户端和服务器之间创建加密通道，确保敏感数据在传输过程中不会被未经授权的第三方截获或篡改。

### 签发 (CA) 机构

签发机构 (Certificate Authority, CA) 是一种可信的第三方机构，负责验证和签发数字证书。CA 在互联网通信中发挥重要作用，确保通信的安全性和可靠性。

### 证书有效期

证书有效期指的是数字证书的有效时间范围，即从 SSL 证书的颁发日期到过期日期之间的时间段。在这段有效期内，SSL 证书被认为是可信和有效的。

### HTTPS 加密协议

HTTPS (Hypertext Transfer Protocol Secure) 是一种通过加密和身份验证来保护数据传输安全的网络通信协议。它是基于 HTTP 协议的安全版本, 通过使用 SSL (Secure Sockets Layer) 或 TLS (Transport Layer Security) 协议来实现通信的加密和认证。

## 域名类型

证书域名类型分为单域名证书、通配符证书 (泛域名证书) 和多域名证书, 不同域名类型的证书对应了它们适用的域名范围:

单域名证书适用于单个特定域名, 例如: ctyun.cn。

通配符证书 (泛域名证书) 适用于一个主域名及其所有的子域名。

多域名证书可适用于多个相似域名, 例如: ctyun.cn、ctyun.com、ctyun.com.cn、\*.ctyun.cn。

## 域名分类

域名可以按照不同的特征进行分类。以下是一些常见的域名分类方式

### 顶级域名 (Top-Level Domain, TLD)

顶级域名是域名系统中最高级别的域名分类。常见的顶级域名包括国家顶级域名 (例如 ".cn" 表示中国) 和通用顶级域名 (例如 ".com" 表示商业机构)。

### 国家顶级域名 (Country Code Top-Level Domain, ccTLD)

国家顶级域名是代表特定国家或地区的域名后缀。每个国家都有自己的国家顶级域名, 例如 ".cn" (中国)、".us" (美国) 和 ".jp" (日本) 等。

## 通用顶级域名 (Generic Top-Level Domain, gTLD)

通用顶级域名是不特定于任何国家或地区的域名后缀。常见的通用顶级域名有".com" (商业机构)、".org" (非营利组织)、".net" (网络服务提供商) 和".edu" (教育机构) 等。

## 子域名 (Subdomain)

子域名是在主域名之前添加的前缀，用于将不同的部分或子网站划分为独立的区域。例如，在"blog.example.com"中，"blog"是一个子域名。"example.com"是一个主域名。

## 国际化域名 (Internationalized Domain Name, IDN)

国际化域名使用非 ASCII 字符集来表示域名，允许使用非拉丁字母、特殊符号和非英语语言的域名。例如，一个使用中文字符的域名"例子.中国"是一个国际化域名。

## 域名后缀 (Domain Suffix)

域名后缀是顶级域名的最后一部分，通常表示域名的分类或性质。例如，".com"、".org" 和".net"都是常见的域名后缀。

## 域名注册者类型

根据域名注册者的类型，域名可以分为个人域名 (由个人注册的域名) 和企业域名 (由公司或组织注册的域名) 等。

## CSR

CSR 代表证书签名请求 (Certificate Signing Request)。它是一种加密通信协议，用于

在申请数字证书时向证书颁发机构（CA）提供必要的信息，包括证书 CN 通用名称等信息。

## 公钥&私钥

公钥（Public Key）：公钥是密钥对中的一部分，用于加密数据和验证数字签名。公钥可以公开共享，用于加密传输的数据。在 SSL 证书中，公钥用于加密客户端与服务器之间的通信。

私钥（Private Key）：私钥是密钥对中的另一部分，与公钥配对使用。私钥应该保密存储，只有服务器拥有者可以访问。私钥用于解密被公钥加密的数据，以及生成和验证数字签名。

公钥（Public Key）与私钥（Private Key）是通过加密算法得到的一个密钥对（即一个公钥和一个私钥，也就是非对称加密方式）。公钥可对会话进行加密、验证数字签名，只有使用对应的私钥才能解密会话数据，从而保证数据传输的安全性。公钥是密钥对外公开的部分，私钥则是非公开的部分，由用户自行保管。

通过加密算法得到的密钥对可以保证在世界范围内是唯一的。使用密钥对的时候，如果用其中一个密钥加密一段数据，只能使用密钥对中的另一个密钥才能解密数据。例如：用公钥加密的数据必须用对应的私钥才能解密；如果用私钥进行加密也必须使用对应的公钥才能解密，否则将无法成功解密。

## SSL 协议

SSL 协议又称为“安全套接层”（Secure Sockets Layer）协议，是通过计算机网络提供通信安全性的加密协议。可在浏览器和网站之间建立加密通道，保证信息传输过程中不被窃取、篡改。

## 1.7 使用限制

浏览器\证书品牌	国际标 准 DV 证书	国际标 准 OV 证书	国际标 准 EV 证书	国 密 标 准 (SM2) DV 证 书	国 密 标 准 (SM2) OV 证 书
Android 2.3 (Gingerbread)	√	√	√	×	×
Android 4.0 (Ice Cream Sandwich)	√	√	√	×	×
Android 4.1 (Jelly Bean)	√	√	√	×	×
Android 4.2 (Jelly Bean)	√	√	√	×	×
Android 4.3 (Jelly Bean)	√	√	√	×	×
Android 4.4 (KitKat)	√	√	√	×	×
Android 5.0 (Lollipop)	√	√	√	×	×
Android 5.1 (Lollipop)	√	√	√	×	×
Android 6.0 (Marshmallow)	√	√	√	×	×
Android 7.0 (Android Nougat)	√	√	√	×	×

浏览器\证书品牌	国际标 准 DV 证书	国际标 准 OV 证书	国际标 准 EV 证书	国 密 标 准 (SM2) DV 证 书	国 密 标 准 (SM2) OV 证 书
Android 7.1 (Android Nougat)	√	√	√	×	×
Android 8.0 (Android Oreo)	√	√	√	×	×
Android 9.0 (Android Pie)	√	√	√	×	×
Android 10.0 (Android Q)	√	√	√	×	×
Android 11.0 (Android R)	√	√	√	×	×
iOS 5	√	√	√	×	×
iOS 6	√	√	√	×	×
iOS 7	√	√	√	×	×
iOS 8	√	√	√	×	×
iOS 9	√	√	√	×	×
iOS 10	√	√	√	×	×
iOS 11	√	√	√	×	×
iOS 12	√	√	√	×	×
iOS 13	√	√	√	×	×
iOS 14	√	√	√	×	×
OS X 10.9 (Mavericks)	√	√	√	×	×
OS X 10.10	√	√	√	×	×

浏览器\证书品牌	国际标 准 DV 证书	国际标 准 OV 证书	国际标 准 EV 证书	国 密 标 准 (SM2) DV 证 书	国 密 标 准 (SM2) OV 证 书
(Yosemite)					
OS X 10.11 (Eicapitan)	√	√	√	×	×
OS X 10.12 (Sierra)	√	√	√	×	×
OS X 10.13 (High Sierra)	√	√	√	×	×
OS X 10.14 (Mojave)	√	√	√	×	×
java 7u181	√	√	√	×	×
java 8u161	√	√	√	×	×
java_8u181	√	√	√	×	×
java_8u202	√	√	√	×	×
java 9	√	√	√	×	×
java 10	√	√	√	×	×
java 11	√	√	√	×	×
java 12	√	√	√	×	×
java 13	√	√	√	×	×
java 17	√	√	√	×	×
Firefox 3.0	√	√	√	×	×
Firefox 3.5	√	√	√	×	×
Firefox 3.6	√	√	√	×	×
Firefox 6.0	√	√	√	×	×



浏览器\证书品牌	国际标 准 DV 证书	国际标 准 OV 证书	国际标 准 EV 证书	国 密 标 准 (SM2) DV 证 书	国 密 标 准 (SM2) OV 证 书
Firefox 16	√	√	√	×	×
Firefox 23	√	√	√	×	×
Firefox 32	√	√	√	×	×
Firefox 42	√	√	√	×	×
Firefox 50	√	√	√	×	×
Firefox 51	√	√	√	×	×
Firefox 54	√	√	√	×	×
Firefox 58	√	√	√	×	×
Firefox 63	√	√	√	×	×
Firefox 65	√	√	√	×	×
Windows XP	√	√	√	×	×
Windows 7	√	√	√	×	×
Windows 8	√	√	√	×	×
Windows 10	√	√	√	×	×
红莲花	√	√	√	√	√
赢达信安全浏览器	√	√	√	√	√
ZoTrus 零信浏览器	√	√	√	√	√
奇安信可信浏览器	√	√	√	√	√
360 安全浏览器	√	√	√	√	√
亚数国密浏览器	√	√	√	√	√

## 1.8 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，CCMS 通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

### 收集范围

CCMS 收集及产生的个人数据如下表所示：

类型	收集方式	是否可以修改	是否必须
租 户 ID	在控制台进行任何操作时 Token 中的租户 ID 在调用 API 接口时 Token 中的 租户 ID	否	是, 租户 ID 是证书资源身份 标识
姓名	在申请 SSL 证书时填写的联系 人姓名	是	是, 证书审核人工认证阶段 必须
邮箱	在申请 SSL 证书或私有证书时 填写的邮箱	申请 SSL 证书 时填写的邮箱: 是 申请私有证书	申请 SSL 证书时填写的邮 箱: 是, 证书审核人工认证 阶段必须 申请私有证书时填写的邮

类型	收集方式	是否可以修改	是否必须
		时填写的邮箱： 否	箱：否
手机号码	在申请 SSL 证书时填写的联系人手机号	是	是，证书审核人工认证阶段必须
企业营业执照	在申请 SSL 证书时，可以选择上传企业营业执照	是	否
银行开户许可	在申请 SSL 证书时，可以选择上传银行开户许可	是	否
企业项目 ID	在申请或使用 SSL 证书、私有证书时，可以为证书分配企业项目	是	已开通企业项目：是 未开通企业项目：否

## 2 计费说明

### 2.1 计费说明

计费项

证书管理服务的计费项具体内容如下表所示：

计费项	计费项说明	适用的计费模式	计费公式
SSL 证书	根据加密标准、证书类型、域名类型、有效期、购买数量计算费用	按次计费	一次性计费：不同规格证书 单价×有效期×购买数量

## 2.2 计费方式

证书管理服务仅支持一次性计费方式。

### 产品价格

证书管理服务为您提供多种规格证书，您可以根据业务需求选择相应的证书规格。

版本	加密标准	证书种类	域名类型	年付价格（元/个/年）
标准版	国际算法	域名型（DV）	单域名	594.15
标准版	国际算法	域名型（DV）	通配符	1699.15
标准版	国际算法	域名型（DV）	多域名	1188.3 起
标准版	国际算法	企业型（OV）	单域名	1912.5
标准版	国际算法	企业型（OV）	通配符	5270
标准版	国际算法	企业型（OV）	多域名	2422.5 起
标准版	国际算法	增强型（EV）	单域名	2720
标准版	国际算法	增强型（EV）	多域名	3740 起
标准版	国密算法	域名型（DV）	单域名	1275
标准版	国密算法	域名型（DV）	通配符	2975
标准版	国密算法	域名型（DV）	多域名	2550 起

版本	加密标准	证书种类	域名类型	年付价格（元/个/年）
标准版	国密算法	企业型（OV）	单域名	3825
标准版	国密算法	企业型（OV）	通配符	11475
标准版	国密算法	企业型（OV）	多域名	6375 起

## 2.3 产品续订

证书管理服务仅支持控制台续订，用户可在控制台实例界面选择续订，按照续订产品规格进行下单。

### 说明：

仅签发成功的证书能够进行续订。

仅支持续订统一规格证书。

### 操作步骤

- 1.进入证书管理服务，选择“我的证书” > “证书管理”。
- 2.在待续费证书的“操作”列单击“证书续订”。
- 3.在跳转的页面中确认续订证书的信息和续订年限，确认无误后单击“立即购买”。

## 2.4 产品退订

如果您通过天翼云证书管理服务控制台购买了证书，在符合退款条件的情况下，可在证书管理服务控制台申请退款。

本章节介绍符合退订的条件以及如何退订天翼云证书管理服务。

### 约束限制

- 满足以下条件（必须全部满足）的证书管理服务订单，可提交工单申请或拨打【400-810-9889】退订：
  - 您通过天翼云证书管理服务控制台购买了证书。
  - 距离证书订单下单时间（完成支付的时间）不超过 7 个自然日，即距离 SSL 证书订单完成支付时间顺延不超过 7\*24 小时。例如，10 月 1 日 12:00 完成 SSL 证书订单支付，则在 10 月 8 日 11:59 前可以退订，10 月 8 日 11:59 后将不支持退订。
  - 已购买的 SSL 证书符合以下情况之一：
    - 未提交证书申请，证书状态为“待申请”。
    - 提交过证书申请，证书未签发，且已取消申请，证书状态为“待申请”。
    - 提交过证书申请，证书已签发，且在下单后 7 个自然日内完成了证书吊销流程（不仅是提交了吊销申请，须完成吊销流程），证书状态为“已吊销”。

#### 注意

在退订成功之前，请勿删除证书。

- 证书管理服务支持 7 日内全额退款，退款需要扣除用户该自然年 7 天无理由退款次数，若用户该自然年内 7 天无理由退款次数已用完则需要扣除手续费（手续费计算方式： $\text{手续费} = \text{订单实付款} \div 36500 \times 7$ ）。
- 多年期证书，第一张证书已签发，并在下单后 7 个自然日内完成了证书吊销流程，支持全额退订。

# 3

## 快速入门

### 3.1 SSL 证书使用简介

通过使用 SSL 证书，您的网站可以实现安全的 HTTPS 数据传输。本文介绍了购买 SSL 证书和使用 SSL 证书的流程，帮助您快速掌握 SSL 证书服务的相关操作。

步骤	任务	说明	相关文档
1	购买一个 SSL 证书。	SSL 证书是天翼云证书管理服务售卖的 SSL 证书资源实体，用于管理与 SSL 证书有关的操作，例如，提交证书申请、在证书签发后下载证书等。	<a href="#">购买证书</a>
2	使用已购买的 SSL 证书，向 CA 中心提交证书申请。	CA 中心是颁发 SSL 证书的机构，您可以通过已购买的 SSL 证书向 CA 中心提交证书申请。只有当 CA 中心审核通过您的证书申请后，才会为您签发 SSL 证书。	<a href="#">申请证书</a>
3	在证书即将过期时，为证书续费并使用新签发的证书替换旧证书。	CA 中心签发的 SSL 证书默认有 1 年有效期。证书过期后将不被浏览器信任，影响客户端通过 HTTPS 协议访问您的业务。您可以在证书到期前的 30 个自然日内，为证书手动续费。 在证书续费后，您还必须将续费签发的新证书重新安装到您的 Web 服务器（或者部署到天翼云产品），替换即将过期的旧证书。	<a href="#">产品续订</a>

步骤	任务	说明	相关文档
4	不再需要使用证书时，向 CA 中心提交证书吊销申请。	如果您不再需要使用仍然有效的 SSL 证书，出于安全性考虑（例如，避免证书被盗用），建议您通过 SSL 证书服务向 CA 中心提交证书吊销申请。吊销证书表示从签发该证书的 CA 中心处注销证书信息。已注销的证书将失效。	<a href="#">吊销证书</a>

# 4 实例

## 4.1 购买 SSL 证书

### 操作步骤

- 1.登录天翼云官网，单击证书管理服务产品详情页。
- 2.单击【立即订购】，进入到证书管理服务产品购买页面。
- 3.输入域名购买方式：填写域名名称，选择证书规格以及购买时长，若您不知道域名可以单击“快速购买方式”切换。
- 4.SSL 证书数量购买方式：选择证书数量、规格以及购买时长，具体的规格选择可参见下表。

证书规格	适用场景	说明
域名型证书 (DV)	如果您的网站主体是个人（即没有企业营业执照），只能申请域名型 (DV) 证书。	信任等级一般，只需验证域名的真实性便可颁发证书保护网站，签发证书速度最快，一般申请通过验证



证书规格	适用场景	说明
		后几分钟即可获取到证书。
企业型证书 (OV)	对于一般企业, 建议购买 OV 型及以上类型的 SSL 证书。(若作为移动端网站或接口调用, 也建议您购买 OV 型及以上类型的 SSL 证书。)	信任等级较高, 必须要验证域名权限以及企业的身份, 审核严格, 安全性高。
增强型证书 (EV)	对于金融、支付类企业, 建议购买 EV 型证书。	信任等级强, 一般用于银行证券等金融机构、大中型企业等, 审核更严格, 安全性更高, 同时在浏览器显示公司名称。

说明:

若您选择购买服务的时长为 2 年期, 那么此服务中包含 2 张有效期为 1 年的 SSL 证书, 在到期 30 天前, 天翼云将会自动为您续期证书。

5. 阅读天翼云《证书管理服务协议》后, 勾选我已阅理解并接受, 即可单击“立即购买”下单。

6. 单击“提交订单”, 在弹出的“订单详情”页确认订单信息。

7. 单击“立即支付”, 完成 SSL 证书在购买。

## 4.2 申请 SSL 证书

开通堡垒机（原生版）后，用户在控制台“云堡垒机实例”页面，在操作列点击“管理”操作，系统单点登录进入云堡垒机实例，通过控制台登录进入默认管理员用户。

登录的时候可选“外网地址登录”或“内网地址登录”。

说明

- 内网地址登录需要确保网络环境互通。
- 外网地址登录需要绑定弹性 IP。

### 首次登录

在未设置初始密码时，需通过云堡垒机控制台单点登入跳转登入堡垒机，并进行初始化管理工作。

- 1.在“云堡垒机实例”列表条目录中选择要管理的实例，单击“管理”。
- 2.根据您的网络环境选择“内网地址登录”或“外网地址登录”。
- 3.登入堡垒机后，通过个人信息进行初始密码设置。

### 4.2.1 申请域名型（DV）型 SSL 证书

成功购买证书后，您需要申请证书，即为证书绑定域名或 IP、填写证书申请人的详细信息并提交审核。所有信息通过审核后，证书颁发机构才签发证书。

#### 前提条件

已成功购买证书并且在控制台的“证书状态”为“待申请”。

## 约束限制

如果您申请的 DV 证书，绑定的域名含有 edu、gov、bank、live 或品牌相关的敏感词，可能无法通过安全审核，建议选择 OV 或 EV 证书。

## 操作步骤

1. 登录“证书管理服务”控制台，在左侧导航栏选择“我的证书 > 证书管理”，随后在顶部导航栏选择“可申请”，进入“证书管理”页面。
2. 选择“域名型 (DV) SSL”证书，单击“操作”列的“证书申请”按钮，进行 SSL 证书申请。
3. 在右侧的对话框中填写证书申请的相关信息。

填写参数	参数说明
证书绑定域名	第一个域名将作为证书通用域名名称（不可修改）。
域名验证方式	仅支持“手工 DNS 验证”。
联系人	选择联系人，如何新建联系人请参考 <a href="#">信息管理</a> 章节。
所在地	根据实际所在地区选择。（目前仅支持选择中国地区）
密钥算法	可选择“RSA”、“ECC”或“SM2”（根据购买证书页面所选的加密标准选择）

填写参数	参数说明
CSR 生成方式	可选择“系统生成”或“手动生成”。

注意:

- 为保障您的证书顺利申请，建议您使用系统生成 CSR 的方式，手动上传将无法署到天翼云产品。建议您使用系统创建的 CSR，避免因内容不正确而导致的审核失败。
- 若您选择手动生成 CSR，使用已创建的 CSR 申请证书，请不要在证书签发完成前删除 CSR。

4. 填写完后，单击“提交审核”。

5. 配置域名验证信息，配置域名信息操作可参考域名验证。配置后完成等待审核签发证书。

6. 若证书已成功签发，可返回到“已签发”页查看签发成功的证书。

## 4.2.2 申请企业型（OV）/增强型（EV）SSL 证书

成功购买证书后，您需要申请证书，即为证书绑定域名或 IP、填写证书申请人的详细信息并提交审核。所有信息通过审核后，证书颁发机构才签发证书。

### 前提条件

已成功购买证书并且在控制台的“证书状态”为“待申请”。

### 操作步骤

1. 登录“证书管理服务”控制台，在左侧导航栏选择“我的证书 > 证书管理”，随后在顶

部导航栏选择“可申请”，进入“证书管理”页面。

2.选择“企业型 (OV) SSL”或“增强型 (EV) SSL”证书，单击“操作”列的“证书申请”按钮，进行 SSL 证书申请。

3.在右侧的对话框中填写证书申请的相关信息。

填写参数	参数说明
证书绑定域名	第一个域名将作为证书通用域名名称（不可修改）
域名验证方式	可选“手工 DNS 验证”或“文件验证”。 “文件验证”目前仅支持绑定 IP 方式的 OV 证书验证。
联系人	选择联系人，如何新建联系人请参考 <a href="#">信息管理</a> 章节。
公司	选择公司，如何新建公司请参考 <a href="#">信息管理</a> 章节。
所在地	根据所选择的公司所在地自动生成。
密钥算法	可选择“RSA”、“ECC”或“SM2”（根据购买证书页面所选的加密标准选择）
CSR 生成方式	可选择“系统生成”或“手动生成”。

注意：

- 为保障您的证书顺利申请，建议您使用系统生成 CSR 的方式，手动上传将无法署到

天翼云产品。建议您使用系统创建的 CSR，避免因内容不正确而导致的审核失败。

- 若您选择手动生成 CSR，使用已创建的 CSR 申请证书，请不要在证书签发完成前删除 CSR。

4. 填写完后，单击“提交审核”。

5. 进行人工验证环节，单击“下载确认函模板”。（仅支持企业型(OV)/增强型(EV)SSL 证书）

6. 查看下载的确认函，若确认无误选择该确认函文件上传，单击“点击上传”进行上传。

说明：

- 确认函需要在模板标黄处填写内容，并在公司名称处盖章后回传。
- 若您申请的是国密证书，还需在填写公司对公账户的开户行名称、对公账户账号及公司地址。
- 如果您申请证书时填写邮箱企业邮箱与企业域名相关（例如申请的域名为 \*.ctyun.com，企业邮箱为\*@chinatelecom.com），并且该企业邮箱可以正常收发外部邮件，这种情形下可以不提供确认函。
- 企业发送工商登记年报的邮箱若可以正常收发外部邮件，使用该邮箱申请证书时可以不提供确认函。
- 非以上场景申请企业型（OV）和增强型（EV）证书必须提供确认函，建议使用 189、126、163、QQ 等免费邮箱。

7 配置域名验证信息，配置域名信息操作可参考[域名验证](#)，配置完成后等待审核签发证书。

8. 若证书已成功签发，可返回到“已签发”页查看签发成功的证书。

## 4.2.3 域名验证

### 4.2.3.1 方式一：手动 DNS 验证

根据 CA 中心的规范要求,如果您申请了 SSL 证书,则必须完成域名验证来证明待申请证书要绑定的域名属于您或您所属的组织。

手动 DNS 验证,是指您需要在域名的 DNS 解析服务商手动修改域名的 DNS 解析记录,在解析记录中添加一条用于验证的记录。CA 机构验证添加的记录能被解析,则表示验证通过。

如果您在申请证书时域名验证方式选择了手动 DNS 验证,请参照本章节进行处理。

#### 约束与限制

手动 DNS 验证的域名解析只能在您的域名管理平台上进行操作,具体的解析方法以域名服务商提供的解析方法为准。

#### 前提条件

绑定的域名须做实名认证,如果未做实名认证,请前往您的域名服务商处完成域名实名认证。

#### 获取域名验证信息

- 1.登录[证书管理服务控制台](#)。
- 2.选择需要进行 DNS 验证的证书,单击“操作”列的“证书验证”。
- 3.在证书验证页面,查看并记录解析记录的**记录类型**、**主机记录**和**记录值**。

#### 在天翼云云解析服务器上进行 DNS 验证

- 1.提交证书申请后,单击“证书验证”,获取证书验证信息。

## 说明

域名型 (DV) 证书无需经过人工审核, 可直接在控制台查阅域名 DNS 验证信息。

企业型 (OV) /增强型 (EV) 证书需先上传证书确认函后, 才可以在控制台查阅域名 DNS 验证信息。

2.下面以天翼云解析为例, 演示为域名添加 DNS 解析记录过程。如果您域名对应的 DNS 域名解析服务不在天翼云, 请您前往域名对应的 DNS 域名解析商添加解析记录。

2.1. 使用域名持有者所在的天翼云账号, 登录[云解析服务管理控制台](#)。

2.2. 在需要添加 DNS 解析记录的域名记录操作列, 单击“解析设置”。

2.3. 在添加记录面板, 将域名认证获取到的验证信息进行添加, 填写规则参加下表。

参数	填写说明
主机记录	证书的验证信息对话框, 域名服务商返回的“主机记录”。
记录类型	证书的验证信息对话框, 域名服务商返回的“记录类型”。
线路类型	选择“默认”。
记录值	证书的验证信息对话框, 域名服务商返回的“记录值”。
MX 优先值	-
TTL	选择默认值, 不作修改。

2.4 单击“√”完成记录添加。



3. 成功配置解析记录后，等待 CA 中心对 DNS 验证信息进行审核，审核通过后，证书变为“已签发”状态。

#### 4.2.3.2 方式二：文件验证

文件验证，是指您手动从证书管理服务控制台获取证书验证文件，然后在服务器的网站根目录下创建指定文件。CA 机构验证文件路径可以被访问，则表示验证通过。

如果您购买的 OV 证书（绑定 IP 形式），您需要完成文件验证，请参照本章节进行处理。

注意：

- 目前 CA 中心仅支持向 80、443 端口发起验证请求，因此您的业务需开放 80、443 端口。
- 天翼云仅支持绑定 IP 购买的 OV 证书进行文件验证。

### 验证步骤

#### 获取验证信息

- 提交证书申请后，单击“证书验证”，获取证书验证信息。如下图所示。
- 您可以直接单击“操作”列的“导出文件”，将需要上传的文件导出至本地。

#### 创建文件

1. 登录您的服务器，并且确保域名已指向该服务器并且对应的网站已正常启用。
2. 在现有网站目录的根目录下，创建指定的文件。该文件包括文件目录、文件名、文件内容。

说明

网站根目录是指您在服务器上存放网站程序的文件夹，大致有这几种表示名称：  
public\_html、htdocs、assets、logs 等。请您根据实际环境进行操作。

2.a. 依次执行以下命令，在服务器的 Web 根目录 (Nginx 服务默认为 `****/var/www/html/`)

下创建文件验证目录（.well-known/pki-validation/）。

```
cd /var/www/html
```

```
mkdir -p .well-known/pki-validation
```

2.b.在 /var/www/html/.well-known/pki-validation/目录下，创建 fileauth.txt 文件，fileauth.txt 为验证信息中显示的文件名。在 fileauth.txt 文件中把验证信息中的文件内容复制粘贴上去。

说明

您可以直接在控制台选择“导出文件”，直接将文件上传至相关目录。

3.打开浏览器，根据验证的域名类型，访问对应的链接地址，确保访问链接地址可获取到文件内容。链接地址格式为：http://域名/文件目录/文件名或者 https://域名/文件目录/文件名。

4.成功配置文件验证信息后，等待 CA 中心对文件验证信息进行审核，审核通过后，证书变为“已签发”状态。

## 4.3 安装 SSL 证书

### 4.3.1 下载 SSL 证书

通过证书管理服务购买并签发 SSL 证书后，您需要将已签发的 SSL 证书安装至服务器，才能使 SSL 证书生效。

不同类型的服务器支持配置的 SSL 证书格式不同。为了便于您安装 SSL 证书，证书管理服务提供了适用于各种服务器（例如，Apache、Exchange、GlassFish、Internet Information

Services,IIS、Nginx、TOMACAT) ) 的 SSL 证书压缩包, 供您直接下载使用 (无需手动转换 SSL 证书格式) 。

如果您已经通过证书管理服务购买并签发了 SSL 证书, 可以执行以下步骤, 将已签发的 SSL 证书下载到本地。

## 下载 SSL 证书

说明:

只有证书“状态”为“已签发”、“即将过期”、“已过期”和“吊销审核中”的证书可以下载。

- 1.登录证书管理服务控制台。
- 2.在左侧导航栏选择“我的证书 > 证书管理”。
- 3.找到需要部署的证书, 单击“操作”列的“证书下载”。
- 4.证书下载后, 需要安装到对应的服务器上, 才能使 SSL 证书生效, 您可以解压对应 SSL 证书的压缩包获得对应的 SSL 证书文件, 解压后的非国密算法证书文件说明如下表所示。

服务器类型	证书文件说明
Apache	Cert 证书公钥: XXXX.cn_cert.pem Chain 证书链: XXXX.cn_chain.pem 私钥文件: XXXX.cn_key.key 部署参考: <a href="#">在 Apache 服务器部署 SSL 证书</a>
Exchange	Cert 证书公钥: XXXX.cn_cert.pem

服务器类型	证书文件说明
	Chain 证书链: XXXX.cn_chain.pem 私钥文件: XXXX.cn_key.key 部署参考: <a href="#">在 Exchange 服务器部署 SSL 证书</a>
GlassFish	Cert 证书公钥: XXXX.cn_cert.pem Chain 证书链: XXXX.cn_chain.pem 私钥文件: XXXX.cn_key.key 部署参考: <a href="#">在 GlassFish 服务器部署 SSL 证书</a>
IIS	PFX 证书密码: README.txt PFX 格式证书: XXXX.cn.pfx 部署参考: <a href="#">在 IIS 服务器部署 SSL 证书</a>
Nginx	Cert 证书公钥: XXXX.cn_cert_chain.pem 私钥文件: XXXX.cn_key.key 部署参考: <a href="#">在 Nginx 服务器部署 SSL 证书</a>
TOMCAT	JKS 证书: XXXX.cn.jks JKS 证书密码: README.txt 部署参考: <a href="#">在 TOMCAT 服务器部署 SSL 证书</a>

### 4.3.2 一键部署 SSL 证书

证书管理服务支持将已签发的证书一键部署至您的服务器上,减少您去手动部署证书的相关操作,提升业务的便捷性。

#### 约束限制

- 只有已签发的证书支持一键部署功能
- 当前仅支持将证书部署到 Web 应用防火墙 (原生版)
- 不支持国密规格证书的一键部署
- 仅支持通过证书管理服务控制台签发的证书使用一键部署功能。
- 每次部署会自动为您在弹性负载均衡平台中创建一个证书。每个用户在弹性负载均衡平台的证书限制为 10 个,如果超出限制请访问弹性负载均衡平台手动删除多余证书
- 目前部署至弹性负载均衡仅支持部分资源池,请以控制台提示为准
- 若您使用的子账号进行一键部署弹性负载均衡,需要在 IAM 给相关子账号配置 default 企业项目权限

#### 操作步骤

- 1.登录“证书管理服务”控制台,在左侧导航栏选择“我的证书 > 证书管理”,进入“证书管理”页面。
- 2.在导航栏选择“已签发”,筛选出已经成功签发的证书。



- 3.选择需要部署的证书,选择“操作”列的“更多 > 一键部署”。



4.在右侧弹出的对话框中，在下方选择需要部署的证书，单击“操作”列的“部署”或“重新部署”，即可完成证书的部署。

说明：

- 您可以批量勾选需要部署的证书（最多支持 5 个整数），单击“批量部署”。
- 若您选择部署至弹性负载均衡服务，则需要先选择资源池，目前仅支持部分资源池部署，请以控制台提示为准。



## 后续操作

查看部署记录：选择“部署记录”，可查看该证书的历史部署情况和回退情况。

回退：在部署记录中找寻需要回退的证书及部署时间，单击“操作”列的“回退”即可回退。

## 4.3.3 安装 SSL 证书至服务器

### 4.3.3.3 Apache 服务器部署 SSL 证书

#### 前提条件

已在当前服务器中安装配置 Apache 服务。

已购买证书并且已获取到证书相关文件。

安装前准备文件

在证书管理服务控制台的证书管理页选择您需要安装的证书，选择“证书下载”。

在弹出的“证书下载”窗口中，服务器类型选择 Apache，单击“下载”并解压缩包至

本地，文件内包含下述 3 个文件：

Cert 证书公钥：XXXX.cn\_cert.pem

Chain 证书链：XXXX.cn\_chain.pem

私钥文件：XXXX.cn\_key.key

### 操作步骤

1.启用 SSL 和 443 端口：将“mod-aviable”文件夹中的“ssl.conf”和“ssl.load”这两个配置文件，复制到“mod-enable”文件夹中。

2.启用 443 端口的 vhost：将“site-aviable”中的 default-ssl 配置，加载到“site-enable”文件中。

（此处环境仅做参考，具体以实际操作环境为准）替换 Cert 证书公钥文件，路径参考：

SSLCertificateFile/xxxx/server.crt。

3.替换 Chain 证书链文件，路径参考：SSLCertificateChainFile/xxxx/ca.crt。

4.替换私钥文件，路径参考：SSLCertificateKeyFile/xxxx/server.key。

5.重启 apache2 服务，即可完成证书导入。

### 4.3.3.4 Exchange 部署 SSL 证书

#### 前提条件

已在当前服务器中安装配置 Exchange 服务。

## 操作步骤

- 1.在证书管理服务控制台的证书管理页选择您需要安装的证书，选择“证书下载”。
- 2.在弹出的“证书下载”窗口中，服务器类型选择 Apache，单击“下载”并解压缩包至本地。

使用第 1 步下载的“xxxx.cn\_cert”证书文件和“xxxx.cn\_key”私钥文件（生成 CSR 请求与之同时生成的 key）通过 openssl 工具或在线工具生成一份 PFX 文件，请妥善保存好生成的 PFX 文件密码。

- 3.使用“Win + R”快捷键组合打开“运行”控制台，输入“mmc”打开“Microsoft 控制台”。

- 4.单击右上角的“文件”选择“添加/删除管理单元”。

- 5.在“可用管理单元”中选择“证书”，并单击“添加”。

- 6.在弹出的对话框中选择“计算机账户”，单击“下一页”后再选择“本地计算机”，单击“完成”将证书模块添加至控制台根节点中。

- 7.在“控制台根节点”中选择“证书 > 个人”，在“对象类型”页面单击右键，选择“所有任务 > 导入”。

- 8 选择第 2 步中生成的 PFX 文件，单击“下一步”后选择“证书存储个人”完成证书导入。

- 9 在命令提示符工具中，使用如下指令检查可用证书列表：

```
Get-ExchangeCertificate
```

- 10.使用如下指令开启相关功能，即可使证书正常生效：

```
Enable-ExchangeCertificate -Thumbprint
```



4A249CB4BA76EBA3E4F59CFD6E34685022158B99 –Services

'IMAP,POP,IIS,SMTP'

### 4.3.3.5 GlassFish 部署 SSL 证书

#### 前提条件

已在当前服务器中安装配置 GlassFish 服务。

#### 文件准备

在证书管理服务控制台的证书管理页选择您需要安装的证书，选择“证书下载”。

在弹出的“证书下载”窗口中，服务器类型选择 Apache，单击“下载”并解压缩包至

本地，文件内包含下述 3 个文件：

Cert 证书公钥：XXXX.cn\_cert.pem

Chain 证书链：XXXX.cn\_chain.pem

私钥文件：XXXX.cn\_key.key

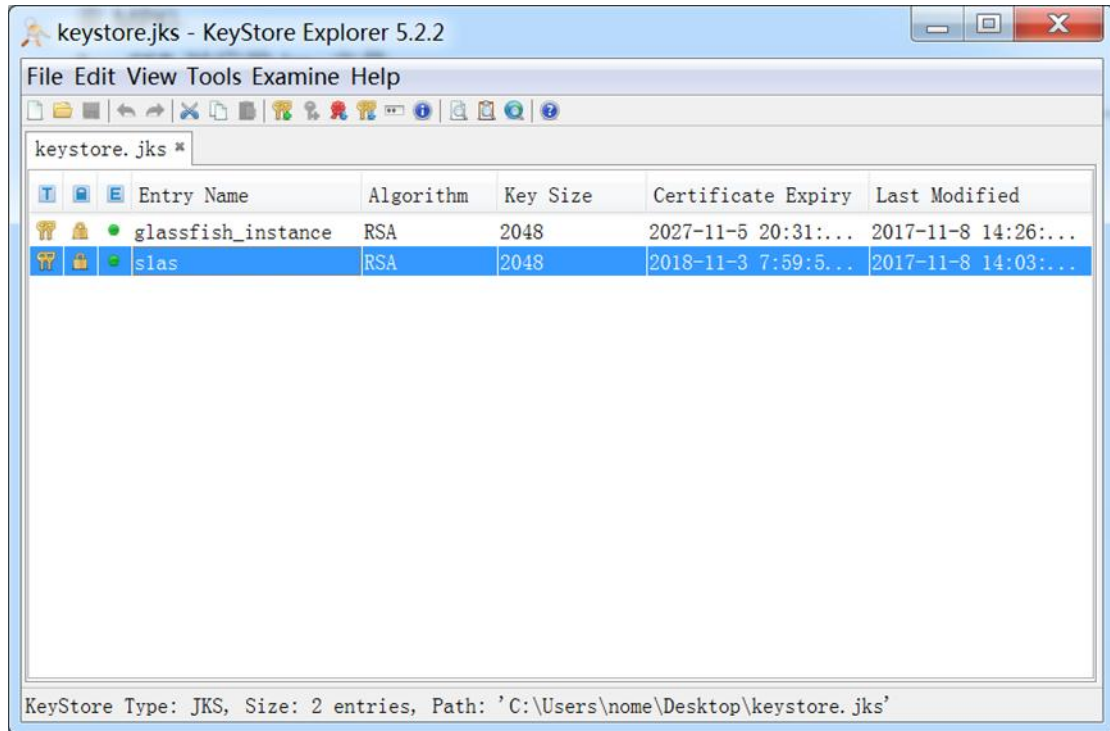
#### 准备 PFX 文件

使用下载的“xxxx.cn\_cert”证书文件和“xxxx.cn\_key”私钥文件（生成 CSR 请求与之同时生成的 key）通过 openssl 工具或在线工具生成一份 PFX 文件，请妥善保存好生成的 PFX 文件密码。

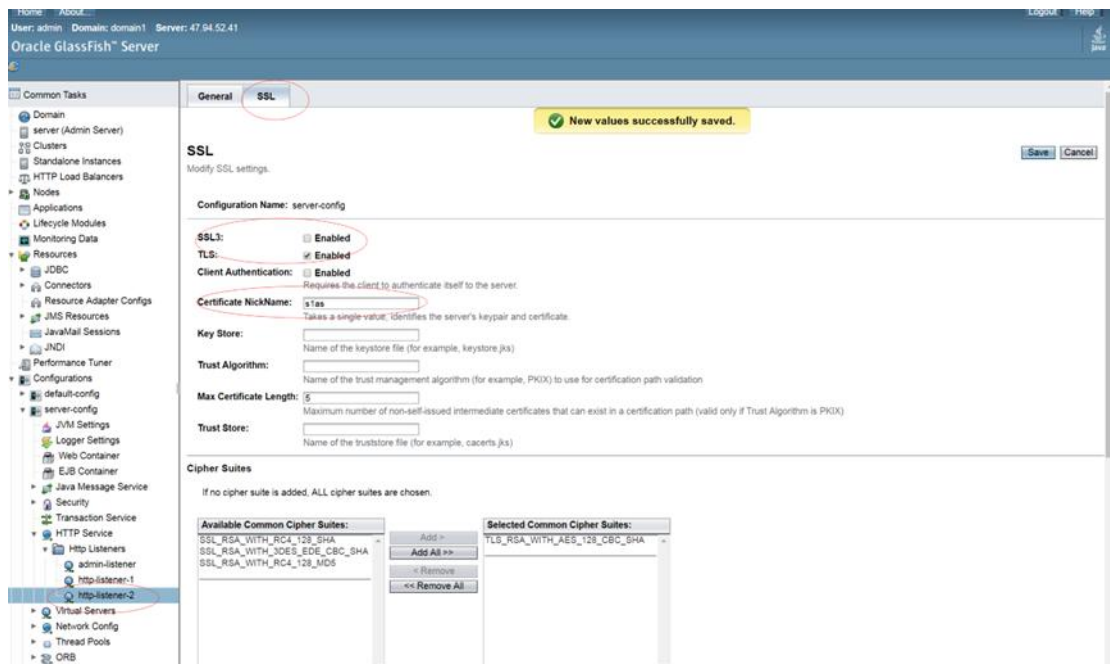
#### 操作步骤

1. 在 GlassFish 的“/domain”目录下 keystore 中，保留“glassfish-instance”并生成 jks 文件。

2.将上文中生成的 PFX 文件导入至 jks 中，重命名为：slas。如下图所示。



3.参考下图，在 GlassFish 的 web 页中进行配置。



4.关闭 SSLv3。按照下图修改 cipher\_suit。

<b>Available Common Cipher Suites:</b> SSL_RSA_WITH_RC4_128_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA SSL_RSA_WITH_RC4_128_MD5	Add > Add All >> < Remove << Remove All	<b>Selected Common Cipher Suites:</b> TLS_RSA_WITH_AES_128_CBC_SHA
<b>Available Ephemeral Diffie-Hellman Cipher Suites:</b> TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_RC4_128_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_NULL_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 TLS_DHE_DSS_WITH_AES_128_CBC_SHA SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	Add > Add All >> < Remove << Remove All	<b>Selected Ephemeral Diffie-Hellman Cipher Suites:</b> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
<b>Available 40 bit and 56 bit Cipher Suites:</b> SSL_RSA_WITH_DES_CBC_SHA SSL_DHE_RSA_WITH_DES_CBC_SHA SSL_DHE_DSS_WITH_DES_CBC_SHA SSL_RSA_EXPORT_WITH_RC4_40_MD5 SSL_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	Add > Add All >> < Remove << Remove All	<b>Selected 40 bit and 56 bit Cipher Suites:</b>
<b>Available ECC Cipher Suites:</b> TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDH_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_RC4_128_SHA TLS_ECDHE_RSA_WITH_RC4_128_SHA TLS_ECDH_ECDSA_WITH_RC4_128_SHA TLS_ECDH_RSA_WITH_RC4_128_SHA TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Add > Add All >> < Remove << Remove All	<b>Selected ECC Cipher Suites:</b> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

### 4.3.3.6 在 IIS 部署 SSL 证书

#### 前提条件

已在当前服务器中安装配置 IIS 服务。

说明：

- 由于服务器系统版本或服务器环境配置不同，在安装 SSL 证书过程中使用的命令或修改的配置文件信息可能会略有不同，证书管理服务提供的安装证书示例，仅供参考，请以您的实际情况为准。

- 部分服务端直接导入 IIS 可能会存在问题,所以本章节的操作步骤为:导入到 Microsoft 管理控制台 > 导入 IIS 服务端。

## 文件准备

在证书管理服务控制台的证书管理页选择您需要安装的证书, 选择“证书下载”。

在弹出的“证书下载”窗口中, 服务器类型选择 IIS, 单击“下载”并解压缩包至本地,

文件内包含下述 2 个文件:

PFX 证书密码: README.txt

PFX 格式证书: XXXX.cn.pfx

## 导入证书至系统

1.使用“Win + R”快捷键组合打开“运行”控制台, 输入“mmc”打开“Microsoft 控制台”。

2.单击右上角的“文件”选择“添加/删除管理单元”。



3.在“可用管理单元”中选择“证书”, 并单击“添加”。

4.在弹出的对话框中选择“计算机账户”, 单击“下一页”后再选择“本地计算机”, 单击“完成”将证书模块添加至控制台根节点中。

5.在“控制台根节点”中选择“证书 > 个人”, 在“对象类型”页面单击右键, 选择“所有任务 > 导入”。



6.选择“文件准备”章节中下载的 PFX 文件，单击“下一步”后选择“证书存储个人”完成证书导入。

7.调整证书链，将中级证书剪切到“中级证书颁发机构”下的“证书”中。

## 导入证书至 IIS

- 1.打开 IIS 服务管理器，选择计算机名称，双击打开“服务器证书”。
- 2.在服务器证书窗口的右侧“操作”栏中，单击“导入”。
- 3.在弹出的“导入证书”窗口中，选择证书文件存放路径，输入密码，单击“确定”。
- 4.选择网站下的站点名称，并单击右侧“操作”栏的“绑定”。



5.在“添加网站绑定”的窗口中，将网站类型设置为 https，IP 地址设置为全部未分配，端口设置为 443，主机名请填写您当前申请证书的域名，并指定对应的 SSL 证书，单击“确定”。

### 4.3.3.7 Nginx 部署 SSL 证书

#### 前提条件

已在当前服务器中安装配置 Nginx 服务。

已购买证书并且已获取到证书相关文件。

#### 安装前准备文件

在证书管理服务控制台的证书管理页选择您需要安装的证书，选择“证书下载”。

在弹出的“证书下载”窗口中，服务器类型选择 Nginx，单击“下载”并解压缩包至本地，文件内包含下述 2 个文件：

Cert 证书公钥：XXXX.cn\_cert\_chain.pem

私钥文件：XXXX.cn\_key.key

## 操作步骤

将已获取到的“XXXX.cn\_cert\_chain.pem”证书文件和“XXXX.cn\_key.key”私钥文件从本地目录复制到服务器的 Nginx 目录下。

编辑 nginx.exe 所在目录下的 conf\nginx.conf 文件。修改内容如下：

```
server {  
  
    listen        443 ssl;  
  
    server_name  qytest.zjrcbank.com; #这里是相当与是域名  
  
    ssl_certificate    /usr/nginxssl/server.crt; #证书文件  
  
    ssl_certificate_key  /usr/nginxssl/key.txt; #私钥文件  
  
  
    ssl_session_timeout 5m;  
  
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
  
    ssl_ciphers  
  
    ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;  
  
    ssl_prefer_server_ciphers on;  
  
  
  
    location / {  
        // 根据实际配置，和证书启用无关  
  
        #  
  
    }  
  
}
```

配置修改完成后，输入如下命令启用 Nginx：

```
start .\nginx.exe
```

### 4.3.3.8 TOMCAT 部署 SSL 证书

#### 前提条件

已在当前服务器中安装配置 Tomcat 服务。

已购买证书并且已获取到证书相关文件。

#### 安装前准备文件

在证书管理服务控制台的证书管理页选择您需要安装的证书，选择“证书下载”。

在弹出的“证书下载”窗口中，服务器类型选择 Tomcat，单击“下载”并解压缩包至本地，文件内包含下述 2 个文件：

JKS 证书：XXXX.cn.jks

JKS 证书密码：README.txt

JKS 证书密码：README.txt

#### 操作步骤

将已获取到的“XXX.cn.jks”密钥库文件拷贝至 Tomcat 安装目录/conf 目录下。

编辑/conf 目录下的“server.xml”配置。

```
<Connector
```

```
protocol="org.apache.coyote.http11.Http11NioProtocol"
```

```
port="8443" maxThreads="200"
```



```
scheme="https" secure="true" SSLEnabled="true"
```

```
keystoreFile="conf\domain.jks" keystorePass="pwd"
```

```
clientAuth="false" sslProtocol="TLS"/>
```

```
//
```

keystoreFile 指向步骤 1 保存的 jks 文件;

keystorePass 值为 jks 证书密码;

Port 是端口;

SSLEnable 是开启 ssl 的意思;

修改完成后, 重启 Tomcat 服务器即可。

### **(可选) HTTP 自动跳转 HTTPS 的安全配置**

1. 打开/conf 目录下的 “web.xml” 文件, 找到标签, 在后面插入如下内容

```
<security-constraint>
```

```
<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>
```

2.后续打开 “server.xml” 文件，修改 redirectPort 端口参数，如下所示：

```
<Connector port="8080" protocol="HTTP/1.1"
```

```
connectionTimeout="20000"
```

```
redirectPort="443" />
```

## 4.4 管理 SSL 证书

### 4.4.1 上传证书

证书管理服务支持您将线下的证书上传至控制台进行统一管理。

### 操作步骤

- 1.登录证书管理服务控制台。
- 2.在左侧导航栏选择“我的证书 > 上传证书”。
- 3.单击“上传证书”，在弹出的对话框中填写相关参数。
- 4.填写完成后，单击“确认”完成证书上传。

## 4.4.2 吊销证书

吊销证书指将已签发的证书从 CA 签发机构处注销。证书吊销后将失去加密效果，浏览器不再信任该证书。

如果您不再需要某张已签发的 SSL 证书或某张 SSL 证书密钥丢失或出于其他安全因素考虑，可以在证书管理控制台申请吊销证书。

### 前提条件

仅支持状态为“已签发”状态的证书吊销。

### 吊销证书操作步骤

吊销域名型（DV）证书

- 1.选待吊销的 DV 证书，在“操作”列中选择“更多” > “吊销”。
- 2.弹出证书吊销弹窗，确认待吊销的证书信息，确认无误后，单击“确认吊销”。
- 3.弹出二次确认弹窗提示，单击“继续吊销”。
- 4.配置域名吊销验证值，等待吊销。

5.待审核通过后，证书吊销成功。

#### **吊销企业型 (OV) 证书/增强型 (EV) 证书。**

1.选择待吊销的 OV/EV 证书，选择“操作”列的“更多” > “下载吊销函”，下载证书吊销函。

2.单击“更多” > “吊销”，进入吊销步骤。

3.在弹出“证书吊销”弹窗，在“导入吊销函”一行导入步骤 1 中下载的吊销函文件。

注意：

吊销函须确认信息无误并签字保存。

吊销函需要盖公司公章回传。

4.单击“确认吊销”按钮。

5.弹出二次确认弹窗，单击“继续吊销”按钮，完成证书吊销。

### **4.4.3 续订证书**

#### **证书续费说明**

续费的证书不支持修改证书的规格。

仅已签发成功的证书支持续费。

#### **续订证书操作步骤**

1.进入证书管理页，选择需要续订的 SSL 证书，单击“证书续订”。

2.跳转至证书续订页面，确认需要续费的证书规格，单击“立即购买”。

3.跳转至“证书续订页面”，确认订单详情无误后，单击“提交订单”。

4.确认订单详情，单击“立即支付”。

#### 4.4.4 删除证书

删除证书是指将 SSL 证书资源从天翼云证书管理服务控制台中删除。

##### 前提条件

已签发的证书无法删除。

##### 删除证书操作步骤

- 1.进入证书管理页面，找到“状态”为“已吊销”的证书，单击“删除”。
- 2.弹出二次确认弹窗，单击“确认”即可删除证书。

#### 4.4.5 查看证书详情

该任务指导用户查看已购买证书的详细信息。

您还可以参考本章节进行查看证书审核进度、修改证书名称和描述的操作，以及证书是否即将到期的提醒。

##### 查看证书详情

进入证书管理页，单击“更多” > “详情”，查看 SSL 证书详情。

##### 查看多年期证书的服务有效期

在您购买多年期证书后，可以在“证书管理”页的列表中查看多年期证书的服务期限。

“当前证书有效期”：指代目前已经申请成功并下发的证书有效期时间。

“服务有效期”：指代您购买的证书管理服务有效期。

“剩余续期次数”：证书申请后，可续期的次数。

“服务开始时间” & “服务结束时间”：多年期证书申请完成后，多年期证书管理服务的起始时间。

#### 4.4.6 证书检测

SSL 域名检测工具可以检测域名绑定的证书相关信息，方便您查看您的域名是否已经成功绑定相关证书。

##### 操作步骤

1. 登录证书管理服务控制台。
2. 在左侧导航栏选择“SSL 证书工具 > SSL 证书检测”。
3. 在下图红框处，输入需要查询的域名地址，例如：ctyun.cn。

说明：

端口号默认为 443，如果您部署证书的服务器端口号有差异，请您按照实际情况修改。

4. 填写完成后，单击“检测”即可查询域名绑定证书的相关信息。

# 5

## CSR 管理

### 5.1 创建 CSR

#### 什么是 CSR?

证书签名请求 (CSR) , 英文全称 Certificate Signing Request, 是一个包含网站、服务、国家、组织、域名、公钥和签名的编码文件, 用于从可信的证书颁发机构 (CA) 获取 SSL 证书。

#### 如何创建 CSR

- 1.单击“证书管理服务”, 选择“我的证书” > “CSR 管理”, 进入“CSR 管理”页面。
- 2.单击“创建 CSR”, 填写 CSR 信息, CSR 填写规则请见下表。

参数	参数说明
CSR 名称	填写您的 CSR 名称, CSR 名称仅支持大小写、数字、“.”、“_”、“-”, 长度为 2-15 个字符。
域名	请输入申请 SSL 证书的主域名, 例如: ctyun.cn。
其他域名	填写与已设置的域名共用一张证书的其他域名。支持填写多个域名。
联系人	选择 CSR 联系人, 创建联系人请参考 <a href="#">联系人管理</a> 章节。

参数	参数说明
公司	选择 CSR 所属的公司，创建公司请参考 <a href="#">公司管理</a> 章节。
密钥算法	选择密钥算法的类型。可选类型：  - RSA  - ECC  - SM2
密钥强度	选择密钥强度。可选强度：  - RSA 支持：2048、3072、4096  - ECC 支持：258、384、521  - SM2 支持：256

3.填写完成后，单击“生成 CSR”完成 CSR 创建。

## 5.2 上传 CSR

您可以在证书管理服务控制台上传您已有的证书签名请求（Certificate Signing Request, CSR），方便您在申请证书的时候可以在操作界面直接选择已经创建完成的 CSR。

### 操作步骤

- 1.点击菜单“证书管理服务”，选择“我的证书” > “CSR 管理”，进入“CSR 管理”页面。
- 2.单击“上传 CSR”。



### 3.填写上传信息。

参数	参数名称
CSR 名称	填写您的 CSR 名称，CSR 名称仅支持大小写、数字、“.”、“_”、“-”，长度为 2-15 个字符。
CSR 文件内容	填写您的 CSR 文件内容。 您可以使用文本编辑工具打开 CSR 文件，复制其中的内容并粘贴到该文本框，或者单击该文本框下的 <b>上传</b> 并选择存储在本地计算机的 CSR 文件，将文件内容上传到文本框。
私钥内容	填写您的 CSR 私钥。 您可以使用文本编辑工具打开 KEY 格式的证书私钥文件，复制其中的内容并粘贴到该文本框，或者单击该文本框下的 <b>上传</b> 并选择存储在本地计算机的证书私钥文件，将文件内容上传到文本框。

### 4.单击“确认”，完成 CSR 上传。

完成以上操作后，您可以在 CSR 列表查看已上传的 CSR。

## 后续操作

### 查看 CSR 详情

您可以通过查看 CSR 的详情，获取已创建或已上传的 CSR 的内容及私钥。

单击“操作”列的“详情”，查看右侧边弹窗展示 CSR 详情。

## 删除 CSR

如果您不再需要某个 CSR，可以将其删除。

注意：

如果您在申请 SSL 证书的时选择使用了某个 CSR，并且该证书待签发，请勿删除对应的 CSR，否则可能导致证书签发失败。CSR 删除后无法恢复，建议您谨慎操作。

选择待删除的 CSR，单击“操作”列的“删除”，二次确认弹窗点击“确认”，删除成功。

# 6 信息管理

---

通过本章，我们可以了解管理员的基本功能，以及给用户创建账号并授权的基本流程。管理员的基础功能包括“管理账号”、“管理资产”、“管理授权”以及“查看审计”。

## 6.1 联系人管理

在提交证书申请时，您需要配置证书联系人，以便 CA 机构审核人员能够与您联系，并进行后续证书申请的验证和审核。同时，该联系人还可用于接收证书业务提醒和技术支持沟通。

### 新建联系人

新建联系人支持以下两种方式：

方式一：在证书管理服务控制台的“信息管理 > 联系人”页面新建联系人。本章节以该方式为例，介绍新建联系人的具体步骤。

方式二：在提交证书申请时，在联系人下拉列表上方单击“新建联系人”，填写证书申请联系人的信息。

1.单击菜单“证书管理服务”，选择“信息管理” > “联系人”，进入“信息管理-联系人”页面。

2.单击“新建联系人”，填写联系人信息，填写内容请参考下表。

参数	参数说明
姓名	请输入证书联系人姓名。
邮箱地址	输入用于接收证书通知的邮箱地址，请确保邮箱地址真实有效。
手机号码	输入用于接收证书通知的手机号码，请确保手机号码真实有效。
身份证号（选填）	输入真实有效的身份证号，申请 OV 国密标准证书需要填写身份证号。

3.单击“确认”，完成创建。

### 编辑联系人信息

1.单击菜单“证书管理服务”，选择“信息管理” > “联系人”，进入“信息管理-联系人”页面。

2.选择待编辑的联系人，单击“操作”列的“编辑”，在弹出的对话框中修改联系人信息，完成信息修改。

## 删除联系人

说明：

若待删除的联系人信息已绑定签发成功的证书，删除后可能无法获取证书管理服务发送的相关通知，请谨慎操作。

- 1.单击菜单“证书管理服务”，选择“信息管理”>“联系人”，进入“信息管理-联系人”页面。
- 2.选择待删除的联系人，单击“操作”列的“删除”，在弹出的对话框中二次确认删除信息。

## 6.2 公司管理

在申请 OV 或 EV SSL 证书时，您需通过天翼云云证书管理服务控制台提交企业营业执照图片和公司相关信息，以便后续 CA 中心对证书申请者的真实性进行审核。

### 新建公司信息

天翼云证书管理服务支持以下两种添加公司信息的方法：

方式一：在证书管理服务控制台的“信息管理 > 公司”页面新建公司信息。本章节以该方式为例，介绍新建公司信息的具体步骤。

方式二：在提交 OV/EV 证书申请时，在“公司”下拉列表上方单击“新建公司”，并填写公司基本信息。使用该方式添加的公司信息将会自动保存在“公司”页面，方便您下次使用。

说明：

请您提供真实有效的公司信息，若公司信息填写有误会影响您企业型（OV）/增强型（EV）

证书的审核结果。

- 1.登录证书管理服务控制台。
- 2.在左侧导航栏选择“信息管理 > 公司”，进入“公司”页面。
- 3.单击页面上方的“新建公司”，按照下表的填写规则填写公司的相关信息。

参数	参数说明
公司类型	请您根据公司的性质，如实选择以下五种类型： <ul style="list-style-type: none"><li>- 私营个体</li><li>- 商业企业</li><li>- 政府实体</li><li>- 事业单位</li><li>- 非营利组织</li></ul>
公司名称	填写待申请证书的公司名称，请保证与营业执照上的公司名称一致。 您为 .gov 后缀的域名申请 OV 类型的证书，域名 WHOIS 注册人联系方式需与公司企业名称保持一致。
部门	输入待申请证书的公司部门。
公司电话	填写公司的联系方式，请保证联系方式真实有效。
组织机构	填写待申请证书公司的组织机构代码或统一社会信用代码。当公司位于海外地区时，您需要在组织机构代码开头添加国际域名缩写（又称“国际代号”）。


参数	参数说明
公司所在区域	填写待申请证书公司的所在地。
详细地址	填写公司的详细地址，请保证与营业执照上的地址一致。
邮政编码	填写公司所在地的邮政编码。
营业执照	上传公司营业执照，只支持 jpg/png 格式。

4.填写完成后，单击“确认”，完成公司新建。


### 后续操作

#### 编辑公司信息

若您需要修改已经纳管入证书管理服务控制台的公司信息，可在“公司”页签，单击需修改

信息的公司卡片上的  图标。在弹出的对话框中修改公司的相关信息，单击“确定”保存。

#### 删除公司信息

若您需要删除已经纳管入证书管理服务控制台的公司信息，可在“公司”页面，单击待删除信息的公司卡片上的  图标。在弹出的对话框中单击“确定”，完成公司信息删除。

# 7 常见问题

## 7.1 SSL 证书订购类

如何进行证书选型？

### 1. 如何选择证书类型

种类	应用场景	签发周期	说明	图示
域名型证书 (DV)	如果您的网站主体是个	1 个工作日	信任等级一般，只需验证域名的真实性便可颁发证书保护网站，签发证书速度最	

种类	应用场景	签发周期	说明	图示
	人  (即  没有  企业  营业  执  照),  只能  申请  域名  型  (D  V)  证  书。		快, 一般申请通  过验证后几分钟  即可获取到证  书。	



种类	应用场景	签发周期	说明	图示
企业型证书 (OV)	对于一般企业, 建议购买 OV 及以上类型的 SSL 证书。(若作为移动	1 ~ 3 个月	信任等级较高, 必须要验证域名权限以及企业的身份, 审核严格, 安全性高。	

种类	应用场景	签发周期	说明	图示
	端网站或接口调用,也建议您购买OV型及以上类型的SSL证书。)			

种类	应用场景	签发周期	说明	图示
增强型证书 (EV)	对于金融、支付类企业，建议购买EV型证书。	3~5个工作日	信任等级强，一般用于银行证券等金融机构、大中型企业等，审核更严格，安全性更高，同时在浏览器显示公司名称。	

说明：

DV 证书：没有经过 CA 机构审核审核，您只要能进行在控制台进行域名解析就可以获取 SSL 证书，缺点是只能进行 HTTPS 加密，适用于个人用户。

OV 证书：经过 CA 机构的组织信息审核后才会获取相应的 SSL 证书，此证书的优点是防止钓鱼劫持，提高组织的公信力。

## 2.如何选择支持域名数量?

种类	应用场景	说明
单域名	单个证书只支持绑定 1 个域名; 例如: 可以是 1 个主域名 ctyun.cn, 也可以是 1 个子域名 example.ctyun.cn, 均可以支持; 域名级数: 每一级域名长度的限制是 63 个字符, 域名总长度则不能超过 253 个字符。	单域名只支持保护申请的单个域名。
多域名	单个证书可以绑定多个域名; 例如: 可以是 ctyun.cn、ctyun.com、ctyun.com.cn、*.ctyun.cn; 最多可以支持域名数量 251 个以内。	多域名支持保护申请的多个域名。
通配符	单个证书支持绑定一个且只有一个泛域名; 例如: 可以申请一个*.ctyun.cn 泛域名, 泛域名只允许添加一个通配符, *.ctyun.cn 多个通配符的泛域名是不支持的;	通配符 SSL 证书可以同时保护一个域名下的所有的下一级子域名网站, 比如*.ctyun.cn, 对子域名网站保护是没有数量限制; 用户可以随时添加对应子域名网站使用 SSL, 而不需要额外购买证书。

说明:

多域名需至少购买 1 个主域名和 1 个附加单域名，主域名仅支持单域名，在此基础上可继续增加附加单域名或附加通配符。

### **SSL 证书购买后一直未使用，是否还可以使用？**

SSL 证书是否可以使用，取决于签发的 SSL 证书是否还在有效期，SSL 证书有效期内证书即可使用；

例如：

第一种情况：证书购买后，没有完成域名验证/组织验证，一直未签发证书的订单，需要使用的时候再继续完成验证，签发证书下载使用即可，证书有效期自签发之日开始计算。

第二种情况：证书购买后，已经完成验证，证书已签发；已签发证书可以在证书有效期内随时开始使用。

### **SSL 证书购买后，可以修改证书类型、域名类型等信息吗？**

不可以。SSL 证书购买后，无法更改证书类型，域名类型以及其他 SSL 证书信息。

## **7.2 SSL 证书申请类**

### **第一次申请 SSL 证书不会操作怎么办？**

SSL 证书申请过程中如有疑问可直接[提交工单](#)。

### **申请 SSL 证书时应该使用哪个域名？**

在申请 SSL 证书时，应该按照需求使用需要建立 https 加密的域名作为申请的域名。通常，一般是您网站的主要访问域名，即用户通过该域名访问您的网站。以下是一些指导原则来确定您应该使用的域名：

**主要域名:**使用您网站的主要域名作为申请的域名是最常见的做法。这是用户最常用的域名,用于访问您的网站的主要内容。

**常用子域名:**如果您的网站使用了一些常用的子域名,例如 "www"、"blog" 或 "shop",您也可以将这些子域名包括在证书申请中。这样,您可以确保这些常用的子域名也得到了加密和认证。

重要的是要确保您选择的域名在证书申请过程中是准确的和一致的。证书颁发机构将验证您对于所申请的域名的控制权,因此提供准确的域名信息是非常重要的。

### 主域名绑定后,是否可以修改?

证书未签发时可至证书管理服务后台进行域名修改,操作步骤如下:

证书名称	算法	状态	标签	绑定域名	有效期限	操作
国际 域名型 (DV) SSL 资源 ID: .....	RSA	待申请	<input type="text"/>	<input type="text" value="test.cn"/>	1年 2024-02-22 14:5 4:39	<a href="#">证书申请</a> <a href="#">详情</a>

### 证书申请 ✕

证书绑定域名 !

\* 域名验证方式

\* 联系人 新建联系人 | 管理联系人

\* 所在地

密钥算法

RSA  ECC  SM2

CSR生成方式

系统生成  手动生成 ?

SSL 证书签发后, SSL 证书签发给的主域名以及其他域名信息都无法修改; 修改 SSL 证书域名需要重新下单, 重新操作 SSL 证书申请签发流程。

## 7.3 SSL 证书验证类

### 证书支持哪些域名验证方式？

域名验证主要通过 DNS 和文件进行验证。单域名证书支持 DNS 验证、文件验证；通配符证书支持 DNS 验证；多域名证书支持 DNS 验证、文件验证。

#### 1. DNS 验证

DNS 验证目前支持 CNAME 解析记录。

实际的操作步骤大同小异，只是在选择记录类型的时候会有所区别。

#### CNAME 解析记录

待用户申请证书后，CA 会返回一串域名验证信息，用户需要根据这串信息到域名解析平台，新增一条解析记录。域名验证信息里面包含了所需要添加的验证内容：主机记录、记录类型、记录值。验证信息里未提到的参数，都保持平台默认即可。

例如：域名 ctyun.cn

验证方式：DNS\_CNAME

CNAME 记录名：2E8305A4DC5CB1263F0B52F18401F8DD.ctyun.cn;

CNAME                    记                    录                    值                    :

700CB5A097F1AF88A1F3CC2D564DFBEC.79AC76780B8CB074F144E4A2BBF1C8A6.

TTDsgCssza.trust-provider.com

#### 2. 文件验证

待用户申请证书后，CA 会返回一串域名验证信息，用户需要根据这串信息到域名应用服务器上，新建一个 TXT 验证文本。域名验证信息里面包含了验证文本的内容以及文本的路径。

例如：



请参照以下的信息进行域名验证配置:

验证方式: 文件验证

验证域: ctyun.cn

文 件 验 证 路 径 : http(s):// ctyun.cn  
/.well-known/pki-validation/DE711C8B63E558F1A2AD8462C2D3F5E2.txt

文 件 验 证 内 容 :  
03763B47C99A2AB850007B69896A73A46F6AAE9ED8ECD952653DE6337091D8A6  
ctyun.cn

cmcdtcqwjfpwpj

CA 需要用户按照该验证信息新建完验证文本后, 访问路径, 成功返回验证值才算验证成功

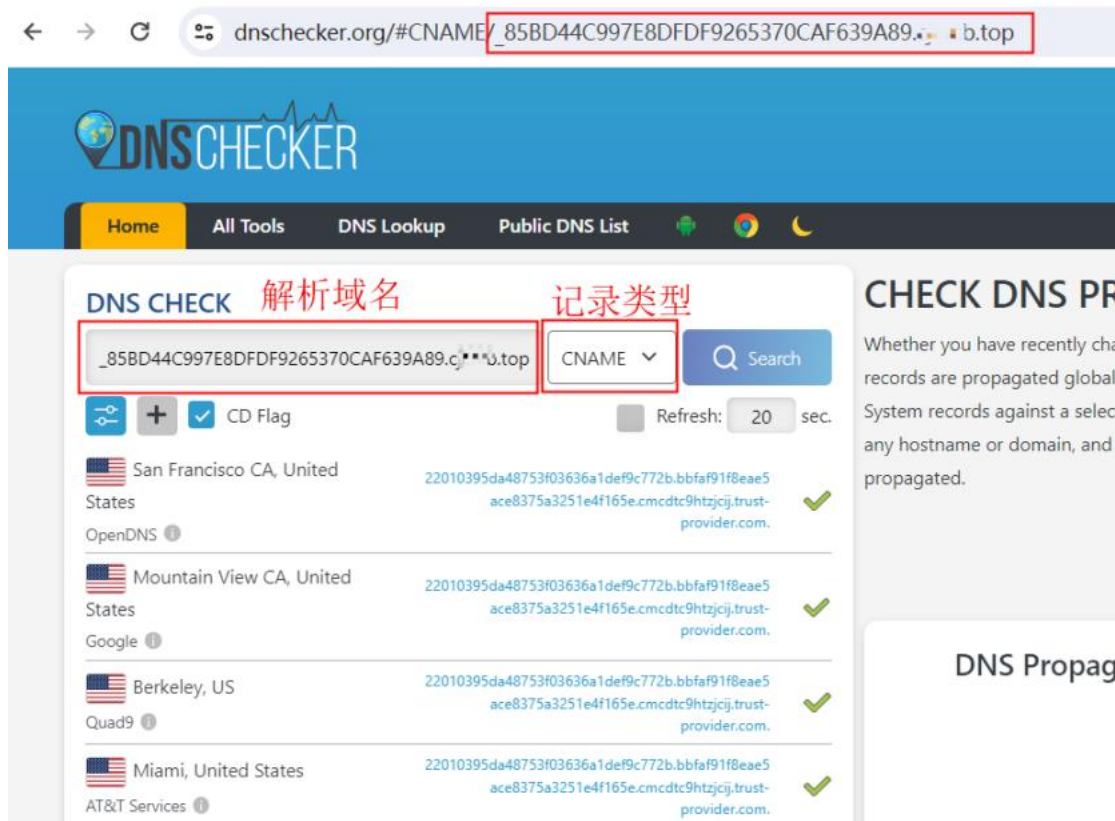
验 证 路 径 : http(s):// ctyun.cn  
/.well-known/pki-validation/DE711C8B63E558F1A2AD8462C2D3F5E2.txt

验 证 值 :  
03763B47C99A2AB850007B69896A73A46F6AAE9ED8ECD952653DE6337091D8A6  
ctyun.cn

cmcdtcqwjfpwpj

### 如何查看域名验证是否生效?

可自行检测域名验证添加的解析是否生效 (文件验证方式则自行访问文件, 看是否能访问到验证文件), 若解析添加通过, 待 CA 验证即可通过域名验证。您可自行查询[解析生效工具](#)。



The screenshot shows the DNS Checker website interface. The search bar contains the domain name `_85BD44C997E8DFDF9265370CAF639A89.cname.b.top`. The record type is set to `CNAME`. The search results show four DNS providers: San Francisco CA, United States; Mountain View CA, United States; Berkeley, US; and Miami, United States. Each provider has a green checkmark indicating that the record is propagated.

Location	IP Address	Status
San Francisco CA, United States	22010395da48753f03636a1def9c772b.bbfaf91f8eae5ace8375a3251e4f165e.cmc9htzjci.trust-provider.com	✓
Mountain View CA, United States	22010395da48753f03636a1def9c772b.bbfaf91f8eae5ace8375a3251e4f165e.cmc9htzjci.trust-provider.com	✓
Berkeley, US	22010395da48753f03636a1def9c772b.bbfaf91f8eae5ace8375a3251e4f165e.cmc9htzjci.trust-provider.com	✓
Miami, United States	22010395da48753f03636a1def9c772b.bbfaf91f8eae5ace8375a3251e4f165e.cmc9htzjci.trust-provider.com	✓

## Windows 系统如何验证 DNS 解析生效?

要验证 Windows 系统中的 DNS 解析是否生效，您可以尝试以下方法：

使用命令提示符（Command Prompt）进行验证：

打开命令提示符。您可以按下 Win + R 键，然后输入 "cmd" 并按下 Enter 键，或者在开始菜单中搜索 "命令提示符" 并打开它。

在命令提示符中，输入以下命令并按下 Enter 键：

```
nslookup -q=cname _DCB4B034115D8FB7F9C9584963F17E0C.baihu2.com
```

## 如何查询域名管理员邮箱并进行验证?

邮箱验证方式：需要是 CA 返回的邮箱来选择，可以在订单中获取到 CA 返回的可选邮箱，

不支持自行指定邮箱来验证。

邮箱验证：待用户进入域名验证环节，CA 会向域名管理邮箱发送一封确认邮件，用户登录对应的管理邮箱，点击其中的确认按钮即可完成验证。域名管理邮箱地址是 CA 指定的，无法自定义。如无法提供，则只能使用另外两种验证方式。

域名管理邮箱包括：

注册域名时填写的邮箱地址（以 CA 返回的为准）

admin@chiantelecom.com

administrator@chiantelecom.com

postmaster@chiantelecom.com

hostmaster@chiantelecom.com

webmaster@chiantelecom.com

### **域名不在天翼云平台管理，如何进行 DNS 验证？**

需要用户登录到待验证域名的域名服务商的域名解析管理平台（申请证书的域名在哪里注册购买的），在对应域名下按照获取的 TXT 验证信息，新建添加一条 TXT 类型的解析记录，具体添加方式以平台具体要求为准，或者修改其他可用验证方式。

### **DV 证书 DNS 验证失败该如何处理？**

若客户添加解析操作导致的失败，可重新添加解析或更换其他可用验证方式；

若由于域名解析平台规则限制原因导致的失败，需联系域名服务商处理。

### **哪些场景企业型（OV）和增强型（EV）证书不需要确认函？**

- 如果您申请证书时填写邮箱企业邮箱与企业域名相关（例如申请的域名为\*.ctyun.com，

企业邮箱为\*@chinatelecom.com) , 并且该企业邮箱可以正常收发外部邮件, 这种情形下可以不提供确认函。

- 企业发送工商登记年报的邮箱若可以正常收发外部邮件, 使用该邮箱申请证书时可以不提供确认函。

- 非以上场景申请企业型 (OV) 和增强型 (EV) 证书必须提供确认函, 建议使用 189、126、163、QQ 等免费邮箱。

## 7.4 SSL 证书审核类

### 证书签发失败有哪些常见原因?

#### 1.当前域名存在 CAA 解析记录

问题现象:

域名管理员设置了 CAA 解析记录来授权指定的 CA 机构为其颁发 SSL 证书, CA 机构在颁发 SSL 证书时会检测域名 CAA 记录, 如果发现未获得授权, 将拒绝为该域名颁发 SSL 证书。

解决办法:

域名管理员前往域名解析平台将 CAA 解析记录删除或将证书 CA 机构名称加入 CAA 解析记录, 操作完成后等待 CA 重新验证。

#### 2.文件验证, 域名站点未支持境外访问

问题现象:

申请证书对应的域名的网站限制海外访问, 由于国际证书的 CA 审核机构基本是海外机构, CA 机构无法进行文件验证扫描审核, 导致证书签发失败。

解决办法:

请确保 Web 网站端口号设置为 80 或 443，所有地区均能匹配到验证值。如应用服务器限制境外访问，需要将 CA 机构的 IP 加入访问白名单，证书颁发完成或域名信息审核通过后，即可还原访问策略以及删除验证文件。

### 3.证书申请涉及高风险，已进行人工复核

问题现象：

您申请的证书未通过证书的签发机构风控系统检测，可能原因：绑定的域名疑似涉及行业品牌、行业商标、违禁词等风控敏感词。所以该证书进入人工复审阶段。

解决办法：

耐心等待人工复审结果，如未审核通过，可更换域名重新申请。如无法更换域名可选购企业型（OV）、增强型（EV）证书，OV/EV 证书会进行企业信息审核，审核通过后即可正常签发证书。

### SSL 证书审核需要多久时间？

SSL 证书审核时间取决于申请的证书类型。

DV 证书：完成域名验证后，立即签发（1 天内）；

OV 证书：确认好组织验证方式，提交审核后 3-5 个工作日审核时间 期间需要配合完成组织和域名验证；

EV 证书：确认好组织验证方式，提交审核后 3-5 个工作日审核时间 期间需要配合完成组织和域名验证。

### 为什么证书验证状态长时间停留在审核中？

域名验证/组织审核未完成前，订单会处于审核中，组织审核问题会有对应交付人员跟进处理，请您耐心等待。

### **SSL 证书提交申请后需要做什么？**

DV 证书需要及时去完成域名验证，即可签发证书；OV/EV 证书需要配合交付人员先完成组织审核。

### **收到 CA 机构的邮件或电话如何处理？**

电话方式：接到审核电话所有问题如实回答即可。

邮箱方式：收到组织验证邮件后，按照邮件提示操作。

### **新购买的 SSL 证书是否需要重新审核？**

需要，购买 SSL 证书都需要完成域名验证/组织审核。

### **域名未通过安全审核该怎么办？**

问题现象：

有的域名由于命中 CA 的品牌高风险保护，则会无法通过安全审核。

解决办法：

通过 400 热线反馈给 CA，等 CA 人工审核结果，若还是无法通过择无法签发证书，需要换域名申请或签发自签发证书。

## 7.5 SSL 证书下载类

### 已签发的 SSL 证书可以多次下载并使用吗？

支持，证书不限制下载次数以及部署次数。

### 如何获取 SSL 证书私钥文件 server.key？

系统生成的 CSR，对应产生的 key 私钥文件会加密存储在云端，直接从订单中下载；

手动生成 CSR，对应产生的 key 私钥文件会保存在生成 CSR 的账号中，需要自行保存好 key

私钥文件；若 key 文件丢失，则提交 CSR 后签发的证书公钥无法找到匹配私钥文件去部署；

需要重新生成 CSR 申请证书。

## 7.6 SSL 证书吊销类

### 吊销证书和删除证书的区别是什么？

吊销证书操作：吊销后该证书即为无效，不可继续使用；

删除证书操作：可以从证书平台重新下载证书使用（删除证书，只要确保没有证书私钥泄露

风险，重新下载证书即可）。

### 提交了吊销或删除证书的申请，是否可以取消？

不可以。

吊销申请提交后或删除证书的操作执行后，将无法取消，请谨慎操作。

证书吊销指将已签发的证书从 CA 签发机构处注销。证书吊销后将失去加密效果，浏览器不

再信任该证书。

提交吊销申请后，将由 CA 机构审核，审核通过后，吊销操作才算完成。

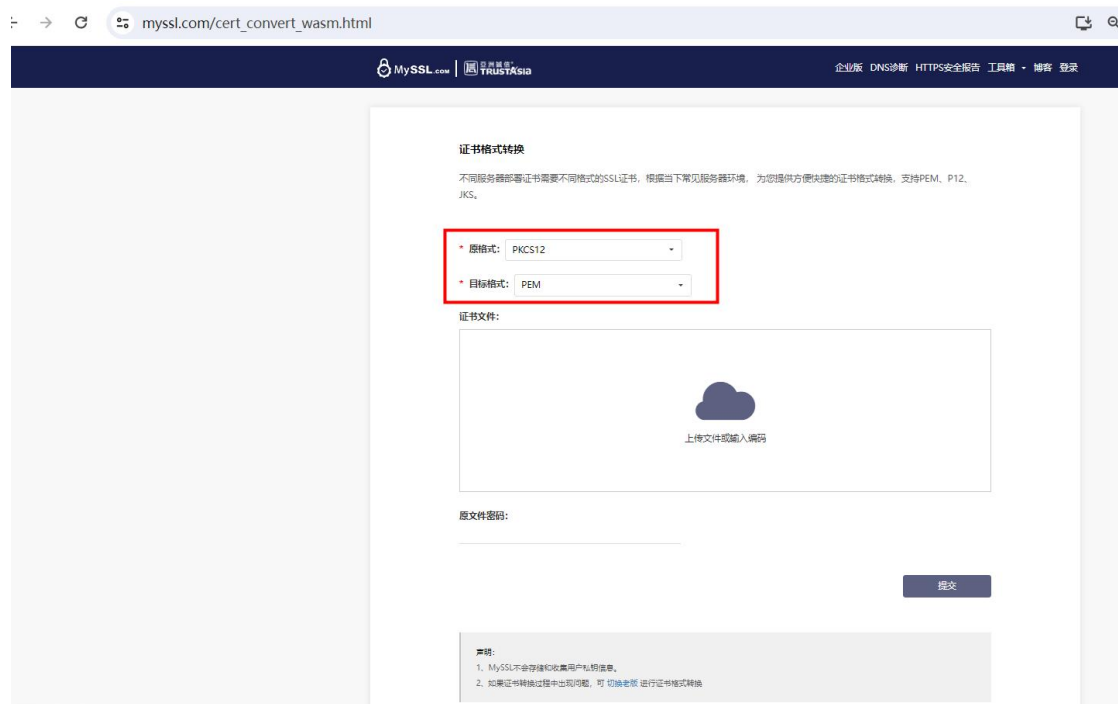
因为吊销过程中无需用户执行任何操作，且 CA 机构审核流程较快，所以，提交吊销申请后，将无法取消，请谨慎操作。

证书删除指将证书资源从天翼云系统中删除。证书仍然有效，浏览器信任该证书。

提交删除操作后，天翼云将直接执行删除操作，无需 CA 机构审核，将立即被删除。因此，执行删除操作后，将无法取消，请谨慎操作。

## 如何将证书格式转换为 PEM 格式？

默认下载或者邮件中获取的证书就是 PEM 格式，或者可以使用[证书格式转换工具](#)。



## SSL 证书为什么没有在证书列表中显示？

证书管理服务产品控制台的证书列表会展示直接通过天翼云购买的证书。

## 吊销证书需要多长时间



需要看客户完成吊销验证的时间，一般验证完的 3~6 个小时内即可吊销完成；建议客户不需要证书的情况下，先停用/替换对应需要吊销的证书，再发起吊销，避免证书吊销后影响使用。

### **内网域名可以申请 SSL 证书吗？**

内网域名或私有 IP 不能申请公网数字证书。

## **7.7 SSL 证书有效期类**

### **SSL 证书过期了怎么办？**

SSL 证书存在有效期限限制。证书过期之后，将无法继续使用，您需要在证书到期前进行续费。

### **SSL 证书的有效期限是多久？**

全球所有 CA 机构在 2020 年 8 月 27 日之后，不允许再发出一年以上有效期的证书，主流浏览器也不再信任 1 年期以上证书。因此 SSL 证书的有效期限为 1 年，即证书在审核通过之后的 1 年内有效，到期后将无法继续使用。

若您购买了天翼云的 2~3 年期证书管理服务，那么在证书到期前 30 天天翼云技术支持会主动联系您提前准备下一个周期的证书审核内容，以保证您 SSL 证书验证的连续性。

### **SSL 证书即将到期，该如何处理？**

证书到期前，提前 30 天下单并申请新证书，并重新部署证书至您的 Web 服务器（或者部署到天翼云产品），替换即将过期的旧证书。

### **SSL 证书购买后多久生效?**

证书购买后，请及时配合完成域名验证/组织审核。完成验证后，证书签发有效期从签发之日起开始计算；可直接下载部署使用。

### **新旧 SSL 证书有效期说明**

手动续费过程中新旧证书有效期分别计算。新签发证书不影响之前旧证书，旧证书到期前均可使用，两张证书均可使用。

### **新旧 SSL 证书替换对业务有影响吗?**

新证书签发后建议尽快下载更新部署，替换旧证书文件配置（建议在旧证书过期前，合理安排更新时间，防止影响网站访问或业务使用）。

### **SSL 证书是一次性产品，到期后如何申请?**

SSL 证书是一次性产品，且存在有效期限限制。证书到期后将无法继续使用。如需继续使用证书，您可以在证书到期前进行续费。

### **SSL 证书到期未更新新证书，会影响业务吗?**

SSL 证书到期了，如果后续不再进行使用，则无需再次购买，不会影响业务。

另外，需要注意的是，如果 SSL 证书过期且未及时更新，用户访问网站时会显示“网站的安全证书已过期”的告警信息。黑客等不法分子可以利用过期的 SSL 证书，篡改或窃取浏览器和服务器之间传输的信息和数据，从而影响用户的数据安全。

当浏览器用户发现网站服务器证书过期，会对该网站不信任，从而为企业的品牌形象带来负面的影响。网站服务器过期后，用户可能会为了避免出现个人损失，而选择停止访问该网站。

### 购买证书后未立即申请，订单多久后会失效？

您购买 SSL 证书后若未申请证书，订单将一直保留，不会失效，您在需要使用时申请即可。

### 如何查询证书还有多久到期？

- 1.登录证书服务管理控制台。
- 2.在左侧导航栏选择“我的证书 > 证书管理”，进入证书管理页面。
- 3.在待查询证书的“当前有效期限”列，查看证书的到期时间。

### 如何查询证书管理服务还有多久到期？

- 1.登录证书服务管理控制台。
- 2.在左侧导航栏选择“我的证书 > 证书管理”，进入证书管理页面。
- 3.在待查询证书的各列，查看证书的到期时间。

“当前证书有效期”：指代目前已经申请成功并下发的证书有效期时间。

“服务有效期”：指代您购买的证书管理服务有效期。

“剩余续期次数”：证书申请后，可续期的次数。

## 7.8 SSL 证书部署类

### SSL 证书对服务器端口是否有限制？

证书签发前：证书签发前的域名验证阶段，如使用的是文件验证，必须通过 http 80 端口 /https 443 端口 来完成文件验证。

证书签发后：部署证书阶段对服务器端口没有限制，证书只匹配域名，不限制端口。

注意

证书部署在 https 443 的默认端口，则 https://example.com 直接访问；部署在非 443 默认端口比如 8443 端口，则需要通过 https://example.com: 8443 域名加端口的形式去访问

### **SSL 证书支持在哪些服务器上部署？**

SSL 证书不限制部署环境，只要对应 web 服务器运行的中间件支持 ssl 模块来部署证书即可。

说明：

常见的部署环境比如：支持在云防护平台、WAF、VPN、F5 等设备上使用该证书，支持包括 Apache、Nginx、IIS、Tomcat 等主流 web 服务器

### **SSL 证书支持在哪些地域部署？**

证书签发后会获取一对证书公私钥文件，只要部署环境的域名与证书域名一致，即可使用。

### **服务器 IP 地址变更后，原 SSL 证书是否仍可用？**

如果申请的是域名证书，只要部署的域名匹配，域名解析的 IP 更改不会影响证书，可以继续使用；

如果申请的是 IP 证书，部署的 IP 更改，证书 IP 和部署 IP 不一致，证书不匹配不可以继续使用。

### **浏览器提示 SSL 证书不可信怎么办？**

导致浏览器提示 ssl 证书不可信/不安全的原因是多样的，简单的原因有以下几种：

访问到的证书是否与访问的域名一致，若不一致一般是部署的证书不匹配，重新部署对应匹配域名证书即可。

服务端部署的证书不完整，缺乏中间证书链，重新部署完整证书即可。

客户若自行无法判断原因，可反馈至技术支持排查处理。

### **部署了 SSL 证书后，为什么通过域名无法访问网站？**

导致域名无法访问的原因是多样的，如端口问题/域名解析问题/证书部署问题。若客户自行无法判断原因，可反馈至技术支持排查处理。

### **为什么安装了 SSL 证书后，https 访问速度变慢了？**

安装 SSL 证书后，HTTPS 访问速度变慢可能是由以下几个原因引起的：

**加密和解密过程：**SSL 证书用于加密在网络中传输的数据，以确保安全性。加密和解密数据的过程需要计算资源和时间，因此会对访问速度产生一定的影响。尤其是在服务器端，需要对大量的数据进行加密和解密操作，可能导致响应时间延长。

**握手过程：**在建立 HTTPS 连接时，客户端和服务器之间需要进行 SSL 握手过程，以协商加密算法和密钥等信息。这个握手过程会增加连接建立的时间和网络延迟，从而影响访问速度。

**证书验证：**在建立 HTTPS 连接时，客户端需要验证服务器端的 SSL 证书的合法性。这涉及到证书链的验证、OCSP 状态、证书吊销列表（CRL）的检查等操作，这些额外的验证步骤可能会增加连接建立的时间。

响应大小增加: SSL 加密会使数据包的大小增加。加密后的数据包通常会比明文数据包更大, 这意味着在网络上传输需要更多的带宽和时间。

服务器处理负载增加: 由于 SSL 加密需要计算资源, 服务器在处理大量 HTTPS 请求时可能会承受更大的负载。如果服务器的计算能力有限或配置不当, 可能导致 HTTPS 访问速度变慢。

但整个 tls 握手、获取 ocsp 状态所耗时间可以忽略不计。

如果您说的访问速度过慢, 可以排查下是否其他因素, 如服务器资源加载以及网络原因。

### **SSL 证书部署后, 浏览器是否会弹出不安全提示?**

正确部署 SSL 证书后, 不会弹出不安全提示。

## **7.9 其他 SSL 证书问题**

### **公钥、私钥、SSL 证书的关系是什么?**

公钥 (Public Key) : 公钥是密钥对中的一部分。它是用于加密和验证数据的非机密密钥, 可以公开共享给其他人。使用公钥加密的数据只能使用与之配对的私钥进行解密。在加密通信中, 公钥用于加密数据, 以确保只有持有相应私钥的人才能解密和访问数据。

私钥 (Private Key) : 私钥是密钥对中的另一部分, 与公钥配对。私钥是保密的, 只有密钥的所有者可以访问和使用。私钥用于解密使用公钥加密的数据, 以及对数据进行签名。私钥应当妥善保管, 不应该暴露给他人。

SSL 证书 (SSL Certificate) : SSL 证书是由数字证书颁发机构 (CA) 签发的包含公钥和

其他相关信息的数字文件。SSL 证书用于建立安全的 HTTPS 连接，验证服务器的真实性，并对通信进行加密。证书中的公钥用于加密会话密钥，确保只有服务器的私钥才能解密它。证书还包含有关证书所有者（例如域名所有者）和证书颁发机构的信息。

综上，SSL 证书包含了公钥，它与私钥配对。公钥用于加密数据和建立安全连接，私钥用于解密数据和进行数字签名。通过 SSL 证书，服务器可以向客户端证明其身份，并确保通信的机密性和完整性。

### **数字证书通常有哪些格式？**

数字证书通常有以下几种常见的格式：

**X.509 证书格式：**X.509 是一种常见的数字证书标准，定义了证书的结构和内容。X.509 证书通常使用基于 ASN.1（Abstract Syntax Notation One）的 DER（Distinguished Encoding Rules）编码格式进行存储和传输。这种格式的证书经常用于 SSL/TLS 证书、代码签名证书和数字身份证书等。

**PEM 格式：**PEM（Privacy-Enhanced Mail）是一种常见的用于存储和传输 X.509 证书以及相关私钥的格式。PEM 格式使用 Base64 编码将证书和私钥转换为文本文件，并使用 "-----BEGIN CERTIFICATE-----" 和 "-----END CERTIFICATE-----" 等标识符来标记证书的起始和结束。

**PKCS#12 格式：**PKCS#12（Public-Key Cryptography Standards #12）是一种常见的证

书格式，用于存储和传输 X.509 证书、相关私钥和其他关联的证书链和密码信息。PKCS#12 格式的文件通常具有.pfx 或.p12 文件扩展名，可以包含公钥证书、私钥以及可选的密码保护。

JKS 格式：JKS (Java KeyStore) 是 Java 平台上常用的证书存储格式。它是一种二进制格式，用于存储 X.509 证书、私钥和可选的密码保护。JKS 格式的文件通常具有.jks 文件扩展名。

这些是常见的数字证书格式，用于存储和传输 X.509 证书及其相关信息。每种格式都具有不同的特点和适用性，取决于使用的平台、工具和应用程序。（以上格式后缀证书，天翼云均可以提供）

### **SSL 证书中包含哪些信息？**

SSL 证书中包含以下重要信息（以 EV 证书为例）：

证书颁发机构（CA）信息：证书中包含颁发该证书的 CA 的信息，包括 CA 的名称、数字签名和公钥等。这些信息用于验证证书的合法性和真实性。

证书序列号：每个证书都有一个唯一的序列号，用于标识和跟踪证书的唯一性。

证书使用者信息：证书中包含了证书所有者的信息，通常是域名所有者的信息。这些信息可能包括组织名称、组织单位、国家/地区、州/省、城市、电子邮件地址等。



证书有效期：证书中包含了证书的有效期限，即证书的开始日期和结束日期。证书在有效期内才被认为是有效的。

支持的加密算法和密钥长度：证书中包含加密算法和密钥长度等信息。

### **SSL 证书可以跨区域、跨帐号或跨平台使用吗？**

证书签发后会获取一对证书公私钥文件，只要部署环境的域名与证书域名一致，即可使用；

SSL 证书不限制使用地区、帐号、平台以及部署次数。

### **SSL 证书与域名的关系？**

单张 SSL 证书能够绑定几个域名？

单张 ssl 证书绑定域名数量与证书域名类型有关；

单域名证书就支持 1 个域名。

### **单个域名能绑定几张 SSL 证书？**

同一个域名支持申请多张证书，看客户需求，没有限制。

### **通配符证书支持哪些域名？**

通配符证书支持一个主域名及其所有的子域名。它使用通配符字符 "\*" 来表示子域名的部分，从而允许在一个证书中保护多个子域名。通配符字符 "\*" 只能出现在证书的最左边的子域名部分，例如 "\*.ctyun.cn"。

以下是一些泛域名证书可以支持的示例域名：

ctyun.cn

blog.ctyun.cn

shop.ctyun.cn

mail.ctyun.cn

api.ctyun.cn

app.ctyun.cn

在上述示例中，泛域名证书 "\*.ctyun.cn" 可以用于保护所有以 ".ctyun.cn" 结尾的子域名，包括 "blog.ctyun.cn"、"shop.ctyun.cn" 等等。然而，它不能用于保护其他顶级域名，如 "ctyun.net" 或 "ctyun.org"。

### **系统生成的 CSR 和自己生成 CSR 的区别？**

系统生成的 CSR，对应产生的 key 私钥文件会加密存储在云端，key 不易丢失，方便下载；自己生成 CSR，对应产生的 key 私钥文件会保存在生成 CSR 的人手中，需要自行保存好 key 私钥文件；若 key 文件丢失，则提交 CSR 后签发的证书公钥无法找到匹配私钥文件去部署；需要重新生成 CSR 申请证书。