

证书与密钥服务

用户指南

产品版本: v1.1.1

发布日期: 2023-06-20

目录

1 用户指南	1
1.1 私有CA	1
1.2 证书管理	3
1.3 密钥管理	6

1 用户指南

1.1 私有CA

本章节主要介绍在“私有CA”页面中，针对私有CA的一系列运维管理操作，如：查看详情、启用、禁用、删除等。其中，在云平台的顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[私有CA]，即可进入“私有CA”页面。

查看详情

- 在“私有CA”页面中，单击私有CA名称链接，跳转至私有CA详情页面，即可查看私有CA详情。

RootCA					
私有CA / 详情					
基本信息					
名称	RootCA	路径深度	7	公司名称 (O)	EasyStack
状态	已启用	描述	test	部门名称 (OU)	Dev
类型	根CA	创建时间	2022-09-16 13:47:01	国家地区 (C)	CN
签发CA	-	到期时间	2025-09-15 13:47:01	省市 (S)	beijing
密钥算法	RSA2048	部门	Default	城市 (L)	beijing
签名哈希算法	SHA256	项目	admin	创建用户	admin
有效期	3年				

从属CA			
名称	状态	到期时间	创建时间
Sub_CA_from_Root_CA	已启用	2024-09-15 13:47:46	2022-09-16 13:47:48

创建私有CA

- 在“私有CA”页面中，单击 **创建私有CA**，进入“创建私有CA”页面。
- 配置参数后，单击 **创建私有CA**，完成操作。其中，各参数的具体说明，请参考 [创建私有CA](#)。

导出

在“私有CA”页面中，单击列表上方的“导出”图标，可将当前云平台所有私有CA的信息导出到CSV文件中。

启用/禁用

私有CA创建完成后默认为“已启用”状态，被禁用后将无法签发下级从属CA和私有证书。

1. 在“私有CA”页面中，单击目标私有CA操作栏的 **启用** 或 **禁用** ，弹出操作提示框。
2. 单击 **启用** 或 **禁用** 完成操作。

下载

在“私有CA”页面中，单击目标私有CA操作栏的 **更多** - **下载** ，完成操作。

编辑

仅支持修改描述信息。

1. 在“私有CA”页面中，单击目标私有CA操作栏的 **更多** - **编辑** ，弹出编辑对话框。
2. 修改信息，单击 **编辑** 完成操作。

删除

若目标私有CA下仍存在从属CA或私有证书时，将无法直接删除目标CA，当删除其签发的全部证书和所有从属CA后，方可删除目标CA。

1. 在“私有CA”页面中，单击目标私有CA操作栏的 **更多** - **删除** ，弹出删除提示框。
2. 单击 **删除** 完成操作。

1.2 证书管理

本章节主要介绍在“证书管理”页面中，针对证书的一系列运维管理操作，如：查看详情、上传第三方证书、删除证书等。其中，在云平台的顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[证书管理]，即可进入“证书管理”页面。

查看详情

用于查看证书的有效期、算法、归属项目等详细信息。

1. 在“证书管理”页面中，单击证书名称链接，即可进入证书详情页面查看信息。

创建私有证书

1. 在“证书管理”页面中，单击 **创建私有证书**，进入“创建私有证书”页面。
2. 配置参数后，单击 **创建私有证书**，完成操作。其中，各参数的具体说明，请参考 [创建私有证书](#)。

导出

在“证书管理”页面中，单击列表上方的“导出”图标，可将当前云平台所有证书的信息导出到CSV文件中。

上传证书

可将第三方生成的证书上传至平台进行存储及统一管理。暂不支持上传国密算法的证书。

1. 在“证书管理”页面中，单击 **上传证书**，弹出“上传证书”对话框。
2. 配置证书名称及描述信息，将证书内容、证书链及证书私钥以文件形式上传或直接输入。
3. 单击 **上传** 完成操作。



上传证书

* 名称

请输入证书名称

*** 类型** ?

请选择 ∨

*** 证书内容**

以"-----BEGIN CERTIFICATE-----"作为开头, "-----END CERTIFICATE-----"作为结尾

支持上传PEM或CRT格式的文件, 您可直接输入证书内容或上传证书文件。

上传文件

证书链

以"-----BEGIN CERTIFICATE-----"作为开头, "-----END CERTIFICATE-----"作为结尾

多个证书链请分段填写。

*** 证书私钥**

以"-----BEGIN RSA PRIVATE KEY-----"作为开头, "-----END RSA PRIVATE KEY-----"作为结尾; 或以"-----BEGIN EC PRIVATE KEY-----"作为开头, "-----END EC PRIVATE KEY-----"作为结尾

支持上传KEY或PEM格式的文件, 您可直接输入私钥文件内容或上传私钥文件, 目前不支持加密后的私钥文件。

上传文件

描述

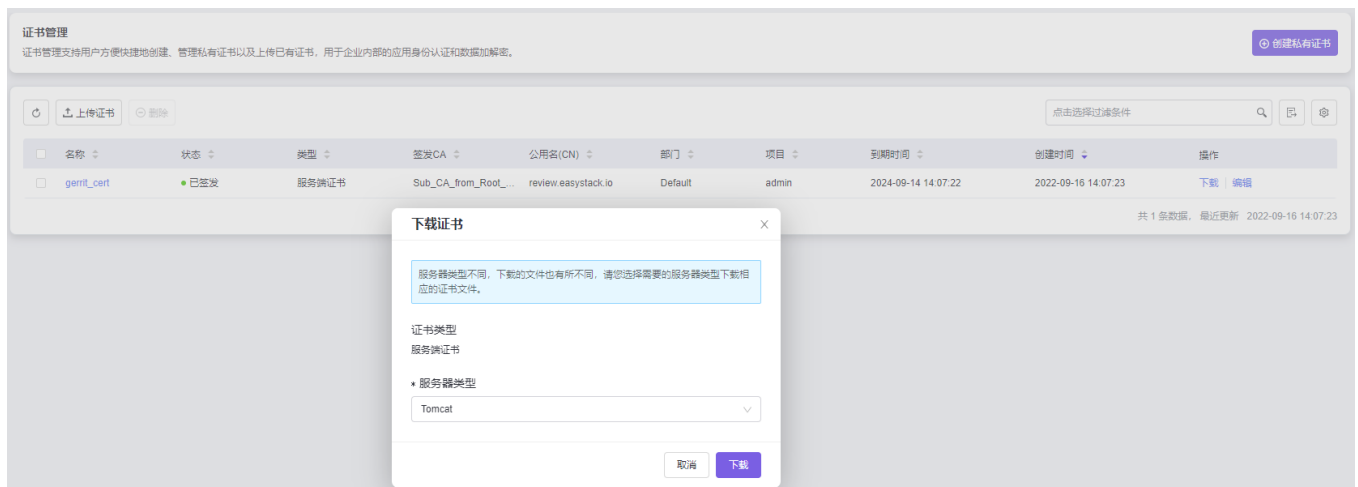
请输入

取消 **上传**

下载

1. 在“证书管理”页面中, 单击目标证书操作栏的 **下载**, 弹出“下载证书”对话框。

2. 选择服务器类型后，单击 **下载** 完成操作。



编辑

仅支持修改描述信息。

1. 在“证书管理”页面中，单击目标证书操作栏的 **编辑** ，弹出“编辑描述”对话框。
2. 修改描述信息，单击 **保存** 完成操作。

删除

1. 在“证书管理”页面中，单击目标证书操作栏的 **删除** ，或选择一个或多个待删除的证书后单击列表上方的 **删除** ，弹出“删除证书”提示框。
2. 单击 **删除** 完成操作。

1.3 密钥管理

本章节主要介绍在“密钥管理”页面中，针对密钥的一系列运维管理操作，如：查看详情、创建密钥、启用、禁用和删除等。其中，在云平台的顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[密钥管理]，即可进入“密钥管理”页面。

查看详情

用于查看密钥的名称、状态、算法、类型、用途、创建时间和保护时间等详细信息。

1. 在“密钥管理”页面中，单击密钥名称链接，即可进入密钥详情页面查看信息。

在指定密钥的详情页面中，还支持对其执行编辑、在线工具加密/解密等操作。具体操作说明如下：

编辑

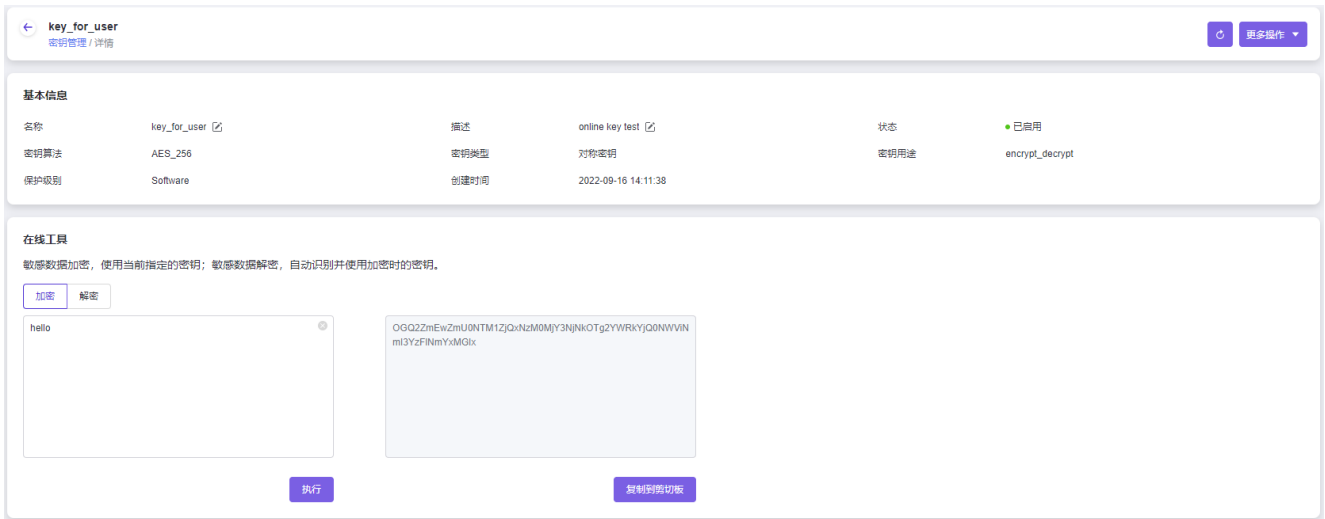
1. 在“基本信息”区域框中单击名称或描述后的“编辑”图标，或在详情页面中单击 **更多操作** - **编辑**，弹出对应对话框。
2. 配置参数后，单击 **保存**，完成操作。

在线工具加密/解密

对于“已启用”状态的对称密钥，支持直接使用该密钥在线对敏感数据执行加密或解密的操作。

1. 在“在线工具”区域框中，选择 [加密] 或 [解密] 页签。
2. 在左侧输入框中对应输入明文或密文后，单击 **执行**，可在右侧显示框中查看到加/解密后的数据。

单击 **复制到剪切板**，可直接复制显示框中的加/解密后数据到剪切板中。



创建密钥

1. 在“密钥管理”页面中，单击 **创建密钥** ，弹出“创建密钥”对话框。
2. 配置参数后，单击 **确认** ，完成操作。其中，各参数的具体说明，请参考 [创建密钥](#)。

导出

在“密钥管理”页面中，单击列表上方的“导出”图标，可将当前云平台所有密钥的信息导出到CSV文件中。

启用

1. 在“密钥管理”页面中，单击目标密钥操作栏的 **启用** ，弹出“启用密钥”提示框。
2. 单击 **启用** ，完成操作。

禁用

本操作用于在云平台中禁用密钥。当密钥被禁用后将无法继续使用，请谨慎操作。

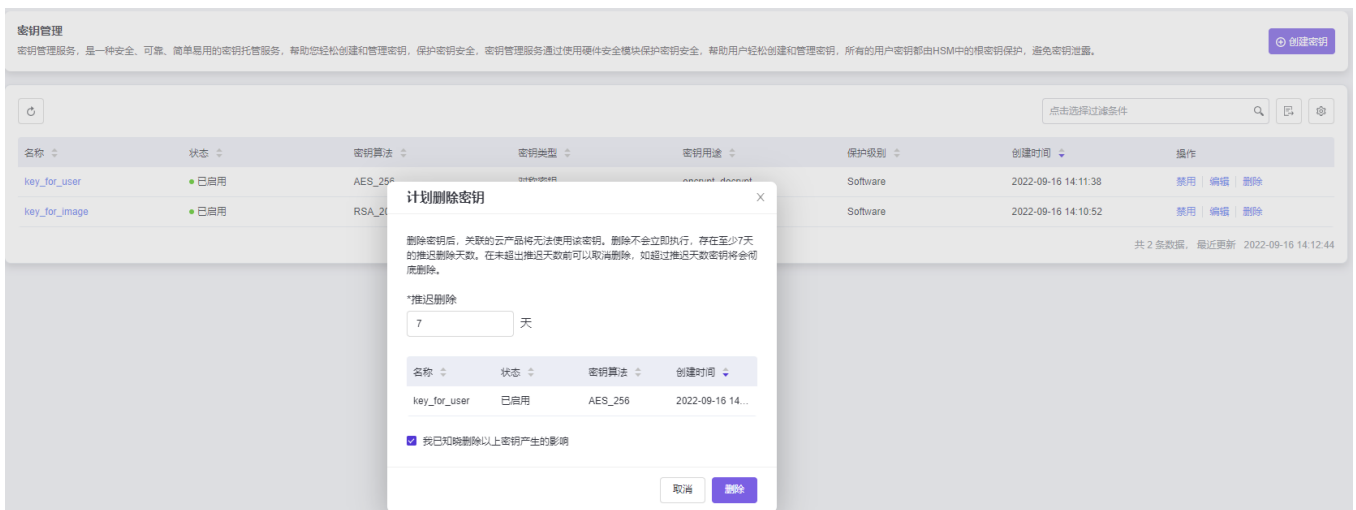
1. 在“密钥管理”页面中，单击目标密钥操作栏的 **禁用** ，弹出“禁用密钥”对话框。
2. 勾选“我已知晓禁用以上密钥产生的影响”后，单击 **禁用** ，完成操作。

删除

本操作用于在云平台中设置密钥删除计划。当密钥被删除后，关联的云产品将无法使用该密钥，请谨慎操作。

1. 在“密钥管理”页面中，单击目标密钥操作栏的 **删除** ，弹出“计划删除密钥”对话框。
2. 配置参数后，单击 **删除** ，完成操作。

参数	说明
推迟删除	<p>该密钥不会在操作后便立即删除，而是在达到所设置的推迟删除天数后才会被彻底删除。</p> <p>在达到推迟删除天数之前，可参考 取消计划删除 取消删除该密钥。</p>



取消计划删除

1. 在“密钥管理”页面中，单击目标密钥操作栏的 **取消计划删除** ，弹出“取消计划删除”提示框。
2. 单击 **确认** ，完成操作。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：

北京市海淀区西北旺东路10号院东区1号楼1层107-2号

南京易捷思达软件科技有限公司：

江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：

contact@easystack.cn (业务咨询)

partners@easystack.cn(合作伙伴咨询)

marketing@easystack.cn (市场合作)