密码服务

目录

产品介绍

产品定义.....3
产品优势.....3
功能特性.....4
应用场景.....4
产品规格.....7
使用限制.....8

计费说明

计费项.....11
购买密码服务.....12
续订及退订.....13

快速入门

密码服务—综合安全网关快速入门.....14
密码服务—数据加密网关快速入门.....14
密码服务—数字证书快速入门.....16
密码服务—协同签名服务快速入门.....17

用户指南

密码产品实例.....22
密码服务—综合安全网关操作指南.....27
密码服务—数据加密网关操作指南.....39
密码服务—数字证书认证系统操作指南.....46
密码服务—协同签名服务操作指南.....54
密码服务—时间戳服务操作指南.....71

最佳实践

使用综合安全网关保护设备的安全.....85
数据加密机网关部署方案.....86
申请PKCS10证书并保存至UKEY中.....89
使用协同签名服务保障数据安全.....92

常见问题

目录

产品咨询类..... 94
产品使用类..... 96

产品介绍

产品定义

密码服务是针对云上租户密评需求提供的端到端密评产品解决方案，产品基于具有商密资质的云密码机、密码服务在云上构建高性能密码资源池，为应用提供密钥管理、综合安全网关、协同签名等云原生密码服务，解决云上应用密评方案复杂、改造时间长问题，帮助租户快速通过密评。

产品优势

满足密评合规

使用的产品都具备商用密码产品认证证书，为应用系统提供严格合规的密码服务，帮助应用系统通过密评。

全场景密码服务

密码服务提供全场景密码服务能力，包括重要数据加解密、身份认证、签名验签、协同签名等服务。

应用快捷改造

提供统一标准的密码服务接口，应用改造简单快捷，具备完备的应用接入指南并提供及时、优质的技术支持服务。

一站式专业服务

一对一专属项目经理，7*24H技术支持，31省本地化的销售网络体系，提供“家门口”的精细化客户服务。

产品介绍

功能特性

数据加解密

提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求，基于数据加密技术，能够在数据进入数据库之前对其进行加密处理，从而确保数据的机密性和完整性。

签名验签

提供重要数据的签名和验签服务，满足密评中对重要数据传输和存储的完整性要求以及操作的不可否认性要求。

密钥管理

提供集中的密钥全生命周期管理服务，满足密评中对密钥管理的安全性要求。

安全传输

提供网络通信通道的加密服务，满足密评中对网络和通信安全层面的数据传输机密性和完整性要求。

协同签名

配合移动端密码模块为应用系统移动端提供协同密码服务，满足应用终端身份认证、数据加密合规性要求。

密评服务

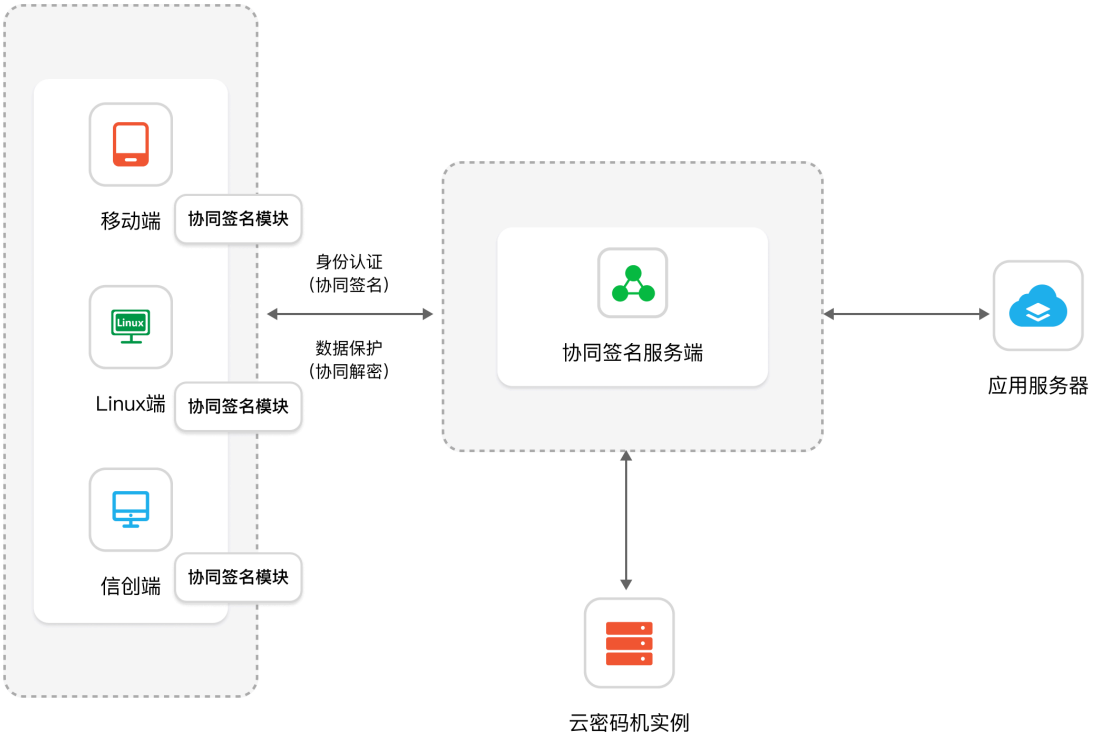
为租户侧提供密码方案设计、应用系统密改指导、应用系统密评支撑等服务。

应用场景

密码服务具有广泛的应用场景，本文为您介绍密码服务常见的应用场景。

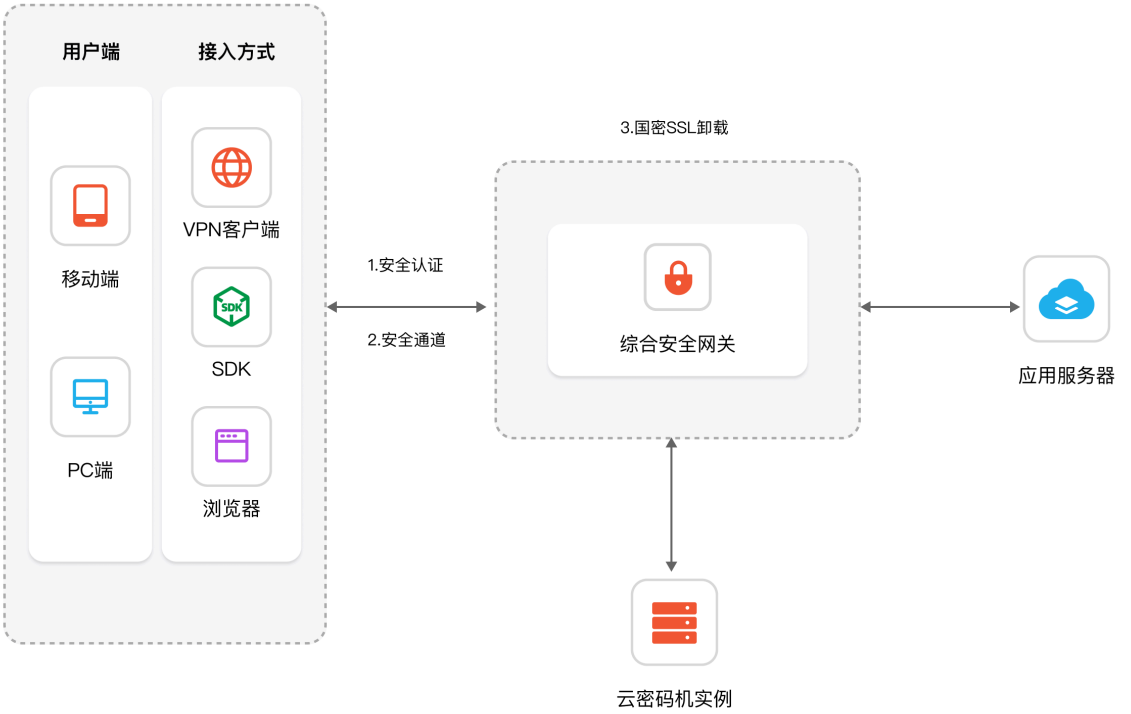
登录用户身份鉴别

密评中应用与数据安全层面的登录用户身份鉴别要求，应用系统的登录用户使用基于国密数字证书的身份认证服务，满足用户身份真实性要求。



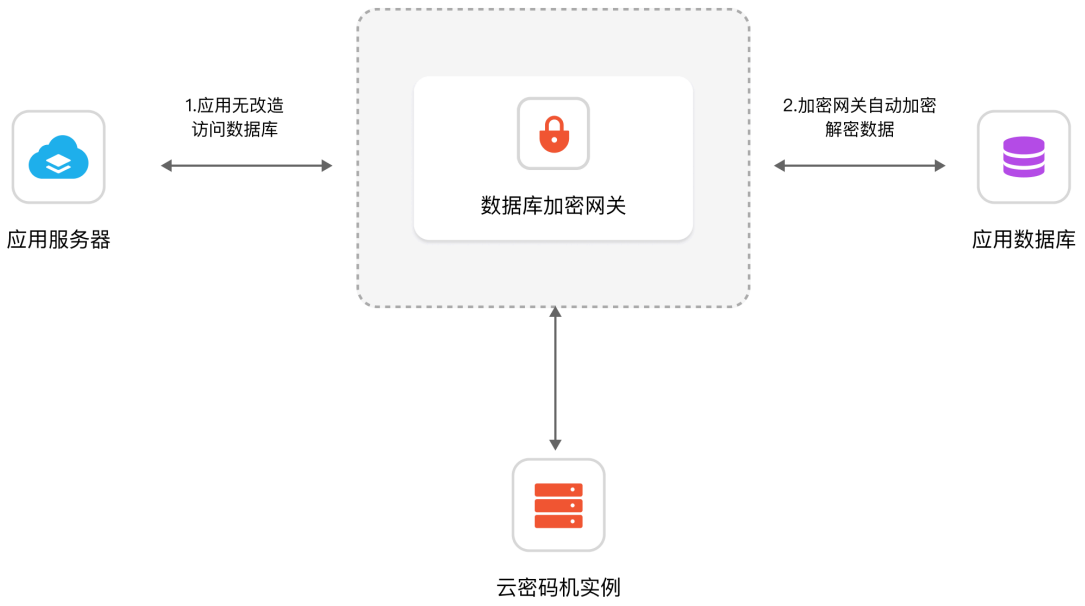
重要数据安全传输

密评中应用与数据安全层面的重要数据传输机密性和完整性要求，应用系统的重要数据在传输前调用密码服务的数据加解服务、签名服务对数据进行机密性和完整性保护，传输完成后进行解密和验签，保障数据传输过程中的安全性。



重要数据加密存储

密评中应用与数据安全层面的重要数据存储机密性要求，应用系统的重要数据存储到数据库时需要进行加密保存，应用系统调用密码服务的数据加密服务进行数据加密，把加密后的密文保存到数据库，满足数据存储机密性要求。



产品规格

密码服务主要包含三大类产品，分别为密码产品、国密套件和密评服务。

密码产品

产品名称	规格/版本	说明
综合安全网关	标准版	每个服务支持1000并发，可叠加，最多支持购买10个，建议搭配EIP使用
密钥管理	企业版	提供安全、可靠的密钥管理服务。 密钥管理购买后保存的密钥请在密钥管理服务中查询。
数据加密网关	标准版	提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求。
协同签名服务	标准版	每个服务支持1000并发，可叠加，最多支持购买10个。
数字证书认证系统	标准版	支持1万证书签发，5个CA，兼容RSA、ECC、SM2算法。
时间戳服务	标准版	为信息系统提供精准、安全和可信时间认证服务。

国密套件

产品名称	规格/版本	说明
国密浏览器	标准版	兼容主流国产操作系统，满足国密安全传输要求。
智能密码钥匙	标准版	用作基于公钥体系的数字证书和私钥的安全载体，并能在硬件中进行加解密运算。

产品介绍

产品名称	规格/版本	说明
协同签名客户端	标准版	支持IOS、Android、Windows、Linux等操作系统，每个端占1个license，最多支持购买10000个。
证书管理服务	国密证书	提供权威证书管理服务（证书有效期至少为一年，购买时长小于一年会默认为一年时长）。 国密证书、国际证书购买后会保存至证书管理服务控制台。
	国际证书	
	个人证书	
	服务器证书	

密评服务

产品名称	规格/版本	说明
密评咨询服务	标准版	为应用设计密码应用方案，协助密评机构开展密评，单个应用配置1套。
密评测评服务	标准版	支持1个应用密码应用安全性评估。
	企业版	
密评改造服务	-	项目特殊需求定制服务，下单前请提前和产品经理沟通并评估工作量，根据工作量确定下单数量。

使用限制

支持的区域

密码服务仅支持在以下资源池部署。

注意

部分资源池存在可见性限制，若您需要在对应资源池购买密码服务，请联系产品经理为您开通可见性。

区域	一类节点资源池
华东地区	芜湖4、华东1、南昌5、上海36
华南地区	海口2、华南2、武汉41、长沙42
西北地区	庆阳2、西安5、西安7、乌鲁木齐7
西南地区	贵州3、成都4、西南2-贵州、西南1
北方地区	北京5、郑州5、华北2、呼和浩特3、青岛20、太原4

网络访问限制

为避免网络故障或网络配置问题影响登录系统，请管理员优先检查网络配置是否允许访问产品实例，并参考下表配置实例安全组。

产品介绍

产品名称	端口	端口用途
综合安全网关	18443	使用综合安全网关的SSL VPN服务必开的端口。
综合安全网关	18444-18454	此端口范围为您新增网关安全服务时预留的端口范围，请您按需选择。
时间戳服务	9080-9083	• 9080端口：Http协议 • 9081端口：Tcp协议 • 9082端口：Https协议 • 9083端口：TLS协议

综合安全网关网络限制条件

您需要在对接综合安全网关实例的**安全组**下放通以下IP，否则无法正常使用：

- 100.89.0.0/16

如何添加安全组规则请参考：添加安全组规则章节。

数据加密网关支持的数据库及版本

数据库类型	支持数据库版本
MySQL	5.7、8.2.0
Mariadb	10.3.35、10.4、11.2.2
Oracle	11g、19c、23c、rac
SqlServer	2008、2016、2022
Percona	8
Oracle	11g、19c、23c、19c-RAC
Postgres	8.4、16.1
Greenplum	7
Opengauss	5.0.0
TiDB	6.5.5
Oceanbase	3.1.0
瀚高Higo	6.0.4
人大金仓Kingbase	V8、V9
海量数据库Vastbase	g100
亚信安慧Antdb	7.2.0
南大通用Gbase	8c
云和恩墨MogDB	5.0.0
神舟通用	opengauss版
达梦	7、8

数据加密网关加密限制

注意

在正式接入生产环境前，强烈建议您使用测试环境配合数据加密网关进行充分调试验证，确保通过后再切换至生产环境。

若因未遵循此操作流程导致的系统故障或数据风险，相关责任需由接入方自行承担。

- 数据加密网关加密字段不支持大小比较，如**大于**、**小于**、order by、between等。
- 不支持计算操作和函数操作，如AVG、MAX、MIN、SUM及计算表达式，不支持if、case、when函数。
- 不支持视图、触发器及存储过程操作，涉及where等条件后的 "=" 号比较必须保证 "=" 号两端字段均做加密或者均未做加密。
- 加密表名及字段名含有通配符（比如：**天翼云中'!'**）的不支持进行配置加密。
- 若您需要进行完整性检验，字段必须非空，否则无法生效。
- 加密列暂不支持任何函数，如果使用到函数，您需要对业务进行改造。

计费说明

计费项

密码服务主要包含三大类计费内容，分别为密码产品、国密套件和密评服务。

说明

密码服务目前支持购买及部署的区域请参考使用限制。

密码产品

密码产品目前包含综合安全网关、数据加密网关、数字证书认证系统、密钥管理服务、协同签名服务、时间戳服务共六个产品，具体计费价格参考下表。

说明

密钥管理购买后保存的密钥请在密钥管理服务中查询。

产品名称	规格/版本	计费模式	标准版价格（元/月）	一年付价格（元/年）	二年付价格（元/2年）	三年付价格（元/3年）
综合安全网关	标准版	包周期	6000	61200	122400	183600
数字证书认证系统	标准版	包周期	5000	51000	102000	153000
密钥管理服务	企业版	包周期	9699	98929.8	197859.6	296789.4
数据加密网关	标准版	包周期	6000	61200	122400	183600
协同签名服务	标准版	包周期	4000	40800	81600	122400
时间戳服务	标准版	包周期	2000	20400	40800	61200

国密套件

国密套件支持的产品、具体计费价格参考下表。

说明

证书购买后会保存至证书管理服务控制台。

产品名称	规格/版本	计费模式	价格
国密浏览器	标准版	按个计费	280元/个
智能密码钥匙	标准版	按个计费	150元/个
协同签名客户端	标准版	按个计费	100元/个
证书管理服务	国密证书（通配符）	按个计费	11475元/个/年
	国密证书（单域名）	按个计费	3825元/个/年
	国际证书（通配符）	按个计费	5270元/个/年

计费说明

产品名称	规格/版本	计费模式	价格
	国际证书（单域名）	按个计费	1912.5元/个/年
	个人证书	按个计费	180元/个/年
	服务器证书	按个计费	3000元/个/年

密评服务

产品名称	规格/版本	计费模式	价格（元/个）
密评咨询服务	标准版	按个计费	60000
密评测评服务	标准版	按个计费	120000
	企业版	按个计费	270000
密评改造服务	-	按个计费	55000

购买密码服务

若您需要购买密码服务的相关业务，可参考本章节进行选购。

说明

您在控制台购买密码服务业务前，请先提交工单申请开通购买白名单。

操作步骤

1. 登录密码服务管理控制台。
2. 单击右上角的“订购密码服务”，跳转至订购页面。
3. 选择您业务所需要的部署地域和可用区。
4. 选择需要购买的产品和规格。

配置项		配置项说明
密码产品	综合安全网关服务	每个服务支持1000并发，可叠加，最多支持购买10个，建议搭配EIP使用。
	密钥管理服务	提供安全、可靠的密钥管理服务，密钥管理购买后保存的密钥请在密钥管理服务中查询。
	数据加密网关服务	提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求。
	协同签名服务	每个服务支持1000并发，可叠加，最多支持购买10个。
	数字证书认证系统	支持1万证书签发，5个CA，兼容RSA、ECC、SM2算法。
	时间戳服务	时间戳服务，可提供标准的时间戳服务功能，可将交易时间和交易内容固化，适用于时间敏感型业务数据的安全保护。
国密套件	国密浏览器	选择需购买的国密浏览器个数，兼容主流国产操作系统，满足国密安全传输要求。
	智能密码钥匙	选择需购买的密钥钥匙个数。

配置项		配置项说明
	协同签名客户端	支持IOS、Android、Windows、Linux等操作系统，每个客户端占1个配额，最多支持购买10000个。
	证书管理服务	提供权威证书管理服务（证书有效期至少为一年，购买时长小于一年会默认为一年时长）。 国密证书、国际证书购买后会保存至证书管理服务控制台。
密评服务	密评咨询服务	为应用设计密码应用方案，协助密评机构开展密评，单个应用配置1套。
	密评测评服务	支持1个应用密码应用安全性评估。
	密码改造服务	项目特殊需求定制服务，下单前请提前和产品经理沟通并评估工作量，根据工作量确定下单数量。

5. 购买密码产品，还需要配置企业项目、网络信息。

配置项	配置项说明
企业项目	选择此次购买的密评服务所属的企业项目，方便您进行管理。
虚拟私有云	选择密码产品实例所要配置的虚拟私有云。 注意 成功创建后，VPC不可更换，请谨慎选择。
安全组	选择密码产品实例所在的安全组。
子网	选择密码产品实例所属的子网。

6. 购买密码产品，还需要配置密码产品管理员账号初始账密。

配置项	配置项说明
用户名	设置购买的密码产品实例管理员初始账号。
密码	设置购买的密码产品实例管理员初始密码。
确认密码	二次确认购买的密码产品实例管理员初始密码。

7. 选择购买密码产品、证书管理服务的时长。

   支持开启“到期自动续费”。开启自动续费后，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。

8. 配置完成后，勾选“我已阅读并同意《天翼云密码服务服务协议》《隐私政策声明》”后，单击“提交订单”。

续订及退订

续订

请联系您的专属客户经理进行续订，如果没有专属客户经理，可拨打天翼云客服电话4008-109-889咨询。

退订

请联系您的专属客户经理进行退订，如果没有专属客户经理，可拨打天翼云客服电话4008-109-889咨询。

密码服务—综合安全网关快速入门

步骤一：新增网关服务证书

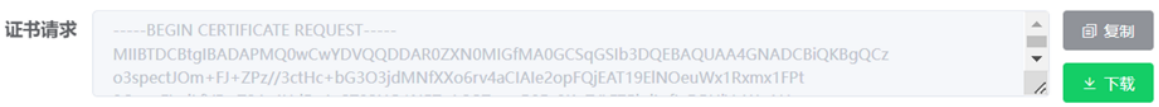
说明

一个综合安全网关实例仅支持创建一个网关服务证书，若您的服务已创建证书则无法再新增。

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务证书”，单击页面左上角的“新增证书”按钮。
3. 在弹出的“新增网关服务证书”对话框中，选择需要新增的证书规格。
4. 选择完成后，单击“确定”完成证书新增。

步骤二：生成证书CSR

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务证书”。
3. 选择需要生成CSR的证书，单击“操作”列的“CSR请求”按钮。
4. 在弹出的对话框中配置CSR相关内容。
5. 配置完成后，单击“生成证书请求”，会在“证书请求”栏中生成CSR。



6. 根据您业务自身需求选择复制保存或者下载文件保存。

步骤三：新增网关服务并配置

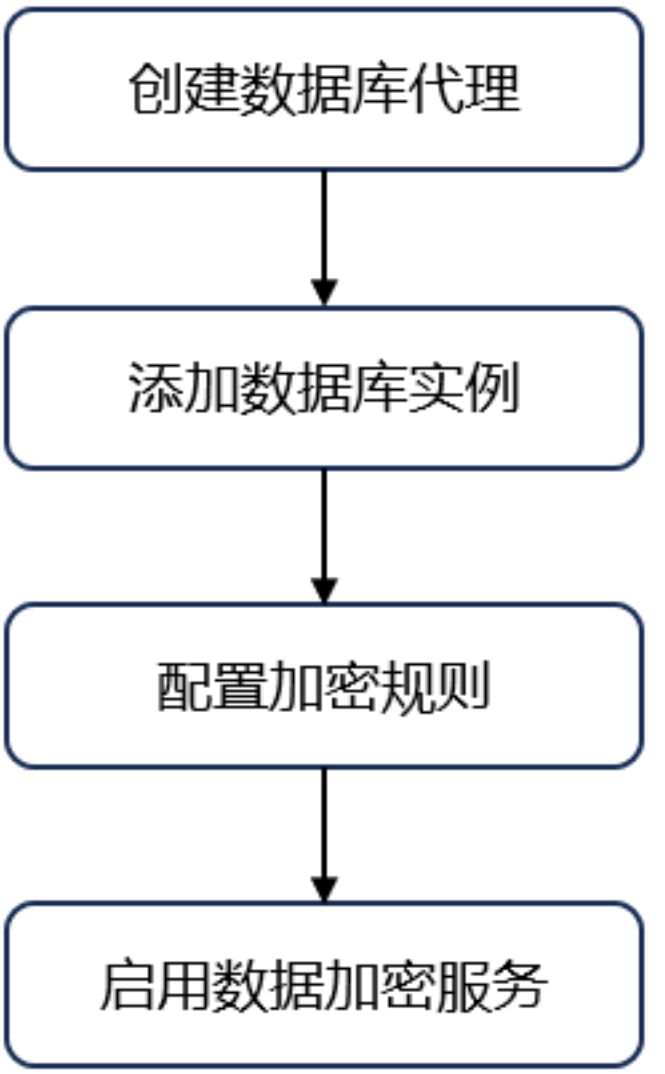
1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务管理”，在页面左上角单击“开通网关服务”。
3. 在弹出的“新增网关服务”的对话框中配置网关服务参数。
4. 确认填写的内容后，单击“确定”完成新增网关服务。
5. 配置完成后返回到“网关服务管理”页面，单击“操作”列的“配置”按钮开始配置网关。
6. 在弹出的“配置网关服务”对话框中，配置相关参数。

密码服务—数据加密网关快速入门

基于透明化服务理念，业务应用无需改造即可实现数据库中敏感数据的保护，支持国密算法，保证存储过程的机密性和完整性，满足应用和数据安全的合规要求。

启用流程

数据加密网关启用流程大致可参考下图：



步骤一：创建数据库代理

1. 使用运维账号登录数据加密网关。
2. 在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。
3. 单击页面左上角的“新增”按钮，进入“新增代理实例”页面。
4. 填写数据库实例代理相关内容，填写完成后单击“提交”，即可完成数据库代理配置。

步骤二：添加数据库实例

1. 使用运维账号登录数据加密网关。
2. 在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。
3. 单击“操作”列的“新增实例”按钮，跳转至“新增实例”页面。

4. 填写相关参数，将实例纳管至数据库代理中。

步骤三：配置加密规则

1. 选择需要配置加密规则的数据库，单击“操作”列的“配置加密”。
2. 在“表名”下拉框中选择需要配置加密规则的数据库表。
3. 单击“加密配置”，选择需要加密的字段开始配置。

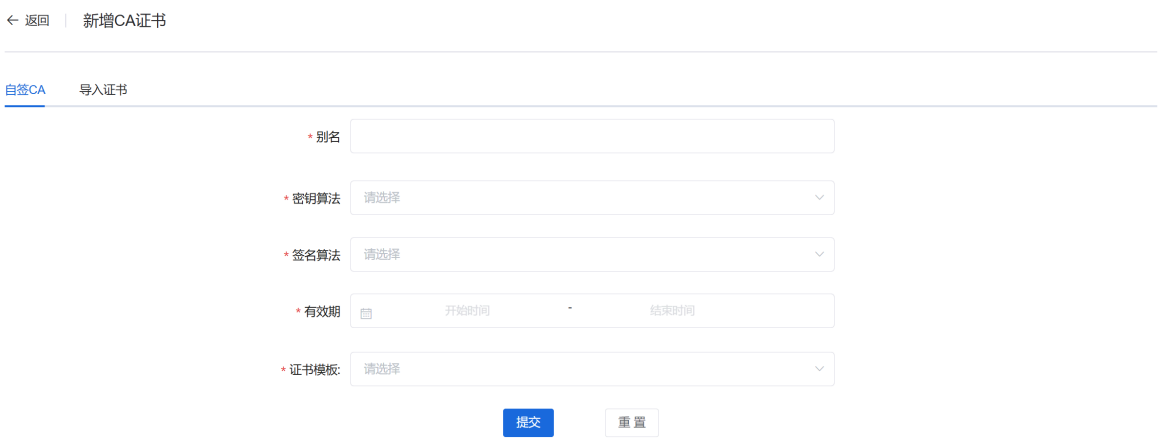
步骤四：启用数据加密服务

配置完成后，单击对应数据库实例的“加密洗数”即可开始使用数据加密服务。

密码服务—数字证书快速入门

步骤一：创建CA证书

1. 使用管理员账号登录数字证书认证系统。
2. 在左侧导航栏选择“机构管理 > CA证书管理”，进入“CA证书管理”页面。
3. 单击“新增按钮”，进入“新增CA证书”页面。
4. 选择“自签CA”，并且填写相关内容。



5.填写完成后单击“提交”，即完成自签CA的导入。

步骤二：新增子CA证书

1.使用管理员账号登录数字证书认证系统。

2.在左侧导航栏选择“机构管理 > 子CA管理”，进入“子CA管理”页面。

3.单击“新增”开始新增子CA证书。

4.单击“上传文件”上传证书文件并且选择所属的CA证书。

5.根据需求选择是否使用模板，选择完成后单击“提交”即可完成子CA证书的新增。

步骤三：证书申请

证书申请请参考：证书申请章节。

密码服务—协同签名服务快速入门

本章节主要了解基础功能并完成必要的配置。通过简明的操作步骤和指导，您可以迅速配置好系统，并为移动端用户启用安全高效的协同签名服务。无论您是初次接触还是经验丰富的管理员，本章节都将为您提供清晰易懂的使用指引。

步骤一：配置第三方CA

1.使用管理员账号登录协同签名服务

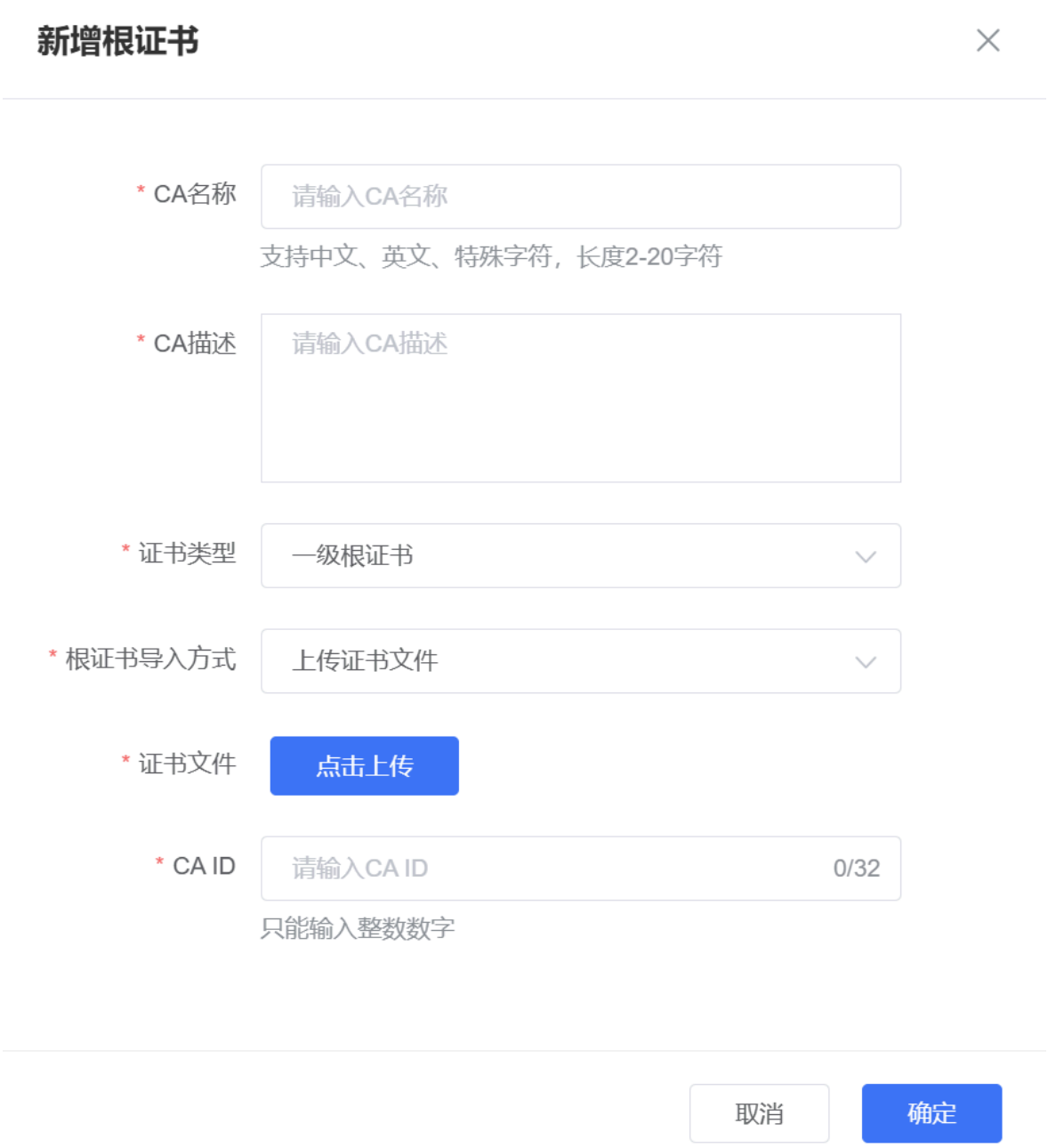
2.在左侧导航栏选择“系统管理 > 第三方CA配置”，进入“连接配置”页面。

3.单击左上角的“添加CA”按钮，在弹出的对话框中填写相关参数。

4.填写完成后，单击“确认”，返回“连接配置”页面。

5.在页面左上方选择“根证书配置”，进入“根证书配置”页面。

6.单击“添加根证书”，在跳转的窗口填写相关参数。



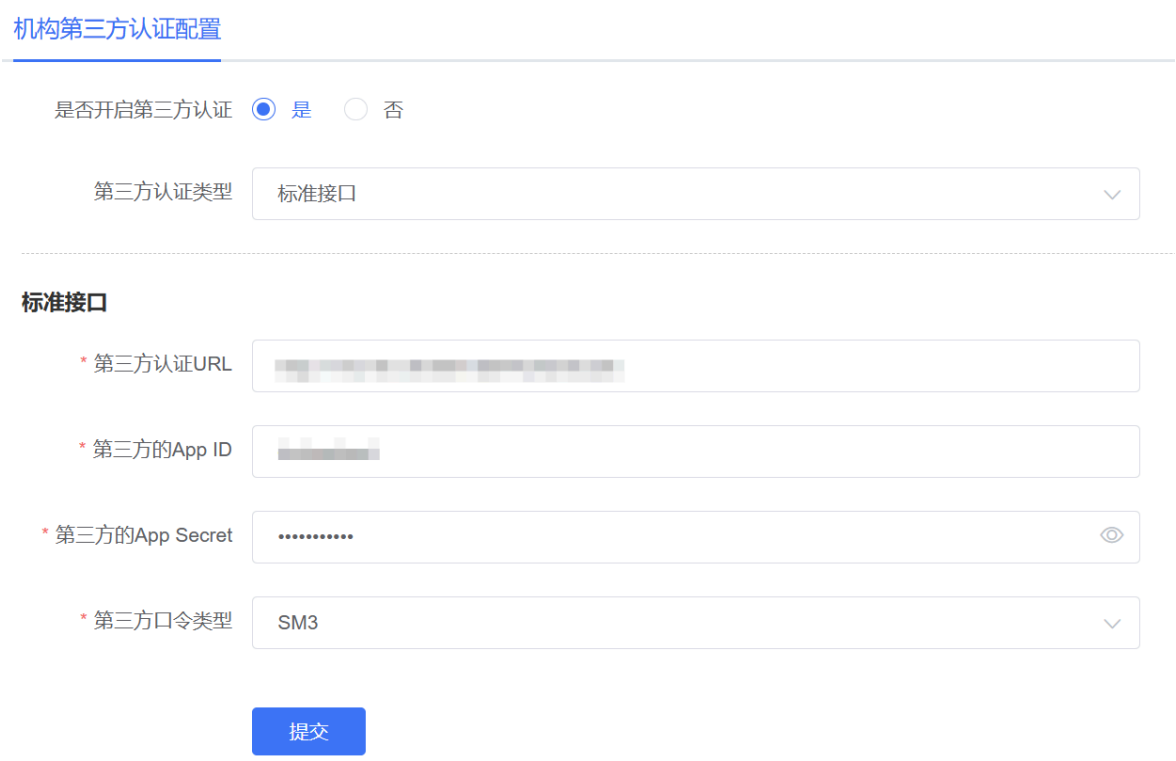
7.填写完成后，单击“确定”完成第三方CA配置。

步骤二：配置第三方认证

第三方认证还要确保签名行为是真实发生的，并且是按照预定的规则进行的。这包括验证签名的时间戳、签名的顺序（在一些有先后顺序要求的协同签名场景中）以及签名的完整性。

1.使用管理员账号登录协同签名服务

2.在左侧导航栏选择“系统管理 > 系统设置”，进入“机构第三方认证配置”页面。



3.开启第三方认证并填写标准接口参数。

第三步：获取鉴权信息

说明

业务系统终端集成协同签名模块后，需要填写鉴权信息才可调用协同签名系统的能力，请将应用的鉴权信息提取后交付终端开发人员

1.使用管理员账号登录协同签名服务

2.在左侧导航栏选择“应用登录 > 应用管理”，进入“应用管理”页面。

3.选择需要获取鉴权信息的应用，单击“操作”列的“密码”按钮，在弹出的对话框中输入管理员密码进行认证。

4.在弹出的对话框中输入管理员密码进行认证并获取应用信息。

5.将获取的信息同步至业务系统终端开发人员，在业务系统终端人员中按照SDK集成文档将鉴权信息内置。

密码产品实例

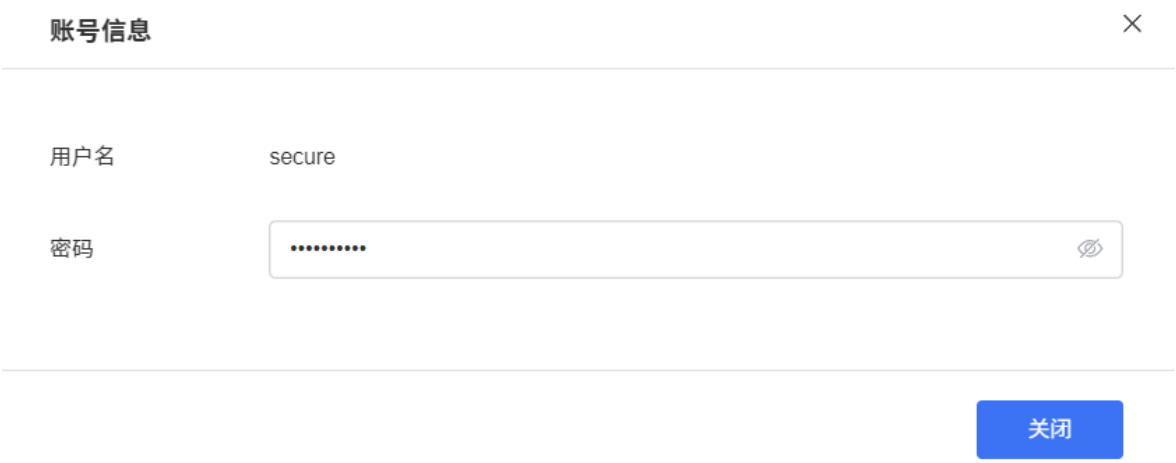
获取初始管理员登录账号

初始登录账号是在购买密码产品时，为实例设置的初始超级管理员账号。可以通过如下步骤获取初始登录账号的用户名和密码。

操作步骤

1. 登录天翼云密码服务控制台。
2. 选择需要登录的实例，单击右上方的“更多 > 获取初始登录账号”。

3. 在弹出的窗口中，查看初始账号信息，包括用户名和密码。

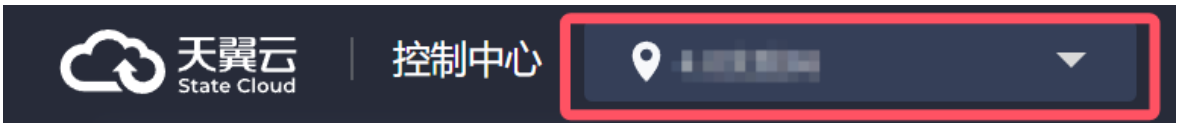


登录实例

在您购买密码服务后，会在控制台生成所选购服务的实例，下面为您介绍如何登录实例。

登录步骤

1. 登录天翼云密码服务控制台。
2. 在界面左上角选择部署业务的资源池，进入实例界面。



3. 选择要登录的实例，单击“管理”，即可进入实例登录页面，在登录页面选择登录方式，并输入用户名和密码等验证信息进行登录。

说明

- 首次登录实例时，请根据界面提示修改密码，否则无法进入系统。
- 首次登录默认账号如下：
  - 管理员首次登录：默认账号为购买密码产品时，自定义设置的用户名和密码，可以参见获取初始登录账号获取初始账密。
  - 其他用户首次登录：默认账号为管理员创建用户时设置的用户名和密码，请联系管理员获取。
- 非首次登录，若用户忘记了密码，可以通过登录页面进行重置密码。

IAM权限管理

天翼云提供统一身份认证（Identity and Access Management，简称IAM）服务，是提供用户进行权限管理的基础服务，可以帮助您安全的控制云服务和资源的访问及操作权限。通过IAM服务定义企业项目、创建子用户，轻松实现IAM子用户对密码服务资源的访问控制、权限分配等。

默认情况下，天翼云主账号拥有管理员权限，而主账号创建的IAM用户没有任何权限。IAM用户需要加入用户组，并给用户组授权相应策略后，IAM用户才能获得策略对应的权限，才可以基于被授予的权限对云服务进行操作。

密码服务支持企业项目管理，若您需要对密码服务资源进行分组和管理，形成逻辑隔离，您可以创建企业项目，并将资源划分至不同的企业项目中，不同的企业项目可以绑定不同的用户组，并给用户组授予密码服务产品的权限策略（包括系统策略和自定义策略），从而实现对特定资源的授权。

说明

仅“一类节点”区域的实例支持企业项目管理。

IAM应用场景

IAM策略主要面向同一主账号下，对不同IAM用户授权的场景：

- 您可以为不同操作人员或应用程序创建不同IAM用户，并授予IAM用户刚好能完成工作所需的权限，比如查看权限，进行最小粒度授权管理。

- 新创建的IAM用户可以使用自己的登录名和密码登录控制台，实现多用户协同操作时无需分享账号密码的安全要求。

密码服务IAM策略说明

天翼云为密码服务提供如下**系统策略**。如果系统策略不满足授权要求，可以创建**自定义策略**，自定义策略是对系统策略的扩展和补充，详情请参见创建自定义策略。

策略名称	策略描述	类别	授权范围
密码服务管理者	密码服务管理员策略，拥有产品所有操作权限。	系统策略	全局级
密码服务查看者	密码服务查看策略，仅支持查看实例列表。	系统策略	全局级

密码服务权限及授权项

策略支持的操作与授权项相对应，授权项列表说明如下：

- 权限：允许或拒绝IAM用户某项操作。
- 授权项：授权操作对应的权限三元组，创建自定义策略时，支持可视化JSON视图写入权限三元组实现策略配置。
- 权限类型：授权操作对应的读写类型。

权限	授权项	权限类型（读/写）	密码服务管理者	密码服务查看者
获取实例列表	ctcsz:service:list	读	√	√
修改实例名称	ctcsz:service:rename	写	√	×
绑定弹性IP	ctcsz:service:bind	写	√	×
创建实例	ctcsz:service:create	写	√	×
解绑弹性IP	ctcsz:service:unbind	写	√	×
启动实例	ctcsz:service:start	写	√	×
关闭实例	ctcsz:service:stop	写	√	×
重启实例	ctcsz:service:restart	写	√	×
管理实例	ctcsz:service:manage	写	√	×
升级实例	ctcsz:service:upgrade	写	√	×

通过IAM授权使用密码服务

详细操作请参考：

1. 创建用户组和授权
2. 创建IAM用户和登录
3. 创建企业项目并基于企业项目完成授权

标签管理

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10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，可以解绑标签后，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 > 密码服务”，进入密码服务实例管理页面。
4. 选择需要添加标签的实例，单击“更多 > 编辑标签”。

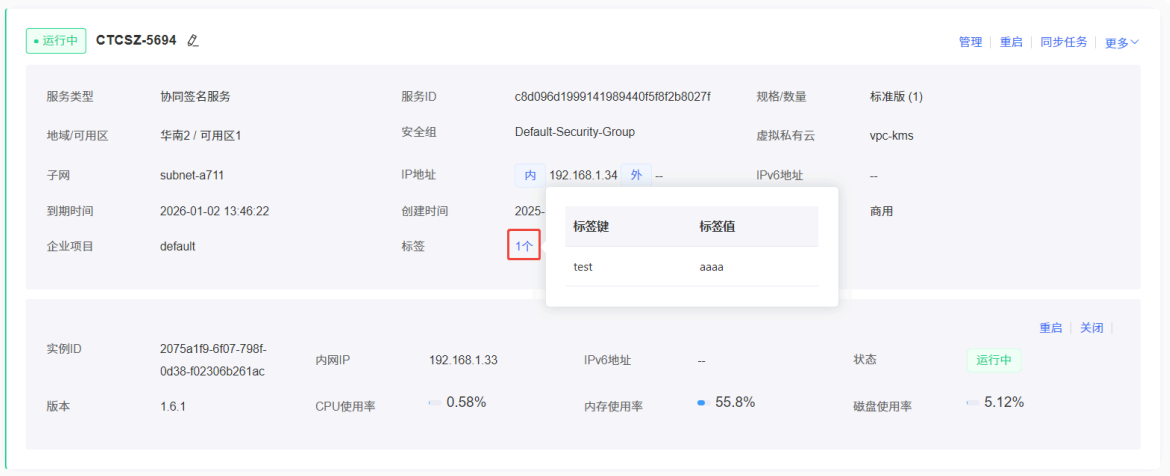
5. 在弹出的编辑标签窗口中，填写标签键和值。

   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。

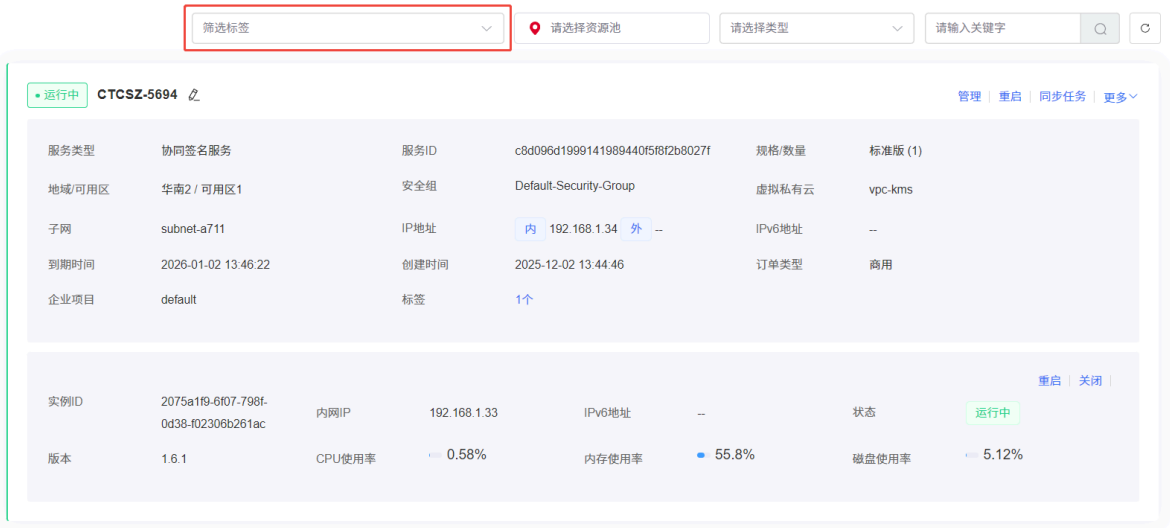
6. 配置完成后，单击“确定”，绑定标签完成。

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 > 密码服务”，进入密码服务实例管理页面。
4. 单击“筛选标签”。



5. 在“标签筛选”弹窗中，下拉选择已有标签。
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 > 密码服务”，进入密码服务实例管理页面。
4. 选择需要添加标签的实例，单击“更多 > 编辑标签”。

5. 在弹出的编辑标签窗口中，单击目标标签操作列的“删除”。

6. 单击“确定”，解绑标签完成。

密码服务—综合安全网关操作指南

登录综合安全网关实例

综合安全网关是一款专为解决网络间安全互联而设计的高性能安全产品。

它基于SSL协议，能够在不可信的公共网络上建立安全、加密的通信隧道，确保数据的机密性和完整性。

该产品提供了强大的身份认证机制，支持多种认证方式，如密码、智能卡和生物识别等，有效防止未经授权的访问。

此外，综合安全网关还具有灵活的访问控制策略，可以根据用户身份和设备类型授予不同的访问权限，保护企业内部资源的安全。它易于部署和管理，支持各种操作系统和移动设备，满足远程办公和移动办公的需求，广泛应用于企业、政府机构和教育领域。

您成功购买综合安全网关服务实例后，可在天翼云密码服务管理控制台登录。

开放端口要求

为避免网络故障或网络配置问题影响登录系统，请管理员优先检查网络配置是否允许访问综合安全网关，并参考下表配置实例安全组。

注意

您需要在对接综合安全网关实例的**安全组**下放通以下IP：

- 100.89.0.0/16

如何添加安全组规则请参考：添加安全组规则章节。

端口	端口用途
18443	使用综合安全网关的SSL VPN服务必开的端口。
18444-18454	此端口范围为您新增网关安全服务时预留的端口范围，请您按需选择。

通过天翼云控制台进入登录页面

1. 登录天翼云密码服务管理控制台。
2. 在左侧导航栏选择“密码服务”，进入“密码服务”页面。
3. 选择需要登录的综合网关服务实例，单击右上角的“管理”，进入实例登录页面，选择登录方式。

登录方式一：口令登录

1. 在登录页面选择“口令登录”。
2. 依次输入用户名、密码、验证码。

> 说明
>
> - 首次登录实例时，请根据界面提示修改密码，否则无法进入系统。
> - 首次登录默认账号如下：
>   - 管理员首次登录：默认账号为购买密码产品时，自定义设置的用户名和密码，可以参见获取初始登录账号获取初始账密。
>   - 其他用户首次登录：默认账号为管理员创建用户时设置的用户名和密码，请联系管理员获取。

3. 单击“登录”，验证后即可成功登录系统。

登录方式二：UKEY登录

> 注意
>
> 首次使用UKEY登录时，需要在综合安全网关服务登录页面下载并安装UKEY插件。

1. 在登录页面选择“UKEY登录”。
2. 依次输入用户名、密码。
3. 接入UKEY，自动识别已签发UKEY。
4. 输入PIN码。
5. 输入验证码。
6. 单击“登录”，验证后即可成功登录系统。

SSL网关服务

功能概述

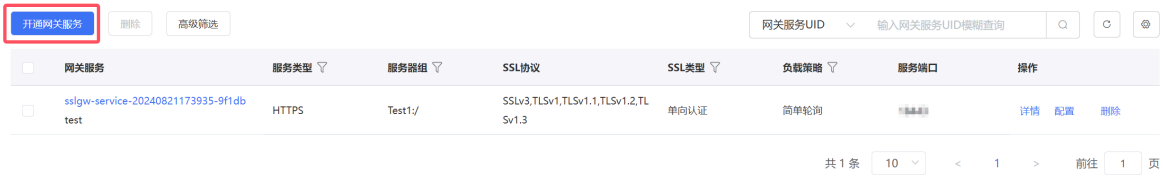
- 网关服务管理：用于维护网关服务，提供开通网关服务，删除，配置，查询详情等功能。
- 网关服务器组：SSL网关服务功能的具体实现是由网关服务器实现的，而网关服务器则由网关服务器组统一管理，网关服务与网关服务器组是1对1的关系，提供服务器组的新增，编辑，删除，查看服务器列表，以及服务器的添加，修改，删除，启用/停用等功能。
- 网关服务证书：SSL网关服务使用网关服务证书来进行安全认证工作，使用SSL网关服务的前提是必须安装相关网关服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR请求，证书应答，导入证书等功能。
- 网关服务优化策略：用于优化外部应用访问。

网关服务管理

网关服务管理是用于维护网关服务，提供开通网关服务、删除、配置、查询详情等功能。

新增网关服务

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务管理”，在页面左上角单击“开通网关服务”。



3. 在弹出的“新增网关服务”的对话框中配置网关服务参数。

参数	参数说明
服务名称	自定义新增的网关服务名称，完成创建后不可修改。
服务类型	选择新增的服务类型。
服务端口	选择新增的服务端口，完成创建后不可修改。端口选择范围为：18444-18454。

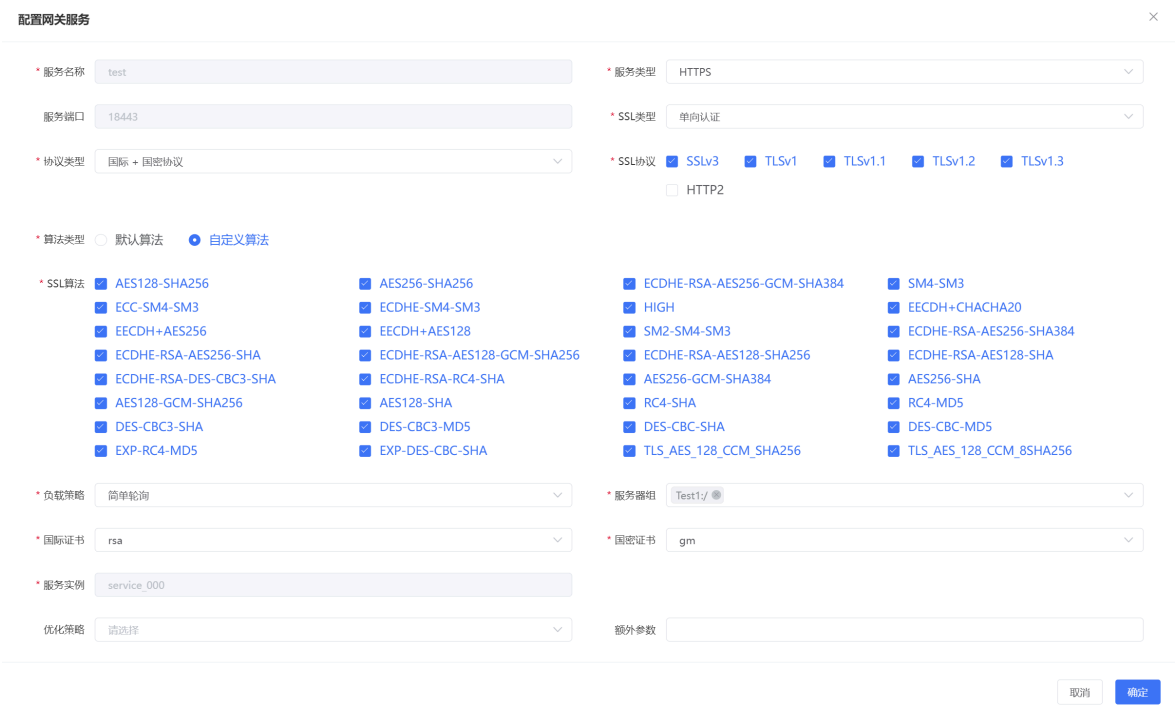
4. 确认填写的内容后，单击“确定”完成新增网关服务。

配置网关服务

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务管理”，选择需要配置的网关服务，单击操作列的“配置”。

3. 在弹出的“配置网关服务”窗口中，配置相关参数。

参数	参数说明
服务名称	不可修改，服务名称是您创建时填写的。
服务类型	选择服务类型。
服务端口	不可修改。
SSL类型	选择需要配置的SSL类型。支持单向认证、双向认证。
协议类型	选择网关服务的协议类型。支持国际协议、国密协议、国际+国密协议。
SSL协议	选择网关服务的SSL协议，目前支持选择：SSLv3、TLSv1、TLSv1.1、TLSv1.2、TLSv1.3、HTTP2。
算法类型	选择“默认算法”或“自定义算法”。
SSL算法	选择**自定义算法**时可选择，根据您业务的需求选择SSL算法。
负载策略	选择网关服务的负载策略。
服务器组	选择服务器组。
证书	选择网关服务的证书。



4. 配置完成后，单击“确定”即可完成配置。

查看网关服务详情

1. 登录综合安全网关实例。

2. 在左侧导航栏选择“SSL网关服务 > 网关服务管理”，选择需要查看详情的网关服务，单击“操作”列的“详情”即可查看网关服务详情。

删除网关服务

注意

删除后的网关数据无法恢复，请您谨慎进行删除操作。

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务管理”，选择需要删除的网关服务，单击“操作”列的“删除”。
3. 在弹出的对话框中，单击“确定”即可完成删除。

网关服务器组管理

SSL网关服务功能是由网关服务器实现的，而网关服务器则由网关服务器组统一管理，网关服务与网关服务器组是一对一的关系。

提供服务器组的新增、编辑、删除、查看服务器列表，以及服务器的添加、修改、删除、启用/停用等功能。

新增服务器组

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务器组”，单击页面左上角的“新增服务器组”。
3. 在弹出的对话框中填写相关内容。

参数	参数说明
分组名称	自定义服务器组的名称。创建完成后不支持修改。
服务类型	选择服务器组的服务类型。

4. 确认后单击“确定”即完成创建。

相关操作：

服务器组创建完成，您可以根据需要编辑、删除服务器组。

- 编辑服务器组：选择需要编辑的服务器组，单击“操作”列的“编辑”即可修改。
- 删除服务器组：选择需要删除的服务器组，单击“操作”列的“删除”即可删除服务器组。
- 查看服务器列表：点击服务器组右侧的“查看服务器列表”，即可跳转到网关服务器组详情页面。

添加服务器

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关服务器组”，选择需要添加服务器的服务器组，单击“操作”列的“添加服务器”。

3. 在弹出的对话框中配置服务器的参数。

参数	参数说明
IP	填写密码机的IP地址。
端口	填写密码机的端口。
权重	选择密码机的权重。
描述	自定义密码机的描述。
启用	选择添加后密码机的启用状态。

4. 填写完成后，单击“确定”完成服务器添加。

相关操作：

添加服务器后，支持对服务器进行管理，包括启用、停用、编辑、删除服务器。

注意

服务器必须停用后才能修改、删除。

点击服务器组名称左边的箭头，展开服务器组的服务器列表。

- 启用/停用服务器：选择需要启停的服务器，单击“操作”列的“启用/停用”即可启停服务器。
- 编辑服务器：选择需要编辑的服务器，单击“操作”列的“编辑”即可修改。
- 删除服务器：选择需要删除的服务器，单击“操作”列的“删除”即可删除服务器。

网关服务证书管理

SSL网关服务使用网关服务证书来进行安全认证工作，使用SSL网关服务的前提是必须安装相关网关服务证书。

提供新增、查看详情、启用、停用、可信证书链管理、CSR请求、证书应答、导入证书等功能。

新增证书

说明

一个综合安全网关实例仅支持创建一个网关服务证书，若您的服务已创建证书则无法再新增。

1. 登录综合安全网关实例。

2. 在左侧导航栏选择“SSL网关服务 > 网关服务证书”，单击页面左上角的“生成证书请求”按钮。

3. 在弹出的“生成证书请求”对话框中，配置证书规格。

参数	参数说明
密钥标识名	根据您证书填写的证书识别名自动填写，无法修改。
密钥算法	根据您证书填写的证书算法自动填写，无法修改。
证书请求类型	自动填写证书请求类型，无法修改。
密钥长度	根据您的需求选择密钥的长度。
请求签名算法	在下拉框中选择请求签名算法。
公钥指数	根据业务需求选择公钥指数。
主题格式	选择主题格式，支持“标准主题”和“自定义主题”。
通用名	仅选择“标准主题”时需填写，填写CSR的通用名。
自定义主题	仅选择“自定义主题”是需填写，根据业务自身需求填写主题内容。

4. 选择完成后，单击“确定”完成证书新增。

后续操作

启用/停用证书：选择需要启用/停用的证书，单击“操作”列的“启用/停用”按钮，即可完成启用/停用。

添加可信证书链

1. 选择需要添加可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。
2. 单击页面左上角的“添加可信证书”按钮，弹出“添加可信证书”对话框。
3. 上传正确的证书文件后，单击“确定”完成添加。

说明

只支持上传.cer/.p7b/.der格式的文件，每次操作仅支持上传单个文件。

网关服务优化策略

网关服务优化策略可以用于优化外部应用访问。

新增优化策略

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“SSL网关服务 > 网关高级设置”，选择“网关服务优化策略”页签。
3. 在实例页面左上角单击“新增优化策略”。

4. 在弹出的对话框中配置相关参数。

参数	参数说明
策略名	自定义需要新增的优化策略名。
IO超时	设置网关策略的IO超时值。
压缩	选择是否开启压缩。
缓存	选择是否开启缓存。
连接复用	选择是否开启连接复用。

5. 配置完成后单击“确定”即可完成新增。

相关操作

编辑优化策略：选择需要编辑的网关服务优化策略，单击“操作”列的“编辑”，在弹出的对话框中修改相关配置，编辑完成后单击“确定”即完成修改。

SSL VPN服务

功能概述

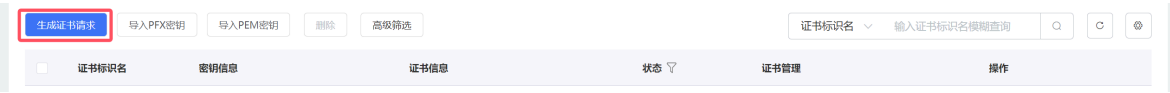
- VPN服务管理：用于维护VPN服务，提供配置VPN服务；对内网控制新增和删除；对静态路由表的新增，修改，删除等功能。
- VPN服务证书：SSL VPN服务使用VPN服务证书来进行安全认证工作，使用SSL VPN服务的前提是必须安装相关VPN服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR请求，证书应答，导入证书等功能。

VPN服务证书

VPN服务证书是进行安全认证工作的必要条件，使用SSL VPN服务的前提是必须安装相关VPN服务证书，综合安全网关提供新增、查看详情、启用、停用、可信证书链管理、CSR请求、证书应答、导入证书等功能。

生成证书请求

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“VPN服务 > VPN服务证书”，进入“VPN服务证书”页面。
3. 单击页面右上角的“生成证书请求”按钮。



4. 在弹出的“生成证书请求”对话框中，配置相关内容。

参数	参数说明
密钥识别名	自定义密钥匙别名。
密钥算法	目前仅支持“SM2”密钥算法。
证书请求类型	选择证书请求类型。
主题格式	选择主题格式，支持“标准主题”和“自定义主题”。
标准主题	仅选择“标准主题”时需填写，仅CSR通用名为必填项。
自定义主题	仅选择“自定义主题”时需填写，根据业务自身需求填写主题内容。

5. 配置完成后，单击“生成证书请求”，会在控制台中生成最新的服务证书及证书请求文件。

相关操作：

启用/停用证书：选择需要启用/停用的证书，单击“操作”列的“启用/停用”按钮，在弹出的对话框中单击“确定”，即可完成“启用/停用”操作。

添加可信证书链

VPN服务证书的可信证书链，需要在选择VPN服务证书信息后才可添加相关内容。

1. 选择需要添加可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。
2. 单击页面左上角的“添加可信证书”按钮，弹出“添加可信证书”对话框。
3. 上传正确的证书文件后，单击“确定”完成添加。

> 说明
>
> 只支持上传.cer/.p7b/.der格式的文件，每次操作仅支持上传单个文件。

相关操作：

- 删除可信证书链
  1. 选择需要删除可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。
  2. 选择需要删除的证书链，单击“操作”列的“删除”按钮。
  3. 在弹出的对话框中单击“确定”即可完成删除。
- 下载可信证书链
  1. 选择需要下载可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。
  2. 选择需要下载的证书链，单击“操作”列的“下载证书”按钮即可下载。

VPN服务管理

VPN服务管理提供以下功能：

- 提供配置VPN服务。
- 对内网控制新增和删除。
- 对静态路由表的新增、修改、删除等。

前提条件

为保障您的SSL VPN服务正常使用，需要在综合安全网关实例所属的安全组中放通18443端口。

新增VPN服务管理

说明

您在首次登录VPN服务页面，界面会提示“该SSL VPN服务尚未配置”。

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“VPN服务 > VPN服务管理”，进入“VPN服务管理”页面。
3. 开始配置“VPN服务”，完成配置后单击“配置”按钮即可完成修改。

参数	参数说明
Vpn服务uid	系统自动生成，无需填写。
服务名称	自定义VPN服务的名称。
证书	选择VPN服务的证书，证书的添加请参加VPN服务证书。
SSL协议	选择VPN服务对应的SSL协议，第一次配置后无法修改。
SSL算法	选择VPN服务对应的SSL算法，第一次配置后无法修改。
服务端口	填写VPN服务对应的端口，第一次配置后无法修改。

新增内网控制

1. 登录综合安全网关实例。

2. 在左侧导航栏选择“VPN服务 > VPN服务管理”，进入“VPN服务管理”页面。
3. 选择“内网控制”页签，单击“创建内网”按钮。
4. 在弹出的对话框中填写“IP地址”或“IP网段”。
5. 填写完成后单击“确定”即可新增内网控制。

新增静态路由

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“VPN服务 > VPN服务管理”，进入“VPN服务管理”页面。
3. 选择“静态路由表”页签，单击“创建路由”按钮。
4. 在弹出的对话框中配置静态路由的相关内容。

参数	参数说明
IP地址	填写静态路由的IP地址。
网关	填写静态路由的网关。
子网掩码	填写静态路由的子网掩码。
网口	填写静态路由的网口。
添加位置	选择静态路由配置所处的位置。

5. 单击“确定”完成新增静态路由。

后续操作

- 修改静态路由信息：选择需要修改的静态路由信息，单击“操作”列的“修改”即可修改静态路由的相关信息。
- 删除静态路由信息：选择需要删除的静态路由信息，单击“操作”列的“删除”即可删除静态路由。

日志审计

日志审计功能是记录机构用户的操作日志，并提供查看详情，审核，批量审核，验签等功能。

查看日志操作记录并审核

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“管理审计日志”，进入“管理审计日志页面”。
3. 查看“操作名称”列的操作情况，进行审计。
4. 单击“操作”列的“验签”按钮，若验签成功则单击“审核”按钮进行审计。

导出日志

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“管理审计日志”，进入“管理审计日志页面”。

3. 若您需要导出所有日志可单击“导出全部”按钮，若您需要导出部分日志可勾选需要导出的日志后单击“导出所选”。

系统管理

用户管理

用户管理是指管理当前实例下所有用户信息，提供新增、编辑、Ukey绑定、重置等功能。

新增用户

1. 登录综合安全网关实例。
2. 选择“系统管理 > 用户管理”，进入“用户管理”页面。
3. 单击页面左上角的“添加用户”，在弹出的“添加用户”窗口中配置用户参数。

参数	是否可选	参数说明
登录名	必选	自定义用户的登录名，配置后不可修改。
别名	可选	设置用户的别名。
角色	必选	选择该登录用户在系统中的角色。 支持如下四种角色： • 操作员（ctyun_operator） • 日志审计员（ctyun_auditor） • 系统管理员（ctyun_user_admin） • 超级管理员（ctyun_admin）
手机号码	可选	填写手机号。
邮箱地址	可选	填写新增用户的邮箱地址。
地址	可选	填写新增用户的地址。
输入密码	必选	设置用户的密码。
确认密码	必选	二次确认密码。

4. 配置完成后，单击“确定”完成用户添加。

后续操作

说明

系统初始的超级管理员用户不支持编辑和删除。

- 编辑用户：选择需要编辑的用户，单击“操作”列的“编辑”按钮，修改用户的相关信息后单击“确定”完成修改。
- 绑定UKey：选择需要绑定UKey的用户，单击“操作”列的“UKEY绑定”按钮，在弹出的对话框中填写UKEY序列号及PIN码完成绑定。

注意

首次使用UKEY需要在综合安全网关登录页面下载并安装UKEY插件。

- 解绑UKey：选择需要解绑UKey的用户，单击“操作”列的“UKEY解绑”按钮，在弹出的对话框中填写PIN码完成解绑。
- 重置用户密码：选择需要重置密码的用户，单击“操作”列的“设置口令”按钮，在弹出的对话框中单击“确定”完成重置。

UKEY管理

UKEY模块提供UKEY管理的相关功能，如：UKEY初始化、UKEY信息查询和备份历史查询等。

说明

首次使用UKEY需要在综合安全网关登录页面下载UKEY插件。

UKEY初始化

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“系统管理 > UKEY管理”，进入UKEY管理页面。
3. 单击“UKEY初始化”，进入UKEY初始化步骤。

4. 将UKEY设备连接，单击“刷新”按钮获取UKEY序列号。
5. 获取UKEY序列号后，输入PIN码并且二次输入进行确认完成初始化。
6. 重复第4步和第5步操作，完成后续步骤。

查看UKEY信息

1. 登录综合安全网关实例。
2. 在左侧导航栏选择“系统管理 > UKEY管理”，进入UKEY管理页面。
3. 选择“UKEY信息”即可查看已经对接的信息。

密码服务—数据加密网关操作指南

登录数据加密网关实例

您成功购买数据加密网关实例后，可在天翼云密码服务管理控制台登录。

通过天翼云控制台进入登录页面

1. 登录天翼云密码服务管理控制台。
2. 在左侧导航栏选择“密码服务”，进入“密码服务”页面。
3. 选择需要登录的数据加密网关实例，单击右上角的“管理”，进入实例登录页面，选择登录方式。

登录方式一：账号及密码登录

1. 在登录页面选择“用户名/口令”。
2. 依次输入用户名、密码。

> 说明
>
> 首次登录默认账号如下：
>
> - 管理员首次登录：默认账号为购买密码产品时，自定义设置的用户名和密码，可以参见获取初始登录账号获取初始账密。
> - 其他用户首次登录：默认账号为管理员创建用户时设置的用户名和密码，请联系管理员获取。

3. 单击“登录”即可登录数据加密网关。

> 注意
>
> 初始管理员首次登录后，进入租户列表列表页面，单击操作列的“初始化人员”，对运维账号、审计账号、管理员账号进行初始化。请妥善保存各个角色账号的密码。

登录方式二：使用UKEY登录

> 注意
>
> 首次使用UKEY登录时，需要根据界面提示下载并安装UKEY插件。

1. 在登录页面选择“USBKEY登录”。
2. 插入UKEY设备后刷新页面。

3. 输入USBKEY口令。
4. 单击“登录”，验证通过后即可登录系统。

数据加密网关概述

数据加密网关是一种专门为保护数据库数据存储安全而设计的高性能密码设备。它基于数据加密技术，能够在数据进入数据库之前对其进行加密处理，从而确保数据的机密性和完整性。这款创新设备在当今数据安全需求日益增长的环境下，扮演着至关重要的角色。

注意

在正式接入生产环境前，强烈建议您使用测试环境配合数据加密网关进行充分调试验证，确保通过后再切换至生产环境。

若因未遵循此操作流程导致的系统故障或数据风险，相关责任需由接入方自行承担。

核心功能与优势

- **数据加密：**数据库加密网关采用先进的加密算法，对数据进行实时加密。无论是静态数据还是传输中的数据，都能得到有效保护，防止未经授权的访问和数据泄露。
- **高性能处理：**作为一款高性能密码网关设备，它具备出色的处理能力，能够在保证数据安全的同时，不降低数据库的读写性能。这使得它在处理大量数据时依然能够保持高效稳定。
- **密钥管理：**内置完善的密钥管理系统，能够安全地生成、存储和管理加密密钥。密钥的严密管理是数据安全的重要保障，防止密钥泄露导致的数据风险。
- **透明加密：**提供透明的加密服务，应用程序无需改动即可享受数据加密保护。数据库加密网关在后台自动完成加密和解密操作，简化了数据安全管理。
- **兼容性强：**支持多种数据库系统和应用程序，无需对现有系统进行大规模改造即可部署。这使得它能够快速融入企业现有的IT架构，提供即时的数据安全防护。

数据库管理

数据库列表

代理管理

数据库加密机网关对数据库的加解密是通过解析改写数据库二进制协议实现的。

本章节将指导您如何将您的数据库服务纳入数据加密网关管理之下。

新增数据库代理

1. 使用运维账号登录数据加密网关。
2. 在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。
3. 单击页面左上角的“新增”按钮，进入“新增代理实例”页面。
4. 填写数据库实例代理相关内容，填写完成后单击“提交”，即可完成数据库代理配置。

参数	参数说明
数据库类型	根据您自身的业务需求选择数据库类型，具体支持选择的数据库类型请参考使用限制。
数据库版本	选择数据库版本号，具体支持的数据库版本请参考使用限制。

参数	参数说明
实例IP	填写物理数据库的IP地址，请确保填写的IP地址准确。
实例端口	填写物理数据库连接端口，请确保填写的实例端口准确。
代理端口	自定义代理数据库的服务端口。
是否大小写敏感	选择是否敏感，请根据物理数据库实际情况选择。
实例类型	选择“单节点”或者“主从”，请确认您的数据库部署方式正确选择。 • 单节点：单节点是指是指数据库软件安装在一台服务器上。 • 主从：主从是指数据库软件安装在两台或多台服务器上。 当您选择“主从”时，需要填写关联实例的IP、端口和代理端口信息。
描述	对新建的代理服务进行描述。
模式名包裹符号	与物理数据库保持一致。
字段值包裹符号	与物理数据库保持一致。
密文数据格式	根据您自身的业务需求选择“base64”或“hex”。
通配符	自定义通配符。

后续操作

- 开启/关闭代理：单击“操作”列的“开启/关闭代理”，可以控制代理数据库的开启和关闭状态，开启代理之后，应用即可将JDBC连接从物理数据库上切换至代理数据库上。
- 开启/关闭仿真模式：选择“操作”列的“仿真 > 开启/关闭”，仿真模式下，代理数据库将会把应用产生的数据SQL根据配置的规则进行解析后，存入仿真文件中，由应用判断改写后的SQL是否符合要求。

实例管理

在添加数据库代理后，可以将您的数据库实例添加至数据库代理下管理。

添加数据库实例

1. 使用运维账号登录数据加密网关。
2. 在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。
3. 单击“操作”列的“新增实例”按钮，跳转至“新增实例”页面。
4. 填写相关参数，将实例纳管至数据库代理中。

参数	参数说明
用户名	填写物理数据库登录用户名
用户口令	填写物理数据库登录用户的口令
实例库名称	填写物理数据库的实例名称
加密密钥	选择加密密钥，若首次添加数据库实例，建议选择“新建加密密钥”。
JDBC URL参数	根据数据库特性配置参数。
描述	填写数据库实例的参数。

5. 配置完成后单击“提交”即可完成数据库实例新增。

加密流程

步骤一：启用/禁用实例

禁用状态下，无法进行规则配置，且已经配置的规则将处于未生效的状态。

步骤二：配置加密规则

1. 单击“实例IP”前的 › 按钮，展开对应实例下的所有数据库实例。
2. 选择需要配置加密规则的数据库，单击“操作”列的“配置加密”。
3. 在“表名”下拉框中选择需要配置加密规则的数据库表。
4. 单击“加密配置”，选择需要加密的字段开始配置。

   加密规则：对指定表的指定字段进行加密规则配置，配置时可自定义密文字段的名称（密文字段用于存储密文数据），选择加密密钥、加密模式、补丁方式。

参数	参数说明
加密密钥	选择加密密钥，用于对明文数据进行加密
加密字段名称	选择加密字段名称，用于存储密文数据
加密模式	根据需求选择加密模式，支持选择一下三种： • ECB • CBC • FPE
补位方式	选择补位方式，目前仅支持：PKCS5Padding

   完整性保护：对指定表的指定字段进行完整性保护规则配置，配置时可自定义完整性保护字段的名称（用于存储校验数据），选择加密密钥。

参数	参数说明
加密密钥	选择加密密钥，用于对明文数据生成校验值

参数	参数说明
加密字段名称	选择加密字段名称，用于存储校验值数据

模糊查询：对指定表的指定字段进行模糊查询规则配置，配置时可自定义模糊查询列的名称。

参数	参数说明
模糊查询字段名	自定义模糊查询列的名称

脱敏：对指定表的指定字段进行脱敏规则配置，配置了脱敏规则的字段可对数据进行脱敏处理。

参数	参数说明
脱敏算法	支持以下规则： • 保留前N后M • 保留X到Y • 遮盖前N后M • 遮盖X到Y • 特殊字符前遮盖 • 特殊字符后遮盖
替换字符	用于遮盖替换敏感数据

步骤三：载入配置

勾选完成“初始化密文列”操作的字段，单击“载入配置”。

此操作是确保您配置的规则进行加载生效。

步骤四：初始化密文列

完成加密规则配置后，单击“操作”列的“初始化密文列”。

可以选择复制SQL语句手动去物理库中执行，也可以选择一键执行。执行成功之后物理库会显示密文字段。

步骤五：加密洗数

注意

进行加密洗数之前请确认仿真模式已关闭，仿真模式开启的情况下禁止加密洗数。

加密洗数是对物理数据库的存量明文数据按照相应的加密规则进行加密得到密文，将密文保存到相应的密文列中。

其他操作

- 完整性校验

  完整性校验用来校验密文数据是否经过篡改。

  完整性校验任务可以到任务列表中查看加密洗数任务完成状态以及洗数进度。

- 解密洗数

  解密洗数是对物理数据库中的密文字段中的密文按照相应的加密规则进行解密得到原文数据保存在明文字段中。

  解密完成后，此字段将不再被数据库加密网关进行管理，密文字段是否删除由用户评估后自行处理。

任务列表

任务列表用于展示洗数任务和完整性校验进度以及状态，并在洗数异常时提供下载异常信息功能，帮助及时排查定位异常原因。

查询步骤

1. 使用运维账号登录数据加密网关。
2. 在左侧导航栏选择“数据库管理 > 任务列表”，进入“任务列表”页面。
3. 选择需要查询的任务类型进行筛选。

密钥管理

密钥列表页面展示系统中当前所有的密钥及其属性，属性包括密钥来源、生成方式、密钥算法等。

新建密钥

1. 使用运维账号登录数据加密网关。
2. 在左侧导航栏选择“密钥管理 > 密钥列表”，进入“密钥列表”页面。
3. 单击“新增”，即可开始新增密钥，填写参数可参考下表。

参数	参数说明
密钥名称	自定义密钥名称。
密钥来源	选择密钥来源： • 密码设备 • KMS

参数	参数说明
密钥算法	选择密钥算法： • SM4 • AES • HMAC_SM3
生成方式	选择密钥生成方式。
密钥因子	生成方式选择“派生”时生效。

查询密钥

1. 使用运维账号登录数据加密网关。
2. 在左侧导航栏选择“密钥管理 > 密钥列表”，进入“密钥列表”页面。
3. 设置查询条件（密钥名称、密钥来源、生成方式），单击“查询”即可查询相关密钥。

日志管理

操作审计日志页面用来展示所有管理操作的日志，审计员可手动对每条日志执行审计。

数据库加密机支持操作日志完整性保护，在存储管理操作日志同时记录对应的完整性校验值，页面展示日志时会自动校验日志完整性，可有效防止非法用户恶意篡改操作审计日志。

查询审计日志

1. 使用审计角色登录数据加密网关。
2. 在菜单栏选择“日志管理 > 审计日志列表”进入审计列表页面。
3. 设置查询条件（时间范围、操作用户、操作描述），单击“查询”即可查询相关审计日志。

审计日志

1. 使用审计角色登录数据加密网关。
2. 在菜单栏选择“日志管理 > 审计日志列表”进入审计列表页面。
3. 选择需要审计的日志，单击“操作”列的“审计”按钮，进行审计。
4. 在审计日志列表页面查看审计结果。

密码服务—数字证书认证系统操作指南

登录数字证书认证系统

您成功购买数字证书认证系统实例后，可在天翼云密码服务管理控制台登录。

通过天翼云控制台进入登录页面

1. 登录天翼云密码服务管理控制台。
2. 在左侧导航栏选择“密码服务”，进入“密码服务”页面。
3. 选择需要登录的数字证书认证系统实例，单击右上角的“管理”，进入实例登录页面，选择登录方式。

登录方式一：账号及密码登录

1. 在登录页面选择“用户名/口令”。

2. 依次输入用户名、密码。

> 说明
>
> 首次登录默认账号如下：
>
> - 管理员首次登录：默认账号为购买密码产品时，自定义设置的用户名和密码，可以参见获取初始登录账号获取初始账密。
> - 其他用户首次登录：默认账号为管理员初始化人员时设置的用户名和密码，请联系管理员获取。

3. 单击“登录”即可登录数字证书认证系统。

> 注意
>
> 初始管理员首次登录后，进入租户列表列表页面，单击操作列的“初始化人员”，对运维账号、审计账号、管理员账号进行初始化。请妥善保存各个角色账号的密码，否则将无法正常登录实例。

登录方式二：使用UKEY登录

> 注意
>
> 首次使用UKEY登录时，需要根据界面提示下载并安装UKEY插件。

1. 在登录页面选择“USBKEY登录”。
2. 插入UKEY设备后刷新页面。
3. 输入USBKEY口令。
4. 单击“登录”，验证通过后即可登录系统。

初始化人员

首次使用初始管理员登录数字证书认证系统后，需要初始化人员，对运维账号、审计账号、管理员账号进行初始化。

操作步骤

1. 使用初始管理员登录数字证书认证系统。
2. 在租户列表页面，单击default租户操作列的“初始化人员”。

3. 在弹出的初始化人员窗口中，设置初始化账号的口令。

   通过左上角切换认证方式，支持**用户名口令认证**和**USBKEY认证**两种方式：

   - USBKEY认证：输入USBKEY口令，单击操作列的“认证”。

     注意

     请妥善保存各个账号的口令，否则将无法登录实例。

     单击列表底部的“新增人员”，可以新增用户。

   - 用户名口令认证：输入用户名、口令。

     注意

     请妥善保存各个账号的口令，否则将无法登录实例。

     单击列表底部的“新增人员”，可以新增用户。

4. 设置完成后，单击“提交”，完成人员初始化。流程状态变为“已初始化人员”。

单击操作列的“人员信息”可以查看账号信息，包括用户名称、角色和登录时间。

CA证书管理

CA证书是一种数字证书，由认证机构（Certificate Authority，简称CA）颁发，用于证明某一主体（如组织机构）的身份合法性，有时也被称为网络的身份证 。

新增自签CA证书

1. 使用管理员账号登录数字证书认证系统。
2. 在左侧导航栏选择“机构管理 > CA证书管理”，进入“CA证书管理”页面。
3. 单击“新增”，进入“新增CA证书”页面。
4. 选择“自签CA”页签，填写相关内容。

参数	参数说明
别名	证书的名称。
密钥算法	选择证书的密钥算法类型，支持选择以下两种类型： • RSA • SM2
密钥长度	选择证书的密钥长度，根据选择的密钥算法会有不同的密钥长度： • RSA支持：1024、2048、3072、4096 • SM2支持：256
签名算法	选择根证书支持的签名算法，根据选择的密钥算法会有不同的签名算法： • RSA支持：SHA256WithRSA、SHA384WithRSA、SHA512WithRSA、SHA256WithRSA/PSS、SHA384WithRSA/PSS、SHA512WithRSA/PSS • SM2支持：SM3WithSM2
有效期	选择开始时间和结束时间。
证书模版	选择证书模版。

是否使用自定义主题	选择是否使用自定义主题：
	• 是：填写指定格式的主题内容，例如C=CN,CN=TEST。
	• 否：填写如下对应项，系统自动拼接主题内容 。
	  • 名称：更新的CA根证书名称，存储在证书中使用者的CN。
	  • 国家：从下拉列表中选择一个国家。
	  • （可选）省份、城市、单位、部门、邮箱：一般填写使用者信息，存储在证书的DN项中。

5. 填写完成后单击“提交”，即完成自签CA的导入。

导入CA证书

1. 使用管理员账号登录数字证书认证系统。
2. 在左侧导航栏选择“机构管理 > CA证书管理”，进入“CA证书管理”页面。
3. 单击“新增”，进入“新增CA证书”页面。
4. 选择“导入证书”页签，并且填写相关内容。

参数	参数说明
导入私钥	根据您自身需要导入的证书有无私钥自行选择。 • 若您选择“否”，不导入私钥，则需要先生成证书CSR。 • 若您选择“是”，则需要上传CA私钥。

参数	参数说明
CA私钥	上传CA私钥（只能上传pem编码的PKCS8私钥，且不超过10kb）
CA证书	上传CA证书。（只能上传pem编码的证书或证书链，且不超过10kb）
别名	别名和证书请求文件中的别名保持一致。

5. 单击“提交”，完成证书导入。

相关操作

- **更新证书**：选择需要更新的证书，单击“操作”列的“更新”按钮，即可开始更新证书相关信息。
- **下载证书**：选择需要下载的证书，单击“操作”列的“下载”按钮，即可下载证书信息。
- **启用/禁用证书**：选择需要启用/禁用的证书，单击“操作”列的“启用/禁用”按钮，即可启用/禁用证书。
- **查看证书详情**：选择需要查看详情的证书，单击证书别名的链接，即可查看证书详情。

子CA管理

子CA证书是由根证书授权的次级证书颁发机构颁发的数字证书 。

新增子CA证书

1. 使用管理员账号登录数字证书认证系统。
2. 在左侧导航栏选择“机构管理 > 子CA管理”，进入“子CA管理”页面。
3. 单击“新增”开始新增子CA证书。
4. 单击“上传文件”上传证书文件并且选择所属的CA证书。
5. 根据需求选择是否使用模板，选择完成后单击“提交”即可完成子CA证书的新增。

后续操作

- **下载子CA证书**：选择需要下载的子CA证书，单击“操作”列的“下载”按钮，即可下载子CA证书信息。
- **注销子CA证书**：选择需要注销的子CA证书，单击“操作”列的“注销”按钮，即可注销子CA证书信息。

CRL管理

CRL（证书吊销列表，Certificate Revocation List）里存储了被注销证书的序列号、注销时间和注销原因。同时，为保证CRL的有效性，CRL携带了CA的签名。

按照签名算法不同，分为RSA CRL和SM2 CRL。

通过CRL管理可实现手动签发CRL、下载CRL、查看和查找功能。

配置CRL

1. 使用管理员账号登录数字证书认证系统。
2. 在左侧导航栏选择“CRL管理 > CRL配置”，进入“CRL配置”页面。
3. 填写CRL配置相关参数。

参数	参数说明
自动启动	• 选择“是”，每次服务启动时立刻开启CRL定时发布任务。 • 选择“否”，停止CRL定时发布任务。

参数	参数说明
类型	选择签发CRL的类型： • 全量：签发全量CRL。 • 增量：签发增量CRL。 • 全量&增量：两者都签发。
生成周期	定时生成CRL的周期，以小时为单位，默认为1小时

4. 单击“提交”完成CRL配置。

生成CRL

1. 使用管理员账号登录数字证书认证系统。
2. 在左侧导航栏选择“CRL管理 > CRL列表”，进入“CRL列表”页面。
3. 在“CRL列表”页单击“生成”，即可生成CRL。

   当前CA可以实现全量CRL和增量CRL，根据系统设置的CRL类型进行生成。

   - 如果只选择全量CRL，每次生成的CRL都会覆盖前一同类型CRL，因此列表里只有一个RSA算法CRL和一个SM2算法CRL。
   - 增量CRL会生成每年产生的证书注销列表，同一个年的会覆盖。

下载CRL

1. 使用管理员账号登录数字证书认证系统。
2. 在左侧导航栏选择“CRL管理 > CRL列表”，进入“CRL列表”页面。
3. 选择需要下载的CRL，单击“操作”列的“下载”按钮，即可下载CRL。

证书管理

证书申请

证书申请分为两种：PKCS10申请和UKEY申请。

- PKCS10申请是指使用P10请求文件的形式进行证书的申请。
- UKEY申请是将用户信息录入进行证书的申请。

申请PKCS10证书

1. 登录数字证书认证系统。
2. 在左侧导航栏选择“证书申请 > PKCS10申请”，进入“PKCS10申请”页。
3. 选择证书模板，选择CA证书，填写证书有效期。

   注意

   证书模板中公钥算法要与证书请求文件中公钥的算法一致。

4. 根据业务需求选择是否使用模板。
5. 选择完成后单击“提交”即完成PKCS10证书申请。

UKEY申请

1. 登录数字证书认证系统。

2. 在左侧导航栏选择“证书申请 > UKEY申请”，进入“UKEY申请”页。
3. 选择所属的“CA”，并且选择“密钥算法”、“密钥长度”、“签名算法”和“有效期”。
4. 选择“模板”并且填写相关信息。
5. 填写完成后，单击“提交”并且在弹出的对话框中选择UKEY类型，并且将UKEY与您的设备连接后单击“确定”。

证书其他操作

您的数字证书在申请完成后可以进行如下操作：证书更新、证书注销、证书冻结、证书解冻、证书延期。

更新证书

证书更新操作就是注销原证书然后签发新的证书。只能对有效证书进行证书更新操作。

1. 使用操作员账户登录数字证书认证系统。
2. 在左侧导航栏选择“证书管理 > 证书更新申请”，进入“证书更新申请”页面。
3. 选择需要更新的证书，单击“操作”列的“更新”按钮，即可开始更新。
4. 在更新申请页填写证书的有效期和主题内容后单击“提交”。

说明

- 更新的证书是PKCS10证书直接下载使用即可。
- 更新的证书是UKEY证书，则需要同步连接UKEY设备进行更新。

注销证书

证书注销就是使证书永久失效。只能对有效证书进行证书注销操作。

1. 使用操作员账户登录数字证书认证系统。
2. 在左侧导航栏选择“证书管理 > 证书注销申请”，进入“证书注销申请”页面。
3. 选择需要注销的证书，单击“操作”列的“注销”按钮，即可开始注销。

冻结证书

证书冻结就是使证书暂时失效。只能对有效证书进行证书冻结操作。冻结后证书可通过解冻操作使证书恢复有效。

1. 使用操作员账户登录数字证书认证系统。
2. 在左侧导航栏选择“证书管理 > 证书冻结申请”，进入“证书冻结申请”页面。
3. 选择需要冻结的证书，单击“操作”列的“冻结”按钮，待程序响应开始冻结。

解冻证书

证书解冻是证书冻结的逆操作，使冻结的证书恢复有效。

1. 使用操作员账户登录数字证书认证系统。
2. 在左侧导航栏选择“证书管理 > 证书解冻申请”，进入“证书解冻申请”页面。
3. 选择需要解冻的证书，单击“操作”列的“解冻”按钮，待程序响应开始解冻。

证书延期

证书延期操作是对已有的证书有效期后延，延长证书的使用期限。

1. 使用操作员账户登录数字证书认证系统。
2. 在左侧导航栏选择“证书管理 > 证书延期申请”，进入“证书延期申请”页面。

3. 选择需要延期的证书，单击“操作”列的“延期”按钮。
4. 在弹出的对话框中选择延期后的到期时间，单击“确定”完成延期操作。

密钥恢复

按照CA标准规范要求，CA需要提供加密证书密钥对恢复功能。安全的恢复加密密钥对到安全存储介质，例如USBKey。

密钥恢复功能有密钥恢复申请和密钥恢复审核组成。其中，密钥恢复申请需要注册操作员权限，密钥恢复审核需要审核操作员权限。

注意

密钥恢复暂不支持ECDSA算法。

操作步骤

1. 使用操作员账户登录数字证书认证系统。
2. 在左侧导航栏选择“密钥恢复 ”，根据您自身的需求选择“有效证书密钥恢复”、“过期证书密钥恢复”或“注销证书密钥恢复”。
3. 进入对应的密钥恢复页面，选择需要恢复密钥的证书，单击“操作”列的“恢复”按钮。
4. 根据弹窗提示插入UKEY设备，选择UKEY类型并输入口令，恢复成功后加密密钥将保存到UKEY中。

密码服务—协同签名服务操作指南

管理员登录协同签名服务实例

您成功购买协同签名服务实例后，可在天翼云密码服务管理控制台登录。

通过天翼云控制台进入登录页面

1. 登录天翼云密码服务管理控制台。
2. 在左侧导航栏选择“密码服务”，进入“密码服务”页面。

3. 选择需要登录的协同签名服务实例，单击右上角的“管理”，进入实例登录页面，选择登录方式。

登录方式一：账号及密码登录

1. 系统默认为“账号密码登录”，在登录页面输入账号及密码。

说明

- 首次登录实例时，请根据界面提示修改密码，否则无法进入系统。
- 首次登录默认账号如下：
  - 管理员首次登录：默认账号为购买密码产品时，自定义设置的用户名和密码，可以参见获取初始登录账号获取初始账密。
  - 其他用户首次登录：默认账号为管理员创建用户时设置的用户名和密码，请联系管理员获取。

2. 单击“登录”即可登录协同签名服务。

登录方式二：使用UKEY登录

注意

- 首次使用需要先下载安装当前版本USBKey登录的websockets控件。
- 仅管理员账号支持使用UKEY登录，如何配置UKEY请参考：编辑管理员章节。

1. 在登录页面右下角选择“UKEY登录”。

2. 插入UKEY设备后刷新页面即可登录。

组织管理

在组织管理界面，管理员在该界面可进行新增，编辑组织以及添加下级组织，查询组织信息，同步组织等操作。

新增组织

说明

- 机构名称则为机构的根组织，首次添加会提示将机构设置为一级组织。
- 选择上级组织，组织类型，输入新组织名称，点击提交完成添加。

1. 使用管理员账号登录协同签名服务。
2. 在左侧导航栏选择“用户管理 > 组织管理”，进入“组织管理”页面。
3. 单击页面的“新增组织”按钮，进入“新增组织”页面，并填写相关参数。

   您也可以在已有组织下新增下级组织，可单击需要新增组织“操作”列的“添加下级”按钮。

参数	参数说明	填写示例
上级组织	选择新增组织所属的上级组织	-
组织名称	填写组织的名称。 支持英文、中文、数字、“_”、“-”，2-200字符。	研发部-_
组织类型	选择组织的类型，支持选择“总公司”、“分公司”、“部门”、“组”。	部门
组织序号	填写组织序号。 可选0-999，数字越小越靠前	999
备注	填写组织的备注。	-

4. 填写完成后，根据需求跟进入如下两种选择：
   - 单击“保存”，可直接保存已填写的组织并回到“组织管理”页面。
   - 单击“保存并新增下一个”，保存已填写的组织并且可重新填写新的组织信息。

批量导入组织

如果您有大量的组织需要添加，可使用批量导入功能。

1. 使用管理员账号登录协同签名服务。
2. 在左侧导航栏选择“用户管理 > 组织管理”，进入“组织管理”页面。
3. 单击“批量导入/导出”按钮，进入“批量导入/导出”页面，单击“下载模板”。

4. 打开下载完成的Excel模板，认真阅读填写须知，并按照规则填写需要新增的组织信息。
5. 保存文件，上传至协同签名服务即可完成组织新增。

其他操作

- 编辑组织：在“组织管理”页面，选择需要编辑信息的组织，单击“操作”列的“编辑”按钮，即可编辑组织信息。

- 删除组织：在“组织管理”页面，选择需要删除的组织，单击“操作”列的“删除”按钮，即可删除组织。

说明

以下情况不支持删除组织，不显示删除按钮：

- 带有下级组织的组织
- 组织下有用户

用户管理

用户管理界面，在该界面可进行新增、导入、导出、编辑、锁定、注销、删除以及重置密码，查询用户信息等操作。

如果是机构管理员登录，则显示该机构下所有用户的信息。

新增用户

1. 使用管理员账号登录协同签名服务。
2. 在左侧导航栏选择“用户管理 > 用户管理”，进入“用户管理”页面。

3. 单击“新增用户”，跳转至“新增用户”界面并填写用户参数。

参数	参数说明	填写示例
账号	填写新增用户的账号名。 账号可以是邮箱、手机号，或由中文、数字、英文字母和下划线组成的4-110位其他字符（不能以特殊字符开头，1个中文算3个字符） 说明 用户账号必须是唯一的，不能重复，包括用户绑定手机号和邮箱。	Test1@chinatelecom.cn
姓名	填写用户的姓名。 支持中文、英文、数字，不能以特殊字符开头，长度2-20字。	张三
组织	选择新增用户所属的组织。	研发部

参数	参数说明	填写示例
密码	填写密码。 密码为8-32位大写字母、小写字母、数字、特殊字符中3种或以上组合。	-
确认密码	再次填写密码。	-
手机号	填写用户的手机号，可填写多个。 手机号说明可选择“主要”、“住宅”、“私人”、“工作”、“其他”，第一个填写的手机号默认为“主要”。	-
邮箱	填写用户的邮箱地址。	Test1@chinatelecom.cn

说明

新增后的用户包括用户绑定手机号，邮箱地址会自动添加到标识列表上。

4. 填写完成后单击“提交”即可完成用户新增。

批量导入用户

如果您有大量的用户需要添加，可使用批量导入功能。

1. 使用管理员账号登录协同签名服务。
2. 在左侧导航栏选择“用户管理 > 用户管理”，进入“用户管理”页面。

3. 单击“批量导入/导出”按钮，进入“批量导入/导出”页面，单击“下载模板”。

4. 打开下载完成的Excel模板，认真阅读填写须知，并按照规则填写需要新增的用户信息。
5. 保存文件，上传至协同签名服务即可完成用户新增。

其他操作

编辑用户

在“用户管理”页面，选择需要编辑信息的用户，单击“操作”列的“编辑”按钮，即可编辑用户信息。

重置用户密码

1. 在“用户管理”页面，选择需要重置密码的用户，单击“操作”列的“更多 > 重置”按钮。
2. 在弹出的对话框中填写用户的新密码，单击“确定”即可完成密码重置。

说明

密码为8-32位大写字母、小写字母、数字、特殊字符中3种或以上组合。

锁定用户

处于“已激活”状态的用户，管理员可以对其进行锁定。

1. 在“用户管理”页面，选择需要锁定的用户，单击“操作”列的“锁定”按钮。
2. 在弹出的对话框中选择需要锁定的时间，支持选择：20分钟、1小时、8小时、24小时、3天、5天、30天、3个月。

3. 选择完成后，单击“确定”即可完成用户锁定。

解锁用户

处于“已锁定”状态的用户，管理员可以对其进行解锁。

在“用户管理”页面，选择需要解锁的用户，单击“操作”列的“解锁”按钮，在弹出的对话框中单击“解锁”即可解锁用户。

注销用户

在“用户管理”页面，选择需要注销的用户，单击“操作”列的“注销”按钮，即可注销用户。

注意

注销后账号无法恢复，请谨慎注销。

删除用户

处于“已注销”状态的用户，管理员可以对其进行删除。

在“用户管理”页面，选择需要删除的用户，单击“操作”列的“删除”按钮，即可删除用户。

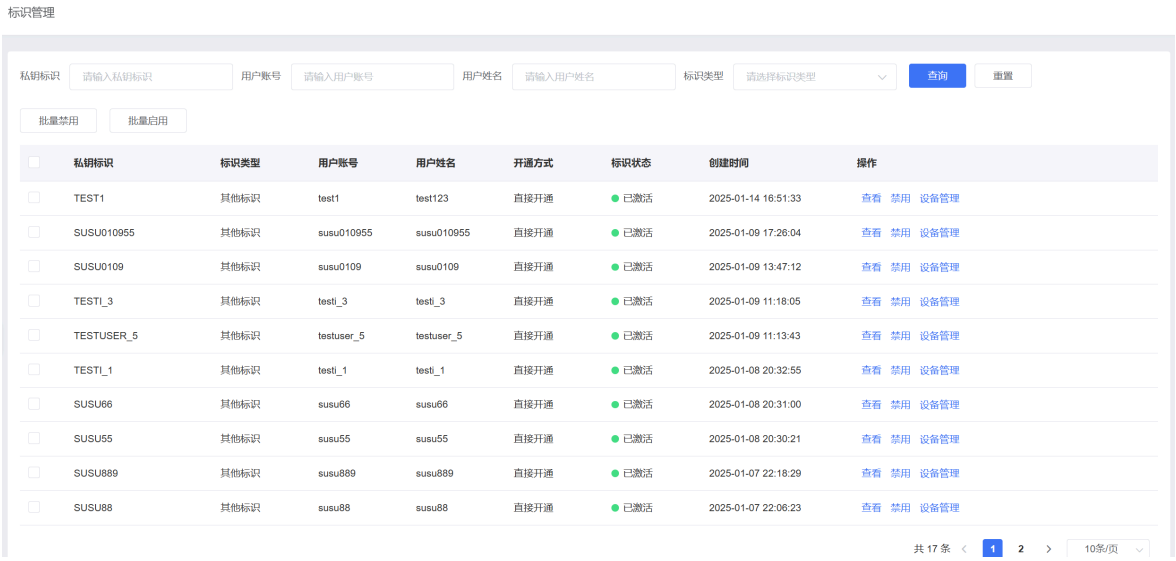
标识管理

标识管理界面，在该界面可进行新增，编辑，查看，管理标识。

- 添加的用户是自动注册到标识列表上，包括绑定的手机号和邮箱地址。
- 标识状态有两种：已激活，未激活。
- 当用户的邮箱地址符合机构域名时，则会自动激活。

查看标识信息

1. 使用管理员账号登录协同签名服务。
2. 在左侧导航栏选择“标识管理”，跳转至“标识管理”页面。



3. 选择需要查看的标识，单击“操作”列的“查看”按钮，即可查看标识信息。

说明

- 查看列表上记录标识的安全属性，如初始服务月数，私钥下载次数，是否自动延期，服务起始时间，结束时间等。
- 记录私钥标识的下载记录，下载时间，下载的密钥类型，绑定的设备信息，对应的密码机等信息。

设备管理

1. 使用管理员账号登录协同签名服务。
2. 在左侧导航栏选择“标识管理”，跳转至“标识管理”页面。
3. 选择需要进行设备管理的标识，单击“操作”列的“设备管理”按钮，即可查看绑定的设备信息。

说明

- 这里记录的是下载私钥标识的设备信息。
- 当标识开启设备认证时，一旦绑定了设备，其他设备就无法下载该标私钥，点击解绑后，则私钥标识可以到其他设备上去下载。

启用/禁用标识

选择需要进行设备管理的标识，单击“操作”列的“启用/禁用”按钮，即可启用/禁用的标识。

系统管理

管理员管理

协同签名服务支持新增、编辑、删除管理员。

新增管理员

1. 使用管理员账号登录协同签名服务实例。
2. 在左侧导航栏选择“系统管理 > 管理员管理”，进入“管理员管理”页面。

3. 单击“新增管理员”，进入新增管理员页面。

4. 在弹出的对话框中填写相关参数。

参数	参数说明
账号	填写新建管理员的登录账号。
所属组织	填写新建管理员所属的组织。
选择角色	在下拉框中选择管理员的角色。 支持机构超级管理员、机构审计管理员、机构业务管理员、机构系统管理员。
设置密码	设置管理员账号的密码。
确认密码	二次确认管理员账号的密码。
姓名	（可选）填写新建管理员账号的姓名。

5. 填写完成后，单击“提交”即完成新建管理员。

编辑管理员

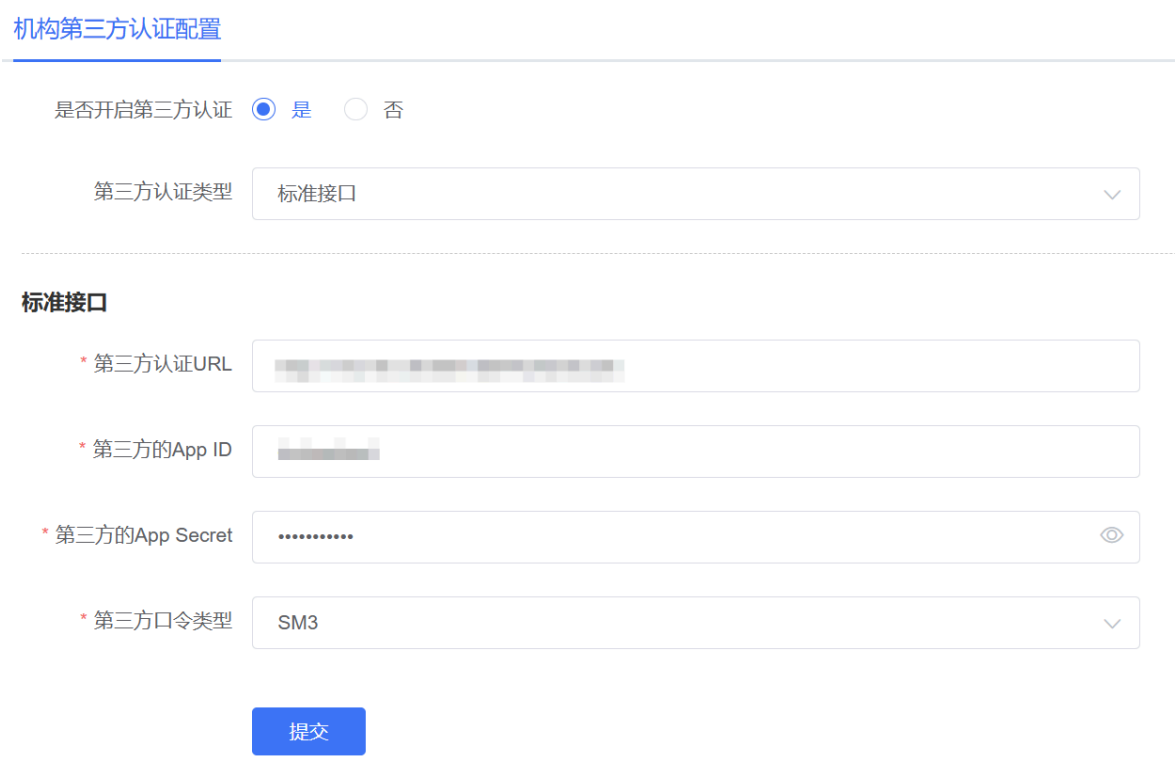
1. 使用管理员账号登录协同签名服务
2. 在左侧导航栏选择“系统管理 > 管理员管理”，进入“管理员管理”页面。
3. 选择需要编辑的管理员信息，单击“操作”列的“编辑”按钮。
4. 在弹出的对话框中编辑相关信息，可在“UKEY绑定”参数右侧，单击“添加UKEY绑定”，为管理员账号绑定UKEY。

开启第三方认证

第三方认证还要确保签名行为是真实发生的，并且是按照预定的规则进行的。这包括验证签名的时间戳、签名的顺序（在一些有先后顺序要求的协同签名场景中）以及签名的完整性。

1. 使用管理员账号登录协同签名服务

2. 在左侧导航栏选择“系统管理 > 系统设置”，进入“机构第三方认证配置”页面。



3. 开启第三方认证并填写标准接口参数。

参数	参数说明	填写示例
第三方认证URL	填写用户校验用户密码的接口地址，该地址请咨询托管用户的业务系统管理员。	-
第三方的App ID	填写用于接口鉴权的APP ID，该地址请咨询托管用户的业务系统管理员	-
第三方的App Secret	填写用于接口鉴权的密钥信息，该地址请咨询托管用户的业务系统管理员	-
第三方口令类型	添加关于密码提交第三方业务系统的加密方式，请咨询托管用户的业务系统管理员（推荐使用SM3）	SM3

配置第三方CA

配置第三方CA系统是为了确保系统在终端用户能够快速签发用户证书。

说明

CA中心已经有相关证书，例如CAID为1855893654128865282。

1. 使用管理员账号登录协同签名服务
2. 在左侧导航栏选择“系统管理 > 第三方CA配置”，进入“连接配置”页面。

3. 单击左上角的“添加CA”按钮，在弹出的对话框中填写相关参数。

参数	参数说明	填写示例
CA名称	填写CA证书的名称。	测试CA
CA地址	填写CA证书的地址。 CA地址为“http(s)://+域名/IP:端口”格式的网址。	https://192.168.0.1:8488
用户名	填写CA接口调用的用户名。	-

参数	参数说明	填写示例
密码	填写CA接口调用的用户密码。	-
类名称	CA证书的类名称，不建议修改使用默认值。	CertDownload
签发证书的CA ID	填写CA ID。	1855893654128865282

4. 填写完成后，单击“确认”，返回“连接配置”页面。
5. 在页面左上方选择“根证书配置”，进入“根证书配置”页面。

6. 单击“添加根证书”，在跳转的窗口填写相关参数。

参数	参数说明	填写示例
CA名称	填写CA证书的名称。	测试CA
CA描述	填写CA证书的描述	-
证书类型	选择待添加的证书类型，可选“证书链”或“一级根证书”。	一级根证书

参数	参数说明	填写示例
根证书导入方式	可选择“上传证书文件”或“输入证书内容”。 • 上传证书文件：上传证书的文件。 • 输入证书内容：输入Base64编码根证书内容。	-
CA ID	填写CA ID。	1855893654128865282

7. 填写完成后，单击“确定”完成第三方CA配置。

密码服务—时间戳服务操作指南

登录时间戳服务

时间戳服务，可提供标准的时间戳服务功能，可将交易时间和交易内容固化，适用于时间敏感型业务数据的安全保护。该服务可以满足信息系统密码应用测评中关于实体行为不可否认性的要求。

开放端口要求

为避免网络故障或网络配置问题影响使用服务，请参考下表配置实例安全组。

注意

如何添加安全组规则请参考：添加安全组规则章节。

端口	端口用途
9080-9083	• 9080端口：Http协议 • 9081端口：Tcp协议 • 9082端口：Https协议 • 9083端口：TLS协议

通过天翼云控制台进入登录页面

1. 登录天翼云密码服务管理控制台。
2. 在左侧导航栏选择“密码服务”，进入“密码服务”页面。

3. 选择需要登录的时间戳服务实例，单击右上角的“管理”，进入实例登录页面，选择登录方式。

时间戳服务配置流程

时间戳服务配置步骤如下：

1. 根证书管理：在时间戳服务-根证书管理页面中导入根证书；可以对导入的证书进行查看，下载证书，删除操作
2. 应用管理：在时间戳服务-应用管理页面中创建应用，可以通过访问密钥管理中对应用访问密钥进行停用和启用操作；在应用授权中可以对时间戳证书(这里的证书对应应用管理中的证书)进行授权和取消授权；进入时间戳密码服务实例管理页面，依次创建对称密钥、配置用户证书及根证书、创建应用并授权证书或密钥；
3. 证书管理：时间戳服务-证书管理中提供生成证书请求，导入PFX密钥两种方法；可以对生成/导入的证书进行查看，更新证书，下载，停用操作
4. 策略管理：时间戳服务-策略管理中包含：时间戳策略管理包括时间戳OID列表，NTP时间源配置管理；在新增完时间戳OID后可以对其进行停用和设置为默认策略操作，NTP时间源配置可以对NTP相关配置进行维护

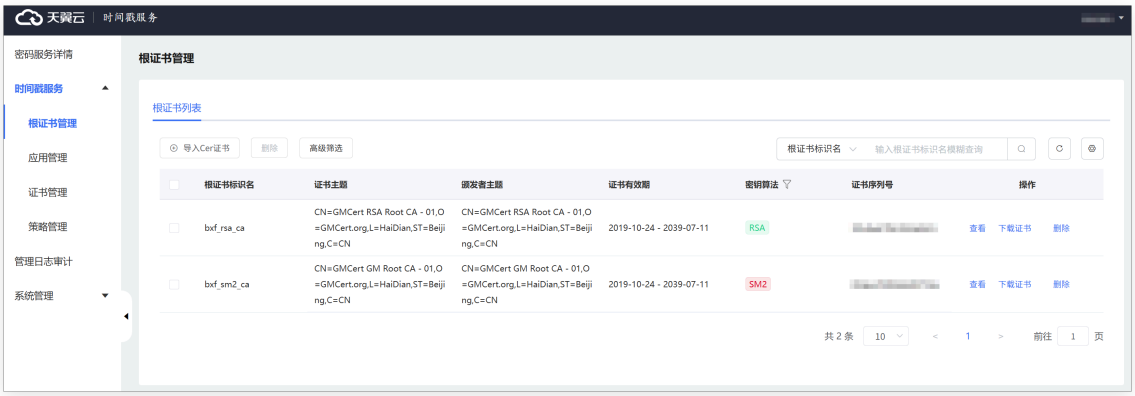
导入根证书

根证书管理的主要目的用于时间戳密码服务进行验签的时候使用根证书对用户证书的有效性进行验证。提供导入cer证书、下载证书、删除、查询详情等功能。

根证书列表

1.通过左侧菜单栏进入根证书管理列表页面，默认进入根证书管理页面。

2.单击列表上方的“导入Cer证书”进入导入Cer证书页面，按照页面要求导入证书文件，并点击“保存”可完成根证书的导入。根证书导入完成后可以对证书进行：查看，下载，删除操作。



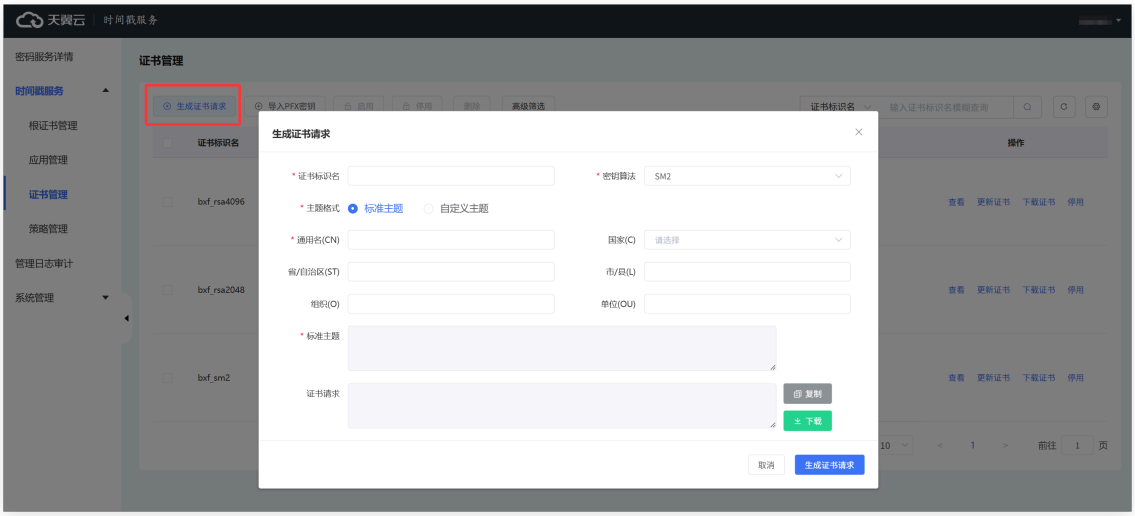
时间戳证书管理

主要用于相关业务操作，提供时间戳证书的配置功能。提供生成证书请求，导入PFX密钥两种方式。

CSR生成证书导入

具体操作步骤如下：

1.单击列表上方的“生成证书请求”按钮，进入生成证书请求页面，在该页面生成证书请求并下载到用户本地；



2.上传CSR证书请求到证书签发机构，完成证书签发并下载到本地；

说明

签发证书的增强型用法中要包含时间戳用法。

3.通过“更新证书”导入证书；

4.完成证书文件导入后，生成可用的时间戳证书。

PFX方式导入证书

具体操作步骤如下：

1.在CA中心签发可用的时间戳证书（单密钥、双密钥均可），选择PKCS12/PFX格式，并下载到用户本地；

说明

签发证书的增强型用法中要包含时间戳用法。

2.在用户证书管理页面选择“导入PFX密钥”，导入PFX文件及密码；

3.完成证书文件导入后，生成可用的时间戳证书。

配置应用

业务应用系统要使用时间戳密码服务前，必须在时间戳密码服务注册，即在时间戳密码服务的应用管理里添加相关的应用信息，提供新增、编辑、删除、启用、停用、访问密钥管理、应用授权等功能。

创建应用

通过左侧菜单栏进入应用管理页面，创建应用，并选择认证方式、是否密钥授权，填入信息后点击“确定”按钮完成应用的新增；

- 应用认证方式支持两种模式，无认证模式和访问密钥认证模式。

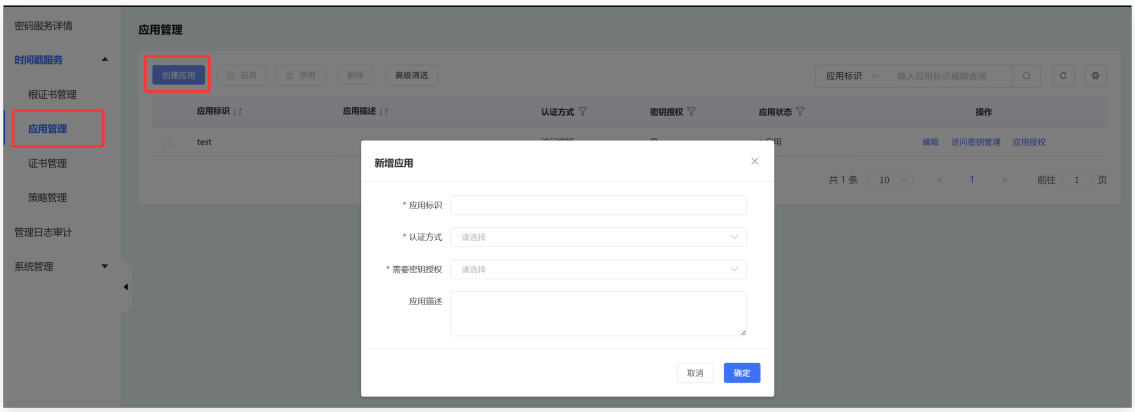
选择“无认证模式”：服务端不会对应用进行校验；

选择“访问密钥认证模式”服务端会校验应用访问密钥「ak」和「sk」的正确性。应用创建之后，需要在应用列表最后的操作列点击“访问密钥管理”，进入访问密钥管理列表页，生成访问密钥，并下载进行妥善保存。

- 需要密钥授权：

选择“是”，该应用只能使用已授权的时间戳证书，用户需要通过列表右侧操作栏中的“应用授权”为用户授权可用的时间戳证书；

选择“否”，该应用可以任意使用所有的时间戳证书，无论时间戳证书是否在应用授权中进行授权，都可以被业务接口调用。



生成并获取应用访问密钥

通过应用列表的操作栏中“访问密钥管理”进入该应用的访问密钥管理列表页，点击“生成密钥”，生成访问密钥并下载至用户本地；

应用授权

如创建应用时“是否需要密钥授权”选择的“是”，则在使用加密机内的密钥或证书时需要对其进行授权。

在“应用管理”列表的操作栏中，单击“应用授权”，选择对应的密钥或证书并单击“授权”按钮对其进行授权。

配置时间戳策略

通过左侧菜单栏进入时间戳策略管理页面，时间戳策略管理包括RFC时间戳策略配置和时间戳OID列表管理功能。

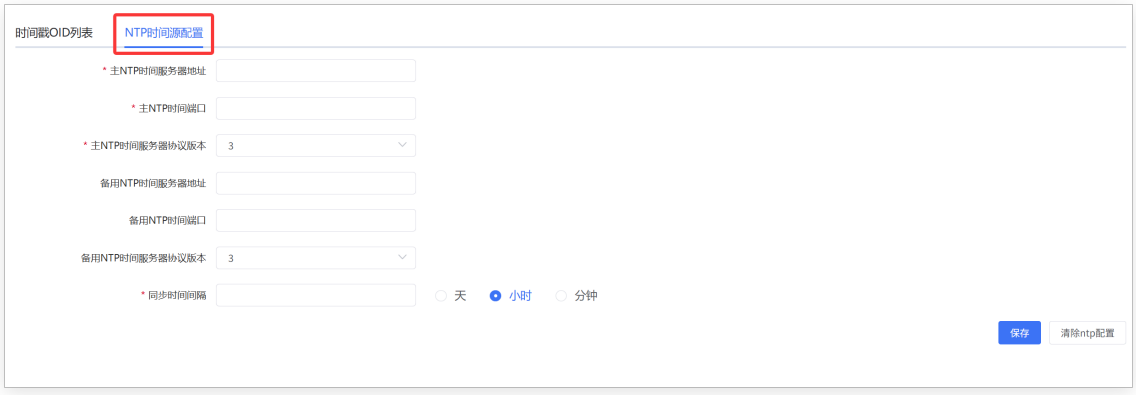
时间戳OID配置

1.选择时间戳OID列表TAB页，单击列表上方的“新增时间戳策略”按钮，进入“新增时间戳策略OID”页面。

2.按照页面要求输入策略OID并选择时间戳证书，点击“确定”可完成时间戳策略OID的创建。

NTP时间源配置

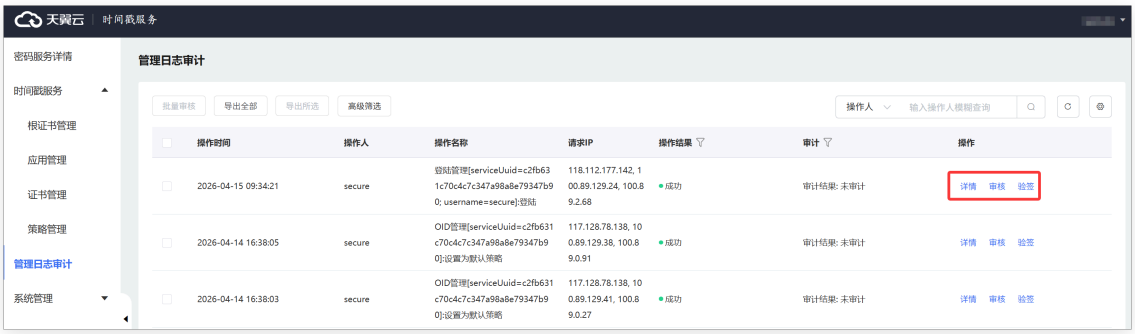
通过左侧菜单栏进入时间戳策略管理页面，进去NTP时间源配置，需要配置主NTP时间服务器地址、主NTP时间端口、协议版本、同步时间间隔等，并单击“保存”按钮，保存配置内容。



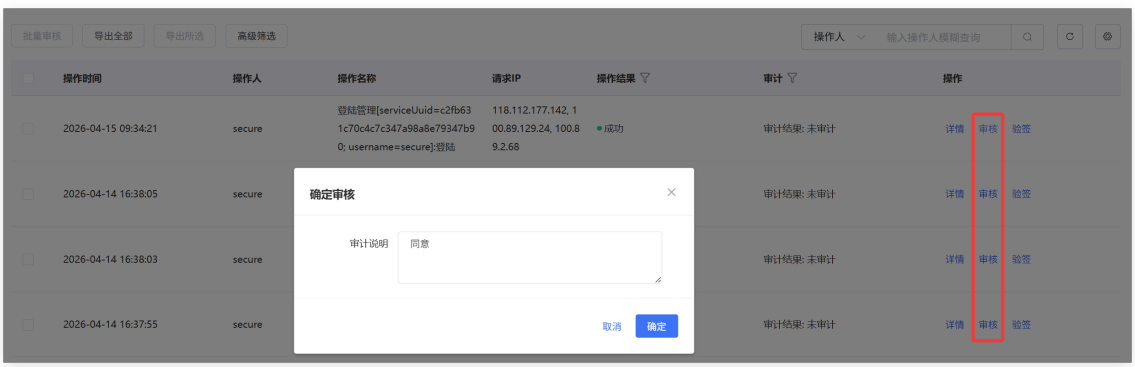
主NTP时间服务器地址、主NTP时间端口、协议版本、同步时间间隔为必填项，其他为非必填项。

管理审计日志

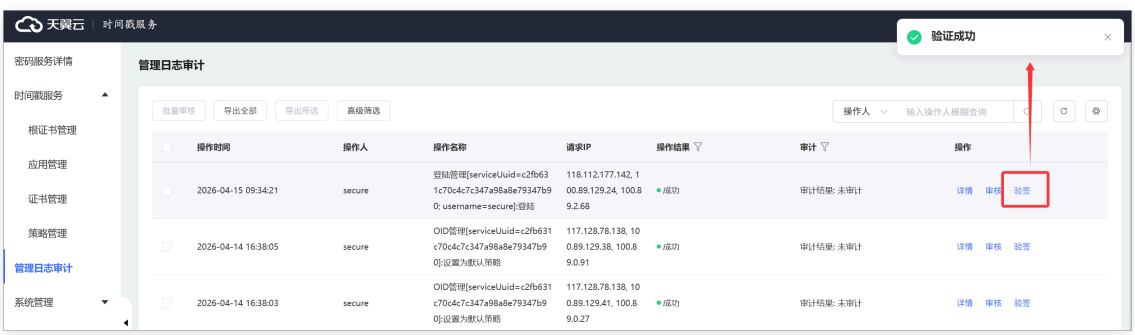
管理日志记录了操作时间，操作人，操作名称，请求IP，操作结果，审计结果等信息，可以对时间戳服务管理中产生的操作日志进行查看详情，审核，验签操作。



在进行审核时可以填写审计说明。



可以对每条操作记录进行验签操作

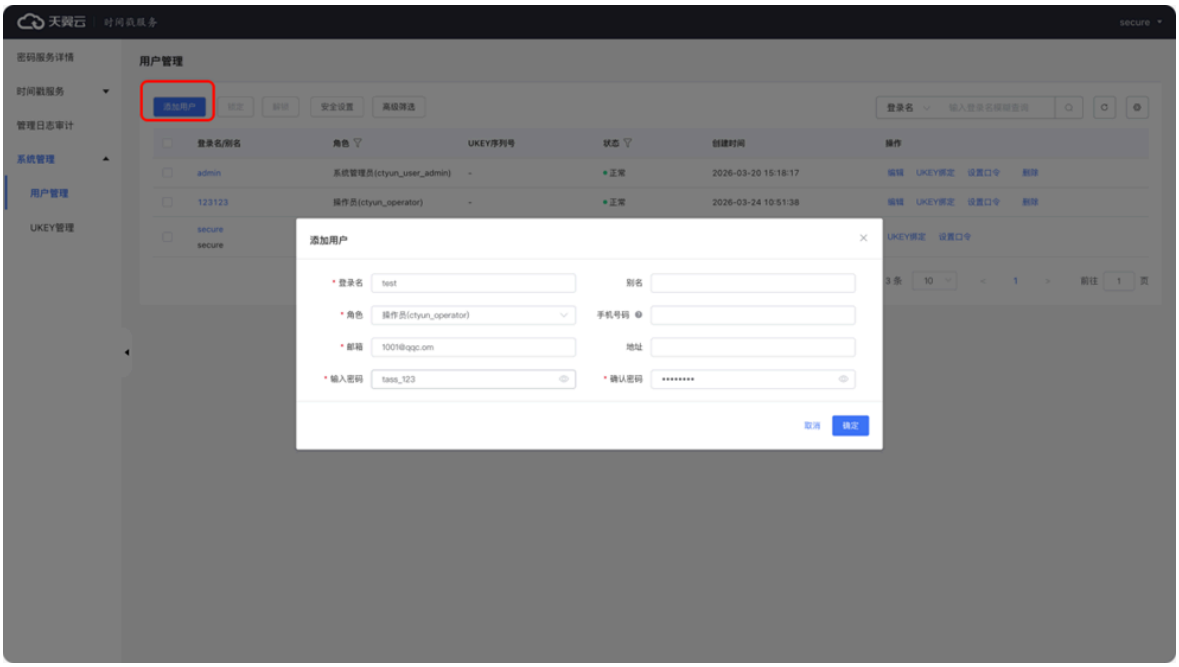


系统管理

用户管理

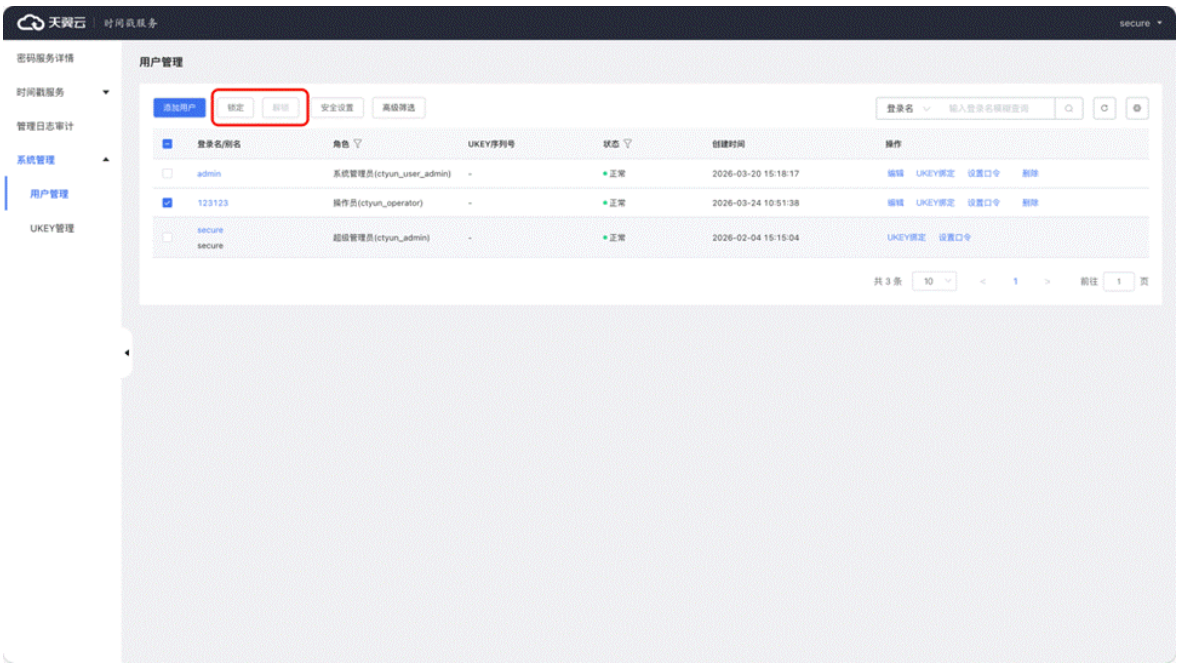
添加用户

按要求填写即可，其中登录名用于登录使用，角色选项即为赋予用户的角色权限，邮箱可用于找回用户密码



锁定/解锁用户

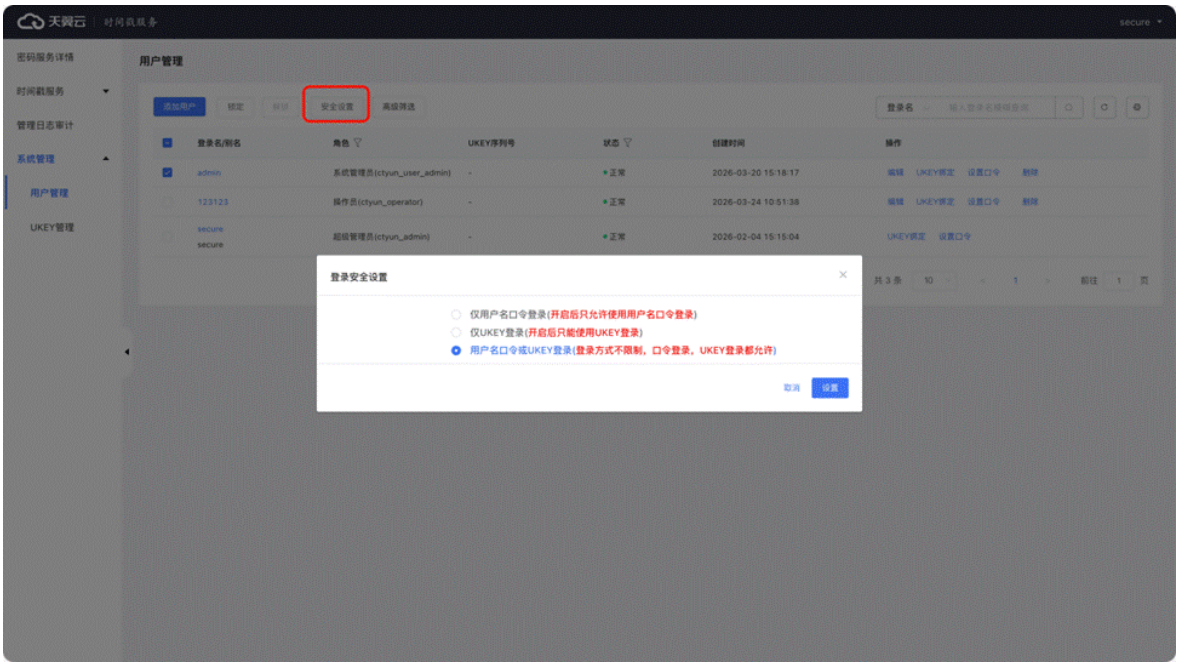
被锁定的用户不能正常进行登录使用，需解锁后才能正常登录使用



安全设置

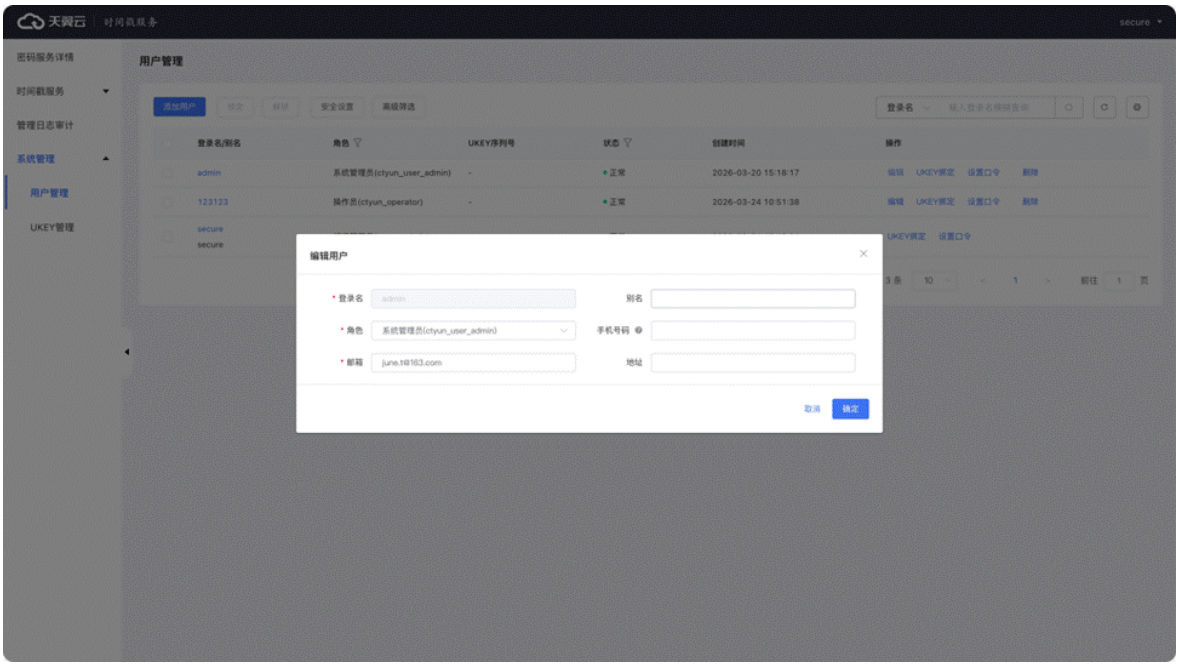
安全设置中有三个选项，按需进行设置即可：

1. 仅用户名口令登录（开启后只允许使用用户名口令登录）
2. 仅UKEY登录(开启后只能使用UKEY登录)
3. 用户名口令或UKEY登录(登录方式不限制，口令登录，UKEY登录都允许)



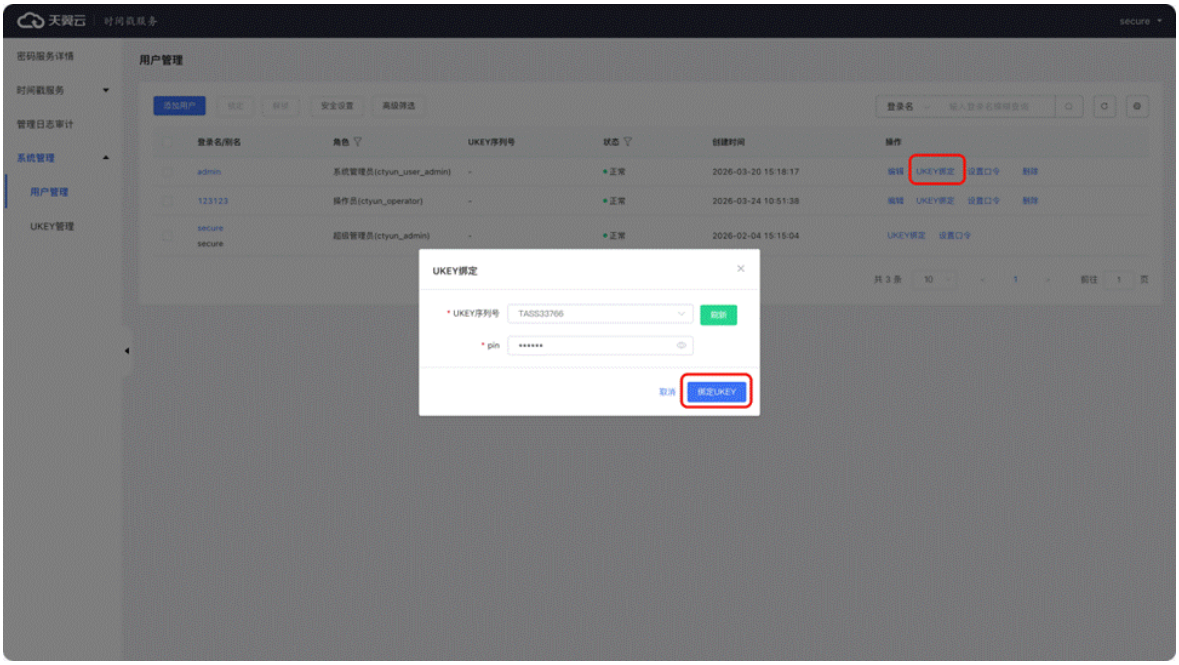
编辑用户信息

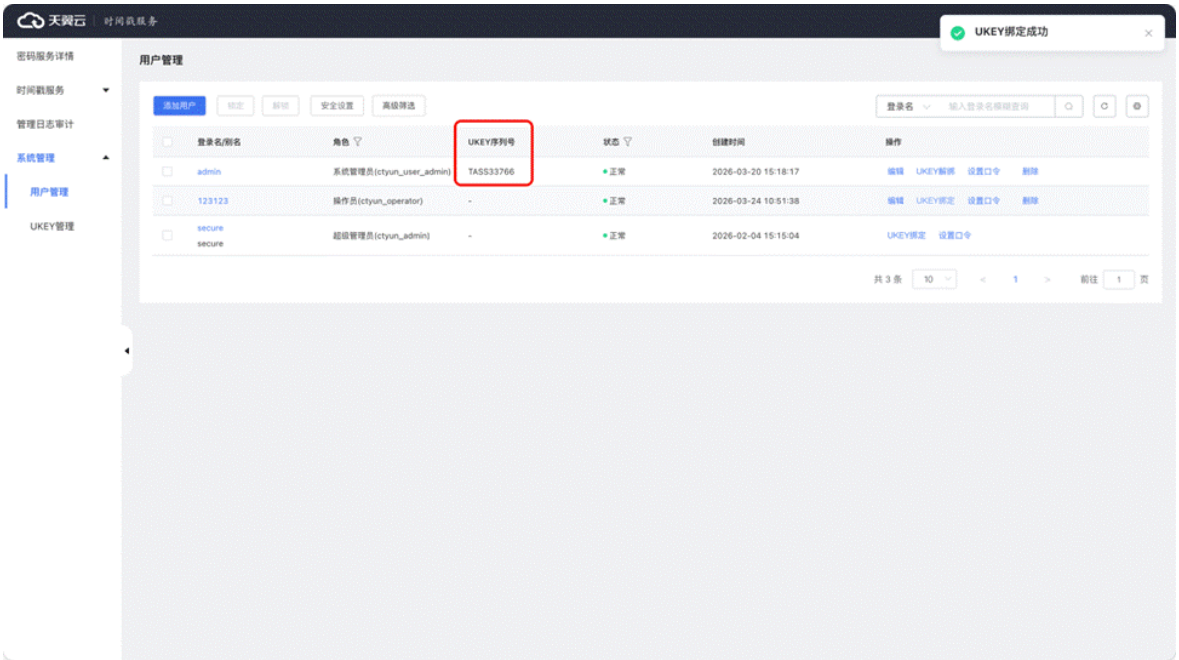
可以对用户基本信息进行编辑（登录名不允许进行编辑）



UKEY绑定

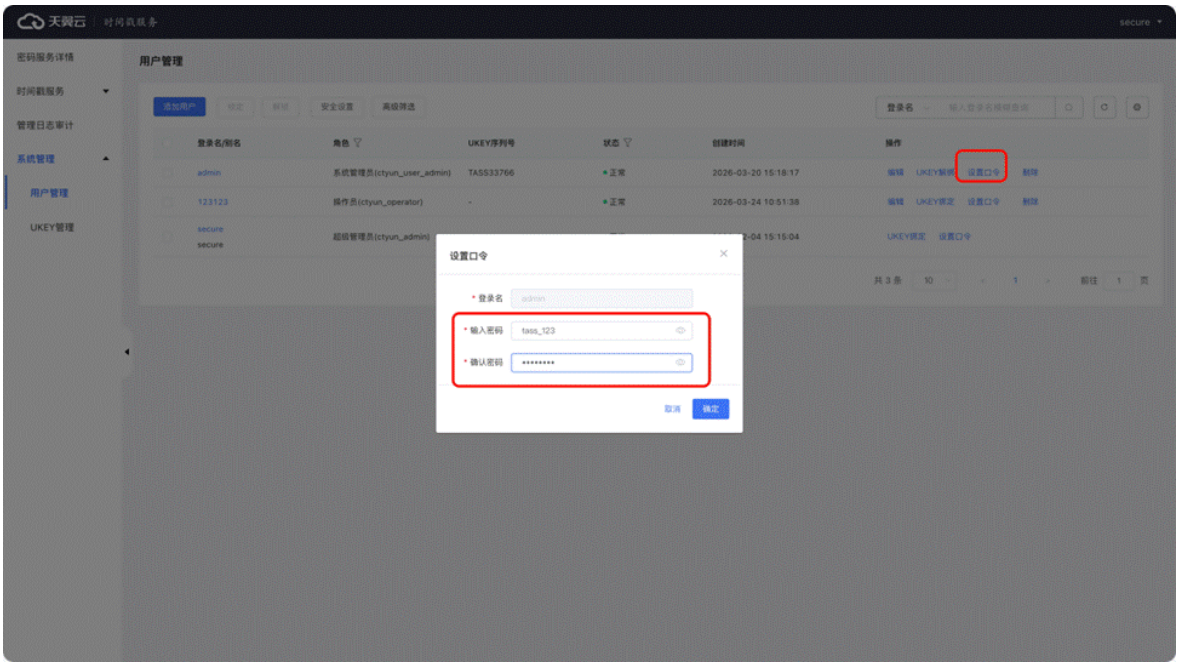
可以为某个用户进行ukey绑定操作（进行ukey绑定前需要下载对应版本的UKEY控件和插入对应的UKEY）绑定完成后对应的用户可以使用UKEY进行登录





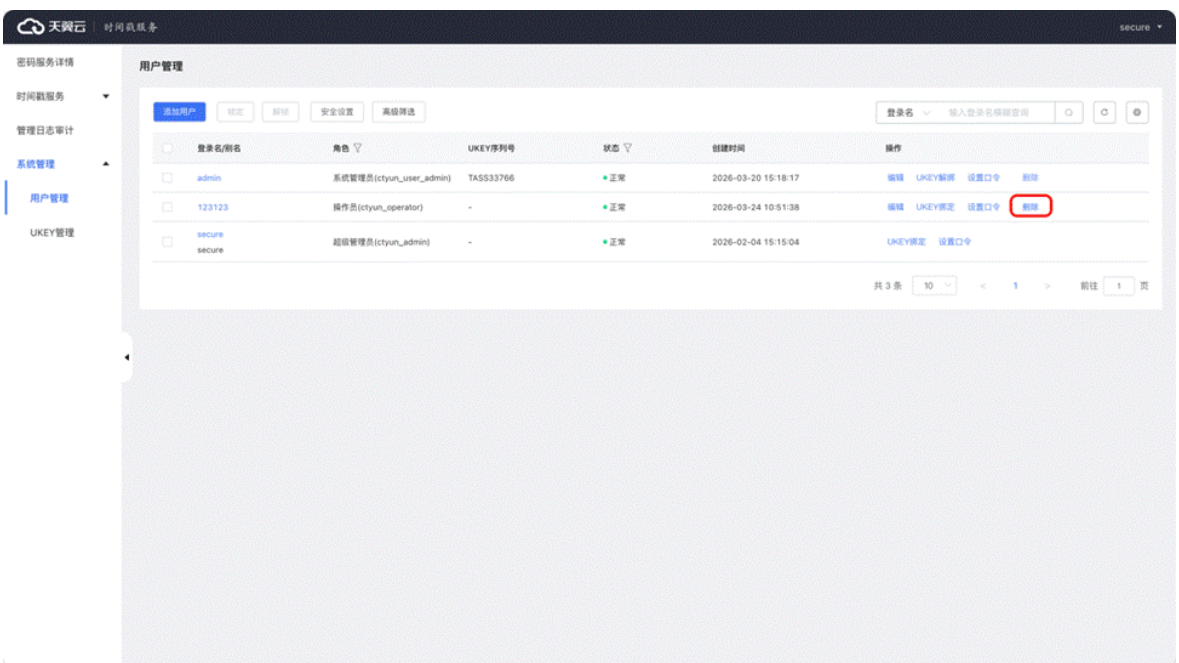
设置口令

可以为某个用户的登录口令（登录密码）进行编辑



删除用户

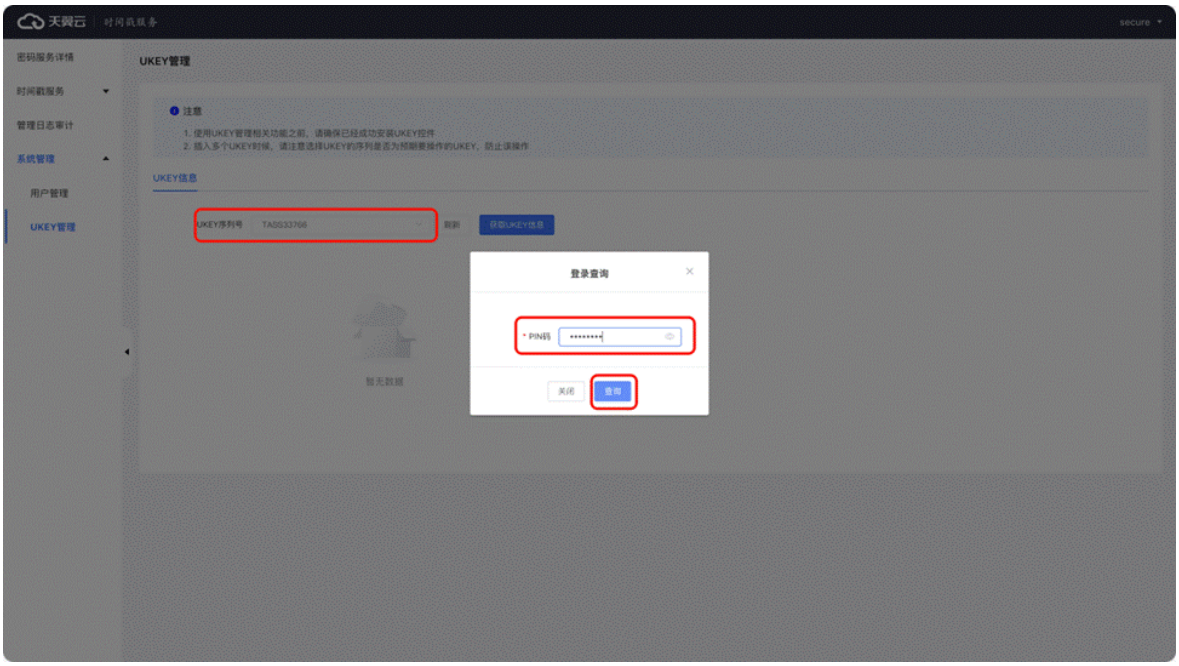
对于冗余的用户可以进行删除



UKEY管理

获取UKEY信息

进入UKEY管理界面后，选择对应的UKEY并输入PIN码，点击查询即可获取到对应的UKEY信息（在进行UKEy信息查询前需要先安装对应版本的UKEY控件和插入对应版本的UKEY）



使用综合安全网关保护设备的安全

网络和通信安全

身份鉴别和通信数据机密性、完整性

满足网络和通信安全的总体要求需要通过国密SSL VPN安全网关配合VPN客户端构建虚拟专用通道来保证对各通道的安全：

- 平台管理员通过CN2网络访问平台的业务通道：部署国密SSL VPN安全网关（配备数字证书），以及为平台管理员用户配备USBKey（配备数字证书）和VPN客户端，建立安全的国密加密通道，在此通道内访问平台；
- 平台运维人员通过CN2网络对平台的运维通道：部署国密SSL VPN安全网关（配备数字证书），以及为运维人员配备USBKey（配备数字证书）和VPN客户端，建立安全的国密加密通道，在此通道内对平台中的各设备和服务器、操作系统等进行运维和管理。

网络边界访问控制

网络边界访问控制信息存储在国密SSL VPN安全网关中，完整性已得到保护。国密SSL VPN安全网关设备取得国家密码检测部门颁发的商用密码产品认证证书，通过国密SSL VPN安全网关自身机制实现访问控制信息的保护，该密码应用要求指标可复用商用密码产品检测结果。

设备与计算安全

概述

系统的设备和计算安全层面，主要涉及业务服务器、数据库服务器、网络设备、安全设备。因此采用合规的SSL VPN安全网关、服务器密码机、智能密码钥匙、数字证书实现各项商用密码技术功能。

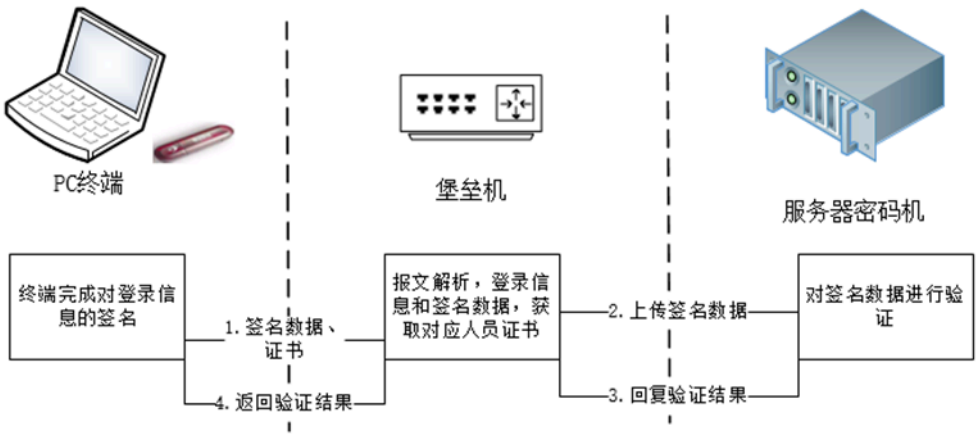
身份鉴别

通过专用SSL VPN安全网关结合运维堡垒机（或者4A安全系统）提供设备和计算层面的身份鉴别，结合智能密码钥匙（内置数字证书），运维人员Ukey数字证书由身份认证系统（CA）签发，并且与堡垒机分配给运维管理员的账户一一对应和绑定。

1. 运维人员首先使用VPN客户端调用智能密码钥匙，通过远程（CN2网络）连通合规SSL VPN安全网关进行双向强身份认证，验证运维人员USBKey证书与SSL VPN服务的双方身份，握手成功后建立国密SSL VPN隧道。

2. 再通过UKey方式登录堡垒机。用户通过智能密码钥匙登录堡垒机，采用挑战/应答机制，采用服务器密码机对登录签名进行验证，实现运维管理用户登录堡垒机的身份鉴别实现。

   具体过程如下：



   a. 用户插入智能密码钥匙访问堡垒机登录页面时，终端将签名数据、证书发送至堡垒机。

   b. 堡垒机将对数据服务器密码机进行签名。

   c. 服务器密码机对签名数据进行验签，并返回验证结果至堡垒机。

   d. 堡垒机完成证书有消息验证，综合签名数据验证结果，将验证结果返回至终端。

   基于密码技术的用户登录堡垒机的身份鉴别中，涉及的密钥为SM2签名算法公私钥，涉及的设备为智能密码钥匙和服务器密码机，不存在出现私钥明文情况。

3. 通过堡垒机登录到服务器/虚机进行维护（SSH V2.0协议），实现对服务器/虚机的管理和维护。

访问控制信息完整性

通过建立基于商用密码算法的SSL VPN安全通道，实现了对网络中的服务器、数据库、安全设备和密码设备等设备资产的集中管理。

运维人员通过SSL VPN和堡垒机进行远程维护：

1. 首先，用户使用VPN客户端登录SSL VPN（运维通道），在运维终端和运维SSL VPN之间建立基于商用密码算法的SSL VPN集中管理通道。
2. 再通过堡垒机管理页面选择不同的管理协议和工具对设备进行管理，实现远程管理通道安全。

数据加密机网关部署方案

数据加密机以透明加密网关模式应用时，数据库加密机部署在业务应用和数据库之间，业务应用通过数据库加密机访问数据库内的敏感数据，数据库加密机根据加密规则自动识别敏感字段并加解密。透明加密网关模式通过网络接入，应用简单修改数据库IP即可接入数据库加密机。

步骤一：启用/禁用实例

禁用状态下，无法进行规则配置，且已经配置的规则将处于未生效的状态。

步骤二：配置加密规则

1. 单击“实例IP”前的 › 按钮，展开对应实例下的所有数据库实例。
2. 选择需要配置加密规则的数据库，单击“操作”列的“配置加密”。
3. 在“表名”下拉框中选择需要配置加密规则的数据库表。
4. 单击“加密配置”，选择需要加密的字段开始配置。

   加密规则：对指定表的指定字段进行加密规则配置，配置时可自定义密文字段的名称（密文字段用于存储密文数据），选择加密密钥、加密模式、补丁方式。

参数	参数说明
加密密钥	选择加密密钥，用于对明文数据进行加密
加密字段名称	选择加密字段名称，用于存储密文数据
加密模式	根据需求选择加密模式，支持选择以下三种： • ECB • CBC • FPE
补位方式	选择补位方式，目前仅支持：PKCS5Padding

   完整性保护：对指定表的指定字段进行完整性保护规则配置，配置时可自定义完整性保护字段的名称（用于存储校验数据），选择加密密钥。

参数	参数说明
加密密钥	选择加密密钥，用于对明文数据生成校验值

参数	参数说明
加密字段名称	选择加密字段名称，用于存储校验值数据

模糊查询：对指定表的指定字段进行模糊查询规则配置，配置时可自定义模糊查询列的名称。

参数	参数说明
模糊查询字段名	自定义模糊查询列的名称

脱敏：对指定表的指定字段进行脱敏规则配置，配置了脱敏规则的字段可对数据进行脱敏处理。

参数	参数说明
脱敏算法	支持以下规则： • 保留前N后M • 保留X到Y • 遮盖前N后M • 遮盖X到Y • 特殊字符前遮盖 • 特殊字符后遮盖
替换字符	用于遮盖替换敏感数据

步骤三：载入配置

勾选完成“初始化密文列”操作的字段，单击“载入配置”。

此操作是确保您配置的规则进行加载生效。

步骤四：初始化密文列

完成加密规则配置后，单击“操作”列的“初始化密文列”。

可以选择复制SQL语句手动去物理库中执行，也可以选择一键执行。执行成功之后物理库会显示密文字段。

步骤五：加密洗数

注意

进行加密洗数之前请确认仿真模式已关闭，仿真模式开启的情况下禁止加密洗数。

加密洗数是对物理数据库的存量明文数据按照相应的加密规则进行加密得到密文，将密文保存到相应的密文列中。

其他操作

完整性校验

完整性校验用来校验密文数据是否经过篡改。

完整性校验任务可以到任务列表中查看加密洗数任务完成状态以及洗数进度。

解密洗数

解密洗数是对物理数据库中的密文字段中的密文按照相应的加密规则进行解密得到原文数据保存在明文字段中。

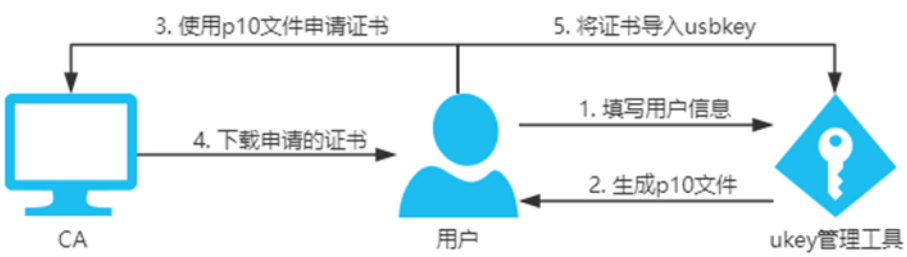
解密完成后，此字段将不再被数据库加密网关进行管理，密文字段是否删除由用户评估后自行处理。

申请PKCS10证书并保存至UKEY中

概述

CA提供使用PKCS10证书申请文件签发证书功能。

用户可以使用USBKey管理员工具生成PKCS10文件，CA将使用PKCS10中的用户信息和公钥签发证书。PKCS10申请时支持使用证书模板，向签发的证书中添加扩展项和选择证书类型。CA签发的证书可以使用USBKey管理员工具导入到USBKey中，完成业务闭环。



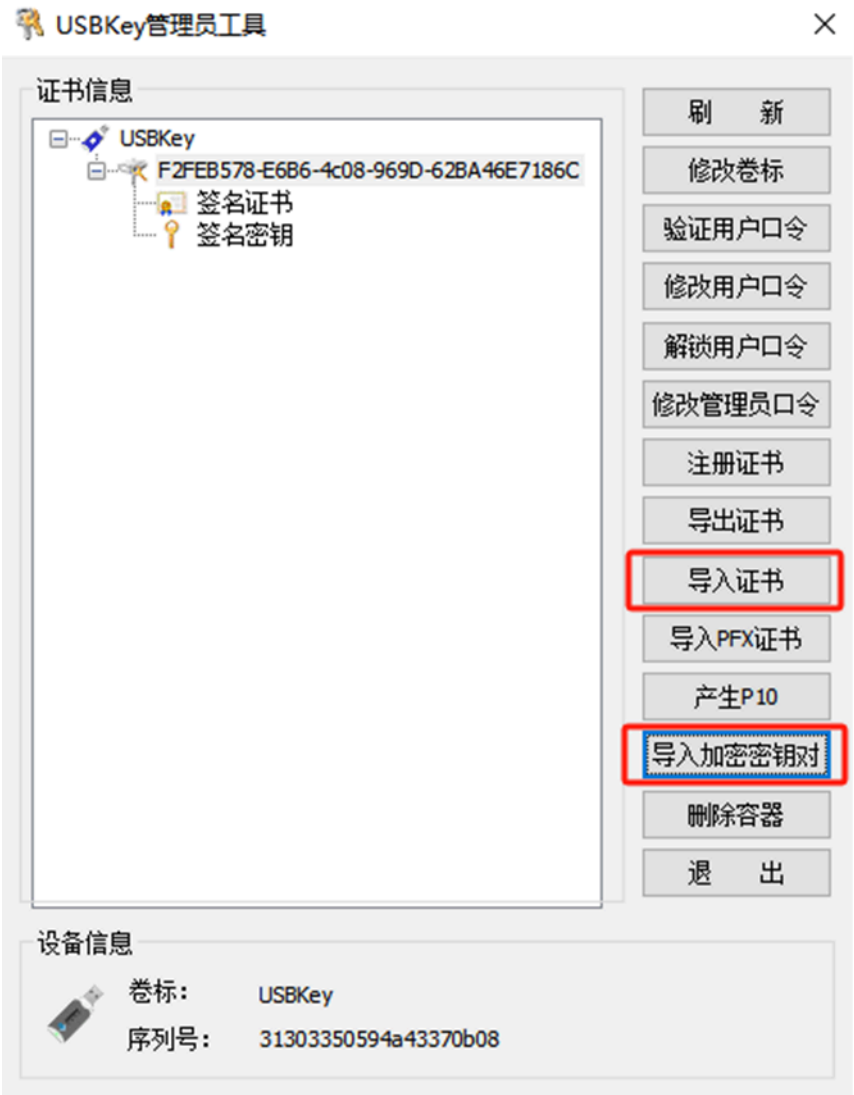
操作步骤

1. 使用USBKey管理员工具生成PKCS10文件。

2. 使用操作员账号登录CA管理页面，在“证书申请 > PKCS10申请”中上传PKCS10文件，并选择CA、模板等。

3. 提交证书申请，申请成功后不要立即下载证书，在“证书下载 > 有效证书下载”中找到刚签发的证书，点击下载，选择不下载到ukey，密钥格式选择ASN1L32。

4. 使用USBKey管理员工具，将下载的签名证书、加密证书和加密密钥分别使用导入证书、导入加密密钥对功能导入到UKEY中。

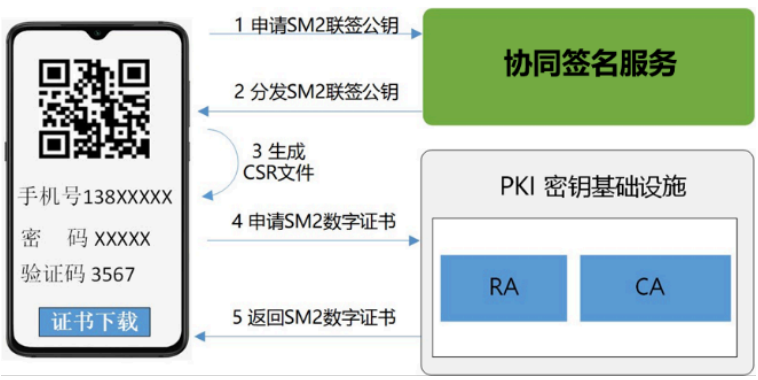


使用协同签名服务保障数据安全

某应用系统为等保3级，用户采用手机端APP通过互联网进行业务访问，为保障APP端身份鉴别的密评合规，通过协同签名服务实现了基于国密算法的身份鉴别以及传输过程中的机密性、完整性保护。

APP应用端证书下载

在APP端实现了用户个人数字证书的线上注册、申请、下载，流程如下：



1. APP集成协同签名客户端（SDK）；
2. APP通过协同签名客户端调用协同签名服务提供的接口申请SM2联签公钥；
3. 协同签名服务生成SM2公钥并返回给协同签名客户端；
4. 协同签名客户端生成请求数字证书的CSR文件，然后提交给CA申请证书；
5. CA根据获取的公钥签发数字证书并返回给协同签名客户端。
6. 在提交CA获取证书时，协同签名客户端可根据CA的管理要求完成数字证书申请的身份认证。

手机端APP身份鉴别

身份鉴别实现说明如下：

1. APP集成协同签名客户端（SDK）；
2. 用户首次使用APP时下载SM2软证书（密钥分片）到本地；
3. 用户登录APP时通过本地软证书基于协同签名机制生成完整签名值；
4. APP服务端验证签名值以确定身份正确性。

协同签名客户端SDK为二级软件密码模块，可达到与硬件智能密码钥匙相同的密钥保护安全强度，认证过程中用户无需使用任何硬件介质，满足等保3级系统应用和数据层面身份鉴别相关要求。

数据传输过程中的机密性、完整性保护

数据安全传输实现说明如下：

1. APP集成协同签名客户端SDK；
2. 用户首次使用APP时下载SM2软证书（密钥分片）到本地；
3. APP端上传重要数据时通过服务端公钥进行数据加密，服务端通过私钥进行解密；
4. 服务端下发重要数据时通过用户公钥进行数据加密，APP端通过软证书以及协同签名服务实现数据解密。

密文采用数字信封方式封装，加解密过程中自动通过SM3算法实现数据完整性保护。

协同签名客户端SDK为二级软件密码模块，可达到与硬件智能密码钥匙相同的密钥保护安全强度，认证过程中用户无需使用任何硬件介质，满足等保3级系统应用和数据层面数据传输机密性相关要求。

产品咨询类

为什么要做密评？

开展密评，是为了解决商用密码应用中存在的突出问题，为网络和信息系统的安全提供科学评价方法，逐步规范商用密码的使用和管理。从根本上改变商用密码应用不广泛、不规范、不安全的现状，确保商用密码在网络和信息系统中有效使用，切实构建起坚实可靠的网络安全密码屏障。

- 《密码法》第二十七条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。
- 《商用密码管理条例》第六章第三十八条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。
- 《商用密码应用安全性评估管理办法（试行）》第一章第三条：“涉及国家安全和社会公共利益的重要领域网络和信息系统的建设、使用、管理单位应当健全密码保障体系，实施商用密码应用安全性评估”。重要领域网络和信息系统包括：基础信息网络、涉及国计民生和基础信息资源的重要信息系统、重要工业控制系统、面向社会服务的政务信息系统，以及关键信息基础设施、网络安全等级保护第三级及以上信息系统。

密评整体流程？

密评整体流程共包括4个阶段，分别为编写密码应用方案、密码应用方案评估、系统建设/改造、密码应用安全性评估。

编号	阶段	描述
1	编写密码应用方案	客户首先自行或委托密评机构按照密评标准对系统进行差距分析，根据差距分析结果结合系统实际情况设计密码应用方案。 密码应用方案应包括系统现状及存在的风险、系统涵盖的重要数据、密码应用需求、方案设计以及使用的密码技术、管理制度、应急方案以及实施方案等。
2	密码应用方案评估	密码应用方案编写完成后，可委托密码专家或密评机构对密码应用方案进行评审。 • 若委托密码专家对方案评审则出具专家评审意见。 • 若委托密评机构评审，则出具密码应用方案评估报告。
3	系统建设/改造	密码应用方案通过评审后，系统集成单位按照通过评审的方案对系统进行建设或改造。
4	密码应用安全性评估	系统建设/改造完成后，被测单位委托密评机构对系统进行测评，密评机构按照GB/T 39786标准测评并出具差距分析报告，客户根据差距分析结果进行整改并申请复测，最终出具符合要求的商用密码应用安全性评估报告。

密码服务的防护功能是否就能满足密评合规需求？

密码服务可满足密评二级、三级的安全技术合规要求，密评第一级~第四级密码应用基本要求见下表。

- 对于“可”的条款，由信息系统责任单位自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照相应的测评指标要求进行测评和结果判定；否则，该测评指标为“不适用”。
- 对于“宜”的条款，密评人员根据信息系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围；若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则“宜”的条款默认纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照测评指标要求进行测评和结果判定。否则，密评人员应根据信息系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，且信息系统的实施情况与所描述的风险控制措施是否一致，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照测评指标要求进行测评和结果判定。
- 对于“应”的条款，密评人员应按照测评指标要求进行测评和结果判定；若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与某项或某些项测评指标相关的密码应用需求，则相应测评指标为“不适用”。

指标体系			第一级	第二级	第三级	第四级
技术要求	物理和环境安全	身份鉴别	可	宜	宜	应
		视频监控记录数据存储完整性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	网络和通信安全	身份鉴别	可	宜	应	应
		通信数据完整性	可	可	宜	应
		通信过程中重要数据的机密性	可	宜	应	应
		网络边界访问控制信息的完整性	可	可	宜	应
		安全接入认证	—	—	可	宜

指标体系			第一级	第二级	第三级	第四级
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	设备和计算安全	身份鉴别	可	宜	应	应
		远程管理通道安全	—	—	应	应
		系统资源访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		日志记录完整性	可	可	宜	应
		重要可执行程序完整性、重要可执行程序来源真实性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	应用和数据安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		重要数据传输机密性	可	宜	应	应
		重要数据存储机密性	可	宜	应	应
		重要数据传输完整性	可	宜	宜	应
		重要数据存储完整性	可	宜	宜	应
		不可否认性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上

产品使用类

如何确定被测信息系统密码应用等级？

GB/T 39786-2021中的**密码应用等级一般由网络安全等级保护的级别确定**。

信息系统根据GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》确定等级保护级别时，同步对应确定密码应用等级：

- 等保定级为第一级的网络与信息系统应遵循GB/T 39786-2021第一级密码应用基本要求。
- 等保定级为第二级的网络与信息系统应遵循GB/T 39786-2021第二级密码应用基本要求，以此类推。
- 对于未完成网络安全等级保护定级的重要信息系统，其密码应用等级至少为第三级。

因此在进行密码测评时，建议至少先完成等保的定级备案。

资源池没过密评，客户能部署密码服务过密评，拿到测评报告吗？

云平台是否过密评不会直接影响租户侧的密评结果。

- 若平台侧已经通过密评，那么云上租户在进行商用密码应用安全性评估时可复用平台侧的部分结果。如云平台已经进行了测评且拿到符合要求的密评报告，那么云上租户在进行测评时可复用物理和环境安全（即机房）的测评结果。
- 若平台侧没有通过密评，那么云上租户在进行密码测评时则不能复用平台侧的测评结果。需要按照密评标准GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》逐条测评。

购买了密码服务是否还需要购买密码测评服务？

需要。

- **密码服务**主要为客户提供密码改造服务，即根据客户的业务需求提供加解密、签名验签、SSL加密服务等接口，协助客户按照密评标准满足身份鉴别、通道加密、重要数据存储等指标，需要**由客户和云公司**共同完成。
- **密码测评**指的是系统建设/改造完成后委托密评机构按照密评标准GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》分别从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等多个维度对系统进行测评，由**测评机构、客户和云公司**共同完成。

  目前全国共有48家密评机构可进行全国系统的测评。

应用系统是否涉及代码改造？

客户在购买了密码服务后还需要对应用系统进行代码改造才能满足业务系统的密码需求。

客户通过业务系统实际需求调用密码服务对应的服务：

- 若身份鉴别不满足需求，则需要调用身份认证服务对应的接口。
- 若未对重要业务数据进行安全存储，则根据实际需求调用加密接口。
- 若重要数据需要进行防泄漏（机密性）保护，则调用加解密服务接口以保证重要业务数据的存储机密性。
- 若重要数据需要进行防篡改（完整性）保护，则调用签名验签及服务接口保证重要数据的存储完整性。

密码服务可提供的服务见下表：

密码服务	服务说明
加解密服务	为应用系统提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求。
身份认证服务	为应用系统提供对登录用户的基于国密数字证书的身份认证服务，保证应用系统用户身份的真实性，满足密评中对用户身份真实性鉴别的要求。
签名验签服务	为应用系统提供重要数据的签名和验签服务，满足密评中对重要数据传输和存储的完整性要求以及操作的不可否认性要求。
密钥管理服务	为应用系统提供集中的密钥全生命周期管理服务，满足密评中对密钥管理的安全性要求。
数字证书服务	为用户、应用或设备提供数字证书的签发、更新、注销等全生命周期的管理，为身份鉴别提供数字证书支撑服务。
SSL加密服务	提供网络通信通道的加密服务，满足密评中对网络和通信安全层面的数据传输机密性和完整性要求。
协同签名服务	配合移动端密码模块为应用系统移动端提供协同密码服务，满足移动端的密码应用合规性要求。

常见问题

SSL VPN网关是什么？

SSL VPN网关是专为解决网络间安全互联设计的一款高性能安全产品，基于SSL协议为应用提供基于数字证书的高强度身份认证服务、高强度数据透明隧道加密服务，可以有效保护网络资源的安全访问。

数据加密网关是什么？

数据加密网关针对于数据库数据存储安全的高性能密码网关设备，是基于数据库透明加密原理的数据库主动防御产品，具有透明加解密及完整性保护、密钥合规生命周期管理、独立于数据库的权限控制等功能特性。

数据加密网关与通用服务器密码机的区别？

通用服务器密码机	数据库加密网关
使用通用服务器密码机对代码进行改造实现对数据库数据加密。	使用专用数据库加密网关进行应用集成实现数据库中数据透明加密。
加密能力深入应用代码，用户自主性高。	应用系统无需进行代码改造，应用集成数据库加密机即可完成数据库的加密改造，数据自动被加密和解密。
应用需进行代码改造，用户、应用开发商、密码机厂商以及测评机构需要紧密配合；应用需要解决加密改造中碰到的技术难题（模糊查询等）。	某些加密模式需要改变应用和数据库的网络拓扑结构。