天翼云数据加密
用户使用指南

中国电信股份有限公司云计算分公司

目 录

1. 产品概述

1.1 什么是数据加密

数据加密服务是天翼云为用户提供的云上数据加密服务，目前提供专属加密服务。

专属加密（Dedicated Hardware Security Module，Dedicated HSM）可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

Dedicated HSM 旨在满足用户将线下加密设备、能力迁移到云上的要求，提供可独占、高性能、安全合规的加密域计算资源。用户作为设备使用者完全控制密钥的产生、存储和访问授权。天翼云只负责监控和管理设备及其相关网络设施。

同时，Dedicated HSM 可提供认证合规的金融数据加密机、服务器加密机以及签名验签服务器等，灵活支撑用户业务场景。能够帮助用户满足数据安全方面的监管要求，以及云上业务数据的隐私性要求。

功能介绍

Dedicated HSM 提供以下功能：

- 生成、存储、导入、导出和管理加密密钥，包括对称密钥和非对称密钥。
- 使用对称和非对称算法加密和解密数据。
- 使用加密哈希函数计算消息摘要和基于哈希的消息身份验证代码。
- 对数据进行加密签名（包括代码签名）并验证签名。
- 以加密方式生成安全随机数据。

支持的密码算法

对称密码算法	SM1、SM4、DES、3DES、AES
非对称密码算法	SM2、 RSA（1024-4096）
摘要算法	SM3、 SHA1、SHA256、SHA384

权限认证

- 专属加密实例设备管理与内容（敏感信息）管理权限分离，即使天翼云的运维人员也无法获取到用户的密钥。
- 可对敏感指令支持分类授权控制，有效防止越权行为。
- 支持用户名口令认证，数字证书认证等多种权限认证方式。

可靠性

专属加密实例之间独享加密芯片，即使部分硬件芯片损坏也不影响使用。

1.2 使用场景

若用户购买了天翼云提供的专属加密实例，可通过天翼云提供 Ukey 初始化并管控专属加密实例。用户作为设备使用者完全控制密钥的产生、存储和访问授权。

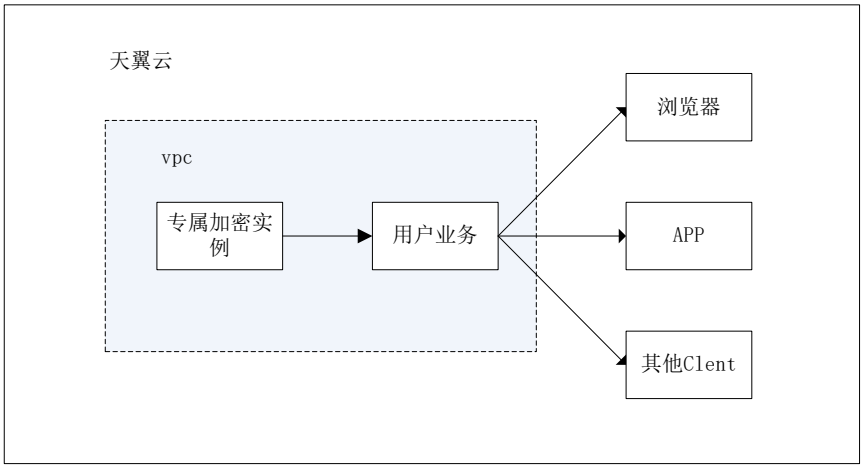
用户可通过专属加密实例加密用户业务系统（包含敏感数据加密、金融支付加密以及电子票据加密），帮助用户加密企业自身的敏感数据（如合同、交易、流水等）以及企业用户的敏感数据（用户身份证号码、手机号码等），以防止黑客攻破网络、拖库导致数据泄露、内部用户非法访问或篡改数据等风险。

说明：

用户需要将专属加密实例和业务系统部署在同一个 VPC 组

以敏感数据加密场景为例说明，如图 1-1 所示

图1-1 敏感数据加密场景



1.3 访问和使用

1.3.1 如何访问

天翼云提供了 Web 化的服务管理平台，即控制中心管理方式。

如果用户已注册天翼云，可直接登录控制中心，单击页面上方的“服务列表”，选择“安全 > 专属加密服务”。

1.3.2 如何使用

- 与弹性云主机配合使用

用户可通过创建专属加密实例的方式，使用专属加密实例生成的密钥加解密部署在弹性云主机内业务系统的敏感数据。

1.3.3 与其他云服务的关系

- 与弹性云主机的关系

Dedicated HSM 提供的专属加密实例可以为部署在弹性云主机内的业务系统加密敏感数据，用户可完全控制密钥的生成、存储和访问授权，保证数据在传输、存储过程中的完整性、保密性。

2 专属加密

本章指导用户如何初始化专属加密实例。使用专属加密的大体流程为：

1. 购买专属加密实例，见 2.3。

2. 安装管理工具及代理软件（此步骤建议运维人员阅读并执行），步骤见帮助中心文档下载的服务安装包。

3. 初始化专属加密实例见，2.1.1。

4. 配置安全代理软件，见 2.1.2。

5. 使用专属加密实例。

2.1 操作指引

前提条件

在获取专属加密实例后，用户需要获取以下信息，初始化专属加密实例，且用户使用产品前需要有至少两台云主机作为安装管理工具和代理软件的工具，管理工具及代理工具部署方案请见帮助中心文档下载的服务安装包，服务安装包包含平台部署手册及代理服务器部署安装手册及安装程序，管理工具使用流程如 2.1.1 所示，代理工具使用流程如 2.1.2 所示。

表2-1 获取初始化专属加密实例的信息

名称	说明	来源
Ukey	保存专属加密实例的权限管理信息。	订单付款后，由天翼云邮寄到用户的 Ukey 收件地址。
Ukey 驱动	Windows 驱动，识别 Ukey。	天翼云安全专家通过用户提供的联系方式联系用户，并提供软件包链接供用户下载。
Dedicated HSM 管理工具	配合 Ukey，远程管理专属加密实例。	
安全代理软件	与专属加密实例建立安全通道。	

名称	说明	来源
SDK	用于提供专属加密实例的 API 接口，用户通过调用 SDK 与专属加密实例建立安全连接。	
天翼云 Windows ECS 实例	运行 Dedicated HSM 管理工具，与专属加密实例处于同一 VPC 组，并分配弹性 IP 地址用于远程连接。	
天翼云 Linux ECS 实例	运行安全代理软件和用户的应用程序，与专属加密实例处于同一 VPC 组。	

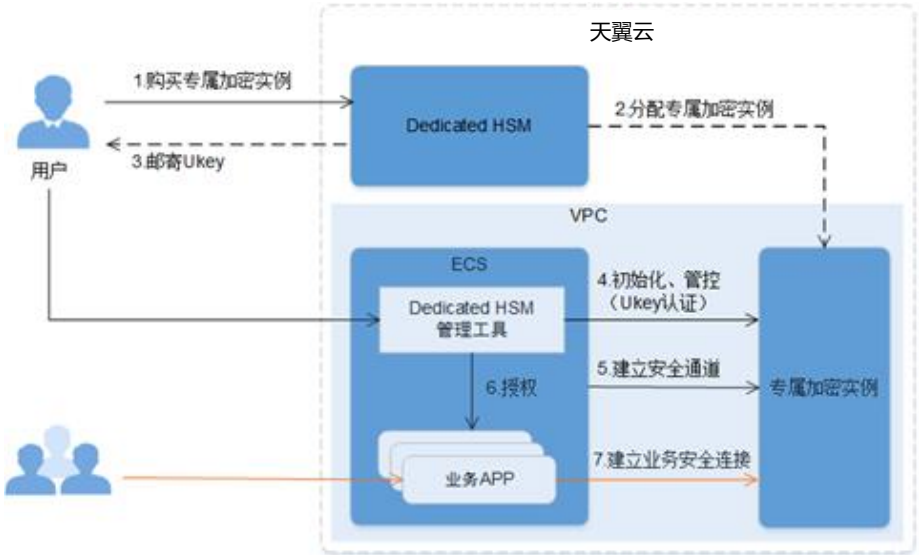
操作指导

当用户需要在云上使用专属加密服务时，可通过 Dedicated HSM 界面购买专属加密实例。购买专属加密实例后，天翼云邮寄 ukey 给用户。当用户收到天翼云邮寄的 Ukey 后，通过 Ukey 初始化，并管控专属加密实例。用户通过 Dedicated HSM 管理工具授权业务 APP，允许业务用户通过 APP 访问专属加密实例。操作指导如图 2-2 所示。

说明：

建议用户将专属加密实例与业务虚机放置于同一 vpc 中，且放开业务节点的 8010,8008 端口（TCP）用于加密实例访问。

图2-2 操作指导



操作指引说明如表 2-2 所示。

表2-2 操作指引说明

编号	说明
1	用户通过 Dedicated HSM 界面购买专属加密实例。
2	天翼云分配专属加密实例给用户。
3	Ukey 是天翼云提供给用户的身份识别卡，此卡仅购买专属加密实例的用户持有，请妥善保管。 天翼云安全专家将通过用户提供的 Ukey 收件地址将 Ukey 邮寄给用户。
4	用户在天翼云弹性云主机中安装管理工具和代理软件，使用 Ukey 和 Dedicated HSM 管理工具初始化专属加密实例，并注册相应的管理员，管控专属加密实例。
5	用户通过 Dedicated HSM 管理工具配置安全代理，建立与专属加密实例之间的安全通道。
6	注册的管理员需要通过 Dedicated HSM 管理工具授予业务 APP 访问专属加密实例的权限。
7	用户将 SDK 安装在业务 APP 上，业务用户通过调用 SDK 与专属加密实例建立安全连接，并访问专属加密实例。

2.1.1 初始化专属加密实例

按照服务安装包的管理平台部署手册安装管理工具后。按照以下初始化实例流程，具体操作步骤如3.管理工具所示。

1. 在用户本地 Windows PC 上安装 Ukey 驱动。
2. 远程连接天翼云 Windows ECS 实例。
   A. 运行本地 Windows PC 的 mstsc 远程连接工具，并通过天翼云上 Windows ECS 实例的弹性 IP 地址远程连接 ECS 实例。
   B. 在本地 PC 的 USB 口插入 Ukey，通过远程连接功能将本地 Ukey 端口映射到天翼云的 Windows ECS 实例。
3. 通过 Dedicated HSM 管理工具管理专属加密实例。
   A. 在天翼云 Windows ECS 实例上运行 Dedicated HSM 管理工具。
   B. 通过与专属加密实例的 VPC 子网 IP 连接，配合 Ukey 初始化专属加密实例，并产生、备份、恢复密钥。

2.1.2 配置安全代理软件

按照代理服务器部署安装手册安装配置代理软件后，以如下流程配置代理软件。

1. 通过 Dedicated HSM 管理工具连接专属加密实例，给天翼云 Linux ECS 实例上的安全代理签发许可文件。
2. 在 Linux ECS 实例上运行安全代理软件，将许可文件导入到安全代理软件，并与专属加密实例建立安全通道，导入许可方式详见代理服务器部署安装手册。

2.1.3 接口调用

应用程序通过 SDK 提供的接口与安全代理软件建立连接，通过安全代理软件调用专属加密实例。

2.2 购买专属加密实例

1. 登录控制中心。
2. 单击页面上方的“服务列表”，选择“安全 > 专属加密服务”，默认进入专属加密服务界面。
3. 在界面右上角，单击“购买专属加密实例”。

4. 填写参数，下表为参数列表

参数名称	说明	取值样例
虚拟私有云	可以选择使用已有的虚拟私有云（Virtual Private Cloud，VPC）网络，或者单击“申请虚拟私有云”创建新的虚拟私有云。	vpc-sec

参数名称	说明	取值样例
	更多关于虚拟私有云的信息，请参见《天翼云 3.0 虚拟私有云用户指南》。	
安全组	界面显示专属加密实例已配置的安全组。选择专属加密实例的安全组后，该专属加密实例将受到该安全组访问规则的保护。 更多关于安全组的信息，请参见《天翼云 3.0 虚拟私有云用户指南》。	sg-533c
网卡	界面显示所有可选择的子网，系统自动分配一个未使用的 IP 地址。 更多关于子网的信息，请参见《天翼云 3.0 虚拟私有云用户指南》。	subnet1(10.1..0.0/16)

5. 选择专属加密实例的规格信息，如下图所示。

图 基础版信息

表2-3 规格参数说明

参数名称	说明	取值样例
服务版本	• 基础版专属加密实例在密码运算上独占加密卡	基础版

参数名称	说明	取值样例
	资源、共享非密钥计算相关资源，满足用户基本加密需求。	
功能类型	可选择的功能类型，包含“金融密码机”、“服务器密码机”和“签名服务器”。	金融密码机
加密算法	基础版专属加密实例支持的加密算法。 • 对称算法：SM1、SM4、DES、3DES、AES* • 非对称算法：SM2、RSA（1024-4096）* • 摘要算法：SM3、SHA1、SHA256、SHA384 说明 带*条目不同型号设备略有不同，请联系客服进行确认。	-
性能规格	基础版专属加密实例支持的性能规格。 • 数据通讯协议：TCP/IP（最大并发链接：64） • SM1 加密运算性能：600tps • SM2 签名运算性能：3000tps • SM2 验签运算性能：2000tps • RSA2048 验签运算性能：3500tps • RSA2048 签名运算性能：400tps 说明 带*条目不同型号设备略有不同，请联系客服进行确认。	-

6. 填写联系方式

图 联系方式

表2-4 联系方式参数说明

参数名称	说明
业务联系人姓名	业务联系人的姓名。
业务联系人手机	业务联系人手机号码。
邮箱	输入邮箱地址。
Ukey 收件地址	输入收取 Ukey 的收件地址。

7. 确认订单信息无误后点击购买

说明：

成功付款后，在专属加密实例列表界面，可以查看购买的专属加密实例信息。

当专属加密实例的“状态”为“创建中”时，如图 2-2 所示，表示专属加密实例购买成功。

图 2-2 购买专属加密实例成功

专属加密实例包含以下三种状态：

创建中：系统正在分配专属加密实例给用户，等待 5-10 分钟，可分配完成。

创建失败：资源不足或网络故障等原因可能导致创建专属加密实例失败。

运行中：系统给用户分配专属加密实例已完成，专属加密实例处于“运行中”。

2.3 查看专属加密实例

该任务指导用户通过专属加密界面查看专属加密实例信息，包括专属加密实例的名称、状态、服务版本、设备厂商、设备型号、IP 地址和到期时间。

操作步骤

1. 登录控制中心
2. 单击页面上方的“服务列表”，选择“安全 > 专属加密服务”，默认进入专属加密服务界面。
3. 在专属加密实例列表中，查看专属加密实例信息，如下图所示。

图 专属加密实例列表

名称/ID	状态	服务版本	设备厂商	设备型号	IP地址	到期时间	操作
test1 189f0e4b-63d5-4d74-a2e9-a0bbd41abe51	运行中	基础版	[redacted]	SJJ1601	192.168.0.61	--	删除

说明：

可在“名称”下拉列表中，选择“名称”或者“设备型号”，输入专属加密实例的名称或者设备型号，单击，搜索对应的专属加密实例。

在专属加密实例处于“创建失败”或者“冻结”时，可单击该专属加密实例所在行的“删除”，删除专属加密实例。

专属加密实例列表参数说明，如表 2-5 所示。

表2-5 专属加密实例参数说明

参数	参数说明
名称/ID	专属加密实例的名称和 ID。
服务版本	基础版：用户享有共享机框和电源，在密码运算上独占加密卡的虚拟化专属加密实例。
状态	专属加密实例的状态： • 创建中 用户购买的专属加密实例后，系统正在分配专属加密实例给用户，专属加密实例处于“创建中”状态。 • 创建失败 资源不够或网络故障等原因可能导致创建专属加密实例失败，专属加密实例处于“创建失败”状态。 • 运行中 系统已将专属加密实例分配给用户，专属加密实例处于“运行中”状态。 • 冻结 用户购买的专属加密实例到期，且没有续费，专属加密实例处于“冻结”状态。
设备厂商	设备厂商的名称。
设备型号	设备型号。
IP 地址	IP 地址。
购买时间	购买专属加密实例的时间。

参数	参数说明
到期时间	购买的专属加密实例的到期时间。

4. 用户可单击专属加密实例的名称，查看专属加密实例的详细信息，如下图所示。

图 专属加密实例

专属加密实例详细信息参数说明，如表 2-6 所示。

表2-6 专属加密实例详细信息参数说明

参数	参数说明
名称	专属加密实例的名称。 可单击，修改专属加密实例的名称。
ID	专属加密实例的 ID。
状态	专属加密实例的状态： • 创建中 用户购买的专属加密实例后，系统正在分配专属加密实例给用户，专属加密实例处于“创建中”状态。 • 创建失败 资源不够或网络故障等原因可能导致创建专属加密实例失败，专属加密实例处于“创建失败”状态。 • 运行中 系统已将专属加密实例分配给用户，专属加密实例处于“运行中”状态。 • 冻结 用户购买的专属加密实例到期，且没有续费，专属加密实例处于“冻

参数	参数说明
	结”状态。
服务版本	基础版：用户享有共享机框和电源，在密码运算上独占加密卡的虚拟化专属加密实例。
可用区	专属加密实例所在的可用分区。
设备厂商	设备厂商的名称。
设备型号	设备型号。
虚拟私有云	专属加密实例所在虚拟私有云。 更多关于虚拟私有云的信息，请参见《天翼云 3.0 虚拟私有云用户指南》。
子网	专属加密实例所在的子网。 更多关于子网的信息，请参见《天翼云 3.0 虚拟私有云用户指南》。
IP	子网内的私有 IP 地址。
安全组	专属加密实例所在的安全组。 更多关于安全组的信息，请参见《天翼云 3.0 虚拟私有云用户指南》。
创建时间	购买专属加密实例的时间。
到期时间	购买的专属加密实例到期的时间。
所属订单	购买专属加密实例的订单号，可单击订单号，查询订单详情。
计费模式	包年/包月计费。

2.4 专属加密价格

实例类型	版本	初装费	标准资费（元/月）
专属加密实例	基础版	无	2000

备注：针对一次性包年付费服务，标准价格按照下述列表内容进行操作，且在订购时间期间不允许退订服务

一次性付费 1 年
包月标准价格*12*85%

3. 管理工具

本节介绍专属加密管理工具的具体使用方式。管理工具及代理工具部署方案请见下载安装包中的平台部署手册及代理服务器部署安装手册。

3.1 系统初始化

初次登陆系统，需要完成系统超级管理员及审计员的初始化。初始化完成后，用超级管理员登陆系统即可添加其他类人员。

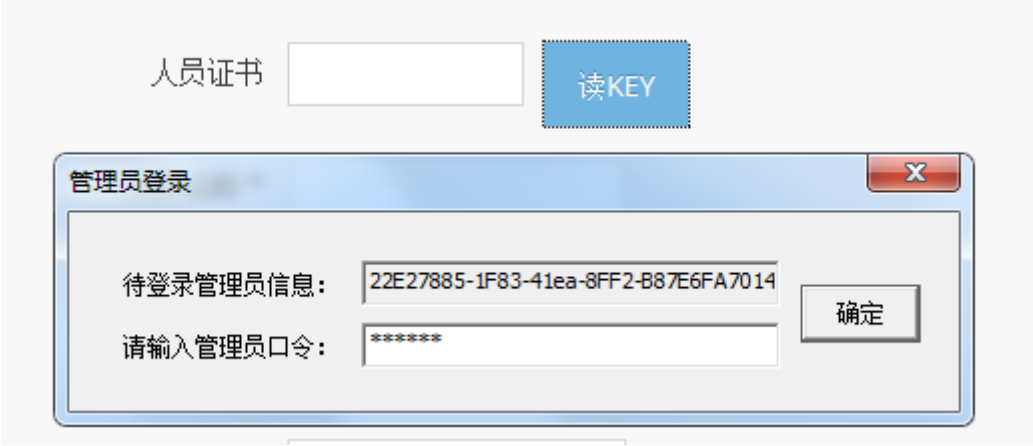
初始化过程分为导入根证书、初始化超级管理员、初始化审计员三步。过程如下

1. 在登陆窗口点击初始化按钮

2. 跳转到初始化功能界面

3. 在此界面选择用来颁发 USBKey 的根证书并导入到系统，导入成功后跳到第二步

4. 插入超管 Key 并点击读 KEY 按钮，在弹出的窗口中输入正确的管理员口令



5. 输入口令，点击“确定”后继续输入其他项信息，所有项都输入完毕后继续点击“确定”，弹出初始化人员成功后，跳转到第三步初始化审计员

6. 审计员初始化操作步骤同上面的超管人员初始化。

7. 审计员初始化完成后弹出如下页面

8. 系统自动跳转到登陆页面

3.2 退出及登录

如下图所示，插入管理员 USB Key 后，点击 key 登录，弹出 key 密码输入框输入 Key 的密码即可登录平台，也可以输入用户名和密码，并点击“登录”键，也可登录进平台。

在平台的右上角有如下提示，标示当前登录的管理员信息：

点击该图标后，在弹出的菜单中点击“注销”可退出登录状态，点击“退出”可注销并关闭浏览器页面：

3.3 权限管理

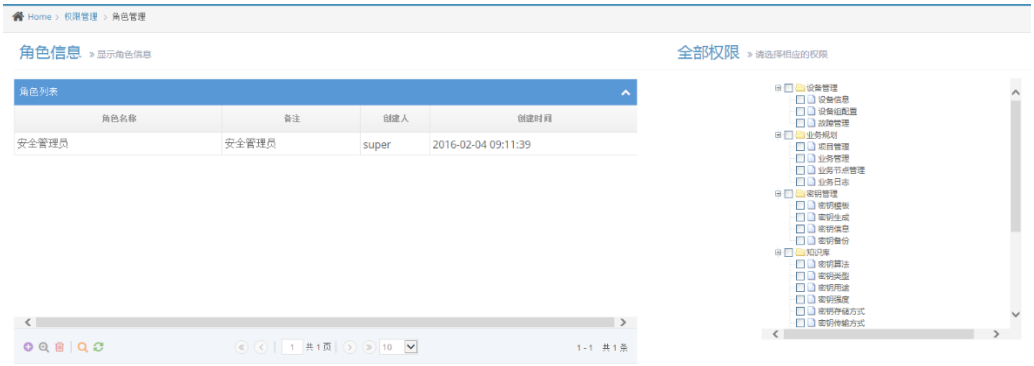
管理工具提供平台管理员的权限管理，采用人员—角色—权限的三级权限管理体系。

初次用超级管理员登陆系统后，先创建相应人员的角色，然后为角色分配相应的权限，最后创建系统人员选择角色即可完成权限分配操作。

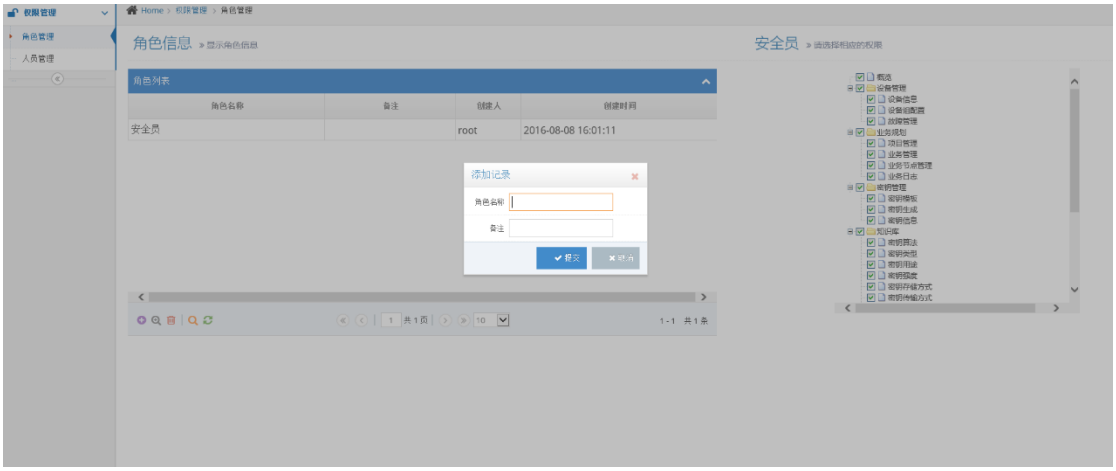
下图是权限管理包含的菜单项：

3.3.1 角色管理

角色列表列出了已有的角色信息，左侧列出角色名称，单选某一个角色，右侧的权限列表列出该角色相应的权限，可直接进行点选编辑，无需提交自动保存。



1. 点击“  ”新增角色按钮，跳转到角色添加界面：

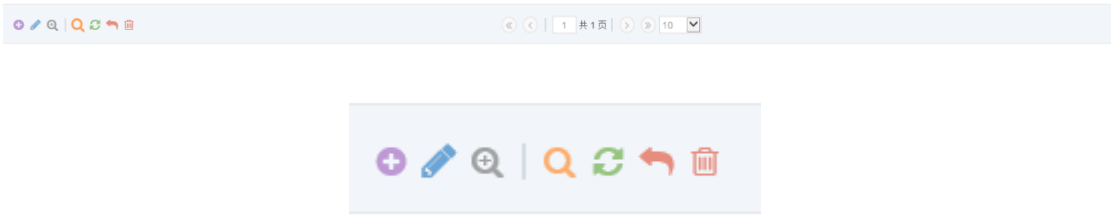


2. 填写角色名称并提交后，会在角色列表中建立一个新的角色，点选该角色后，右侧的权限列表列出该角色的权限，可直接进行点选编辑，无需提交自动保存：

3.3.2 权限管理

由超级管理员创建安全管理员，为安全管理员分配角色。角色可在角色管理中创建。人员信息列表列出已有的管理员及其角色：

提供新增管理员、编辑管理员、查看及删除管理员、重置密码功能：



点击“”新增管理员按钮，添加系统安全管理员信息。

管理员由数字证书作为身份标识，采用 USBKey 作为数字证书载体。USBKey 需先由第三方 CA 或平台认证管理功能签发数字证书。

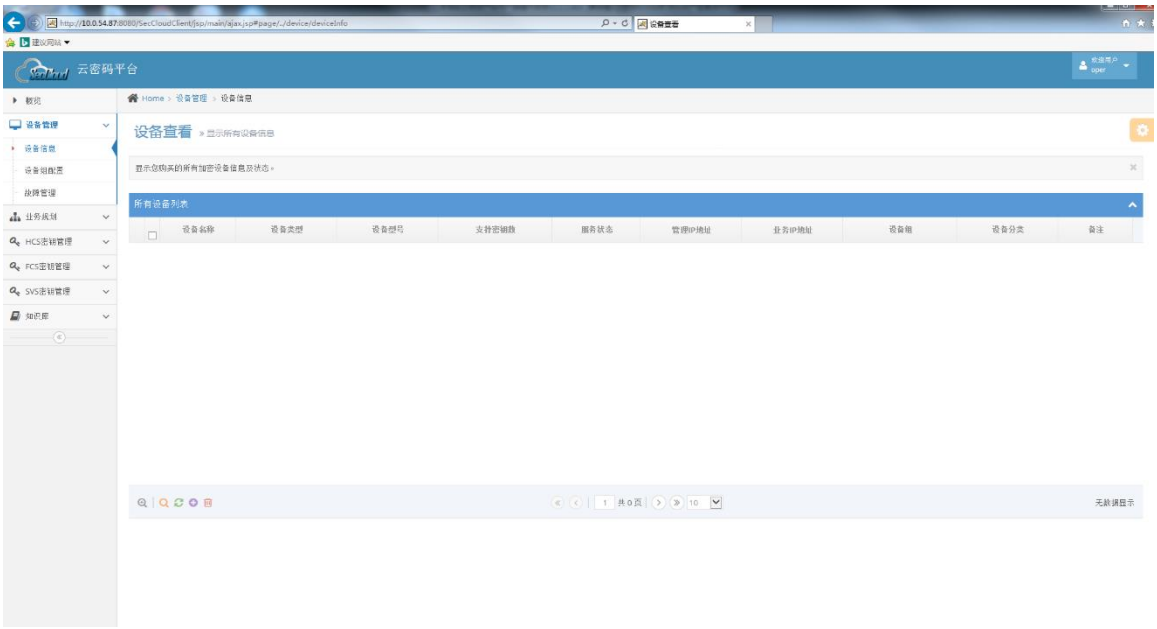
3.4 设备管理

设备管理提供虚拟加密实例的管理功能。

如下是设备管理包含的菜单项：

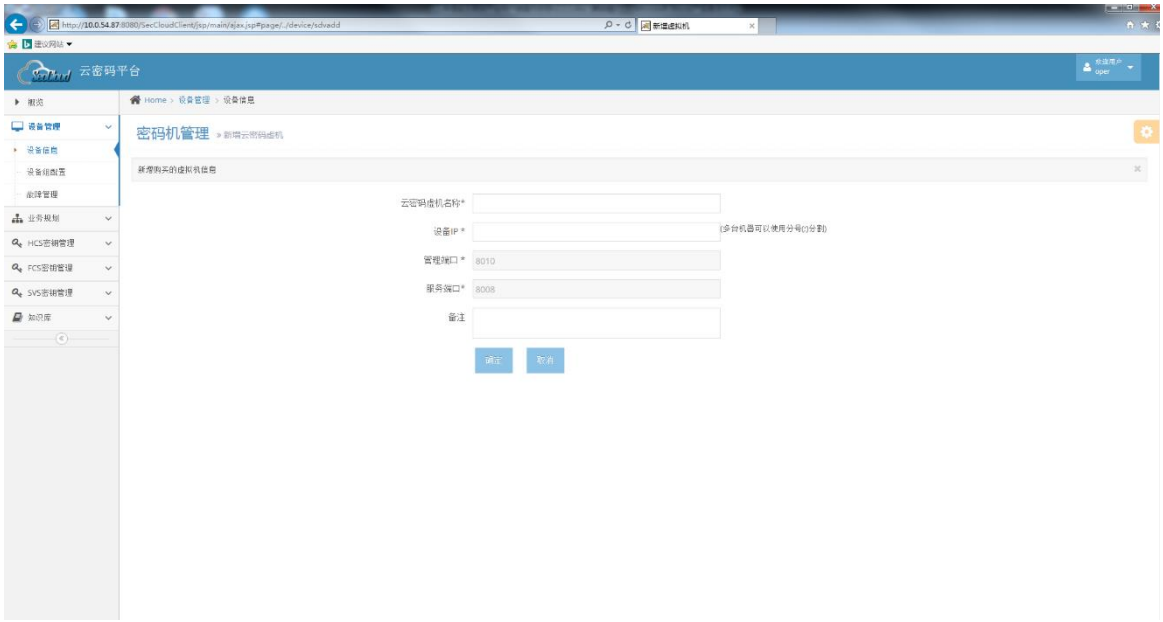
3.4.1 查看设备信息

1. 设备查看页面：



2. 设备录入按钮：

3. 设备录入界面：



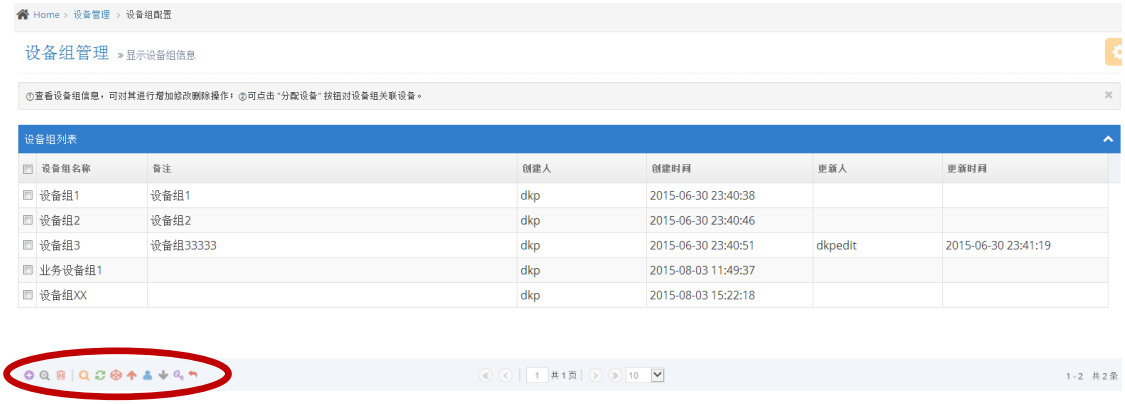
3.4.2 设备组配置

提供设备组的增删改查功能，用户将设备按照一定的规则进行分组，设备组内的设备具备相同的类型、型号，并作为一个整体存储相同的密钥。每个设备组内可以有一个或多个设备。设备为虚拟加密实例。

已建立的设备组信息通过下面图中列表的形式展示出来，页面底部的操作栏提供增删改查功能。编辑、删除、查看功能需要先选定至少一条设备组记录，然后再进行相应操作，对页面提示框进行确认。

注意：

每个安全管理员有权创建设备组，并只能看到和编辑自己创建的设备组。



放大后如图：

对应功能为：

1 添加设备组；2 修改设备组；

3 查看设备组；4 删除设备组；

5 设备组搜索；6 设备组刷新；

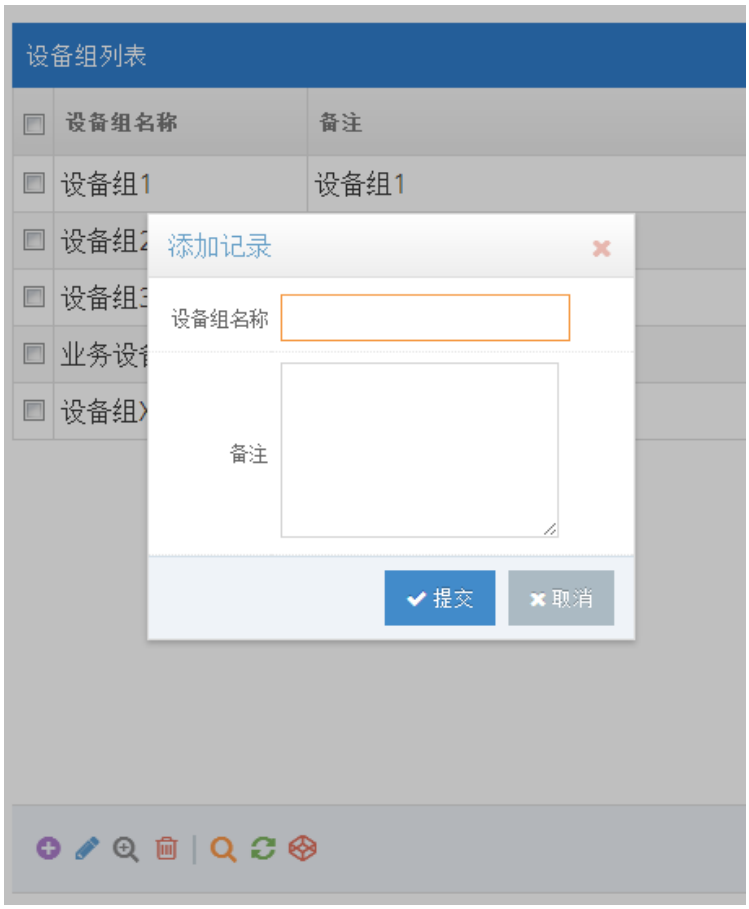
7 设备组绑定设备；8 查看设备组登陆状态；

9 下载设备组凭证；10 启动设备组内所有设备的业务服务；

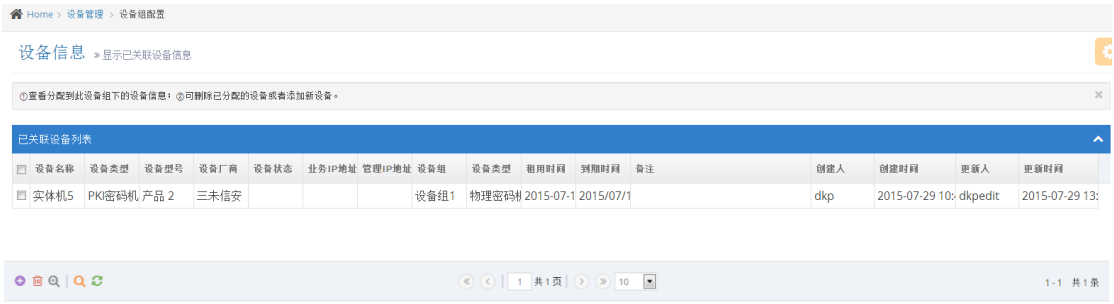
11 设备组密钥备份；12 设备组密钥恢复；

3.4.3 添加设备组

1. 点击“ ”按钮，弹出添加设备组输入框，添加设备组需填写设备组名称：



2. 分配设备，选中设备组列表中的一条记录，点击“”分配设备按钮，会列出该设备组已分配的密码设备：



3. 选择其中的一条或多条已分配设备记录，然后点击“”删除设备按钮，即可将该设备从设备组中移去。

注意：

移去时会清空密码设备上的所有密钥及权限信息，并进行初始化，请谨慎操作。

4. 点击“”新增设备按钮，用户平台会跳转到未分配设备页面，列出所有未分配设备：

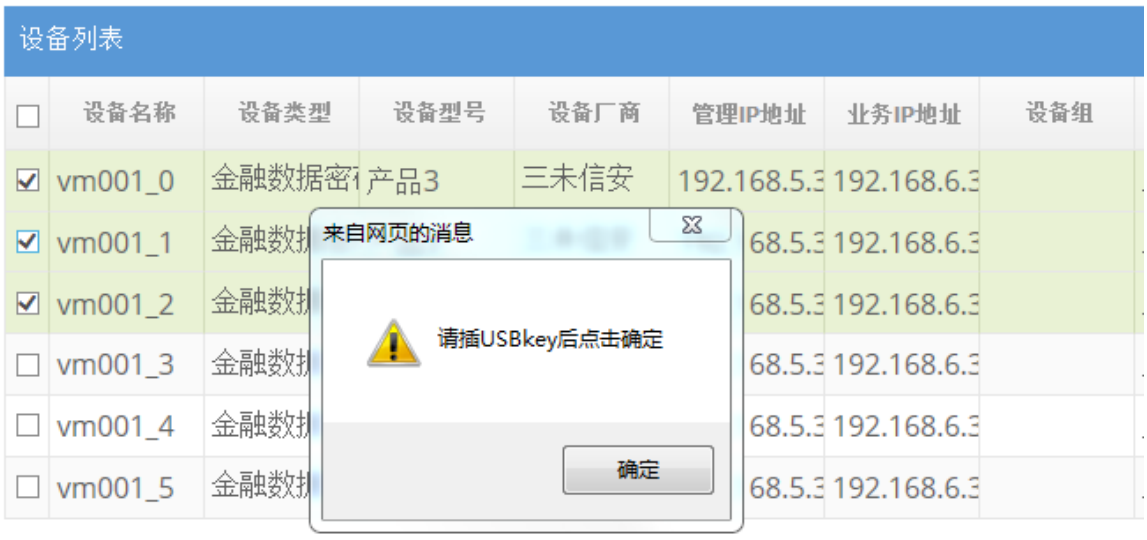
说明：

可选择其中的一条或多条未分配设备，添加到当前设备组。

设备添加到设备组的同时会完成设备人员的初始化。设备管理员至少是三个，管理员的存储介质为 USBKey。所以绑定到设备组之前应准备好三个 USBKey 供初始化使用。

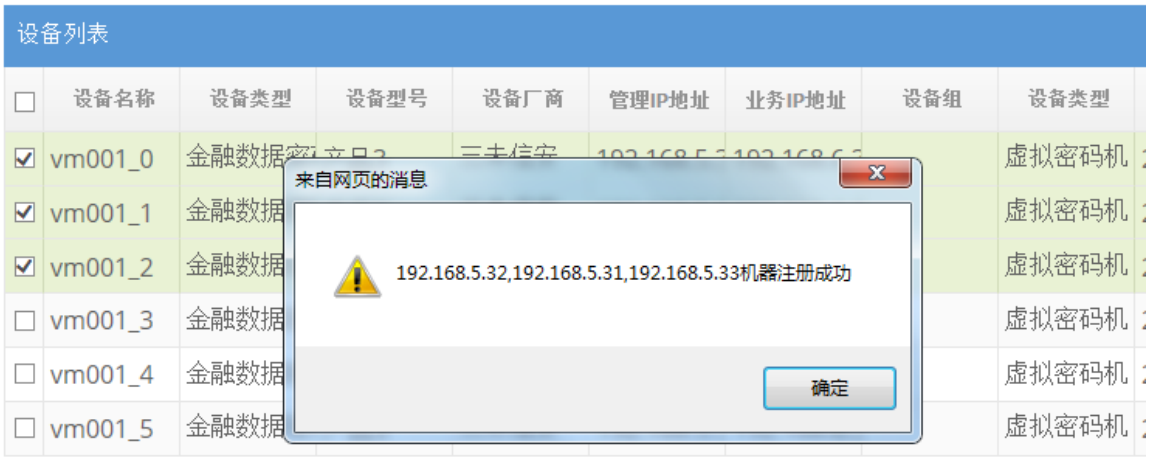
5. 在未分配设备列表页面，点击“”添加到设备组按钮

6. 输入当前系统管理员口令，验证通过后，弹出：



7. 此时插入其中一个 Key，然后点击“确定”，弹出：

8. 输入当前设备管理员 Key 的口令点击“确定”按钮。如果是同时注册多个设备，会提示如下：



9. 点击“确定”完成第一个设备管理员的注册。

之后进行第二个、第三个设备管理员的注册。所有设备管理员都注册完成后，系统会自动跳转到已关联到当前设备组的设备列表，如下：

至此，设备添加到设备组的操作完成。

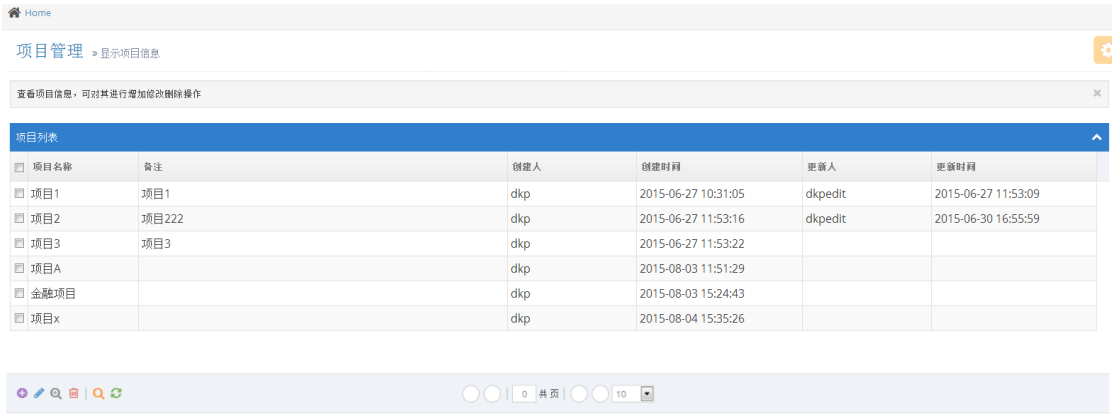
3.5 设备与业务关联

业务规划帮用户建立业务与设备组的关联关系，通过用户平台的业务规划，业务系统在使用密码服务时就可以免除对设备的依赖关系，降低开发和维护的耦合性。

3.5.1 项目管理

项目为用户提供了业务的第一层分类，用户可通过创建项目，并将相同或相关的业务归在相同的项目下，将业务进行归类，便于理清业务的逻辑关系。

下图是项目管理页面，列出所有已创建的项目，并提供项目的增加、编辑、查看、删除、搜索、刷新等功能：



放大下部操作按钮：

新增项目：点击页面底部“  ”新增项目按钮，开始录入项目信息：

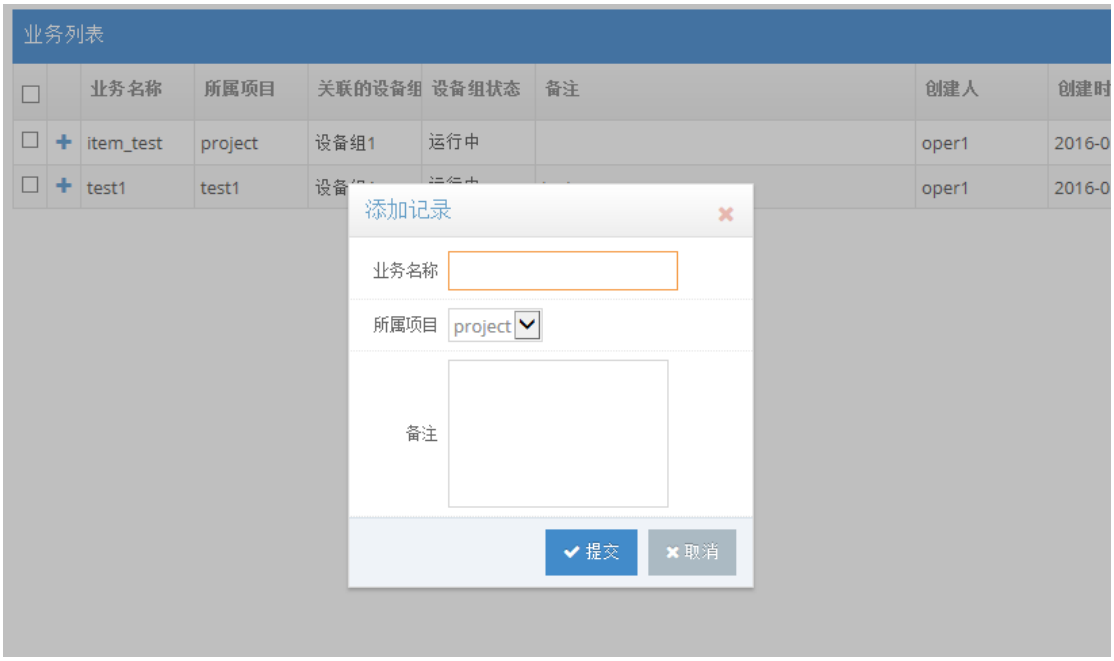
3.5.2 业务管理

业务代表用户使用密码服务的逻辑单位，一个业务可以绑定一个设备组，使用该设备组的一种或多种密码服务。例如，文件加密业务，通过用户平台绑定设备组 X，使用对称加密服务对文件进行加密。

如下是业务管理页面，列出所有已创建的业务，并提供业务的增加、编辑、查看、删除、搜索、绑定设备组、启动停止设备组等功能：

放大下部操作按钮：

1. 创建业务，点击页面底部“  ”创建业务按钮，进入创建业务页面。
2. 填写业务名称，并选择业务所属项目，即可创建业务。

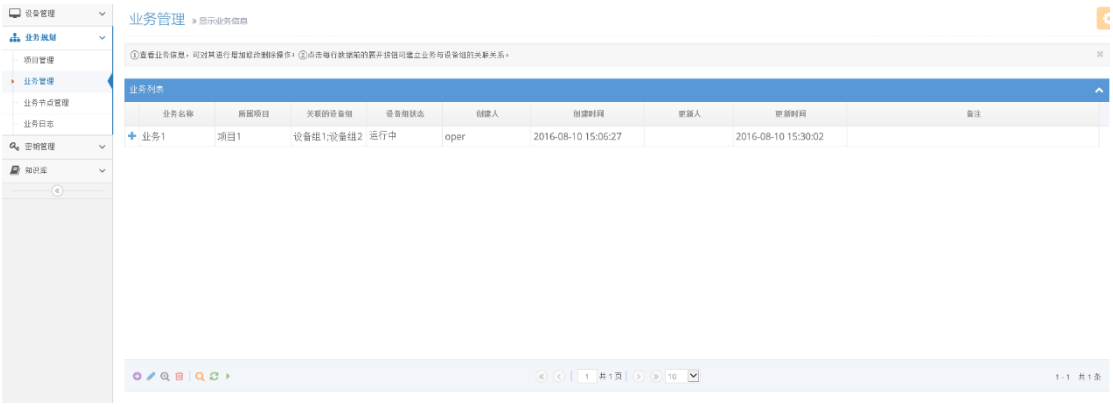


3. 关联设备组，业务创建后默认未关联任何设备组。

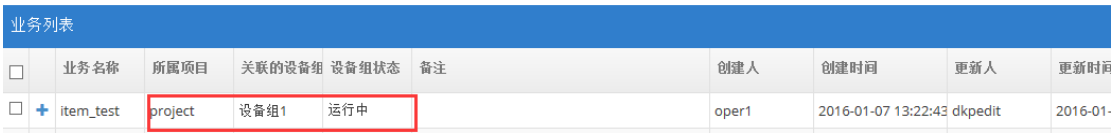
4. 在业务管理页面，点击某个业务记录左侧的“ ”，用户平台会展开所有可选的设备组供选择：

5. 首先选中一个设备组，点击展开项中的“ ”关联选中设备组按钮，将该设备组关联给指定业务。

6. 关联成功会提示操作成功。并且一个业务可以关联多个设备组。



7. 启动/关闭设备组，关联到设备组以后，点击“ ”，便可以把设备组的服务启动，可在业务列表中设备组的状态中查看设备组是否是运行状态。



3.5.3 业务节点管理

业务只是逻辑单元，一个业务可能需要一个或多个业务服务器并行完成，因此每个业务下需要建立具体的业务节点，即业务服务器。业务节点上需部署密码服务套件，通过套件调用密码设备完成密码运算服务。

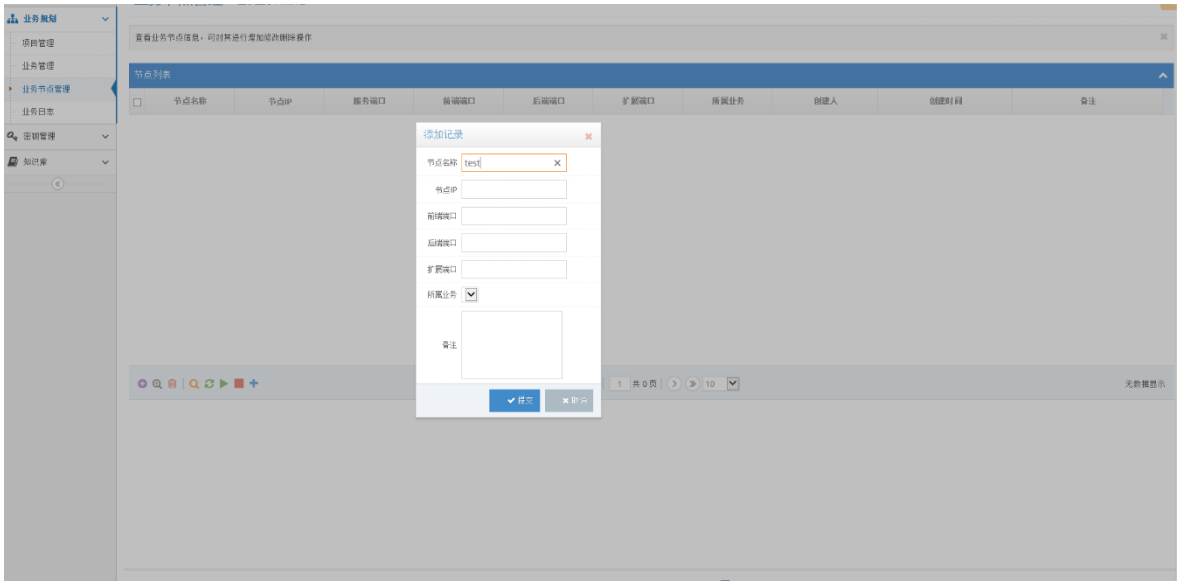
说明：

服务套件为代理软件。

业务节点管理首先列出了所有的业务节点，包括该节点的服务器 IP，密码套件端口，所属业务等信息：

1. 创建业务节点

2. 点击“  ”创建业务节点按钮，列出业务节点所需填写的信息



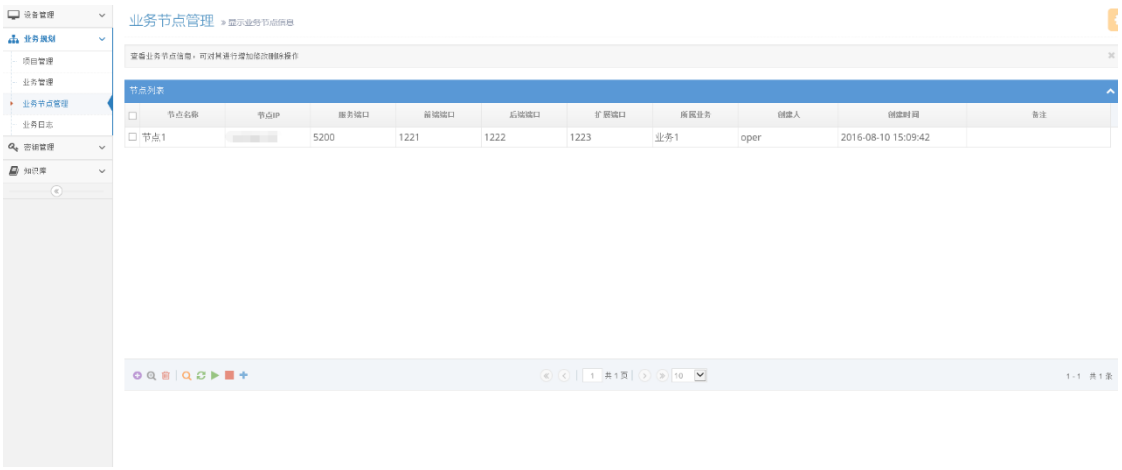
说明：

节点 IP ：这是负载均衡的 IP，需要把业务下所绑定设备推送到负载均衡服务里

前端端口：是做业务时需要用的端口，通过 IP 和前端端口就可以访问负载均衡，就可以访问到端口下所对应的密码机

后端端口：是负载均衡与密码机之间所需要的端口

扩展端口：会将不同的消息转发到不同的密码机中



4. 常见问题

4.1 什么是专属加密？

专属加密（Dedicated Hardware Security Module，Dedicated HSM）是天翼云为用户提供的云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

Dedicated HSM 旨在满足用户将线下加密设备能力转移到云上的要求，提供可独占、高性能、安全合规的加密域计算资源。用户作为设备使用者完全控制密钥的产生、存储和访问授权。天翼云只负责监控和管理设备及其相关网络设施。

同时，Dedicated HSM 可提供认证合规的金融数据加密机、服务器加密机以及签名验签服务器等，灵活支撑用户业务场景。能够帮助用户满足数据安全方面的监管要求，以及云上业务数据的隐私性要求。

4.2 如何获取身份识别卡（Ukey）？

购买专属加密实例后，需要使用身份识别卡（Ukey）来进行实例的管理。

请登录天翼云网站，购买专属加密实例并留下 Ukey 收货地址，天翼云专家将尽快将身份识别卡(USB key)邮寄给您。

4.3 用户本地部署的加密机如何迁移到云上专属加密服务？

用户需要联系天翼云专家，详细核对当前使用的接口、功能等规格参数，制定迁移方案，确保本地密钥能够批量、安全地迁移到云上进行平滑过渡。

4.4 专属加密中，如何保障密钥生成的安全性？

密钥是由用户自己远程创建，且创建过程需要仅用户持有的 Ukey 参与认证。

加密机的配置和内部密钥的准备，都必须要使用这一组 Ukey 作为鉴权凭证才能操作。

用户作为设备使用者完全控制密钥的产生、存储和访问授权，天翼云只负责监控和管理设备及其相关网络设施。

4.5 机房管理员是否有超级管理权限，在机房插入特权 Ukey 窃取信息？

机房管理员没有超级管理权限，Ukey 是天翼云提供给用户的身份识别卡，此卡仅购买专属加密实例

的用户持有。

敏感数据（密钥）存储在国家规定的硬件加密卡中，即使加密机制造商也无法读取内部密钥信息。