目录

第1步 补全信息

本文档介绍了完成证书购买后，申请证书并提交信息审核的相关操作流程。

前提条件

您的证书状态为未补全。

操作步骤

1. 登录金山云SSL证书管理控制台。
2. 选择状态为**未补全**证书的域名，在右侧操作栏中点击**补全**按钮。

3. 在**补全证书**的弹窗中，首先填写域名信息，若您购买的证书支持多域名或多通配符，还需填写附加域名和附加通配符域名，具体可以填写的个数与用户购买证书时选择的证书名称及其配置个数一致，点击这里查看价格总览。

4. 域名信息填写完毕后，点击**下一步**按钮。若申请的是DV证书，需填写申请人的个人信息，可以选择**复制已有证书信息**的方式，系统会自动填入所选证书的申请人个人信息。关于域名验证方式，我们强烈推荐**DNS验证**，具体DNS验证及文件验证的区别详见DNS和文件验证有什么不同？

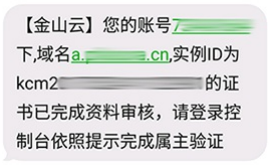
5. 若申请的是OV或EV证书，需填写企业及联系人信息，带*的均为必填项；可以选择**复制已有证书信息**的方式，系统会自动填入所选证书的各项信息。提交的公司联系人信息需真实有效，确保能够接

收到CA中心签证人员的电话和邮件信息。

6. 点击**下一步**，选择CSR生成方式，若选择**系统生成CSR**，系统会帮助用户生成CSR文件，关于CSR的解释，详见名词解释；

若选择**自己生成CSR**，用户需自己生成CSR文件，并将文件内容提交至系统，关于CSR文件的制作方法，详见CSR文件生成方法；

若申请的是OV或EV证书，还需上传**JPG格式**的企业营业执照；



7. 以上操作全部完成后，点击**确定**，补全信息提交成功，同时我们会将提示短信发送至用户在补全信息时填写的手机号中。

第2步 属主验证

第1步补全信息完成后，您需按照CA机构的规范完成属主验证，来证明您对申请证书绑定域名的所有权。您的属主验证信息提交完成后，需等待CA机构中心审核通过，此时您的证书状态为显示为**审核中(购买)**。

金山云SSL证书管理提供DNS验证和文件验证两种方式

- DNS验证
- 文件验证

前提条件

1. 若申请的是OV或EV证书，认证机构会在线下电话联系用户确认企业信息，属主验证信息由售后技术人员推送给用户。
2. 若申请的是DV证书，用户需要依照控制台提示配合完成属主验证。
3. 证书状态为审核中(购买)。

操作步骤

1. 登录SSL证书管理控制台。
2. 在证书实例列表中，点击对应实例的**点击完成属主验证**按钮，在弹窗中得到需添加的DNS记录值或文件验证流程。

DNS验证

DNS验证，是指在域名管理平台通过解析指定的DNS记录，验证域名所有权。 本部分内容将指导您如何在金山云的云解析服务上完成DNS验证。如果您是在金山云平台管理您的域名，可以参考此步骤修改；如果您的域名管理在其他平台，您可咨询自己的域名服务提供商。

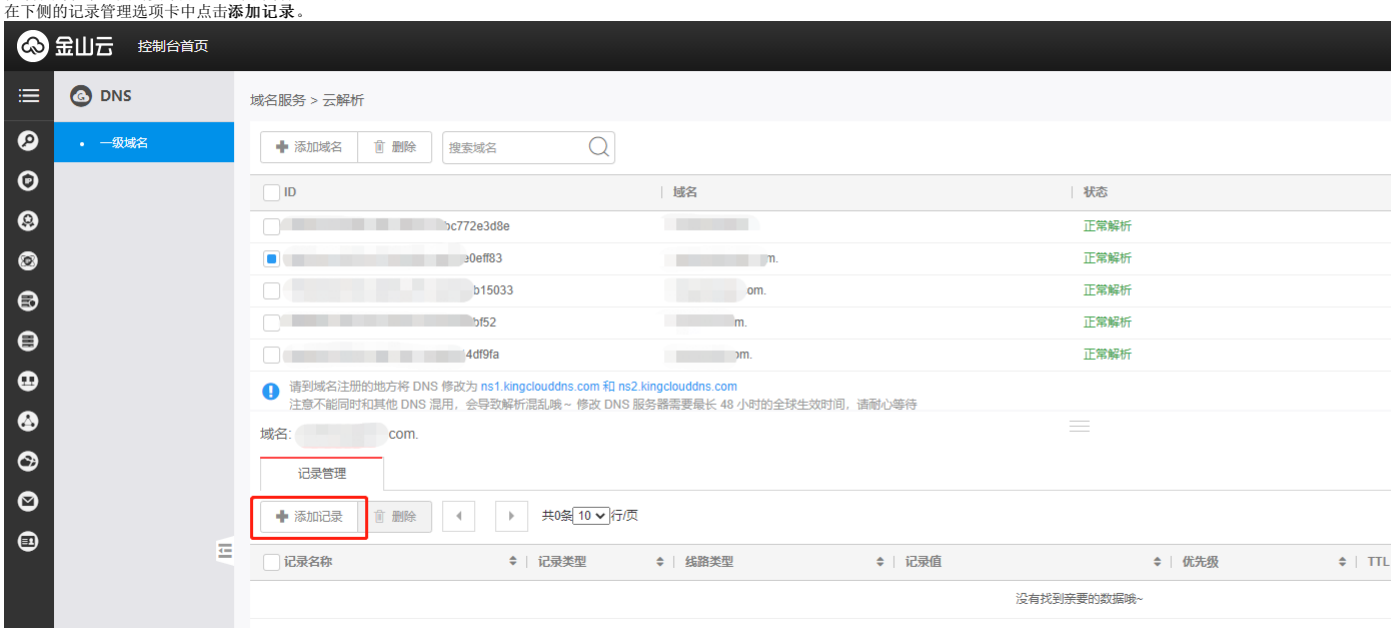
如果您购买的是多域名类型的证书，且选择的域名验证方式为DNS验证，则每个域名均需要做DNS验证。

获取主机记录和记录值

1. 登录SSL证书管理控制台
2. 在证书实例列表中，点击对应实例的**点击完成属主验证**按钮。
3. 记录下弹窗内给出的记录类型、主机记录和记录值，如下图所示。

在金山云的云解析平台添加DNS记录

1. 登录金山云云解析控制台。
2. 在域名列表中，点击要添加DNS记录的域名。
3. 在下侧的记录管理选项卡中点击**添加记录**。



4. 在添加记录的弹窗中按照属主验证信息中给出的信息选择记录类型，填写记录名称和记录值。

主机记录为域名前缀，如a.ksyun.com的主机记录为a，填写时请注意不要带上域名

5. 点击确定，记录添加成功。

文件验证

文件验证指通过在服务器上创建指定文件的方式来验证域名所有权。 文件验证方式一般需要由您的服务器管理人员进行操作。若您在补全信息时选择的域名验证方式为“文件”，在点击**点击完成属主验证**后，会弹出以下提示信息，请认真阅读提示并配合完成验证操作。

如果您购买的是多域名类型的证书，且选择的域名验证方式为文件验证，则每个域名均需要做文件验证。

第3步 下载证书

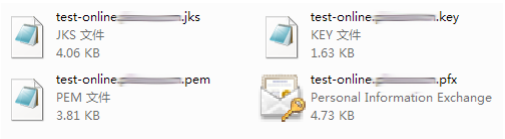
本文档指导用户在金山云SSL证书管理控制台下载证书。

前提条件

1. 已获取金山云控制台的登录账号与密码。
2. 证书状态为“已签发”，“已签发(重新签发)”。

约束条件

1. 仅支持在证书签发后7天内，不限次数的下载证书，下载后即可在服务器上进行部署。
2. 若您在补全时选择了“系统生成CSR”，则压缩包中包含jks、key、pem、pfx四个文件。



   - jks文件：证书文件，Tomcat、Weblogic、JBoss等，证书密码为下载文件中的“passwd.txt”
   - key文件：私钥文件
   - pem文件：证书文件，适用于Apache、Nginx等
   - pfx文件：二进制格式，同时含证书和私钥，一般有密码保护，证书密码为下载文件的“passwd.txt”
3. 若您在补全时选择了“自己生成CSR”，则压缩包中只包含pem文件。

操作步骤

1. 登录SSL证书管理控制台。
2. 在需要下载的证书所在行的“操作”列，点击**下载**按钮。

3. 在弹窗中点击**点击下载**按钮，即开始下载证书文件。

4. 下载完成后，需将证书安装在相应的服务器上，详见安装证书。