证书管理服务

目录

产品公告

【产品公告】关于SSL证书有效期政策变更的重要通知

尊敬的天翼云用户：

您好！

为确保您的SSL证书持续符合行业安全规范，我们特此通知一项由全球证书颁发机构与浏览器论坛（CA/B Forum）制定的重要政策变更。

变更背景

根据CA/B论坛最新投票决议（SC-081），自2026年3月15日起，所有公开信任的SSL/TLS证书最长有效期将缩短至200天；

有效期具体时间如下：

- 自2026年3月15日起证书的最长有效期 200 天；
- 自2027年3月15日起证书的最长有效期 100 天；
- 自2029年3月15日起证书的最长有效期 47 天。

此项变更是全球范围内提升网络安全的重要举措，极大地降低了私钥在签发前泄露的风险，从而加强了数字证书作为互联网信任基石的安全性。

影响范围

证书版本	加密标准	有效期
Secursite、Geotrust、TrustAsia	国际标准	2026年2月24日~2027年3月15日签发的证书，有效期最长为200天。
标准版	国际标准	2026年3月1日~2027年3月15日签发的证书，有效期最长为200天。
CFCA	国际标准	2026年3月14日~2027年3月15日签发的证书，有效期最长为200天。
Globalsign	国际标准	2026年3月15日~2027年3月15日签发的证书，有效期最长为200天。
Secursite、Geotrust、TrustAsia、标准版、CFCA、Globalsign	国际标准	2027年3月15日之后签发的证书，有效期最长为100天。

说明

- 国密算法证书：标准版、CFCA、TrustAisa品牌国密算法SM2证书，有效期不变，暂不受该政策影响。
- 私有（内网）证书：有效期不变，暂不受该政策影响。
- 测试证书：免费的测试证书有效期依然为3个月，暂不受该政策影响。

天翼云应对方案

为保障您的服务连续性，我们将采取以下措施：

- 服务承诺不变，在2026年3月15日之前购买SSL证书服务权益不受影响：
  - 在2026年3月15日前购买且在2026年3月15日后签发的证书，签发多张连续有效期的证书（如：1年期内签发2张有效期最长为200天的证书），确保您在购买的有效期内证书可用。
  - 请注意查收证书到期提醒邮件，您也可以登录证书管理控制台，进入“信息管理 > 消息管理”配置短信提醒。
- 您需要配合的操作：
  - 手动验证域名的证书：域名验证频率将提高（约6个月验证一次），您需及时 验证域名 。

    注意

    首张证书到期后，系统将自动计算后续证书的有效期。若因未及时验证域名导致证书未签发，后续证书的有效期不会被延长。

    例如：

    首张证书有效期：2026年3月16日-2026年9月16日；第二张证书计划有效期：2026年9月16日-2027年3月16日；若在第二张证书的计划有效期内完成验证，证书将正常签发，有效期截止至2027年3月16日；若超过该期限完成验证，则第二张证书将失效。
  - 天翼云上资源部署的证书：请开启 自动续费 + 证书托管 服务，新证书签发后，系统将自动更新替换您部署在云上资源的旧证书。
  - 服务器上部署的证书：证书替换频率将提高（约6个月替换一次），您需及时 下载新证书并部署替换旧证书 。

如您有任何问题，可随时通过 工单 或者服务热线（400-810-9889）与我们联系。

【产品公告】关于谨防假冒天翼云SSL证书供应商的说明

尊敬的天翼云用户：

您好！

近期，我们接到用户反馈，存在不法企业或个人假冒天翼云 SSL 证书供应商，通过电话、微信等方式，以“低价续费、套件服务升级、测试证书不安全”等话术，试图诱导用户前往非天翼云官方平台购买或续费 SSL 证书，请您务必提高警惕，避免因轻信虚假信息导致经济损失或信息泄露风险。天翼云不会将用户数据泄露或出售给第三方公司，天翼云合作伙伴也不会让客户去非天翼云平台购买产品。

为避免给您造成困扰，天翼云 SSL 团队特此声明：

1. 您在天翼云证书管理服务购买的 SSL 证书即将到期时，天翼云会在证书到期前20天、前30天通过官方渠道（邮件、短信、400-810-9889热线）的方式通知您及时续费，不会通过微信或其他个人形式直接联系您办理续费业务。如遇类似情况，请提高警惕并及时核实信息真实性。

2. 天翼云合作的 CA 厂商只有在证书审核环节和证书使用过程出现特殊情况（例如：私钥泄漏、申请强制吊销等）时才会主动联系您，否则不会以天翼云合作厂商的身份主动联系您。

天翼云合作的 CA 厂商信息如下表，若收到非官方来源的联系，请务必谨慎核实。

合作 CA 厂商	外呼电话号码	对外邮箱后缀
亚数信息科技（上海）有限公司	021-54970081、021-54971631	@trustasia.com
中金金融认证中心有限公司	010-87549888、010-87549666	@cfca.com.cn

如果您无法判断收到信息的真实性，烦请您记录对方联系方式和信息详细内容，及时 提交工单 反馈给天翼云。

天翼云服务团队

【产品公告】关于标准版证书根证书升级公告

尊敬的天翼云用户：

您好！

天翼云证书管理服务标准版证书将于12月正式启动专用根证书升级。此次升级旨在打造更安全可信的数字环境，为您带来以下核心价值：

- 安全加固：支持DCV多网络视角验证，抵御BGP攻击。
- 数据合规：审核资料境内处理，满足数据合规要求。
- 国密国际：一次审核，支持RSA/ECC/SM2三种证书算法切换。
- 自动化友好：支持ACME协议，提供域名、组织预审核。
- 滥用预警：基于日志，提供证书资产发现、滥用预警。

我们将于2025年12月4日，对标准版证书进行升级，其中涉及根证书的变更详情如下：

原根证书	新根证书
DigiCert Global RootG2	TrustAsia TLS ECC RootCA
DigiCert Global RootG3	TrustAsia TLS RSA RootCA
DigiCertGlobalRootCA(交叉老根证书)	CertumTrustedNetworkCA(交叉老根证书)
Certum EC-384 CA	TrustAsia TLS ECC RootCA
Certum Trusted RootCA	TrustAsia TLS RSA RootCA
CertumTrustedNetworkCA(交叉老根证书)	CertumTrustedNetworkCA(交叉老根证书)

2025年12月4日之后，您需要关注：

- 针对您所有标准版证书新订单，我们将自动升级。
- 针对您订阅的标准版证书多年期服务，在此执行日期之后提交申请的证书将自动升级。

- 本次升级不涉及域名验证方式的变更。

如果您无法判断收到信息的真实性，烦请您记录对方联系方式和信息详细内容，及时 提交工单 反馈给天翼云。

天翼云服务团队

【产品公告】关于DigiCert证书品牌企业身份确认的相关通知

尊敬的天翼云用户：

您好！

接DigiCert厂商通知，DigiCert需通过企业对外公示的第三方联系方式进行订单信息和申请人身份确认，不再接受使用律师信来证明电话号码所属的方式确认。若您的三方电话号码无法使用，年报电话、邮箱等不能配合验证，请您尽可能在DigiCert厂商认可的数据来源库中，更新或登记三方联系方式。

DigiCert认可的数据来源库（以下平台任选一个进行登记即可，登记后请告知鉴证人员进行验证）：

- 企查查网站 （需要登记贵单位信息，包含单位完整名称、联系电话/邮箱、详细地址。）
- 百度地图 （需要登记贵单位信息，包含单位完整名称、联系电话/邮箱、详细地址。）
- 谷歌地图 （需要登记贵单位信息，包含单位完整名称、联系电话/邮箱、详细地址。）

给您带来的不便，敬请谅解。如您有任何问题，可及时 提交工单 反馈给天翼云。

产品介绍

产品简介

证书管理服务（Certificate Management Service，CCMS）是一款集证书购买、申请及安全应用于一体的云上证书管家，提供SSL证书管理、私有（内网）证书管理和个人证书管理功能，并支持一键部署证书、证书托管等服务。该服务支持国密和国际算法，帮助用户实现数据传输加密和身份认证，保障数据安全。

SSL证书管理

SSL证书是一种遵守SSL协议的数字证书，用于在互联网上建立安全通信连接，常用于网站安全加密，是保护网站数据的必备证书。

- 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。
- 可以在证书管理服务控制台上购买SSL证书，并向CA机构提交证书申请，待CA机构审核通过并签发证书后，你可以下载证书并将其安装到您的应用服务器中。
- 支持将第三方证书上传到证书管理服务控制台进行统一管理。
- 支持一键部署SSL证书至天翼云其他云产品中，还提供了证书托管功能，可以自动替换天翼云上云产品证书。

私有（内网）证书管理

私有（内网）证书是CA颁发的内部专用数字凭证，用于内网身份认证、系统间加密通信和设备安全管理。

提供私有（内网）证书的全生命周期管理能力，包括购买、申请、下载、吊销等。

个人证书管理

个人证书是由CA机构核验身份后颁发的数字凭证，用于强身份认证、电子签名和加密通信等场景。

提供个人证书的全生命周期管理能力，包括购买、申请、下载、吊销等。

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7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。

全生命周期管理

支持SSL证书、个人证书的全生命周期管理，包括申请、域名验证、续订、下载、吊销等。

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。

功能特性

证书管理

统一管理云上用户SSL证书、个人证书申请使用，提供证书申请、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。

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》 。

CCMS权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组/用户授予策略或角色，才能使得用户组/用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CCMS部署时不区分物理区域，为全局级服务。授权时，在全局项目中设置权限，访问CCMS时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于天翼云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- 策略：IAM提供的一种细粒度授权的能力，可以具体到服务的操作。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CCMS服务，管理员能够控制IAM用户仅能对CCMS进行指定的管理操作。

如下表所示，包括了CCMS所有系统角色。

角色名称/策略名称	描述	类别	依赖关系
ccms admin	SSL证书管理服务管理员权限，拥有服务的所有权限。	系统策略	购买证书需要依赖bss admin策略、mkt admin策略。 • bss admin策略：系统策略，订单-费用中心（BSS）管理员，拥有该服务下的所有权限。 • mkt admin策略：系统策略，营服中心管理员，拥有该服务下的所有权限。
ccms viewer	SSL证书管理服务只读权限，拥有该权限的用户仅能查询证书信息，不具备对证书、csr、联系人、公司进行增删改权限。	系统策略	无

说明

如需购买SSL证书，账号除了必须拥有“ccms admin”之外，还需要拥有“bss admin”权限和“mkt admin”权限。

常用操作与系统权限的关系

下表列出了SSL证书管理常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

操作	ccms admin	cms viewer
获取SSL证书列表	✓	✓
获取SSL证书详情	✓	✓
获取SSL证书申请信息	✓	✓
SSL证书状态统计	✓	✓
查询联系人	✓	✓
获取SSL证书下载列表	✓	✓
查询csr列表	✓	✓
查询公司	✓	✓
获取csr详情	✓	✓
查询csr可用列表	✓	✓
获取域名认证信息	✓	✓
SSL证书申请	✓	×

操作	ccms admin	cms viewer
SSL证书申请撤回	✓	×
SSL证书下载	✓	×
SSL证书吊销	✓	×
添加联系人	✓	×
删除联系人	✓	×
编辑联系人	✓	×
吊销函下载	✓	×
删除SSL证书	✓	×
添加公司	✓	×
编辑公司	✓	×
删除公司	✓	×
证书标签编辑	✓	×
添加csr	✓	×
删除csr	✓	×
上传csr	✓	×

证书选型

服务类型

证书管理服务提供SSL证书、私有（内网）证书、个人证书：

分类	SSL证书-域名证书	SSL证书-IP证书	私有（内网）证书	个人证书
应用场景	用于网站安全加密，是保护网站数据的必备证书。 仅支持能进行互联网验证的域名。	用于网站安全加密，是保护网站数据的必备证书。 仅支持能进行互联网验证的IP。	用于内网身份认证、系统间加密通信和设备安全管理。	用于个人电子邮件或文档签名，无法用于网站HTTPS加密，常用于密评场景。
支持的加密标准	• 国际标准 • 国密标准 • 国际+国密	国际标准	• 国际标准 • 国密标准	国密标准

分类	SSL证书-域名证书	SSL证书-IP证书	私有（内网）证书	个人证书
支持的证书种类	• 域名型证书（DV） • 企业型证书（OV） • 企业型基础版（OVBasic） • 企业型专业版（OVPro） • 增强型证书（EV） • 增强型基础版（EVBasic）	• 企业型证书（OV） • 企业型专业版（OVPro） • 企业型基础版（OVBasic）	企业型证书（OV）	-
支持的证书版本	• 标准版 • SecureSite • GeoTrust • GlobalSign • CFCA • TrustAsia	• 标准版 • SecureSite • GeoTrust • GlobalSign • CFCA • TrustAsia	标准版	-
支持的域名类型	• 通配符 • 单域名 • 多域名	单IP	• 通配符 • 单域名 • 多域名	-

证书种类

分类	域名型证书（DV）	企业型证书（OV）	增强型证书（EV）
应用场景	• 适用于个人站点、中小型企业网站、APP、小程序等。 • 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。	• 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。	一般用于银行证券等金融机构、大中型企业，例如金融、支付类企业，建议购买 EV 型证书。
信任等级	信任等级一般	信任等级较高	信任等级强
认证强度	只需验证域名的真实性便可颁发证书保护网站	必须要验证域名权限以及企业的身份，审核严格，安全性高	审核更严格，安全性更高
签发周期	1个工作日	5~7个工作日	5~7个工作日
支持的域名类型	通配符、单域名、多域名	通配符、单域名、多域名、单IP	单域名、多域名

分类	域名型证书（DV）	企业型证书（OV）	增强型证书（EV）
支持的证书版本	• 标准版 • GlobalSign • TrustAsia	• 标准版 • SecureSite • GeoTrust • GlobalSign • CFCA • TrustAsia	• 标准版 • GeoTrust • GlobalSign • CFCA • TrustAsia
浏览器图示			

SSL证书版本

分类	标准版	SecureSite	GeoTrust	GlobalSign	CFCA	TrustAsia
应用场景	适用于政府、金融、中小企业等客户。	适用于金融、电商有高安全性要求的数字交易场景。	适用于中小企业和个人网站快速启用HTTPS加密。	适用于跨境业务的身份验证与数据安全需求。	满足政府、金融等行业对SSL证书国产化的相关要求。	满足政府、金融等行业对SSL证书国产化的相关要求。
版本优势	精选一线品牌证书，通过国内、国际CA双重认证，为企业和个人提供安全可靠的加密数据传输和身份验证服务，全方位满足客户的不同要求。	DigiCert 旗下的旗舰品牌，安全、稳定、兼容性好。	DigiCert 旗下的子品牌，性价比高。	老牌CA机构，25 万 + 域名全球信任背书。	国产证书品牌，审核信息不出境。	全球知名SSL证书服务提供商，国内、国际双重认证CA机构。
是否支持域名型证书（DV）	支持 支持的域名类型：通配符、单域名、多域名	不支持	不支持	支持 支持的域名类型：通配符、单域名	不支持	支持 支持的域名类型：通配符、单域名、多域名

分类	标准版	SecureSite	GeoTrust	GlobalSign	CFCA	TrustAsia
是否支持企业型证书（OV）	支持 支持的域名类型：通配符、单域名、多域名、单IP	支持 支持的域名类型：通配符、单域名、多域名、单IP	支持 支持的域名类型：通配符、单域名、多域名、单IP	支持 支持的域名类型：通配符、单域名、多域名、单IP	支持 支持的域名类型：通配符、单域名、多域名、单IP	支持 支持的域名类型：通配符、单域名、多域名、单IP
是否支持企业型基础版（OVBasic）	不支持	不支持	不支持	不支持	支持 支持的域名类型：通配符、单域名、多域名、单IP	不支持
是否支持企业型专业版（OVPro）	不支持	支持 支持的域名类型：单域名、多域名、单IP	不支持	不支持	不支持	不支持
是否支持增强型证书（EV）	支持 支持的域名类型：单域名、多域名	不支持	支持 支持的域名类型：单域名、多域名	支持 支持的域名类型：单域名、多域名	支持 支持的域名类型：单域名、多域名	支持 支持的域名类型：单域名、多域名
是否支持增强型基础版（EVBasic）	不支持	不支持	不支持	不支持	支持 支持的域名类型：单域名、多域名	不支持

域名类型说明

域名类型	应用场景
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ctyuntest.cn，也可以是1个子域名example.ctyuntest.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。
多域名	单个证书可以绑定多个域名。例如：可以是 ctyuntest.cn、ctyuntest.com、ctyuntest.com.cn、*.ctyuntest.cn。 最多可以支持250个域名。 说明 多域名需只能购买1个主单域名，至少购买1个附加单域名，在此基础上可继续增加附加单域名或附加通配符。

域名类型	应用场景
通配符	通配符SSL证书可以同时保护一个域名及所有的下一级子域名网站，比如*.ctyun.cn。 • 单个证书支持绑定带1个通配符（*）的域名，不支持多个通配符的域名。例如：不支持*.*.ctyuntest.cn。 • 单个证书可以同时保护一个域名及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。 • 只能匹配主域名及同级别的子域名，不能跨级匹配。例如：*.ctyuntest.cn的域名证书可以匹配ctyuntest.cn、demo.ctyuntest.cn、example.ctyuntest.cn等域名， 但是不匹配guide.demo.ctyuntest.cn、developer.demo.ctyuntest.cn等域名。

支持的加密算法

天翼云证书管理服务签发的SSL证书支持RSA、ECC、SM2三种加密算法：

- RSA是目前应用最广泛的非对称加密算法。在三种算法中兼容性最佳，支持主流浏览器及各类操作系统平台。
- ECC是基于椭圆曲线结构的非对称加密算法。相较于 RSA，ECC 加密速度更快、效率更高、服务器资源消耗更低，已在主流浏览器中广泛推广，正逐渐成为新一代主流算法。
- SM2是中国国家密码管理局发布的商用密码算法，基于椭圆曲线密码（ECC）体系，是中国商用密码体系中用于替代RSA的国产算法。

不同类型的证书支持的加密算法如下：

证书版本	证书种类	域名类型	支持的加密算法
标准版	域名型DV	通配符、单域名、多域名	国际标准：RSA/ECC 国密标准：SM2
	企业型OV	通配符、单域名	国际标准：RSA/ECC 国密标准：SM2 国际+国密：SM2、RSA/ECC
		单IP	国际标准：RSA/ECC
		多域名	国际标准：RSA/ECC 国密标准：SM2
	增强型EV	单域名、多域名	国际标准：RSA/ECC
SecureSite	企业型证书（OV）	通配符、单域名、多域名、单IP	国际标准：RSA/ECC
	企业型专业版（OVPro）	单域名、多域名、单IP	国际标准：RSA/ECC
GeoTrust	企业型证书（OV）	通配符、单域名、多域名、单IP	国际标准：RSA/ECC
	增强型证书（EV）	单域名、多域名	国际标准：RSA/ECC
GlobalSign	域名型证书（DV）	通配符、单域名	国际标准：RSA/ECC
	企业型证书（OV）	通配符、单域名、多域名、单IP	国际标准：RSA/ECC
	增强型证书（EV）	单域名、多域名	国际标准：RSA/ECC

证书版本	证书种类	域名类型	支持的加密算法
CFCA	企业型证书（OV）	通配符、单域名、多域名	国际标准：RSA 国密标准：SM2
		单IP	国际标准：RSA
	企业型基础版（OVBasic）	通配符、单域名、多域名、单IP	国际标准：RSA
	增强型证书（EV）	单域名、多域名	国际标准：RSA
	增强型基础版（EVBasic）	单域名、多域名	国际标准：RSA
TrustAsia	域名型证书（DV）	通配符、单域名、多域名	国际标准：RSA/ECC 国密标准：SM2
	企业型证书（OV）	通配符、单域名、多域名	国际标准：RSA 国密标准：SM2
		单IP	国际标准：RSA
	增强型证书（EV）	单域名、多域名	国际标准：RSA

应用场景

公众服务类网站、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，解决用户在浏览器打开网页时提示“不安全”，导致用户无法访问网站信息或APP/小程序无法上架的问题，可验证企业身份，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

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等保、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。

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。

公钥与私钥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。

使用限制

证书支持的浏览器版本

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)	√	√	√	×	×
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)	√	√	√	×	×

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
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 (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	√	√	√	×	×

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 6.0	√	√	√	×	×
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	√	√	√	√	√

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 申请私有证书时填写的邮箱：否	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

存储方式

CCMS通过加密算法对您个人敏感数据加密后进行存储。

- 租户ID：不属于敏感数据，明文存储
- 姓名、邮箱、手机号码：加密存储

计费说明

计费项

计费说明

证书管理服务的计费项具体内容如下表所示：

服务类型	计费项说明	适用的计费模式	计费公式
SSL证书	根据证书版本、加密标准、证书种类、域名类型、有效期、购买数量计算费用。	按个计费	所选规格证书单价×购买数量 × 有效期（购买年份）
私有（内网）证书	根据证书版本、加密标准、证书种类、域名类型、有效期、购买数量计算费用。	按个计费	所选规格证书单价×购买数量 × 有效期（购买年份）
个人证书	个人证书是由权威CA机构颁发的数字身份证，用于身份认证、数据签名和加密通信等场景。	按个计费	个人证书单价 ×购买数量 × 有效期（购买年份）
证书托管服务	对于天翼云上云产品，实现证书更新后的自动替换能力。	按次计费	托管证书服务单价 × 购买数量
第三方证书部署服务	上传证书一键部署到云产品的服务，将证书部署到一个云产品资源，需要消耗一次部署服务。	按次计费	部署服务单价 × 购买数量
域名监控服务	开启域名监控后，可帮助监测多个站点的HTTPS业务状态，并及时发现站点上的SSL证书安全问题，方便统一维护多站点HTTPS。	按次计费	域名监控服务单价 × 购买数量

计费方式

证书管理服务仅支持一次性计费方式。

标准版证书价格

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。

加密标准	证书种类	域名类型	年付价格（元/个/年）
国际算法	域名型（DV）	单域名	594.15
		通配符	1699.15
		多域名-主单域名	594.15

加密标准	证书种类	域名类型	年付价格（元/个/年）
		多域名-附加单域名	594.15
		多域名-附加通配符	1699.15
	企业型（OV）	单域名	1912.5
		通配符	5270
		多域名-主单域名	1912.5
		多域名-附加单域名	510
		多域名-附加通配符	4760
		单IP	1912.5
	增强型（EV）	单域名	2720
		多域名-主单域名	2720
		多域名-附加单域名	1020
国密算法	域名型（DV）	单域名	1275
		通配符	2975
		多域名-主单域名	1275
		多域名-附加单域名	1275
		多域名-附加通配符	2975
	企业型（OV）	单域名	3825
		通配符	11475
		多域名-主单域名	3825
		多域名-附加单域名	2550
		多域名-附加通配符	11475
国际+国密算法	企业型（OV）	单域名	5737.50
		通配符	16745

多证书包

标准版如下证书支持购买多证书包，多证书包内包含10张证书，总价为10张证书的8折。

加密标准	证书种类	域名类型	年付价格（元/份/年）
国际算法	企业型（OV）	通配符	42160

SecureSite证书价格

加密标准	证书种类	域名类型	年付价格（元/个/年）
国际算法	企业型（OV）	单域名	5990
		通配符	42800
		多域名-主单域名	5990

加密标准	证书种类	域名类型	年付价格（元/个/年）
		多域名-附加单域名	5990
		多域名-附加通配符	42800
		单IP	5990
	企业型专业版（OV Pro）	单域名	9620
		多域名-主单域名	9620
		多域名-附加单域名	9620
		单IP	9620

GeoTrust证书价格

加密标准	证书种类	域名类型	标准资费（元/个/年）
国际算法	企业型（OV）	单域名	2970
		通配符	7840
		多域名-主单域名	2970
		多域名-附加单域名	2330
		多域名-附加通配符	7200
		单IP	2970
	增强型（EV）	单域名	6420
		多域名-主单域名	6420
		多域名-附加单域名	3210

GlobalSign证书价格

加密标准	证书种类	域名类型	标准资费（元/个/年）
国际算法	域名型（DV）	单域名	1980
		通配符	6930
	企业型（OV）	单域名	3728
		通配符	13048
		多域名-主单域名	3728
		多域名-附加单域名	1980
		多域名-附加通配符	13048
		单IP	3728
	增强型（EV）	单域名	9880
		多域名-主单域名	9880
		多域名-附加单域名	2980

CFCA证书价格

加密标准	证书种类	域名类型	标准资费（元/个/年）
国际算法	企业型（OV）	单域名	4900
		通配符	16000
		多域名-主单域名	4900
		多域名-附加单域名	2500
		多域名-附加通配符	8000
		单IP	4900
	企业型基础版（OVBasic）	单域名	3000
		通配符	9000
		多域名-主单域名	3000
		多域名-附加单域名	1500
		多域名-附加通配符	4500
		单IP	3000
	增强型（EV）	单域名	10000
		多域名-主单域名	10000
		多域名-附加单域名	5000
	增强型基础版（EVBasic）	单域名	8000
		多域名-主单域名	8000
		多域名-附加单域名	4000
国密算法	企业型（OV）	单域名	4900
		通配符	16000
		多域名-主单域名	4900
		多域名-附加单域名	2500
		多域名-附加通配符	8000

TrustAsia证书价格

加密标准	证书种类	域名类型	标准资费（元/个/年）
国际算法	域名型（DV）	单域名	699
		通配符	1999
		多域名-主单域名（默认支持3个主单域名）	4900
		多域名-附加单域名	950

加密标准	证书种类	域名类型	标准资费（元/个/年）
		多域名-附加通配符	1999
	企业型（OV）	单域名	4500
		通配符	13500
		多域名-主单域名	4500
		多域名-附加单域名	2000
		多域名-附加通配符	13500
		单IP	4500
	增强型（EV）	单域名	9500
		多域名-主单域名	9500
		多域名-附加单域名	3500
国密算法	域名型（DV）	单域名	699
		通配符	4900
		多域名-主单域名（默认支持3个主单域名）	4900
		多域名-附加单域名	950
		多域名-附加通配符	1999
	企业型（OV）	单域名	4500
		通配符	13500
		多域名-主单域名	4500
		多域名-附加单域名	2000
		多域名-附加通配符	13500

私有（内网）证书

加密标准	证书种类	域名类型	标准资费（元/个/年）
国际算法	企业型（OV）	单域名	1912.5
		通配符	5270
		多域名-主单域名	1912.5
		多域名-附加单域名	510
		多域名-附加通配符	4760
国密标准	企业型（OV）	单域名	3825
		通配符	11475
		多域名-主单域名	3825
		多域名-附加单域名	2550

加密标准	证书种类	域名类型	标准资费（元/个/年）
		多域名-附加通配符	11475

个人证书

个人证书是由权威CA机构颁发的数字身份证，用于身份认证、数据签名和加密通信等场景。

服务类型	加密标准	计费方式	标准资费（元/个/年）
个人证书	国密标准	按个计费	150

证书托管服务

证书托管服务仅支持天翼云上产品，实现证书更新后的自动替换能力。

服务类型	计费方式	标准资费（元/次）
证书托管服务	按次计费	30

第三方证书部署服务

已上传的第三方证书支持一键部署到天翼云上产品，提升业务便捷性。

服务类型	计费方式	标准资费（元/次）
第三方证书部署服务	按次计费	30

域名监控服务

域名监控可帮助监测多个站点的HTTPS业务状态，并及时发现站点上的SSL证书安全问题，方便统一维护多站点HTTPS。

服务类型	计费方式	标准资费（元/次）
域名监控服务	按次计费	30

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。

手动续订操作步骤

1. 进入证书管理服务，选择“SSL证书管理”>“SSL证书列表”。
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，选择证书有效期。

4. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，单击“立即购买”。

自动续订操作步骤

1.进入证书管理服务，选择“SSL证书管理”>“SSL证书列表”。

2.选择需要开启自动续订功能的证书，将“开启自动续费”开关调整至 

状态，即可开始自动续费功能。

说明

- 自动续费生效后，会在您证书到期前30个自然日为您自动续费；若您在到期30个自然日前开启自动续费功能，则不会为您自动续费，请您注意。
- 新生成的订单和您旧证书的订单信息保持一致。例如：您购买3年期的企业型（OV）单域名证书，会在到期前30个自然日自动续费3年期的企业型（OV）单域名证书。
- 自动续费生成的证书会为您自动提交申请，但是需要您手动提交确认函和解析记录后才会签发，后续操作可参考： 申请SSL证书 。

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：手续费 = 订单实付款 ÷ 36500 × 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。

前提条件

证书状态在“待申请”或者“已吊销”的状态下可直接进行退订操作。

> 说明
>
> 若证书在“申请审核中”需要撤销申请后，才可以进行退订操作。

退订步骤

1. 登录证书管理服务控制台。
2. 选择需要退订的证书，单击“操作”列的“更多 > 证书退订”。

3. 在弹出的对话框中，确认信息内容单击“确定”，进入退订申请页面。
4. 在退订申请页面中，选择退订原因并勾选“我已确认本次退订金额和相关费用”后，单击“退订”完成退订申请。
5. 后续您可在订单详情中查看退款进度。

快速入门

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。	购买证书
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。	申请证书
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。	产品续订
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。	吊销证书

用户指南

购买证书&服务

购买SSL证书

SSL证书用于网站安全加密，是保护网站数据的必备证书。支持域名证书和IP证书：

服务类型	说明
SSL证书-域名证书	仅支持绑定能进行互联网验证的域名。
SSL证书-IP证书	仅支持能进行互联网验证的IP。

购买SSL-域名证书

> 注意
>
> 若您购买的证书为多年期证书，在服务期内续期证书时不支持更换域名，若您需要为新域名绑定证书请新购证书。

1. 登录 证书管理服务控制台 。
2. 单击“购买证书”，进入到证书管理服务产品购买页面。
3. 服务类型选择“SSL证书-域名证书”。
4. 选择证书数量、域名类型、证书版本、证书种类、加密标准、服务有效时长、企业项目。具体的规格选择可参见下表。

参数	说明
证书数量/域名名称	支持两种购买方式，通过点击参数下方的链接进行切换。 • 证书数量（默认方式）：如果不知道域名，可以通过该方式快速购买。 • 域名名称：填写您需要申请SSL证书的域名，支持单域名（例如：ctyun.cn或1.1.1.1）、通配符域名 （例如：*.ctyun.cn）、多域名（例如：*.189.cn,ctyun.cn）。
域名类型	支持通配符、单域名、多域名。关于域名类型的区别，请参见 证书选型 > 域名类型说明 。
证书版本	支持标准版、SecureSite、GeoTrust、GlobalSign、CFCA、TrustAsia。关于证书版本的区别，请参见 证书选型 > SSL证书版本 。

参数	说明
证书种类	关于证书版本的区别，请参见 证书选型 > 证书种类 。 若您域名类型选择“通配符”，证书版本选择“标准版”，OV企业型证书支持购买多证书包（包含10张证书，总价为八折）。 说明 您购买多证书包后，不支持单独退订证书包内的证书，若需要退订只支持10张证书一起退订，且10张证书都处于可退订的状态。
加密标准	根据所选证书规格，选择加密标准。关于各证书支持的加密标准及算法，请参见 证书选型 > 支持的加密算法 。
服务有效时长	可选择： • 1年 • 2年 • 3年 2026年2月24日起，单张国际算法SSL证书有效期将陆续调整为199天。您可正常选购1年/2年/3年服务套餐，天翼云将自动为您提供多张证书，保障证书全程有效、服务无间断。
企业项目	从下拉框中选择。 如需创建新的企业项目，您可以点击“ 去创建 ”。

5. 选择有效期。

   证书管理服务有效时长内包含多张SSL证书。每张证书到期前30天，天翼云将会自动为您续期证书，请配合天翼云 验证域名 。
6. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，单击“立即购买”下单。
7. 在弹出的“订单详情”页确认订单信息，单击“提交订单”。
8. 单击“立即支付”，完成SSL证书的购买。

购买SSL-IP证书

说明

目前SSL证书-IP证书仅支持国际标准OV单域名规格。

1. 登录 证书管理服务控制台 。
2. 单击“购买证书”，进入到证书管理服务产品购买页面。
3. 服务类型选择“SSL证书-IP证书”。
4. 选择证书数量、域名类型、证书版本、证书种类、加密标准、服务有效时长、企业项目。具体的规格选择可参见下表。

参数	说明
证书数量/域名名称	支持两种购买方式，通过点击参数下方的链接进行切换。 • 证书数量（默认方式）：如果不知道域名，可以通过该方式快速购买。 • 域名名称：填写您需要申请SSL证书的域名，支持单域名（例如：ctyun.cn或1.1.1.1）、通配符域名（例如：*.ctyun.cn）、多域名（例如：*.189.cn,ctyun.cn）。
域名类型	仅支持“单IP”，即单个证书仅支持绑定单一公网IP。
证书版本	支持标准版、SecureSite、GeoTrust、GlobalSign、CFCA、TrustAsia。关于各证书版本的区别，请参见 证书选型 > SSL证书版本 。
证书种类	支持OV企业型和OVPro企业型专业版。关于证书种类的区别，请参见 证书选型 > SSL证书种类 。
加密标准	SSL证书-IP证书仅支持“国际标准”。
服务有效时长	可选择： • 1年 • 2年 • 3年 2026年2月24日起，单张国际算法SSL证书有效期将陆续调整为199天。您可正常选购1年/2年/3年服务套餐，天翼云将自动为您提供多张证书，保障证书全程有效、服务无间断。
企业项目	从下拉框中选择。 如需创建新的企业项目，您可以点击“ 去创建 ”。

5. 选择有效期。

   证书管理服务有效时长内包含多张SSL证书。每张证书到期前30天，天翼云将会自动为您续期证书，请配合天翼云 验证域名 。
6. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，单击“立即购买”下单。
7. 在弹出的“订单详情”页确认订单信息，单击“提交订单”。
8. 单击“立即支付”，完成SSL证书的购买。

购买私有（内网）证书

操作场景

私有（内网）证书是CA颁发的内部专用数字凭证，用于内网身份认证、系统间加密通信和设备安全管理。

操作步骤

> 注意
>
> 若您购买的证书为多年期证书，在服务期内续期证书时不支持更换域名，若您需要为新域名绑定证书请新购证书。

1. 登录 证书管理服务控制台 。

2. 在左侧导航栏，选择“私有证书管理 > 私有证书列表”，进入私有证书管理页面。
3. 单击“购买证书”，进入购买证书实例页面。
4. 服务类型选择“私有（内网）证书”。

5. 选择证书数量、域名类型、证书版本、证书种类、加密标准、服务有效时长、企业项目。具体的规格选择可参见下表。

参数	说明
证书数量/域名名称	支持两种购买方式，通过点击参数下方的链接进行切换。 • 证书数量（默认方式）：如果不知道域名，可以通过该方式快速购买。 • 域名名称：填写您需要申请内网证书的域名，支持单域名（例如：ctyun.cn或1.1.1.1）、通配符域名（例如：*.ctyun.cn）、多域名（例如：*.189.cn,ctyun.cn）。
域名类型	支持通配符、单域名、多域名。关于域名类型的区别，请参见 证书选型 > 域名类型说明 。
证书版本	仅支持“标准版”。
证书种类	仅支持“OV企业型”。
加密标准	支持“国际标准”和“国密标准”。关于各证书支持的加密标准及算法，请参见 证书选型 > 支持的加密算法 。
服务有效时长	可选择： • 1年 • 2年 • 3年
企业项目	从下拉框中选择。 如需创建新的企业项目，您可以点击“ 去创建 ”。

6. 选择有效期。

   若您选择购买服务的有效期为2年（或3年），那么此服务中包含2张（或3张）有效期为1年的证书，在到期30天前，天翼云将会自动为您续期证书，请配合完成天翼云定期发起的 域名验证 。
7. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，单击“立即购买”下单。
8. 在弹出的“订单详情”页确认订单信息，单击“提交订单”。
9. 单击“立即支付”，完成购买操作。

购买个人证书

操作场景

个人证书是由CA机构核验身份后颁发的数字凭证，用于强身份认证、电子签名和加密通信等场景，1-2个工作日签发证书。

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“个人证书管理 > 个人证书列表”，进入个人证书管理页面。
3. 单击“购买证书”，进入购买证书实例页面。
4. 服务类型选择“个人证书”。

5. 选择需要购买的个人证书数量，单次最多支持选购200个。
6. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，单击“立即购买”下单。
7. 在弹出的“订单详情”页确认订单信息，单击“提交订单”。
8. 单击“立即支付”，完成个人证书的购买。

购买证书托管服务

操作场景

对于天翼云上云产品，证书托管服务可以实现证书更新后的自动替换能力。

操作步骤

1. 登录 证书管理服务控制台 。

2. 单击“购买证书”，进入到证书管理服务产品购买页面。
3. 服务类型选择“证书托管服务”。

4. 选择证书托管服务的购买数量，单次最多可购买100个。
5. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，单击“立即购买”下单。
6. 在弹出的“订单详情”页确认订单信息，单击“提交订单”。
7. 单击“立即支付”，完成证书托管服务的购买。

购买第三方证书部署服务

操作场景

已上传的第三方证书支持一键部署到天翼云上弹性负载均衡、Web应用防火墙（原生版）、CDN加速相关产品，提升业务便捷性。

操作步骤

1. 登录 证书管理服务控制台 。
2. 单击“购买证书”，进入到证书管理服务产品购买页面。
3. 服务类型选择“第三方证书部署服务”。

4. 选择第三方证书部署服务的购买数量，单次最多可购买200个。
5. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，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”，完成第三方证书部署服务的购买。

SSL证书

申请SSL证书

准备证书审核材料

申请企业型(OV)/增强型(EV)SSL证书、私有（内网）证书、个人证书时，部分证书需要在人工验证阶段提供审核材料，您可以根据实际情况提前准备相关材料。

服务类型	证书版本	证书种类	加密标准	下载审核材料模板
SSL证书	标准版	OV	国际标准、国密标准	标准版授权书模板.zip
	CFCA	OV、EV	国际标准	（国际标准）CFCA证书申请表模版.xlsx
			国密标准	（国密标准）CFCA证书申请表&授权书模版.zip
	Globalsign	OV、EV	国际标准	Globalsign确认函模版.doc
私有（内网）证书	标准版	OV	国际标准、国密标准	私有（内网）证书申请表模版.xlsx
个人证书	-	-	国密标准	个人证书申请表模版.xlsx

说明

自2026年3月15日起，所有公开信任的SSL/TLS证书最长有效期将缩短至199天，具体通知可参考： 【产品公告】关于SSL证书有效期政策变更的重要通知 。

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。

在申请证书时，您可以参考 SSL证书申请常见问题 。

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”。如何购买证书请参考： 购买SSL证书 。

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“SSL证书管理 > SSL证书列表”，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。

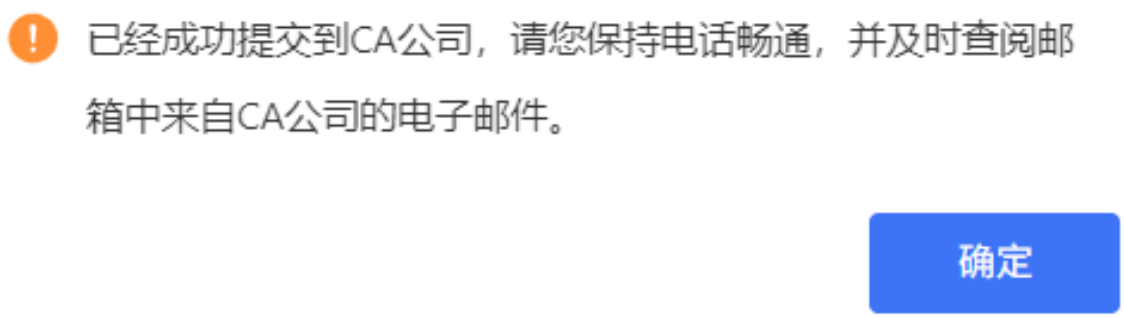
3. 在右侧弹出的窗口中填写证书申请的相关信息。

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）。 注意 • 在申请单域名规格证书时： - 所填域名不含www时，填写主域名，系统赠送域名：www.主域名。 例如，填写ctyun.cn（主域名），系统赠送域名：www.ctyun.cn；填写二级及以上子域名，系统不赠送域名。 - 所填域名含www时，填写www域名，系统赠送上一级域名。 例如，填写www.a.ctyun.cn，系统赠送域名：a.ctyun.cn。 • 若您的域名为中文域名，可使用 Punycode编码转换工具 将中文域名编码为Punycode填入域名栏。
域名验证方式	可选“文件验证”、“手工DNS验证”、“代理文件验证”、“代理DNS验证”。 • “手工DNS验证”、“代理DNS验证”：不支持GlobalSign版本的证书验证。 • “文件验证”、“代理文件验证”：目前仅支持绑定IP方式的OV证书验证，不支持通配符域名类型的证书验证。 说明 • 申请提交后，不支持更改域名验证方式，请谨慎选择。若已经提交申请，只能撤回申请后重新提交申请。 • 证书管理服务有效时长内包含多张SSL证书。每张证书到期前30天，天翼云将会自动为您续期证书，此处的“域名验证方式”建议选择“代理文件验证”或“代理DNS验证”，每次续期证书将无需手动验证域名。
联系人	选择联系人，如何新建联系人请参考 信息管理 章节。
所在地	选择公司实际所在地区（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）。

<table>
<tr><th>填写参数</th><th>参数说明</th></tr>
<tr><td>CSR生成方式</td><td>CSR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。
支持“系统生成”或“手动生成”两种方式：
• 系统生成：根据用户所配置的信息，系统自动生成一个CSR。为保障您的证书顺利申请，建议您使用系统生成CSR的方式，避免因内容不正确而导致的审核失败。
• 手动生成：在下拉框中选择已手动创建的CSR，使用已创建的CSR申请证书。
注意
- 请不要在证书签发完成前删除CSR。
- 手动生成将无法署到天翼云产品。</td></tr>
<tr><td colspan="2">提醒事件管理
说明
证书过期将影响业务正常运行，因此，建议设置证书临期提醒，联系人建议填写运维人员。</td></tr>
<tr><td>联系人</td><td>建议填写运维人员。如果需要新增联系人，请参见 联系人管理 。</td></tr>
<tr><td>提醒方式</td><td>可选择“邮件方式”、“短信方式”。</td></tr>
<tr><td>提醒内容</td><td>支持多选：
• 当天到期提醒
• 30天到期提醒
• 15天到期提醒
• 证书验证提醒
• 证书下载提醒</td></tr>
</table>

4. 填写完后，单击“提交审核”。

提交审核后，CA颁发机构将对您提交的申请进行处理并给您填写的邮箱发送一封验证邮件。您需要按照要求进行域名验证。



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”页签查看签发成功的证书。

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、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”。如何购买证书请参考： 购买SSL证书 。

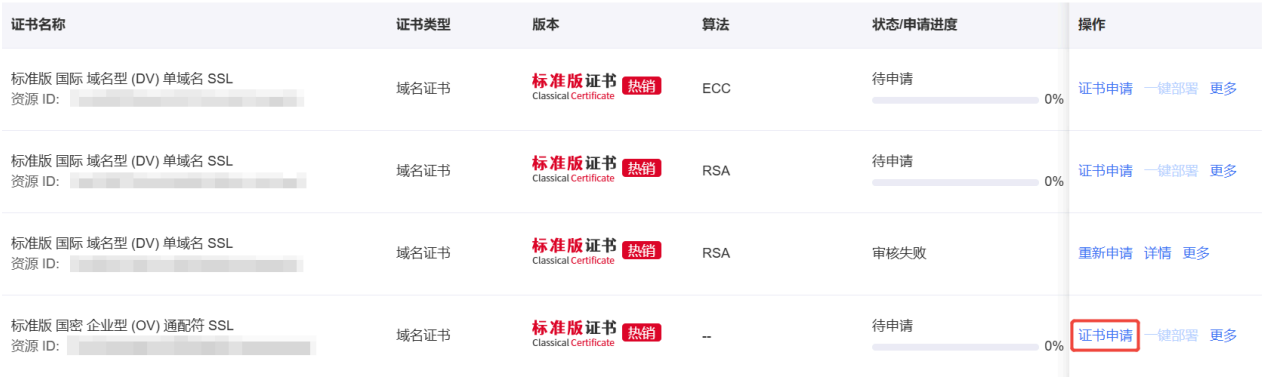
准备证书审核材料

申请企业型(OV)/增强型(EV)SSL证书时，部分证书需要在人工验证阶段上传证书申请表、授权书等材料，您可以提前下载相关模版并进行填写。

服务类型	证书版本	证书种类	加密标准	下载审核材料模板
SSL证书	标准版	OV	国际标准、国密标准	标准版授权书模板.zip
	CFCA	OV、EV	国际标准	（国际标准）CFCA证书申请表模版.xlsx
			国密标准	（国密标准）CFCA证书申请表&授权书模版.zip
	Globalsign	OV、EV	国际标准	Globalsign确认函模版.doc

申请企业型(OV)/增强型(EV)SSL证书

1. 登录“证书管理服务”控制台。
2. 在左侧导航栏选择“SSL证书管理 > SSL证书列表”，随后在顶部导航栏选择“可申请”，进入“证书管理”页面。
3. 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。

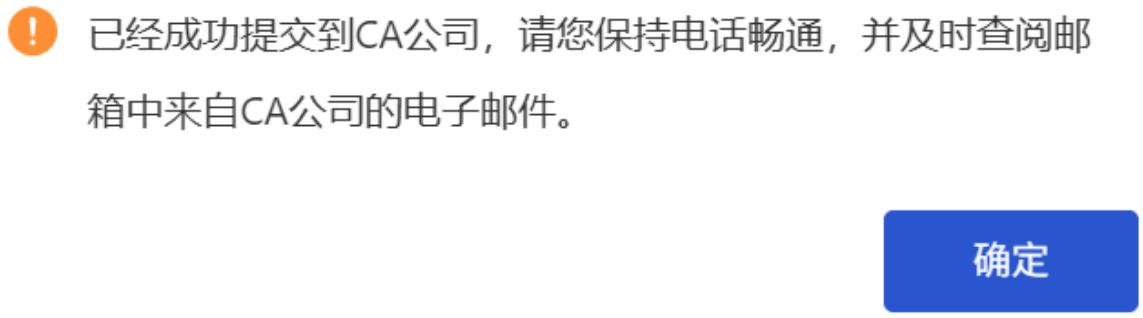


4. 在右侧的对话框中填写证书申请的相关信息。

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）。 注意 • 在申请单域名规格证书时： - 所填域名不含www时，填写主域名，系统赠送域名：www.主域名。 例如，填写ctyun.cn（主域名），系统赠送域名：www.ctyun.cn；填写二级及以上子域名，系统不赠送域名。 - 所填域名含www时，填写www域名，系统赠送上一级域名。 例如，填写www.a.ctyun.cn，系统赠送域名：a.ctyun.cn。 • 若您的域名为中文域名，可使用 Punycode编码转换工具 将中文域名编码为Punycode填入域名栏。

填写参数	参数说明
域名验证方式	可选“文件验证”、“手工DNS验证”、“代理文件验证”、“代理DNS验证”。 • “手工DNS验证”、“代理DNS验证”：不支持GlobalSign版本的证书验证。 • “文件验证”、“代理文件验证”：目前仅支持绑定IP方式的OV证书验证，不支持通配符域名类型的证书验证。 说明 • 申请提交后，不支持更改域名验证方式，请谨慎选择。若已经提交申请，只能撤回申请后重新提交申请。 • 证书管理服务有效时长内包含多张SSL证书。每张证书到期前30天，天翼云将会自动为您续期证书，此处的“域名验证方式”建议选择“代理文件验证”或“代理DNS验证”，每次续期证书将无需手动验证域名。
联系人	选择联系人，如何新建联系人请参考 联系人管理 。
公司	选择公司，如何新建公司请参考 公司管理 。
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	CSR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。 支持“系统生成”或“手动生成”两种方式： • 系统生成：根据用户所配置的信息，系统自动生成一个CSR。为保障您的证书顺利申请，建议您使用系统生成CSR的方式，避免因内容不正确而导致的审核失败。 • 手动生成：在下拉框中选择已手动创建的CSR，使用已创建的CSR申请证书。 注意 - 请不要在证书签发完成前删除CSR。 - 手动生成将无法署到天翼云产品。
提醒事件管理 说明 证书过期将影响业务正常运行，因此，建议设置证书临期提醒，联系人建议填写运维人员。	
联系人	建议填写运维人员。如果需要新增联系人，请参见 联系人管理 。
提醒方式	可选择“邮件方式”、“短信方式”。
提醒内容	支持多选： • 当天到期提醒 • 30天到期提醒 • 15天到期提醒 • 证书验证提醒 • 证书下载提醒

5. 填写完后，单击“提交审核”，并提示如下内容，单击“确定”进行下一步。



6. 进行人工验证环节。

   支持多种审核方式，审核人员会根据您提交的组织信息来确认可用的审核方式，可能是电话、邮箱等，请您按照要求提供相关资料，完成验证操作。

审核方式	说明	支持的证书版本
电话审核	【企业年报公示电话、114电话】，请保持电话畅通。	标准版、TrustAsia、SecureSite、GeoTrust
邮箱审核	【企业年报公示邮箱】，请注意查收邮件，并按要求完成相关验证操作。	标准版、TrustAsia、SecureSite、GeoTrust
电话账单审核	请提供电话公司出具的近三个月的电话账单（需包含组织名称及组织地址）。	标准版
资料审核	a. 根据界面提示，下载并填写相关材料，包括申请表、授权书等。 如果在申请证书前已准备好 证书审核材料 ，此处直接上传即可。 b. 填写完成并确认无误后，单击“点击上传”进行上传。	标准版、CFCA、Globalsign

7. 配置域名验证信息，详细操作可参考 域名验证 ，配置完成后等待审核签发证书。

   说明

   验证信息将会在确认函审核完毕后才会在证书管理控制台中显示，请您耐心等待。

8. 若证书已成功签发，可返回到“已签发”页签查看签发成功的证书。

重新申请已吊销的证书

吊销SSL证书后，若需要再使用证书，可以重新申请证书。

约束限制

证书状态为“已吊销”，且吊销时间距签发时间满足如下要求，支持重新申请证书。

- GlobalSign证书：吊销时间距签发时间5天内，支持重新申请。
- 标准版、SecureSite、GeoTrust、CFCA证书：吊销时间距签发时间28天内，支持重新申请。

注意事项

吊销后重新申请的证书不支持进行二次吊销及退订。

操作步骤

1. 选择待重新申请的证书，选择“操作”列的“更多 > 重新申请”。
2. 在右侧弹出的证书申请窗口中配置相关信息，参数说明请参见 申请SSL证书 。

申请测试证书

天翼云证书管理服务提供证书版本为TrustAsia、证书类型为DV、域名类型为单域名、有效期为3个月的测试证书。

约束限制

- 一个账号每年最多可以申请10张测试证书，单次只能创建1张测试证书。
- 1张测试证书仅支持绑定一个单域名，不支持保护通配符、IP。
- 测试证书的信任等级较低，建议只用于测试。
- 测试证书签发后，有效期为3个月。不支持续订，若需继续使用SSL证书，请在控制台重新创建测试证书或升级为正式证书，购买正式证书请参见 升级测试证书为正式证书 。

测试证书使用流程

步骤	说明
步骤一：创建测试证书	填写域名创建证书。
步骤二：提交申请证书	填写测试证书申请信息，提交审核。
步骤三：域名验证	在域名控制台添加DNS解析记录，完成域名所有权验证。
步骤四：签发证书	CA将在1个工作日完成审核签发证书，请耐心等待。

步骤一：创建测试证书

1. 登录 证书管理服务控制台 。
2. 在左侧导航栏选择“SSL证书管理 > SSL证书列表”。
3. 选择“测试证书”页签，单击“创建证书”。

4. 在创建证书页面，配置域名名称。

5. 单击“确定”，完成测试证书创建。

步骤二：提交证书申请

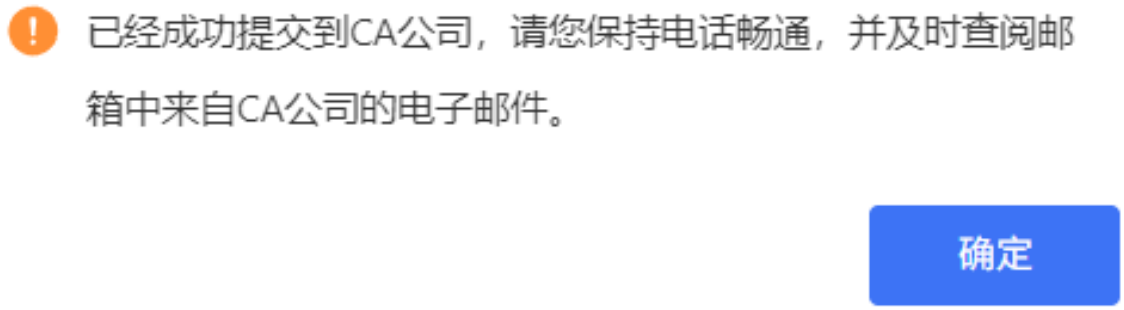
1. 登录 证书管理服务控制台 。
2. 在左侧导航栏选择“SSL证书管理 > SSL证书列表”。
3. 选择“测试证书”页签，在待申请的证书操作列，单击“证书申请”按钮，进行测试证书申请。

4. 在右侧弹出的窗口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）。 注意 在申请单域名规格证书时： • 所填域名不含www时，填写主域名，系统赠送域名：www.主域名。 例如，填写ctyun.cn（主域名），系统赠送域名：www.ctyun.cn；填写二级及以上子域名，系统不赠送域名。 • 所填域名含www时，填写www域名，系统赠送上一级域名。 例如，填写www.a.ctyun.cn，系统赠送域名：a.ctyun.cn。
域名验证方式	支持“手动DNS验证”和“文件验证”。
联系人	选择联系人，如何新建联系人请参考 信息管理 章节。
所在地	选择公司实际所在地区。（目前仅支持选择中国地区）
密钥算法	可选择“RSA”、“ECC”。
CSR生成方式	CSR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。 支持“系统生成”或“手动生成”两种方式： • 系统生成：根据用户所配置的信息，系统自动生成一个CSR。为保障您的证书顺利申请，建议您使用系统生成CSR的方式，避免因内容不正确而导致的审核失败。 • 手动生成：在下拉框中选择已手动创建的CSR，使用已创建的CSR申请证书。 注意 - 请不要在证书签发完成前删除CSR。 - 手动生成将无法署到天翼云产品。

5. 填写完后，单击“提交审核”。

   提交审核后，CA颁发机构将对您提交的申请进行处理并给您填写的邮箱发送一封验证邮件。您需要按照要求进行域名验证。



步骤三：域名验证

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。

步骤四：签发证书

CA机构审核通过后，将会签发证书。

等待证书成功签发，可返回到“已签发”页签查看签发成功的证书。

后续操作

您可以将已签发的测试证书安装到您的服务器，详细操作请参考 安装SSL证书 。

域名验证

文件验证

按照CA中心的规范，如果您申请了SSL证书，则必须完成域名验证（又称验证域名所有权）来证明待申请证书要绑定的域名属于您。

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。

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域名和单域名类型证书使用文件验证。

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。

   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
   ```

   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。

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

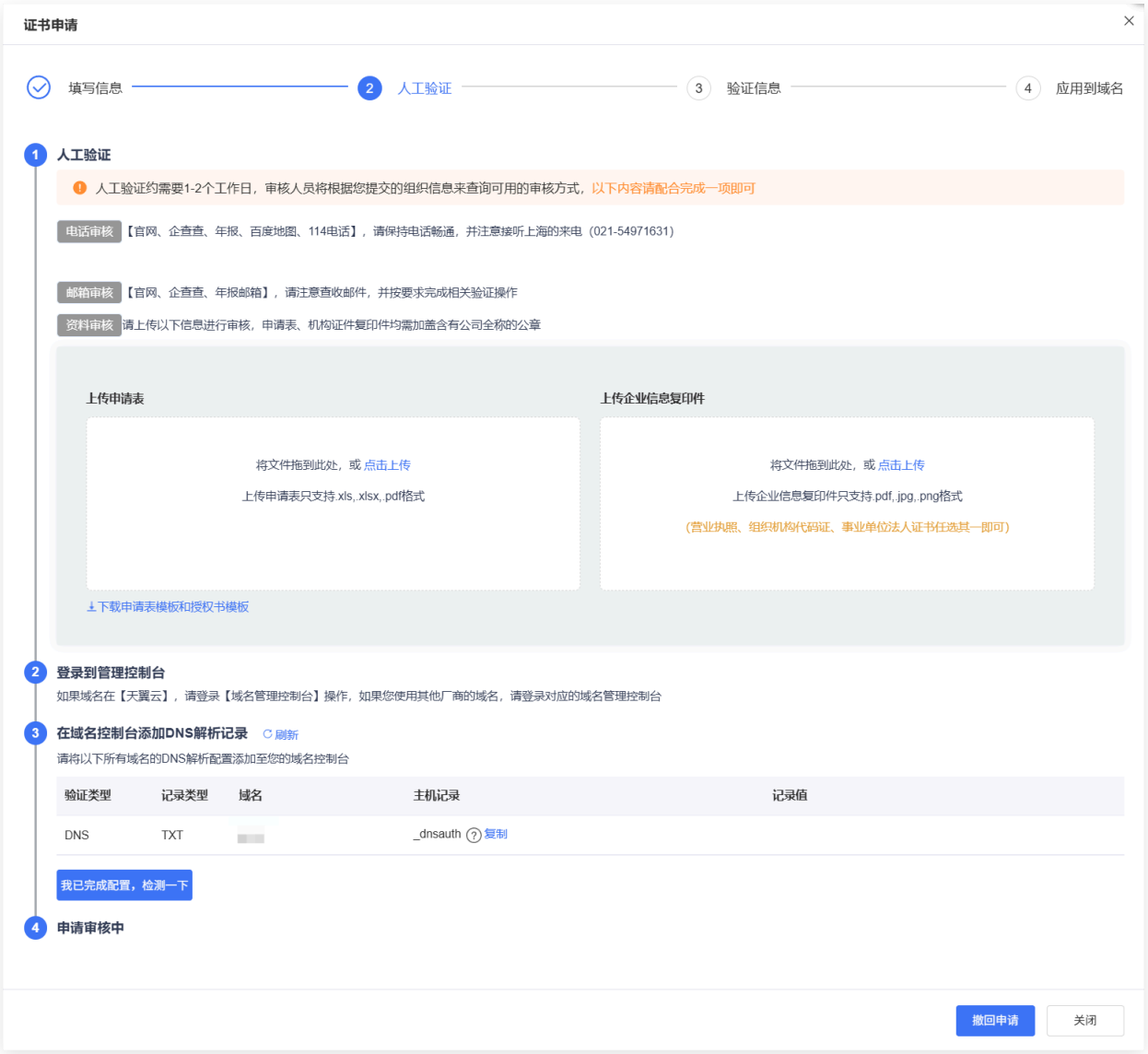
手动DNS验证的域名解析只能在您的域名管理平台上进行操作，具体的解析方法以域名服务商提供的解析方法为准。

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。



在天翼云新域名服务上进行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）证书需在确认函进入预审流程后（约提交确认函1~2个工作日左右），才可以在控制台查阅域名DNS验证信息。

2. 下面以天翼新域名服务为例，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。

   a. 使用域名持有者所在的天翼云账号，登录 新域名服务管理控制台 。

   b. 在需要添加DNS解析记录的域名记录操作列，单击“域名解析”。

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

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优先级	-
TTL	选择默认值，不作修改。

   d. 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。

代理文件验证

按照CA中心的规范，如果您申请了SSL证书，则必须完成域名验证（又称验证域名所有权）来证明待申请证书要绑定的域名属于您。

代理文件验证，是指授权证书管理服务从管理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。

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域名和单域名类型证书使用文件验证。

约束与限制

绑定域名是在天翼云本平台上申请的域名，且已使用天翼云云解析服务。

操作步骤

在用户当前购买的证书服务有效期内，只要满足以下前提条件，后续所有续订订单的域名验证环节将由系统自动完成，无需您进行任何操作：

- 域名所有权未发生变更。
- 服务器权限未变更，且已配置的授权信息持续有效。
- 用户未主动删除系统创建的验证记录或文件。

请您耐心等待系统进行代理文件验证。CA机构完成文件验证信息的审核后（约1个工作日）即可签发证书。

代理DNS验证

按照CA中心的规范，如果您申请了SSL证书，则必须完成域名验证（又称验证域名所有权）来证明待申请证书要绑定的域名属于您。

代理DNS验证，是指授权证书管理服务修改域名的DNS解析记录，自动在解析记录中添加一条用于验证的记录，无需您手动修改域名解析记录。CA机构添加的记录能被解析，则表示验证通过。

约束与限制

绑定域名是在天翼云本平台上申请的域名，且已使用天翼云云解析服务。

操作步骤

在用户当前购买的证书服务有效期内，只要满足以下前提条件，后续所有续订订单的域名验证环节将由系统自动完成，无需您进行任何操作：

- 域名所有权未发生变更。
- 域名解析服务商未变更，且已配置的授权信息持续有效。
- 用户未主动删除系统创建的验证记录或文件。

请您耐心等待系统进行代理DNS验证。DNS验证完成后，CA机构需要2~3个工作日对DNS验证信息进行审核，审核通过后，才会签发证书。

安装SSL证书

安装SSL证书至服务器

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。

前提条件

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。

下载正式证书

1. 登录证书管理服务控制台。
2. 在左侧导航栏选择“SSL证书管理 > SSL证书列表”。
3. 找到需要下载的证书，单击“操作”列的“证书下载”。

4. 根据您的服务器类型选择需要下载的证书，如果不确定，可以下载“ALL”。

下载测试证书

1. 登录证书管理服务控制台。
2. 在左侧导航栏选择“SSL证书管理 > SSL证书列表”。
3. 选择“测试证书”页签，找到需要下载的证书，单击“操作”列的“证书下载”。

4. 根据您的服务器类型选择需要下载的证书，如果不确定，可以下载“ALL”。

下载的证书文件说明

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	部署参考文档
Apache	Cert证书公钥：`XXXX.cn_cert.pemChain`证书链：`XXXX.cn_chain.pem`私钥文件：`XXXX.cn_key.key`	在Apache服务器部署SSL证书
Exchange	Cert证书公钥：`XXXX.cn_cert.pemChain`证书链：`XXXX.cn_chain.pem`私钥文件：`XXXX.cn_key.key`	在Exchange服务器部署SSL证书
GlassFish	Cert证书公钥：`XXXX.cn_cert.pemChain`证书链：`XXXX.cn_chain.pem`私钥文件：`XXXX.cn_key.key`	在GlassFish服务器部署SSL证书
IIS	PFX证书密码：`README.txt`PFX格式证书：`XXXX.cn.pfx`	在IIS服务器部署SSL证书
Nginx	Cert证书公钥：`XXXX.cn_cert_chain.pem`私钥文件：`XXXX.cn_key.key`	在Nginx服务器部署SSL证书
TOMCAT	JKS证书：`XXXX.cn.jks` JKS证书密码：`README.txt`	在TOMCAT服务器部署SSL证书

下载根证书

如果您的业务用户通过Java等客户端访问Web业务，您需要下载与服务端证书类型一致的根证书，并手动安装到对应的客户端，确保客户端与服务端建立HTTPS安全连接。

背景概述

根证书是建立信任链的基础。一旦客户端安装了根证书，它即可验证由该根证书签发的所有证书。这使得客户端可以信任与该根证书相关的所有服务器和应用程序，从而建立起一个完整的信任链。

- 如果您的业务用户通过浏览器访问您的Web业务，则您无需关注根证书和中间证书，因为根证书和中间证书已经内置在浏览器，您只需在Web服务器安装经CA签发的SSL证书，即可实现客户端与服务端的HTTPS通信。如何获取SSL证书（服务端证书），请参见 购买SSL证书 。
- 如果业务用户通过Java等客户端访问您的Web业务，由于客户端没有内置根证书和中间证书，您可能需要在对应客户端或者系统默认信任库手动安装根证书和中间证书，保证客户端能够校验服务端的加密信息。例如，服务端安装了标准版SSL证书，则客户端需要有标准版OV型根证书，才能实现客户端与服务端的HTTPS通信。

下载根证书

证书分类	下载根证书
标准版	国密标准： 国密版本根证书.zip
	国际标准： • 2025年4月3日之后签发： 国际版本根证书（20250403后）.zip • 2025年1月14日-2025年4月3日之间签发： 国际版本根证书（20250114-20250403）.zip • 2025年1月14日前签发： 国际版本根证书（旧）.zip
SecureSite GeoTrust TrustAsia	ECC算法： DigiCertGlobalRootG3_root.rar
	RSA算法： DigiCertGlobalRootG2_root.rar
GlobalSign	OV证书、EV证书： GlobalSign Root CA - R3.zip
	DV证书： GlobalSign Root CA - R6.zip
CFCA	国密标准： CFCA CS SM2 CA.zip
	国际标准： CFCA EV ROOT.zip
个人证书	国密标准： 个人证书根证书.zip

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。
3. （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。

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

   替换私钥文件，路径参考：SSLCertificateKeyFile/xxxx/server.key。
4. 重启apache2服务，即可完成证书导入。

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。

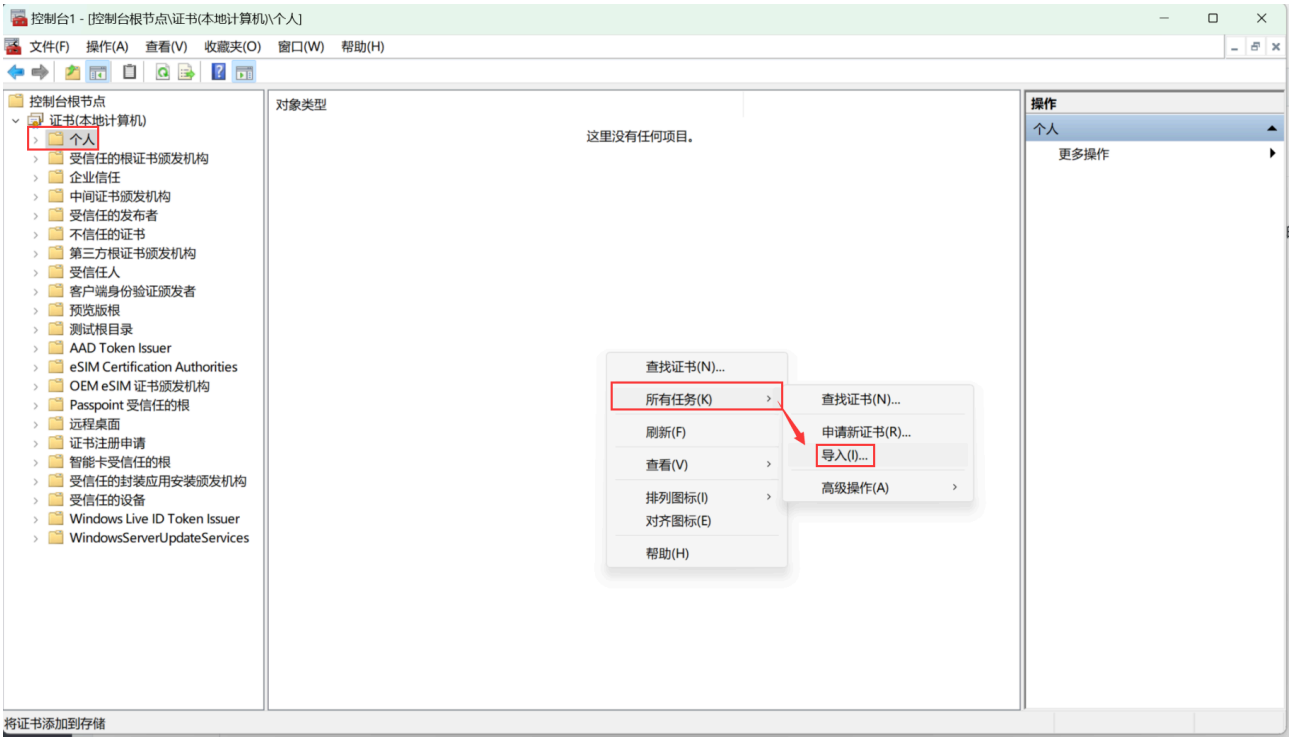
操作步骤

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”。

   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。
2. 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-ExchangeCertifcate

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’

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**

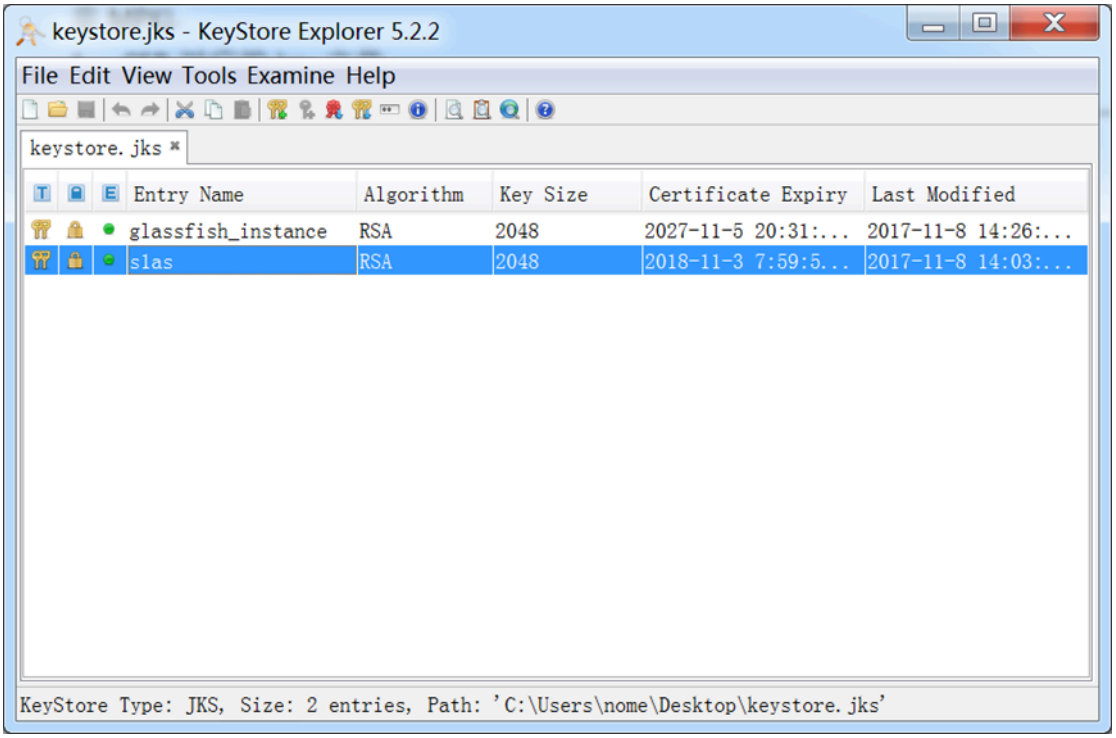
- 私钥文件： **XXXX.cn_key.key**

准备PFX文件

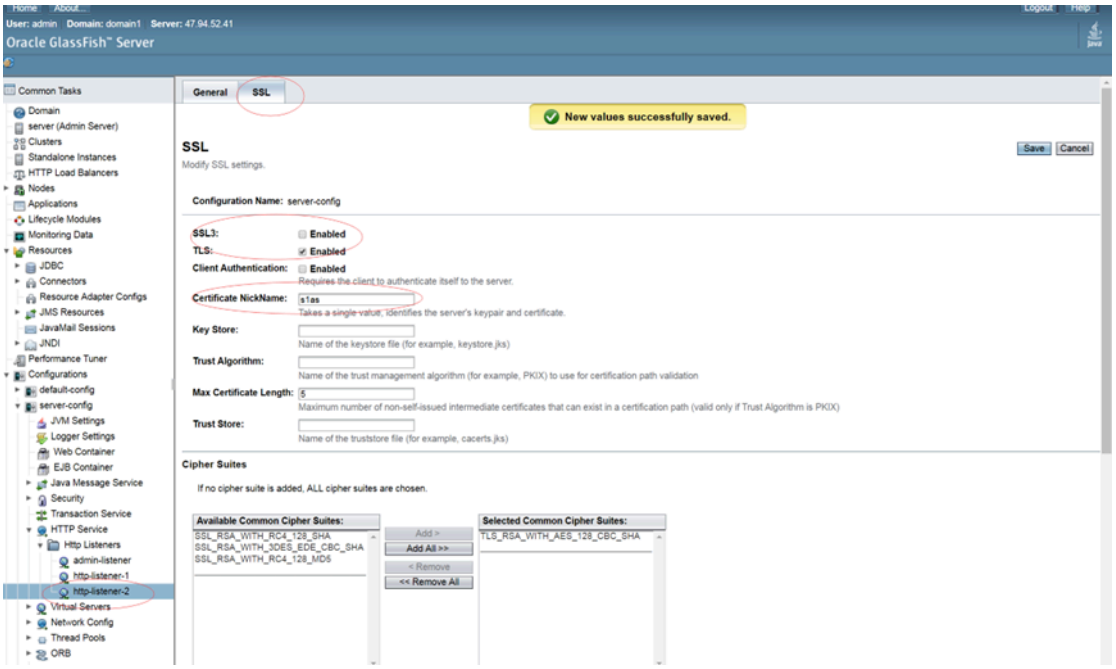
使用下载的“xxxx.cn_cert”证书文件和“xxxx.cn_key”私钥文件（生成CSR请求与之同时生成的key）通过openssl工具或 在线工具 生成一份PFX文件，请妥善保存好生成的PFX文件密码。

操作步骤

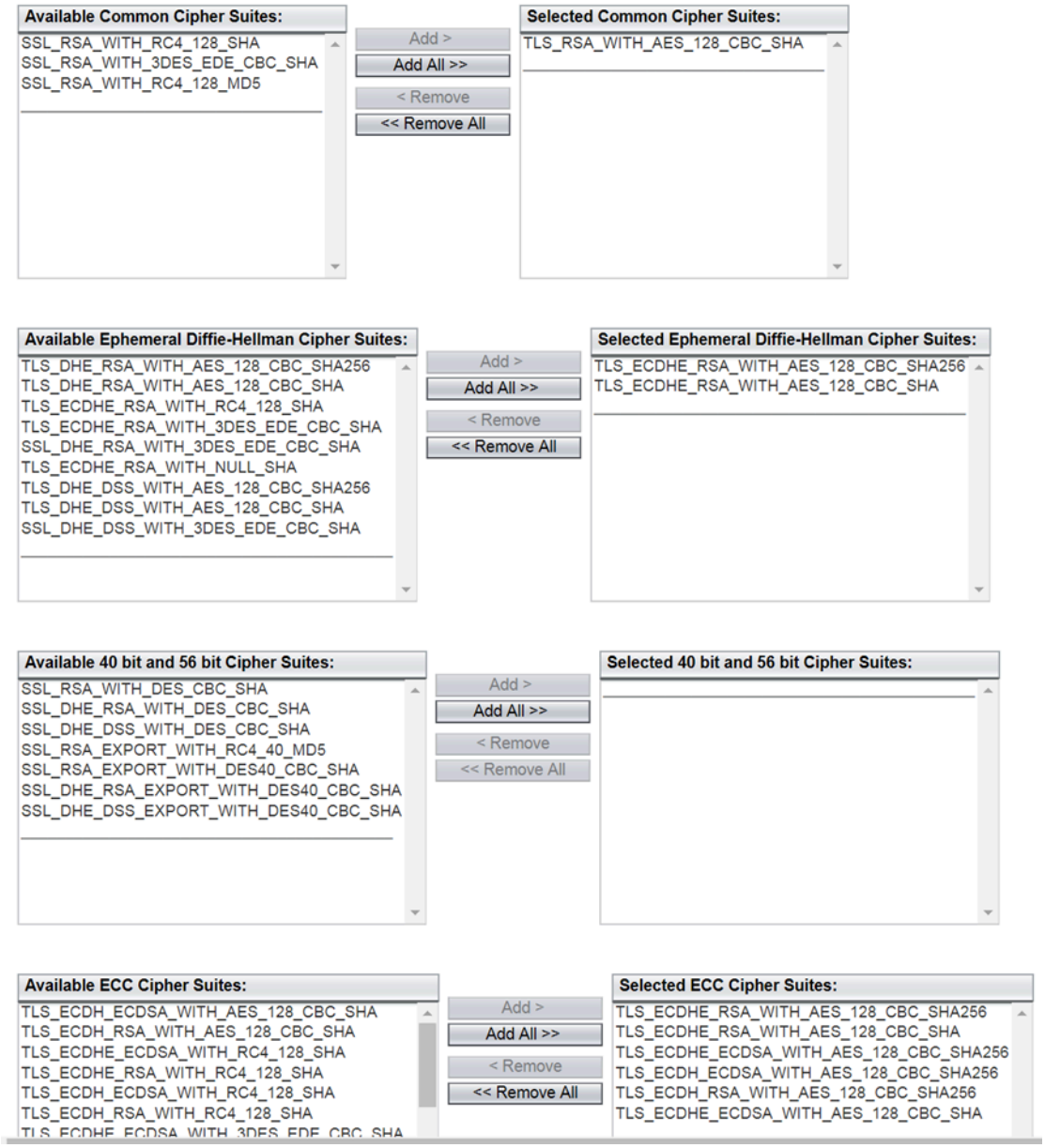
1. 在GlassFish的“/domain”目录下keystore中，保留“glassfish-instance”并生成jks文件。
2. 将上文中生成的PFX文件导入至jks中，重命名为：slas。如下图所示。



3. 参考下图，在GlassFish的web页中进行配置。



4. 关闭SSLv3。
5. 按照下图修改cipher_suit。



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” 。

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

1. 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。
2. 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; ##########
          ssl_certificate      /usr/nginxssl/server.crt; #####
          ssl_certificate_key  /usr/nginxssl/key.txt; #####

        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 / {                //  ##############
        #
                }
     }
```

3. 配置修改完成后，输入如下命令启用Nginx：

   start .\nginx.exe

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**

操作步骤

1. 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。
2. 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####1####jks###
keystorePass##jks#####
Port####
SSLEnable###ssl####
```

3. 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" />
```

一键部署SSL证书至天翼云服务

证书管理服务支持将已签发的证书一键部署至天翼云服务上，减少您去手动部署证书的相关操作，提升业务的便捷性。

约束条件

- 当前支持将证书一键部署到如下产品：

产品	说明	支持的证书
Web应用防火墙（原生版）	单次最多可部署5个资源。	国际证书
弹性负载均衡	仅支持部分资源池，请以控制台提示为准。 单次最多可部署5个资源。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。	国际证书
CDN相关产品	“CDN相关产品”服务为集成产品，一键部署证书将同时生效于其包含的 CDN、Aone边缘安全加速平台、Web应用防火墙（边缘云版）。 单次最多可部署5个资源。	国际证书、国密证书
综合安全网关	单次最多可部署5个资源。	国际证书、国密证书

- 若您使用的子账号进行一键部署，需要在IAM给相关子账号配置default企业项目权限。

部署“证书管理服务签发的证书”至天翼云服务

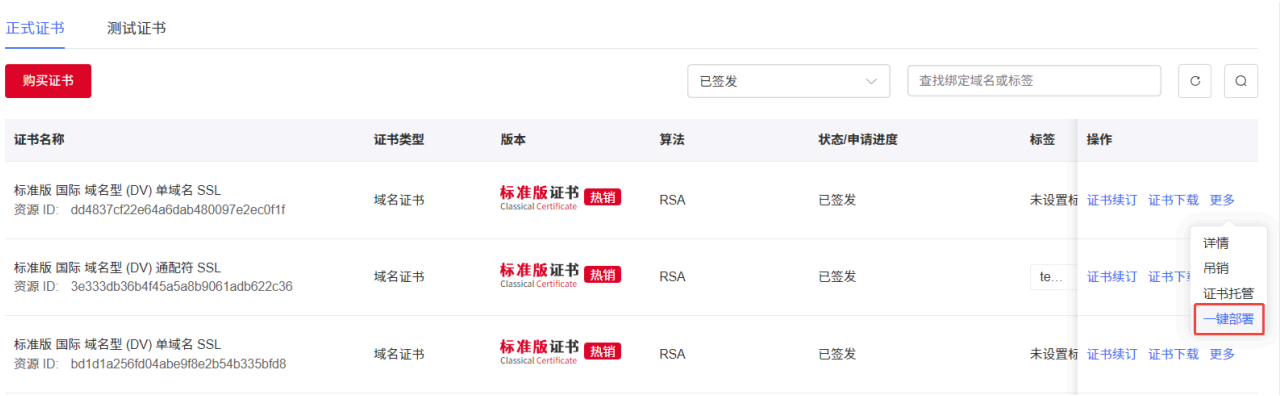
前提条件

已在证书管理服务中申请SSL证书且状态为“已签发”。

操作步骤

1. 登录“证书管理服务”控制台，在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入证书管理页面。
2. 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. 右侧弹出部署证书窗口，默认选择“证书详情”，在下方部署详情中选择需要部署证书的服务，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证书的资源（单次最多支持5个资源），单击“批量部署”。
- 部署至弹性负载均衡服务：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。
- 部署至CDN相关产品：
  - 需要先选择部署该证书的域名，请注意，部分域名可能因解析或配置原因未被列出。证书部署至CDN相关资源约需要5~10秒。在此期间，您可能会查到旧证书信息，请耐心等待。
  - 如果CDN相关产品账号不在白名单中，请您提交 工单 向CDN服务团队申请开通白名单或拨打服务热线（400-810-9889）与我们联系。
- 一键部署后的证书支持使用 证书托管 功能。

部署“第三方证书”至天翼云服务

前提条件

- 已将第三方证书上传至证书管理服务中且状态为“上传成功”。
- 已购买第三方证书部署服务配额，详细操作请参见 购买第三方证书部署服务 。

操作步骤

1. 登录“证书管理服务”控制台，在左侧导航栏选择“SSL证书管理 > 上传证书”。
2. 选择需要部署的证书，单击“操作”列的“ 一键部署”。

3. 右侧弹出部署证书窗口，默认选择“证书详情”，在下方部署详情中选择需要部署的服务，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证书的资源（单次最多支持5个资源），单击“批量部署”。
> - 部署至弹性负载均衡服务：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。
> - 部署至CDN相关产品：
>   - 需要先选择部署该证书的域名，请注意，部分域名可能因解析或配置原因未被列出。证书部署至CDN相关资源约需要5~10秒。在此期间，您可能会查到旧证书信息，请耐心等待。
>   - 如果CDN相关产品账号不在白名单中，请您提交 工单 向CDN服务团队申请开通白名单或拨打服务热线（400-810-9889）与我们联系。

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。回退成功则恢复成上一张证书。

SSL证书跨云一键部署

证书管理服务支持将证书管理服务签发的SSL证书一键跨云部署，减少手动操作步骤，提升业务的便捷性。

约束条件

- 只支持证书管理服务签发的证书，不支持第三方证书。
- 若您使用的子账号进行跨云部署，需要在IAM给相关子账号配置default企业项目权限。

跨云部署操作步骤

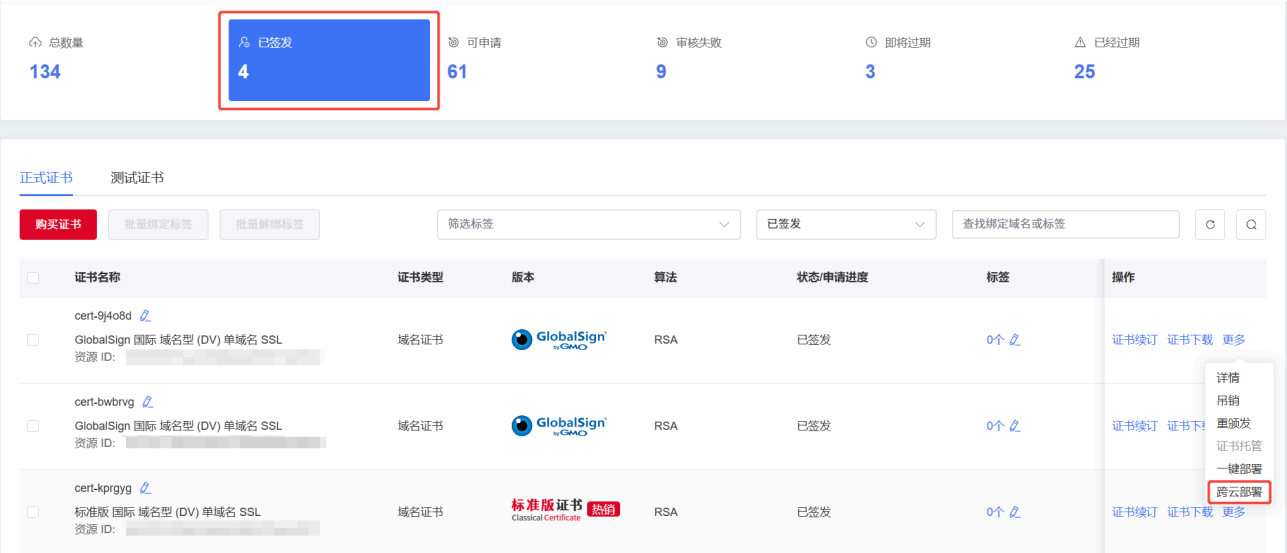
前提条件

已在证书管理服务中申请SSL证书且状态为“已签发”。

操作步骤

1. 登录 “证书管理服务”控制台 ，在左侧导航栏选择“SSL证书管理 > SSL证书列表”，进入证书管理页面。
2. 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 > 跨云部署”。



4. 在弹出的对话框中，根据证书部署的需求填写参数。

参数	说明
AK	AK（Access Key ID）：公开的访问密钥ID，用于标识用户身份。 选择已有的AK，若没有AK可单击右侧的“新增AK”，在弹出的对话框中新增AK。
资源	目前仅支持部署华为云弹性负载均衡。
资源池	选择所需部署资源所属的资源池，若您资源所在的资源池无法选择，请提交工单联系天翼云支撑。
项目	选择需要部署资源所属的华为云项目。

5. 选择需要部署证书的域名，单击“更新”即可完成证书部署。

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。

管理SSL证书

上传证书

您可以将线下的SSL证书（已在其他平台购买并签发的SSL证书）上传至证书管理服务控制台进行统一管理。

证书上传后，支持查看证书详情，上传后的证书支持一键部署到天翼云服务。

约束限制

- 不支持上传已过期的证书。
- 已上传的证书不支持重复上传。

前提条件

目前仅支持上传PEM格式的证书。若证书为其他格式，需要转换成PEM格式后才能上传，详细操作请参见 SSL证书格式转换 。

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证书管理 > 上传证书”。
3. 单击“上传证书”，页面右侧弹出上传证书窗口。

4. 在上传证书窗口中，选择证书标准、配置证书名称。

参数	说明
证书标准	支持上传“国际标准”和“国密标准”的证书。
证书名称	自定义证书的名称。 名称仅支持英文、数字、“.”、“_”、“-”，长度为2-15个字符。

5. 上传证书文件。

证书标准	需要上传的文件	格式说明	上传说明
国际标准	证书文件	证书里的PEM格式的文件（后缀名为“.pem”）	• 方式一：单击“上传”，直接上传满足需求的证书文件。 • 方式二：以文本方式打开待上传的证书文件，将证书内容复制到参数框。
	证书私钥	证书里的KEY格式的文件（后缀名为“.key”）	
	证书链	可选，若有则上传	

证书标准	需要上传的文件	格式说明	上传说明
国密标准	证书文件	证书里的签名证书文件（后缀名为“.pem”）	
	证书私钥	证书里的签名私钥文件（后缀名为“.key”）	
	加密证书	证书里的加密证书文件（后缀名为“.pem”）	
	加密私钥	证书里的加密私钥文件（后缀名为“.key”）	
	证书链	可选，若有则上传	

6. 填写完成后，单击“确认”。

   待证书状态为“上传成功”时，操作完成。

相关操作

证书上传后，支持一键部署到天翼云服务，详细操作请参见 一键部署SSL证书至天翼云服务 。

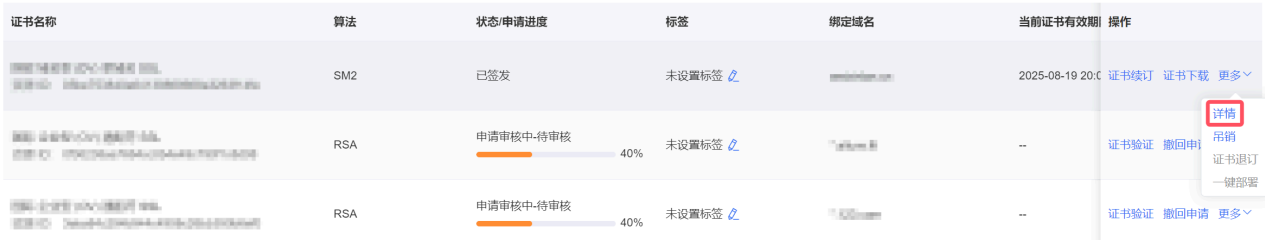
查看证书详情

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。

重颁发

操作场景

通常在下述场景下，需要重颁发证书：

- 密钥泄露或丢失：为了网站的安全，建议重颁发一张新证书。
- 域名删减：原有的证书将不再适用，需要重颁发证书以匹配新域名。
- 密钥算法升级：通过密钥算法升级，可优化安全性、性能、合规性，系统性地提升安全防护能力并优化资源效率。

约束限制

- 适用产品：SSL证书、私有（内网）证书
- 适用品牌：CFCA、GlobalSign、标准版、DigiCert（SecureSite、GeoTrust、TrustAsia）
- 适用算法：国际、国密
- 重颁发次数限制：单张证书在有效期内（199天 ）最多可申请3次重颁发，第3次申请后，重颁发按钮置灰。
- 重颁发后新证书的有效期：
  - CFCA、GlobalSign：原证书剩余时间，仅在证书到期前30天内重颁发时将获得199天续期证书。
  - 标准版、DigiCert（SecureSite、GeoTrust、TrustAsia）：199天。

操作步骤

1. 登录 证书管理服务控制台 。
2. 选择“SSL证书管理 > SSL证书列表”或“私有证书管理 > 私有证书列表”。
3. 选择需要进行重颁发的证书，单击“操作”列的“重颁发”。
4. 填写证书申请的相关信息。

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）。只可删减其他域名。
密钥算法	可选择“RSA”、“ECC”或“SM2”。
证书请求文件	CSR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）获取证书。 支持“系统生成”或“手动生成”两种方式： • 系统生成：根据用户所配置的信息，系统自动生成一个CSR。为保障您的证书顺利申请，建议您使用系统生成CSR的方式，避免因内容不正确而导致的审核失败。 • 手动生成：在下拉框中选择已手动创建的CSR，使用已创建的CSR申请证书。 注意 - 请不要在证书签发完成前删除CSR。 - 手动生成将无法署到天翼云产品。
私钥文件	填写您的CSR私钥。 您可以单击“上传”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，或者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。

5. 单击“确定”，提交申请。

   证书状态更新为“申请审核中-重颁发”。申请通过后，证书状态将更新为“已签发”。

   新证书签发后，原证书吊销说明：

品牌	是否吊销	吊销说明
CFCA	是	原证书将在3天内吊销。
GlobalSign	否	原证书与新证书可同时使用。
标准版、DigiCert（SecureSite、GeoTrust、TrustAsia）	-	• 吊销的场景：仅当申请重颁发时删减域名，原证书将在新证书签发3 天后吊销。 • 不吊销的场景：其他场景不吊销原证书。

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。

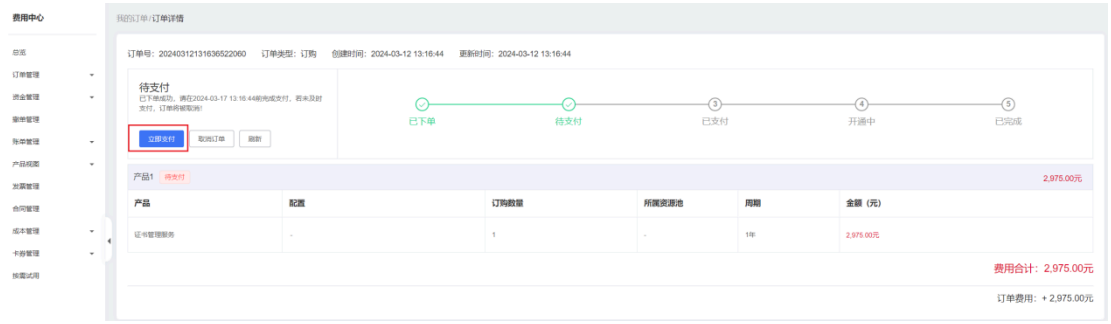
续订证书操作步骤

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”。



自动续订操作步骤

1.进入证书管理服务，选择“SSL证书管理”>“SSL证书列表”。

2.选择需要开启自动续订功能的证书，将“开启自动续费”开关调整至 

状态，即可开始自动续费功能。

说明

- 自动续费生效后，会在您证书到期前30个自然日为您自动续费；若您在到期30个自然日前开启自动续费功能，则不会为您自动续费，请您注意。
- 新生成的订单和您旧证书的订单信息保持一致。例如：您购买3年期的企业型（OV）单域名证书，会在到期前30个自然日自动续费3年期的企业型（OV）单域名证书。
- 自动续费生成的证书会为您自动提交申请，但是需要您完成域名验证后才会签发（OV、EV证书还需完成组织验证），后续操作可参考： 申请SSL证书 。

托管证书

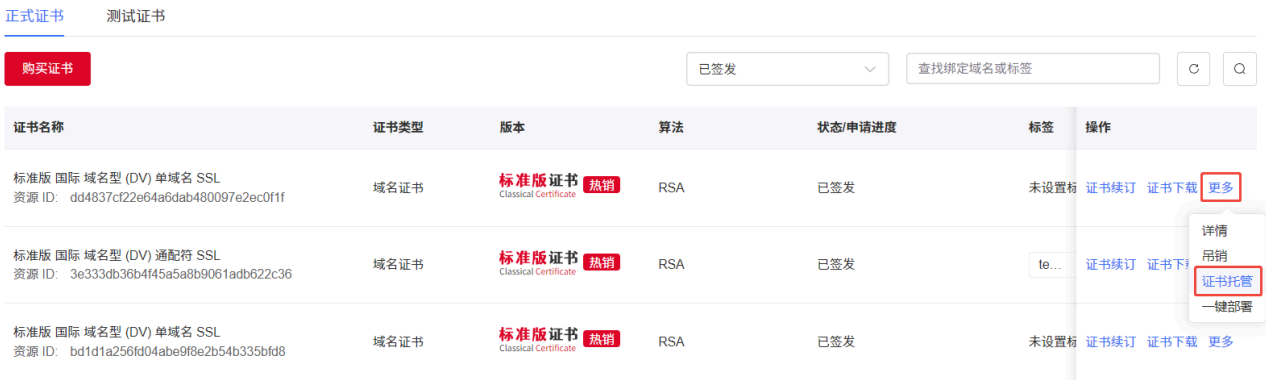
证书托管功能支持您自动替换天翼云上云产品证书的能力。

约束限制

- 仅支持 一键部署“证书管理服务签发的证书”至天翼云服务 的证书使用此功能。
- 一年期证书需开启 自动续费 功能才可使用托管功能。
- 多年期证书需要自动续期次数≥1次才可使用托管功能，若剩余续期次数为0则需要开启 自动续费 功能。

操作步骤

1. 登录 证书管理服务控制台 。
2. 选择需要进行托管的证书，选择“操作”列的“更多 > 证书托管”。



3. 在“证书托管”窗口，选择需要托管的服务及证书，将开关调整至开启状态，即表示已经开启了证书托管能力。

验证域名

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. 选择需要进行域名验证（“状态/申请进度”为“申请审核中-待域名验证”）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. 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。

a. 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 。
b. 在需要添加DNS解析记录的域名记录操作列，单击“解析设置”。
c. 在添加记录面板，将域名认证获取到的验证信息进行添加，填写规则参见下表。

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优先级	-
TTL	选择默认值，不作修改。

d. 单击“√”完成记录添加。

2. 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。

升级测试证书为正式证书

您可以随时在控制台将测试证书升级为正式证书。

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证书管理 > SSL证书列表”。
3. 选择“测试证书”页签，在待升级的证书操作列，单击“证书升级”。

4. 进入证书升级页面，配置证书相关参数，详细信息请参见 购买SSL证书 。

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。

> 注意
>
> 已签发的证书成功吊销后，若吊销时间距签发时间未超过28个自然日，支持重新申请证书，有且仅有一次重新申请的机会。

前提条件

仅支持状态为“已签发”状态的证书吊销。

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。

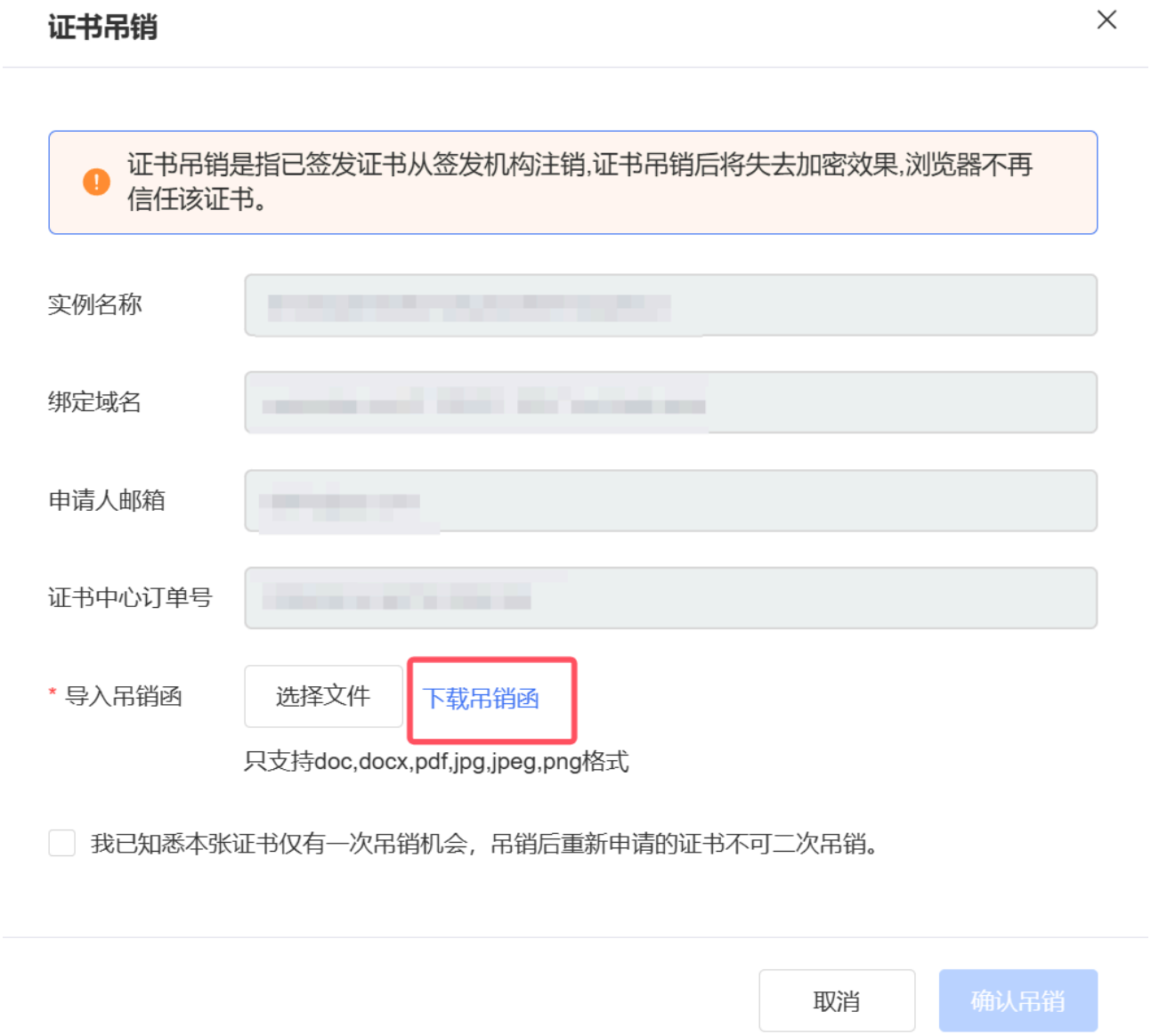
3. 确认证书仅有一次吊销机会后，勾选确认框。

4. 确认无误后，单击“确认吊销”，完成证书吊销操作。

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 > 吊销”。

2. 在弹出的窗口中确认吊销信息，确认完毕后单击“下载吊销函”。



3. 确认吊销函的内容后，填写相关信息并且上传。

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. 确认证书仅有一次吊销机会后，勾选确认框。

5. 单击“确认吊销”，完成证书吊销操作。

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。

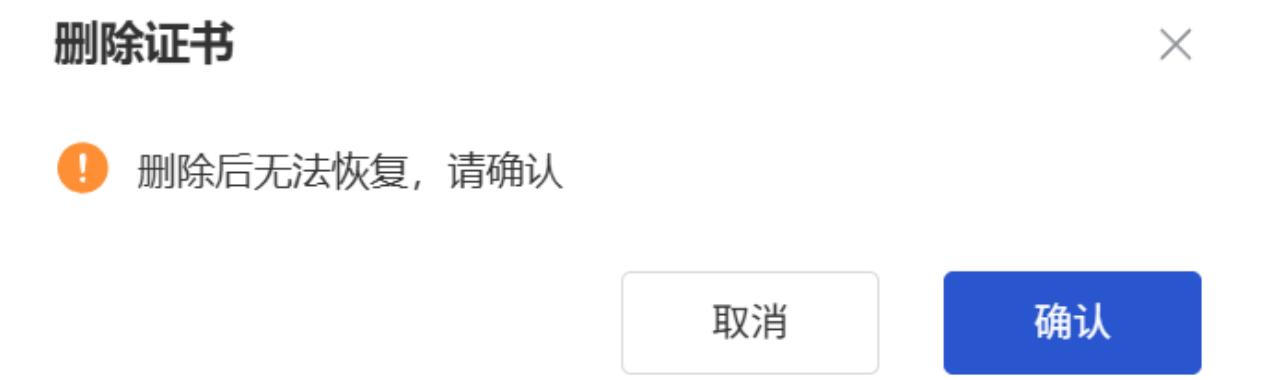
前提条件

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。



管理标签

标签是对实例的标识。基于标签，您可以实现对实例的便捷搜索和整理。 标签由键值对（Key-Value）组成，您可以为实例绑定和解绑标签，在控制台中通过标签快速查找实例。

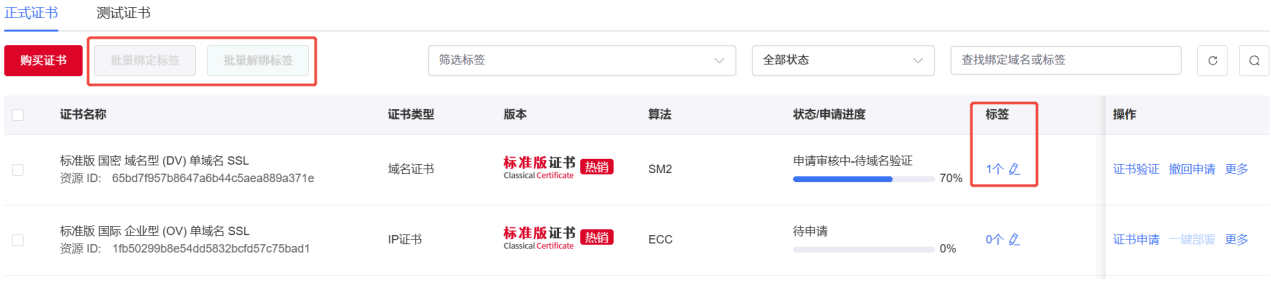
约束限制

- 每个实例最多可绑定50个标签。
- 每个实例下的标签键是唯一的，不可绑定相同标签键。
- 不支持修改标签，支持解绑标签后，绑定新的标签。

绑定标签

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全管理 > 证书管理服务”，进入“SSL证书列表”页面。
4. 选择需要添加标签的实例，单击“标签”列的 。

   支持批量绑定：勾选多个实例，在实例列表上方，单击“批量绑定标签”，为多个实例批量绑定标签。



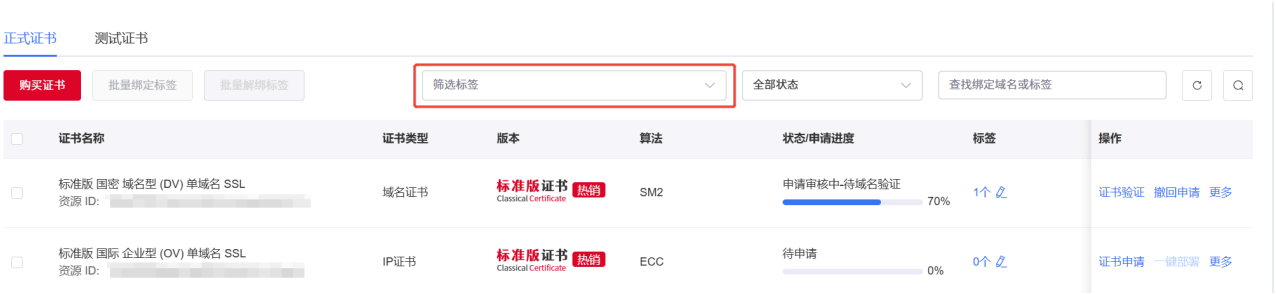
5. “编辑标签”弹窗中，填写标签键和值。

   方式一：在输入框中输入新的标签键和值，新增标签。

   方式二：下拉选择已有标签。
6. 配置完成后，单击“确定”，绑定标签完成。
7. 标签绑定成功后，鼠标点击实例信息的“标签”数量，可查询标签绑定情况。

使用标签筛选实例

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全管理 > 证书管理服务”，进入“SSL证书列表”页面。
4. 单击“筛选标签”。



5. 在“筛选标签”弹窗中，填写标签。
6. 单击“确定”，执行筛选标签操作，列表将展示标签筛选结果。筛选结果返回包含所选择的多项键值的实例。

解绑标签

1. 登录天翼云控制中心。
2. 单击页面顶部的区域选择框，选择区域。
3. 在产品服务列表页，选择“安全管理 > 证书管理服务”，进入“SSL证书列表”页面。
4. 选择需要解绑标签的实例，单击“标签”列的  。

   支持批量解绑：勾选多个实例，在实例列表上方，单击“批量解绑标签”，为多个实例批量解绑标签。
5. 在“编辑标签”弹窗中，单击目标标签操作列的“删除”。

6. 单击“确定”，解绑标签完成。

CSR管理

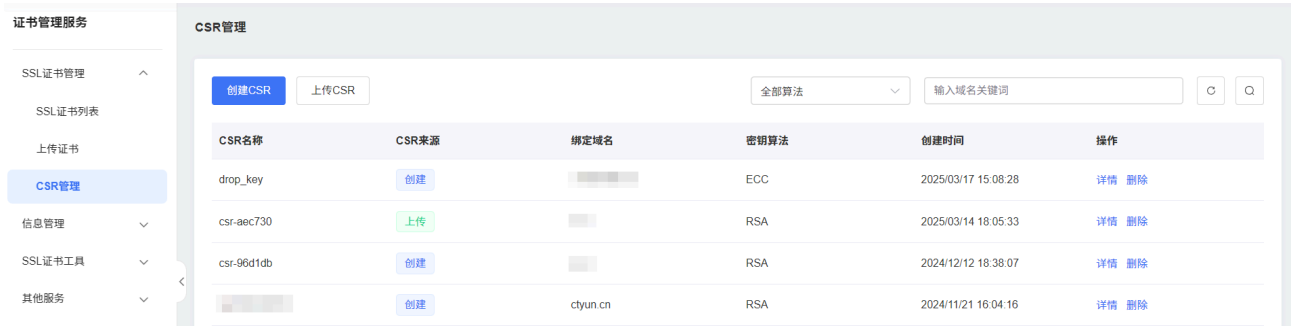
创建CSR

什么是CSR?

CSR（证书签名请求，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. 登录 证书管理服务控制台 。
2. 在左侧导航栏，选择“SSL证书管理 > CSR管理”，进入“CSR管理”页面。



3. 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名称仅支持英文大小写、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。

参数	参数说明
联系人	选择CSR联系人，创建联系人请参考 联系人管理 章节。
公司	选择CSR所属的公司，创建公司请参考 公司管理 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：256、384、521 • SM2支持：256

4. 填写完成后，单击“生成CSR”完成CSR创建。

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. 登录 证书管理服务控制台 。
2. 在左侧导航栏，选择“SSL证书管理 > CSR管理”，进入“CSR管理”页面。
3. 单击“上传CSR”，填写上传信息。

参数	说明
CSR名称	填写您的CSR名称，CSR名称仅支持字母大小写、数字、“.”、“_”、“-”，长度为2-15个字符。
CSR文件内容	填写您的CSR文件内容。 您可以单击“上传”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，或者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。
私钥内容	填写您的CSR私钥。您可以单击“上传”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，或者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。

4. 单击“确认”，完成CSR上传。

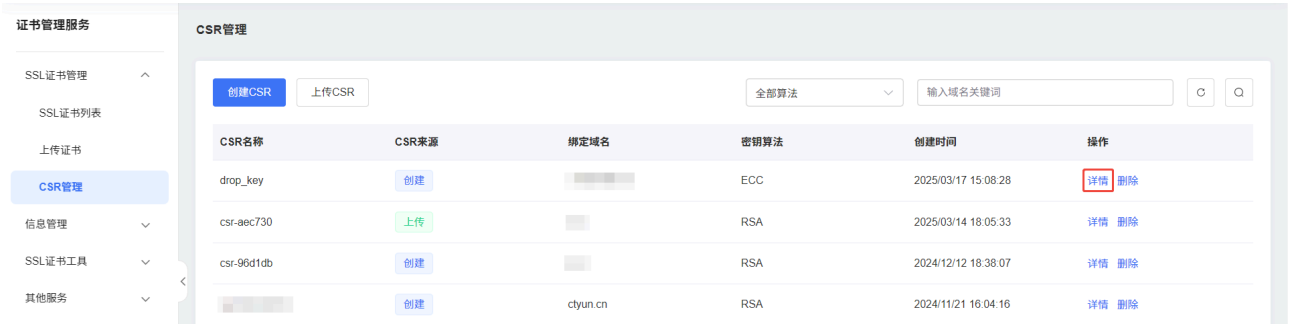
   完成以上操作后，您可以在CSR列表查看已上传的CSR。

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。



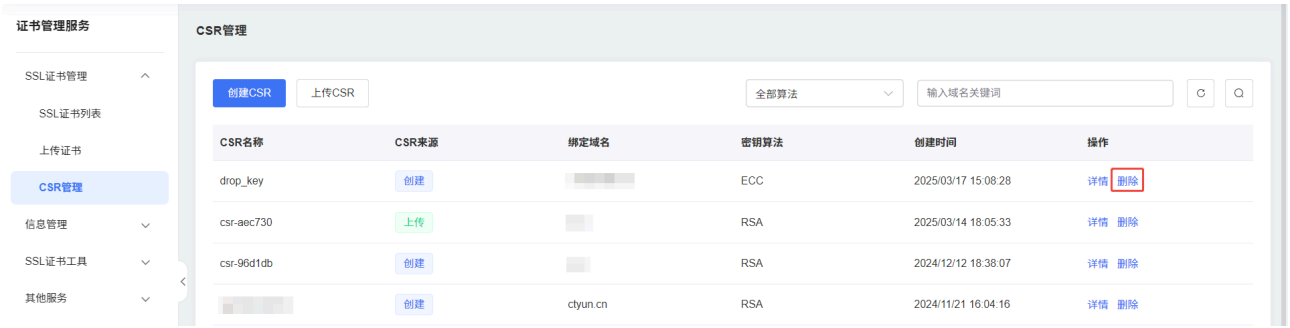
删除CSR

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。



域名监控服务

域名监控概述

应用场景

开启域名监控后，可帮助用户监测多个站点的HTTPS业务状态，及时发现站点上的SSL证书安全问题，方便统一维护多站点HTTPS。

说明

- 每个用户免费拥有1个域名监控配额，您可以通过该配额体验域名监控服务，具体操作请参见 添加域名 。
- 若需要持续监控多个域名，您可以购买更多配额，具体操作请参见 购买域名监控服务 。

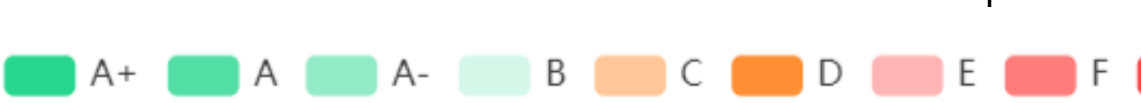
功能优势

- 域名监控服务操作简单，无需花费大量时间和精力维护已有证书。
- 支持证书到期预警，不用担心证书到期而影响业务。

配额及有效期说明

- 每添加1个域名，消耗1个域名监控配额。添加域名后有效期为365天，“监控剩余天数”从添加域名成功后开始计时。
- 每续期1个配额，消耗1个域名监控配额。每个配额可续期365天，续期的天数将累加至原“监控剩余天数”。

监控指标

监控指标	说明
证书到期预警	按证书到期时间统计域名证书： • 已到期证书 • 到期时间<=30天 • 到期时间>30天 • 证书未知：统计未绑定证书的域名、域名信息配置错误的域名数量。
SSL漏洞扫描	支持统计如下类型的漏洞： • 高风险漏洞 • 中风险漏洞 • 低风险漏洞
合规检测	统计ATS和PCI DSS合规情况： • ATS（应用程序安全传输，App Transport Security）为Apple ATS规范，是苹果在iOS 9中首次推出的隐私安全保护功能。从2017年1月1日起，所有提交到App Store的App必须强制开启ATS。启用ATS后，它会屏蔽明文HTTP资源加载，强制App通过HTTPS连接网络服务，对传输数据进行加密，保障用户数据安全。 • PCI DSS（支付卡协会数据安全标准，Payment Card Industry Data Security Standard）为支付卡行业安全标准，是目前广受国际认可的数据安全标准。PCI DSS要求在开放的公共网络上传输持卡人数据，需使用高强度加密算法对数据进行保护。
域名安全等级分布	共支持如下9个等级，A+为最高级。 

购买域名监控服务

操作场景

当域名监控服务配额不足时，请参照本文进行购买。

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证书管理 > 域名监控服务”，单击“购买域名监控”，进入到证书管理服务产品购买页面。
3. 服务类型选择“域名监控服务”。

4. 选择域名监控服务的购买数量，单次最多可购买100个。
5. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，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”，完成域名监控服务的购买。

后续操作

购买域名监控服务配额后，即可添加域名对域名进行监控，详细操作请参见 添加域名 。

添加域名

域名监控可帮助监测多个站点的HTTPS业务状态，并及时发现站点上的SSL证书安全问题，方便统一维护多站点HTTPS。

说明

- 每个用户免费拥有1个域名监控配额，您可以通过该配额体验域名监控服务。
- 若需要持续监控多个域名，您可以购买更多配额，具体操作请参见 购买域名监控服务 。

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证书管理 > 域名监控服务”。
3. 在域名列表上方，单击“添加域名”。

4. 在右侧弹出的“添加域名”窗口中根据提示配置参数。

参数说明如下：

参数	说明
当前可监控	显示当前剩余监控域名数量。如果配额不足，单击“前往扩容”可进行购买。
域名/IP	填写需要被监控的域名或IP地址。单次只能输入一个域名或IP。 注意 添加域名后，域名或IP地址不支持修改，请确保配置的域名或IP地址正确且有效。
端口	端口号，默认为443。
开启监控	添加域名时，监控开关默认开启。开启监控后，将对域名所使用证书的状态和有效期进行持续监控。

5. 配置完成后，单击“确定”。

   添加完成后，将立即对域名进行扫描，“状态”为“扫描中”。添加域名后有效期为365天，“监控剩余天数”从添加域名成功后开始计时。

后续操作

待扫描完成后，域名状态变为“正常”，可查看监控详情，详细操作请参见 查看监控数据 。

查看监控数据

域名监控页面和监控详情页均展示最新的监控数据，若域名监控处于“未开启”状态，则监控详情页展示关闭前最后一次扫描结果。

查看监控列表

1. 登录 证书管理服务控制台 。
2. 在左侧导航栏选择“SSL证书管理 > 域名监控服务”。
3. 查看已经添加的域名监控列表。

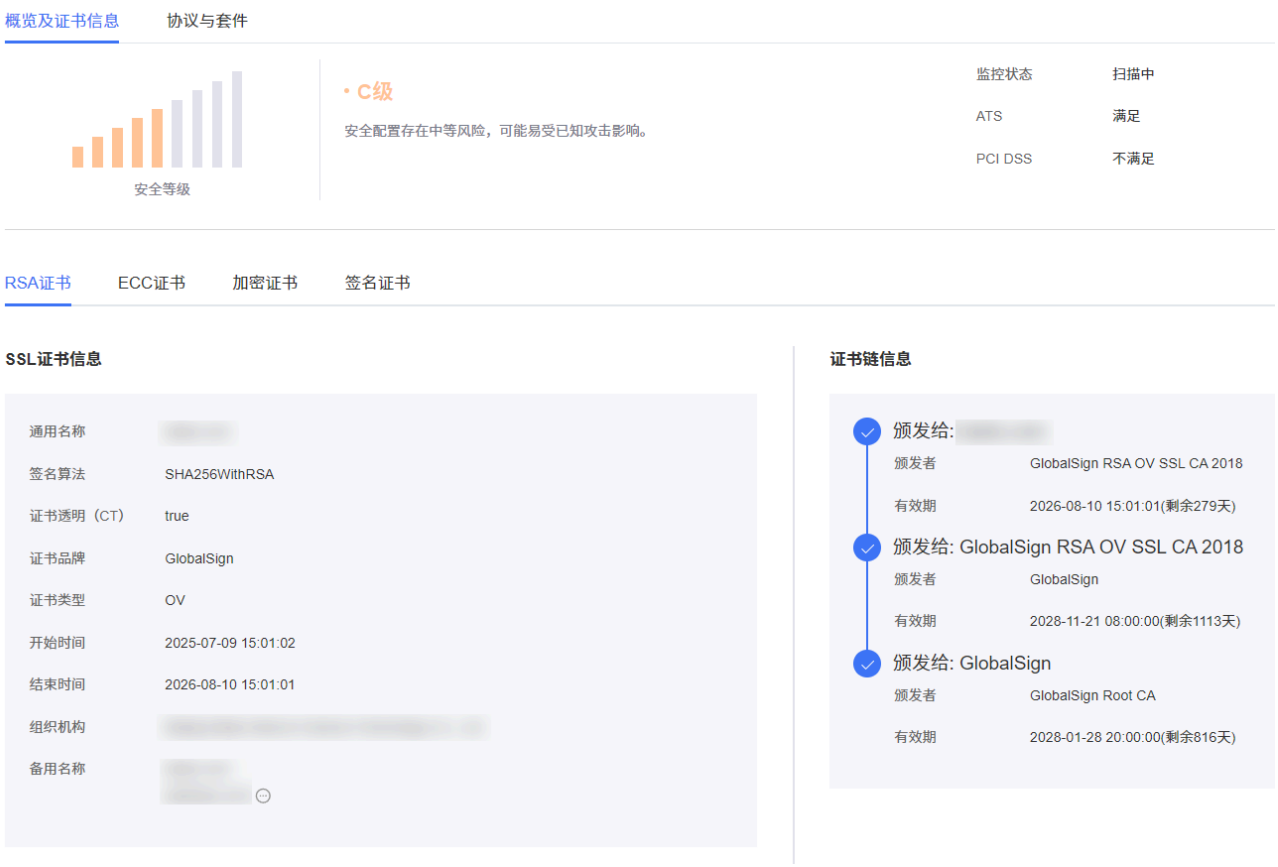
参数	说明
绑定域名/IP	已添加至域名监控列表的域名或IP地址。
状态	域名监控状态： • 扫描中：已成功添加域名，正在对域名进行扫描。 • 正常：域名监控状态正常。 • 失败：可能由于网络波动或域名填写有误，造成扫描失败。建议检查域名信息和网络连接后，尝试重新扫描。 • 未开启：未开启域名监控，单击“监控”列的开关可以随时开启域名监控。
证书品牌	域名绑定的证书的版本。例如：标准版、SecureSite、GeoTrust、GlobalSign、CFCA、TrustAsia等。
证书类型	域名绑定的证书的种类。包括DV、OV、EV。
证书到期时间	域名绑定的证书的到期时间。
安全等级	共支持如下9个等级，A+为最高级。 
监控剩余天数	域名监控的剩余天数。 • 域名监控服务有效期为365天，从添加域名成功后开始计时，关闭域名监控功能，计时不会停止。 • “监控剩余天数”不充足时，可单击“续期”延长使用时长，详细操作请参见 延长监控剩余天数 。
监控频率	域名监控频率，默认为30分钟，即每30分钟会自动扫描一次。
端口	监控域名的端口。
监控	可随时开启监控或关闭监控。详细操作请参见 开启/关闭域名监控 。

查看监控详情

1. 登录 证书管理服务控制台 。
2. 在左侧导航栏选择“SSL证书管理 > 域名监控服务”。

3. 在域名监控列表找到需要查看监控数据的域名，单击操作列的“监控详情”。

4. 查看详细监控数据。



监控数据说明如下：

分类	参数	说明
概览	安全等级	域名安全评级。
	监控状态	• 扫描中 • 正常
	ATS	• 满足 • 不满足
	PCI DSS	• 满足 • 不满足

分类	参数	说明
证书信息	SSL证书信息	• 通用名称：当前SSL证书的通用名称。 • 签名算法：当前SSL证书使用的签名算法。 • 证书透明（CT）：当前证书签发行为是否透明公开。true表示公开。 • 证书品牌：当前SSL证书的版本。包括标准版、SecureSite、GeoTrust、GlobalSign、CFCA、TrustAsia。 • 证书类型：当前SSL证书的种类。包括DV、OV、EV。 • 开始时间：当前SSL证书签发时间。 • 结束时间：当前SSL证书到期时间。 • 组织机构：组织名称。 • 备用名称：当前SSL证书的备用名称。
	证书链信息	• 颁发给：需要颁发证书的域名。 • 颁发者：SSL证书的颁发机构名称。 • 有效期：证书有效期。
协议与套件	协议	展示TLS协议类型的支持情况。
	SSL漏洞检测	展示SSL漏洞检测信息。
	套件	展示支持的加密套件详情。

延长监控剩余天数

监控剩余天数不充足时，可对域名监控服务进行“续期”，延长使用时长。

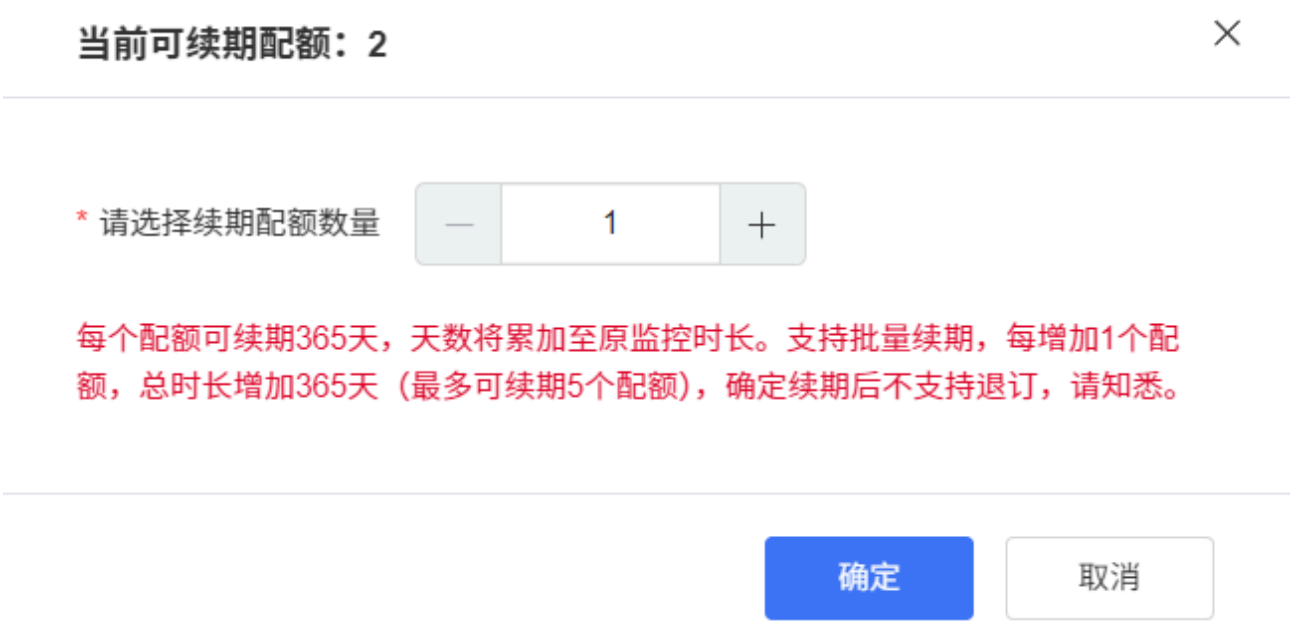
注意事项

续期后不支持退订，请充分评估业务需求后再进行操作。

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证书管理 > 域名监控服务”。
3. 在域名监控列表找到需要续期的域名，单击剩余天数列的“续期”。

4. 在弹出的对话框中，选择续期配额数量。
   - 单次最多续期5个配额。
   - 每个配额可续期365天，续期的天数将累加至原“监控剩余天数”。



5. 配置完成后，单击“确定”，完成操作。

管理域名监控服务

开启/关闭域名监控

1. 登录 证书管理服务控制台 。
2. 在左侧导航栏选择“SSL证书管理 > 域名监控服务”。
3. 在域名监控列表找到需要修改监控状态的域名，单击“监控”列的开关。

4. 在弹出的提示框中，单击“确定”，完成操作。
   - 关闭监控后，监控状态变为“未开启”。

     注意

     “监控剩余天数”从添加域名成功后开始计时，关闭域名监控功能，计时不会停止。
   - 重新开启监控，立即对域名进行扫描，监控状态变为“扫描中”。

删除域名监控

若不需要对域名的证书使用情况进行监控了，可随时在域名监控服务页面删除域名。域名监控开启或关闭状态都可以对其进行删除操作。

注意

在配额有效期内删除域名监控，配额也不会释放，请谨慎操作。

1. 登录 证书管理服务控制台 。
2. 在左侧导航栏选择“SSL证书管理 > 域名监控服务”。

3. 在域名监控列表找到需要删除的域名，单击操作列的“删除”。

4. 在弹出的提示框中，单击“确定”，完成操作。

个人证书

申请个人证书

个人证书是由CA机构核验身份后颁发的数字凭证，用于强身份认证、电子签名和加密通信等场景，1-2个工作日签发证书。

成功购买个人证书后，您需要申请证书，即提交证书申请人的详细信息审核。所有信息通过审核后，证书颁发机构才签发证书。

在申请证书时，您可以参考 SSL证书申请常见问题 。

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”，如何购买证书请参考： 购买个人证书 。

准备工作

申请个人证书时，需要在人工验证阶段上传证书申请表，您可以提前下载个人证书申请表模版，申请表需填写个人签名和日期。

服务类型	加密标准	下载审核材料模板
个人证书	国密标准	个人证书申请表模版.xlsx

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“个人证书管理 > 个人证书列表”。
3. 选择需要申请的个人证书，单击“操作”列的“证书申请”按钮，开始申请个人证书。

4. 在右侧弹出的窗口中填写联系人信息。

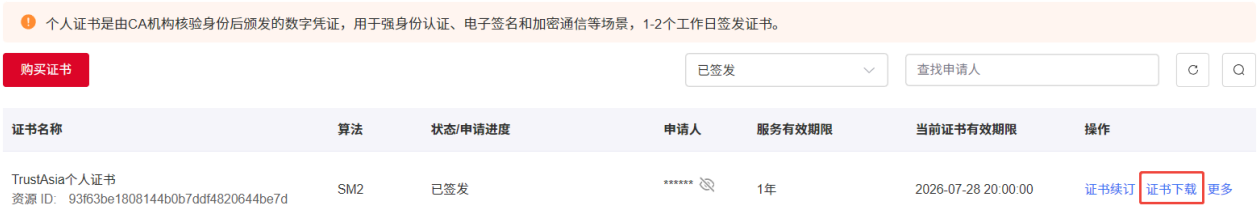
说明

目前个人证书仅支持国密算法。

5. 填写完后，单击“确定”，进入验证环节，根据页面提示填写申请表并上传。
6. 上传完成后，等待CA签发机构完成验证，若验证通过则可以在控制台下载个人证书。

下载个人证书

1. 登录证书管理服务控制台。
2. 在左侧导航栏选择“个人证书管理 > 个人证书列表”。
3. 找到需要下载的证书，单击“操作”列的“证书下载”。

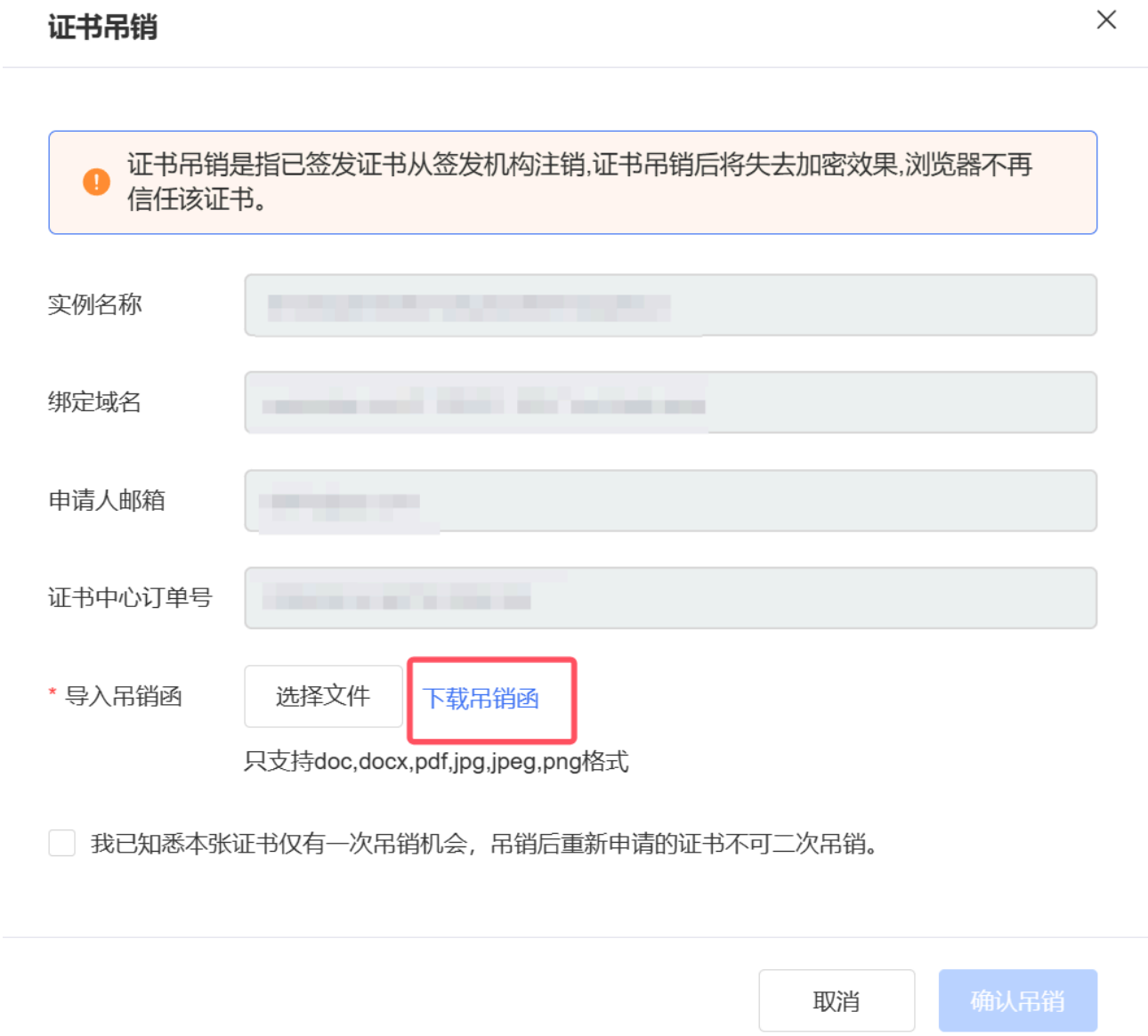


4. 根据您的服务器类型选择需要下载的证书，如果不确定，可以下载“ALL”。

吊销个人证书

1. 登录证书管理服务控制台。
2. 在左侧导航栏选择“个人证书管理 > 个人证书列表”。
3. 选择需要吊销的个人证书，选择“操作”列的“更多 > 吊销”。

4. 在弹出的窗口中确认吊销信息，确认完毕后单击“下载吊销函”。



5. 确认吊销函的内容后，填写相关信息并且上传。

> 注意
>
> 吊销函须确认信息无误并签字保存。

6. 确认证书仅有一次吊销机会后，勾选确认框。

7. 单击“确认吊销”，完成证书吊销操作。

私有（内网）证书

申请私有（内网）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

已成功购买私有（内网）证书并且在控制台的“证书状态”为“待申请”。如何购买私有（内网）证书请参考： 购买私有（内网）证书 。

准备工作

申请私有（内网）证书时，需要在人工验证阶段上传证书申请表，您可以提前下载私有（内网）证书申请表模版，申请表需经办人签字并加盖公章。

服务类型	证书版本	证书种类	加密标准	下载审核材料模板
私有（内网）证书	标准版	OV	国际标准、国密标准	私有（内网）证书申请表模版.xlsx

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“私有证书管理 > 私有证书列表”。
3. 选择待申请的证书，单击“操作”列的“证书申请”按钮，进行私有（内网）证书申请。
4. 在右侧弹出的窗口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）。 注意 在申请单域名规格证书时： • 所填域名不含www时，填写主域名，系统赠送域名：www.主域名。 例如，填写ctyun.cn（主域名），系统赠送域名：www.ctyun.cn；填写二级及以上子域名，系统不赠送域名。 • 所填域名含www时，填写www域名，系统赠送上一级域名。 例如，填写www.a.ctyun.cn，系统赠送域名：a.ctyun.cn。
联系人	选择联系人，如何新建联系人请参考 联系人管理 章节。
公司	选择公司，如何新建公司请参考 公司管理 章节。
所在地	选择公司实际所在地区。（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	CSR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。 支持“系统生成”或“手动生成”两种方式： • 系统生成：根据用户所配置的信息，系统自动生成一个CSR。为保障您的证书顺利申请，建议您使用系统生成CSR的方式，避免因内容不正确而导致的审核失败。 • 手动生成：在下拉框中选择已手动创建的CSR，使用已创建的CSR申请证书。 注意 - 请不要在证书签发完成前删除CSR。 - 手动生成将无法署到天翼云产品。

5. 填写完后，单击“提交审核”，进入验证环节，根据页面提示填写证书申请表并上传。
6. 上传完成后，等待CA签发机构完成验证，若验证通过则可以在控制台下载私有（内网）证书。

续订私有（内网）证书

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。

手动续订

1. 登录证书管理服务控制台。
2. 在左侧导航栏，选择“私有证书管理 > 私有证书列表”。
3. 在待续费证书的“操作”列单击“证书续订”。
4. 在跳转的页面中确认续订证书的信息，选择证书有效期。

5. 阅读并同意天翼云证书管理服务的服务协议和服务等级协议后，单击“立即购买”。

自动续订

1. 登录证书管理服务控制台。
2. 在左侧导航栏，选择“私有证书管理 > 私有证书列表”。

3. 选择需要开启自动续订功能的证书，将“开启自动续费”开关调整至 

状态，即可开始自动续费功能。

说明

- 自动续费生效后，会在您证书到期前30个自然日为您自动续费；若您在到期30个自然日前开启自动续费功能，则不会为您自动续费，请您注意。
- 新生成的订单和您旧证书的订单信息保持一致。例如：您购买3年期的企业型（OV）单域名证书，会在到期前30个自然日自动续费3年期的企业型（OV）单域名证书。
- 自动续费生成的证书会为您自动提交申请，但是需要您手动提交确认函和解析记录后才会签发，后续操作可参考： 申请私有（内网）证书 。

管理私有（内网）证书

私有（内网）证书的管理操作与SSL证书的管理操作一致，请参见 管理SSL证书 。

信息管理

消息管理

在您成功购买证书后，可在消息管理界面设置对应证书的消息通知模式及内容，以便您能及时得知证书的状态信息。

配置消息通知

说明

天翼云签发的证书将默认开启消息提醒策略，您可以为每类消息设置接收人，天翼云证书管理服务不会将接收人信息对外披露或向第三方提供。

1. 登录“证书管理服务”控制台，在左侧导航栏选择“信息管理 > 消息管理”，进入“消息管理页面”。

   消息管理页面展示证书资源ID、绑定域名、证书状态、通知方式、提醒内容及通知开关。

2. 选择需要编辑消息通知的证书资源ID，单击“操作”列的“编辑”按钮。
3. 在右侧弹出的对话框中，编辑证书通知信息。


编辑消息提醒
基础信息
证书名称
国际标准企业型 (OV) 通配符SSL证书
资源ID
证书状态
待申请
绑定域名
--
到期时间
--
详细配置
* 提醒开关
* 联系人
新建联系人
管理联系人
可输入关键字搜索
* 提醒方式
邮件提醒
短信提醒
* 提醒内容
当天到期
30天到期提醒
15天到期提醒
证书验证提醒
证书下载提醒

参数	参数说明
提醒开关	默认开启，可选择关闭消息通知。
联系人	选择需要发送通知信息的联系人，如何新建联系人请参考： 联系人管理 。
提醒方式	可选择“邮件方式”、“短信方式”。
提醒内容	• 当天到期：在证书到期当日，给相关联系人发送提醒。 • 30天到期提醒：在证书到期前的30个自然日内，给相关联系人发送提醒。 • 15天到期提醒：在证书到期前的15个自然日内，给相关联系人发送提醒。 • 证书验证提醒：适用于多年期证书更新场景，开启后可及时收取新证书的验证提醒信息。 • 证书下载提醒：适用于服务有效期内证书更新场景，开启后可及时收取新证书的下载部署信息。

4. 完成后单击“确定”即可完成消息提醒设置。

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. 登录证书管理服务控制台。
2. 在左侧导航栏选择“信息管理 > 联系人”，进入“联系人”页面。
3. 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。

4. 单击“确认”，完成创建。

相关操作

- 编辑联系人信息：若您需要修改已经纳管入证书管理服务控制台的联系人信息，可在联系人列表，在目标联系人操作列单击“编辑”，在弹出的对话框中修改联系人信息，单击“确认”保存，完成信息修改。

- 删除联系人：若您需要删除已经纳管入证书管理服务控制台的联系人信息，可在联系人列表，在目标联系人操作列单击“删除”，在弹出的提示框中单击“确认”，完成联系人删除。

> 注意
>
> 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。

公司管理

在申请OV或EV SSL证书时，您需通过天翼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： • 私营个体 • 商业企业 • 政府实体 • 事业单位 • 非营利组织
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。
组织机构代码	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”）。
公司所在区域	填写待申请证书公司的所在地。

参数	参数说明
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。

相关操作

- 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“确认”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。在弹出的提示框中单击“确认”，完成公司信息删除。

常见问题

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	信任等级	签发周期	图示
域名型证书（DV）	建议个人（即没有企业营业执照）使用。 说明 若作为移动端网站或接口调用，建议办理企业营业执照，并购买 OV 型及以上类型的 SSL 证书。	基础	1个工作日	
企业型证书（OV）	建议非金融/支付类企业使用。 建议购买 OV 型及以上类型的 SSL 证书。	较高	5~7个工作日	
增强型证书（EV）	建议金融/支付类企业使用。	高	5~7个工作日	

说明

- 域名型证书（DV）：只验证域名所有权，颁发最快（1个工作日）。适用于个人博客、内部测试系统、信息展示类网站等无需身份信任的场景，仅提供基础加密。
- 企业型证书（OV）：验证域名所有权和基本企业身份。适用于企业官网、SaaS服务、机构登录入口等需要让用户识别主办方身份，且防范钓鱼网站的场景。
- 增强型证书（EV）：执行最严格的企业实体资质审核。过去多用于银行、金融支付、大型电商等高敏感交易场景（浏览器地址栏曾显示绿名），目前因浏览器UI策略调整，其视觉差异缩小，主要在高合规行业或合同约定中要求使用。

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ctyuntest.cn，也可以是1个子域名example.ctyuntest.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 ctyuntest.cn、ctyuntest.com、ctyuntest.com.cn、*.ctyuntest.cn。最多可以支持域名数量250个以内。	多域名支持保护申请的多个域名。
通配符	支持绑定带1个通配符（*）的域名，通配符域名证书只能匹配主域名及同级别的子域名，不能跨级匹配。 说明 *.ctyuntest.cn的域名证书匹配ctyuntest.cn、demo.ctyuntest.cn、example.ctyuntest.cn等域名， 但是不匹配guide.demo.ctyuntest.cn、developer.demo.ctyuntest.cn等域名。	通配符SSL证书可以同时保护一个域名及所有的下一级子域名网站，比如*.ctyun.cn，对子域名网站的保护没有数量限制。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。

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：

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。

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

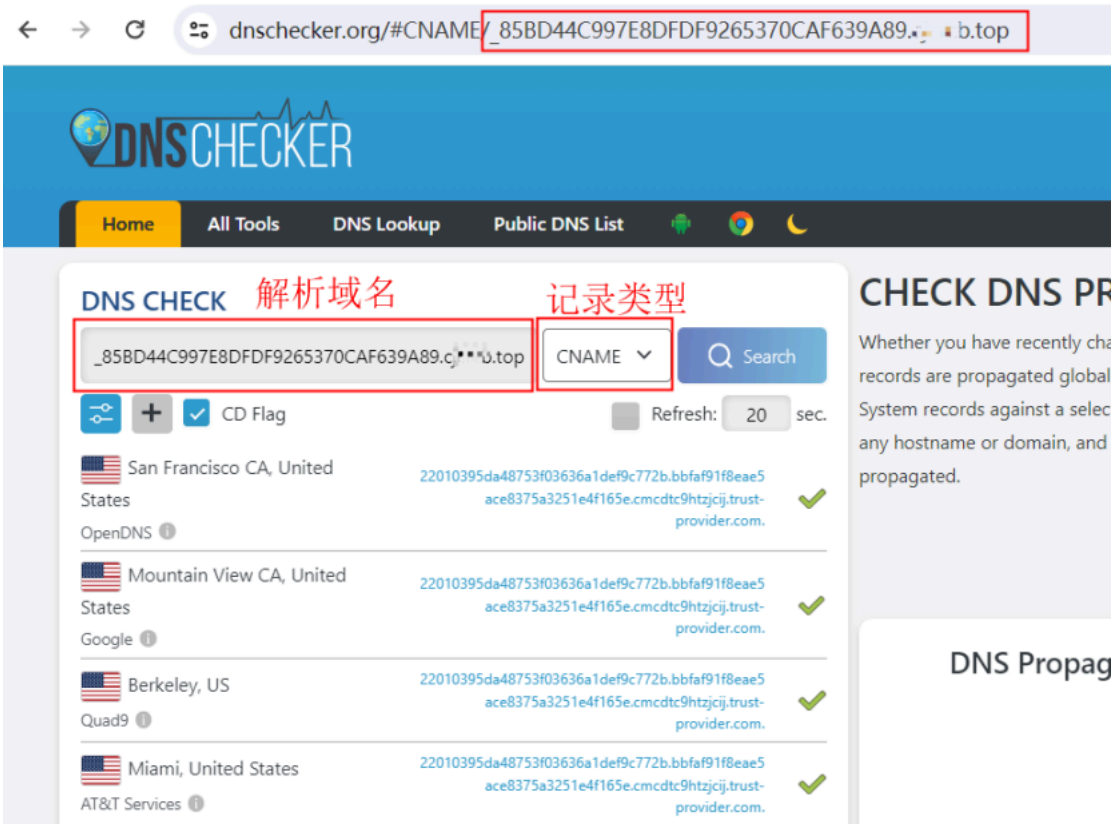
ctyun.cn

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 。



Windows系统如何验证DNS解析生效?

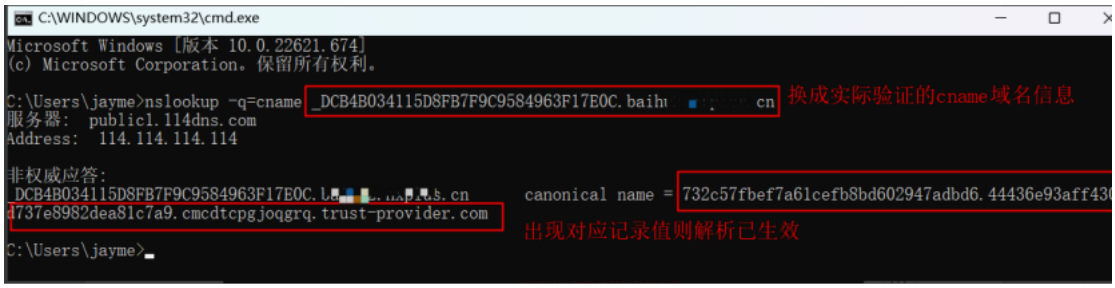
要验证Windows系统中的DNS解析是否生效，您可以尝试以下方法：

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?

1. 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。
2. 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。
3. 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。

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5-7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，若还是无法通过则无法签发证书，需要换域名申请或签发自签发证书。

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。

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。

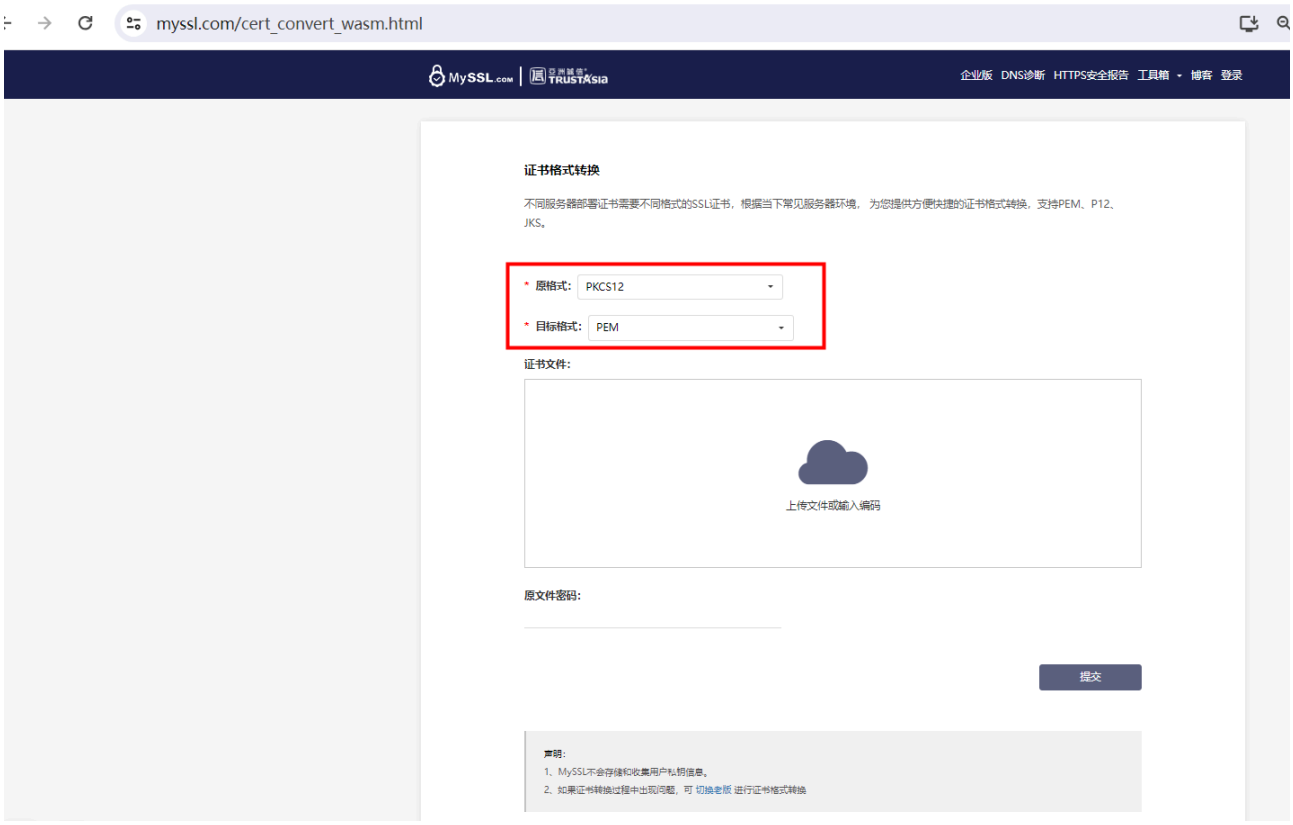
证书吊销指将已签发的证书从CA签发机构处注销。证书吊销后将失去加密效果，浏览器不再信任该证书。 提交吊销申请后，将由CA机构审核，审核通过后，吊销操作才算完成。

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。

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证书的有效期是多久?

参见 【产品公告】关于SSL证书有效期政策变更的重要通知 。

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“SSL证书管理 > SSL证书列表”，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。
   - 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。

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。

如何验证部署的SSL证书是否生效?

直接浏览器访问对应网址，访问到的证书是匹配的证书即可。步骤如下：

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。

其他SSL证书相关问题

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。

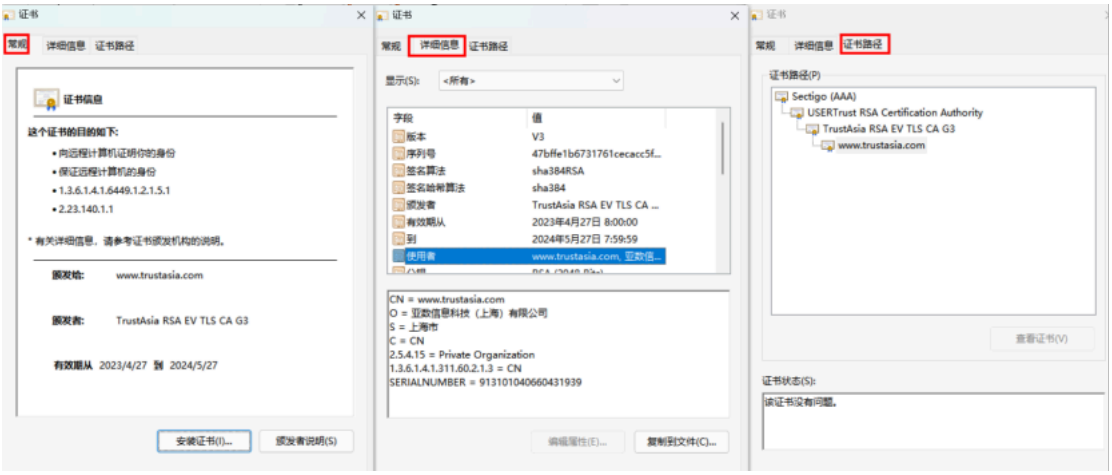
这些是常见的数字证书格式，用于存储和传输X.509证书及其相关信息。每种格式都具有不同的特点和适用性，取决于使用的平台、工具和应用程序。（以上格式后缀证书，天翼云均可以提供）

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、账号、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。