中安云科
SINOCIPHER

中安云科数据库加密网关 V1.0 实施文档

中安云科科技发展（山东）有限公司

2023 年 11 月 8 日

目录

1. 产品介绍

中安云科数据库加密网关是一款针对于数据库数据存储安全的基础密码设备，是基于数据库透明加密原理的数据库主动防御产品，具有对数据库敏感数据进行加密解密、完整性保护、基于加密的权限控制、加密密钥管理等功能。

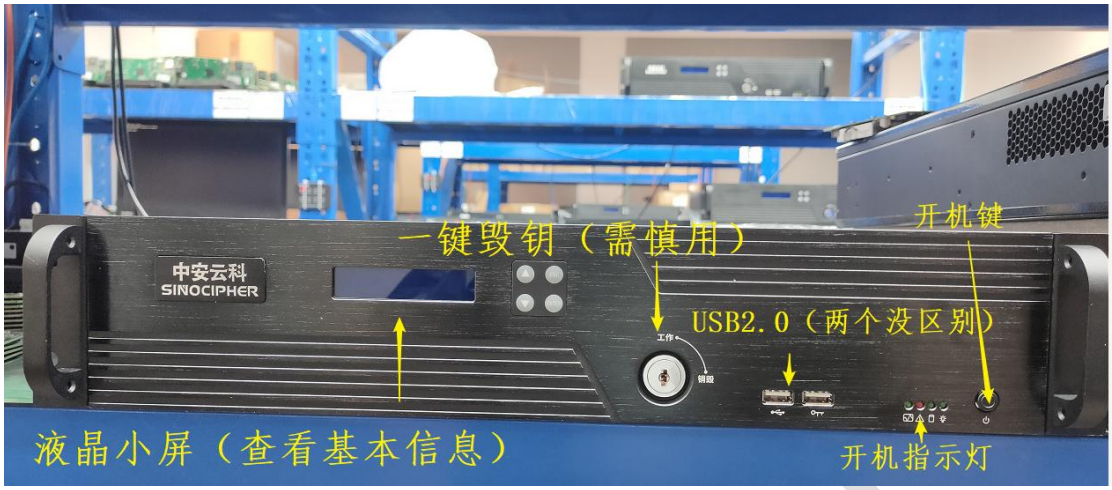
数据库加密网关能够防止数据库明文存储的数据泄露引发的数据泄密、防止突破边界防护的外部黑客攻击、防止内部高权限用户对数据库数据的窃取。数据库加密网关使用密码技术对敏感数据进行加密和完整性保护，在数据写入数据表前保护数据，在数据返回前解密或验证数据，加密和解密过程是在数据库逻辑层面调用数据库加密网关进行的，对应用程序和用户是透明无感知的。

数据库加密网关可对加密数据设置独立于数据库的、基于加密的权限控制，可以限制数据库用户对加密数据执行的操作，防止高权限用户或普通用户越权访问敏感数据，也可以基于客户端名称、时间等环境因素限制对加密数据库的访问，实现更加细粒度的访问控制。

数据库加密网关使用不同密钥加密数据库不同的敏感数据，采用密钥管理与数据存储分离的核心理念，通过集中安全的密钥管理保护加密密钥整个生命周期的安全。

2. 产品上架

- 打开包装，对照“装机清单”检查配件是否齐全、并检查所有部件是否完好。如果有任何部件缺少或者损坏，请不要进行安装，应立即与厂商进行联系。
- 取出设备及其他配件；
- 产品外观以及功能介绍（部分机箱外观有差异）



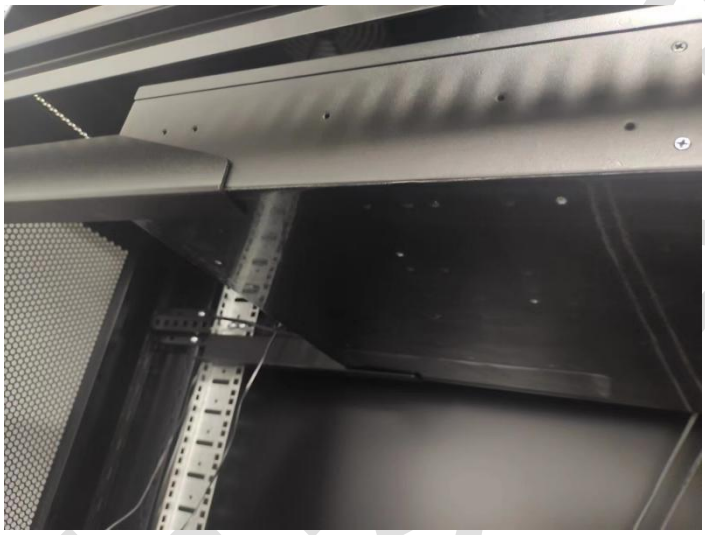
- 将机器上架

设备支架入下图，安装在机柜后部左右各一个。

支架安装过程如下（螺丝固定）：

安装完成图示如下：

设备后部放置在支架上，前部耳片螺丝固定，图示如下：



- 连接电源，连接网线及需要的接口线，然后开机

3. 产品实施

3.1 数据库加密网关登录

- 将电脑与设备的 eth3 口直连
- 使用非 ie11 内核浏览器登录，在浏览器中直接输入：“192.168.6.10”，进入登录界面。
- 登录前需要运行托盘程序，如果未安装先点击下载 UKEY 插件进行安装，安装成功后，运行客户端，右下角显示图标，则表示正在运行

3.1.1 密码方式登录

- 如下图所示，登录方式选择密码登录(默认的登录方式)。

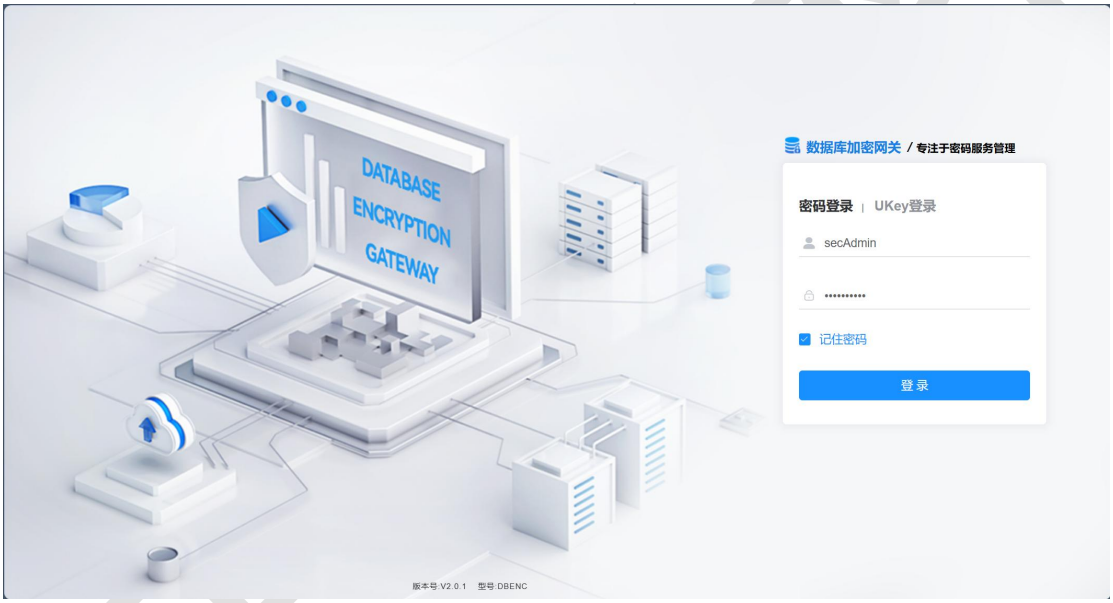
- 在登录界面中分别输入账号、密码，然后点击登录即可。其中，系统管理员和安全管理员账户将在登录超级管理员后进行添加管理，具体步骤参见第 3.2.3 节。
- 默认用户名/密码如下：

  超级管理员用户名/密码：supAdmin/admin@2030

  审计管理员用户名/密码：audAdmin/admin@2030

  系统管理员用户名/密码：sysAdmin/admin@2030

  安全管理员用户名/密码：secAdmin/admin@2030



3.1.2 Ukey 方式登录

Ukey 方式登录步骤如下:

- 登录前需要运行托盘程序，如果未安装先点击下载客户端进行安装，安装成功后，运行客户端，右下角显示图标，则表示正在运行
- 如下图所示，登录方式选择 UKey 登录。

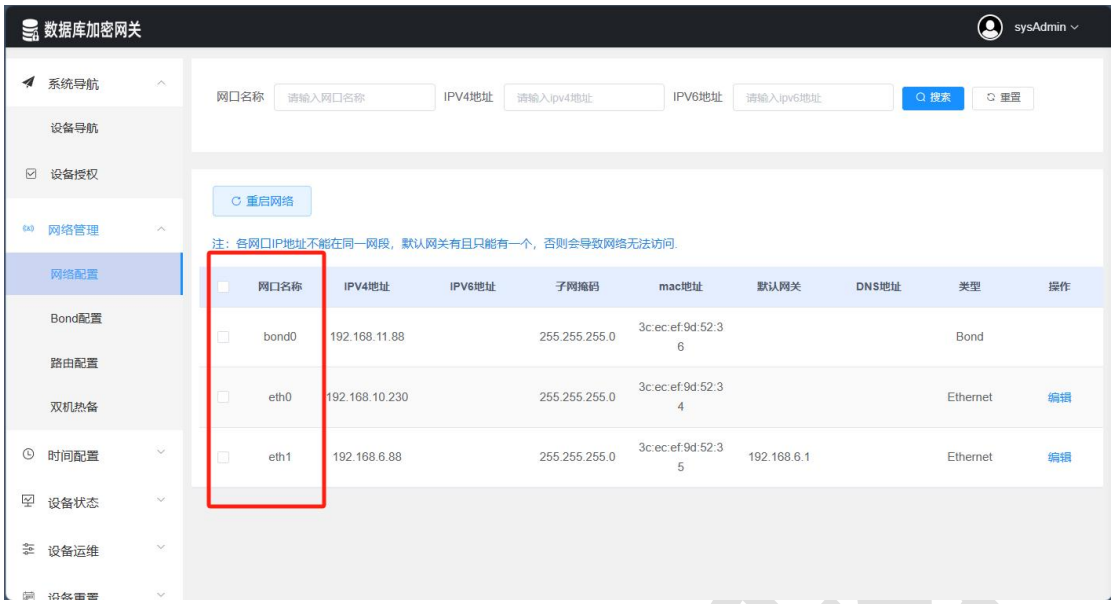
- 将管理员 Ukey 插入 PC 的 USB 接口，输入管理员 Ukey 口令（admin@2030），验证成功后进入首页。
- 在登录时若密码输入错误次数超过 8 次将锁定该用户无法登录，若非超级管理员被锁定，可登录超级管理员开启用户状态。

3.2 网络配置

3.2.1 ip 修改

- 通过登录【系统管理员】来进行设备 ip 的修改
- 提前沟通好 ip 地址掩码以及网关等网络信息（客户提供）

使用安全管理员，点击“网络管理”->“网络配置”选择。出现弹框填写相关信息 IP 信息、子网掩码、网关后点击保存按钮后生效。



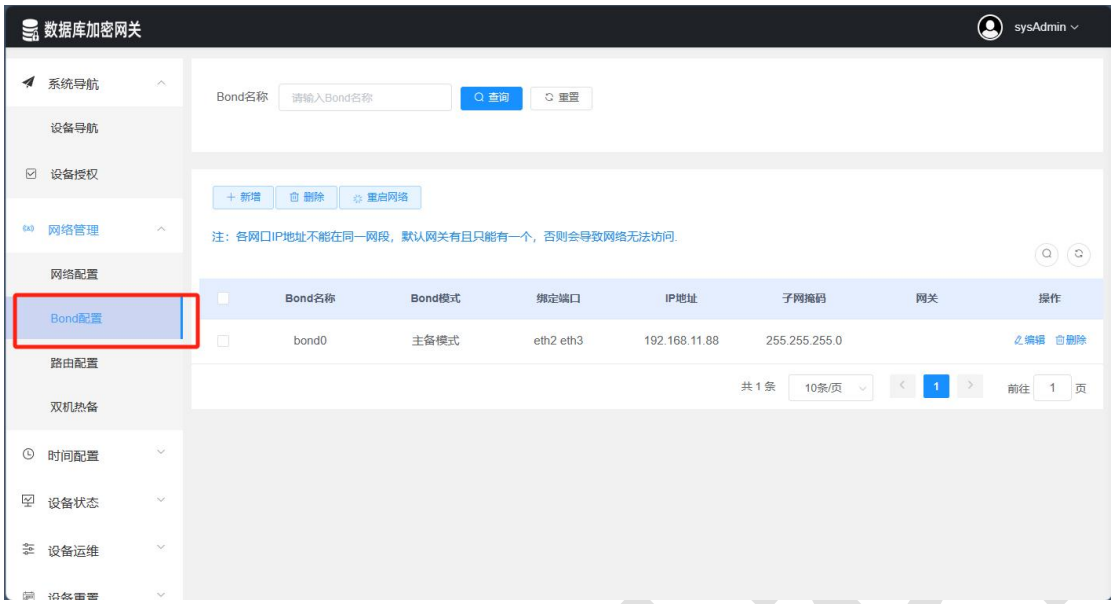
3.2.2 Bond 配置

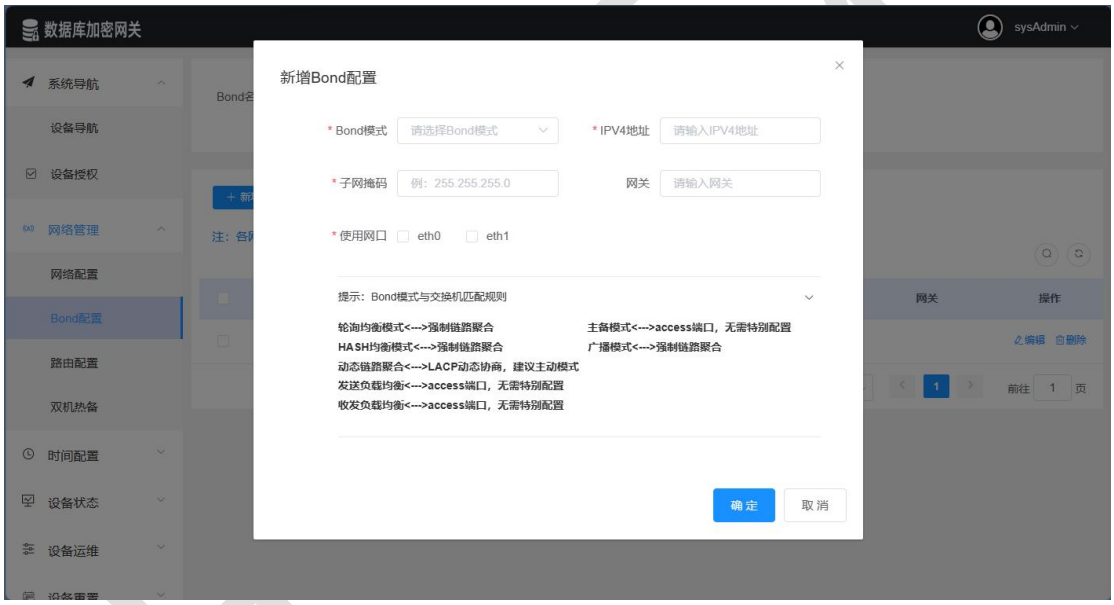
（如需配置 bond，参考该操作）

点击【网络管理】，点击【Bond 配置】进入到 Bond 配置页面。

点击【新增】，在弹出的对话框中选择 Bond 模式、子网掩码，输入 IPV4 地址、网关、使用网口，点击【确定】保存配置。注意每个的格式都要填写正确，若设备已经配置网关则 bond 时不能配置网关，否则会导致网络异常（每台设备只能配置一个网关，其他配置路

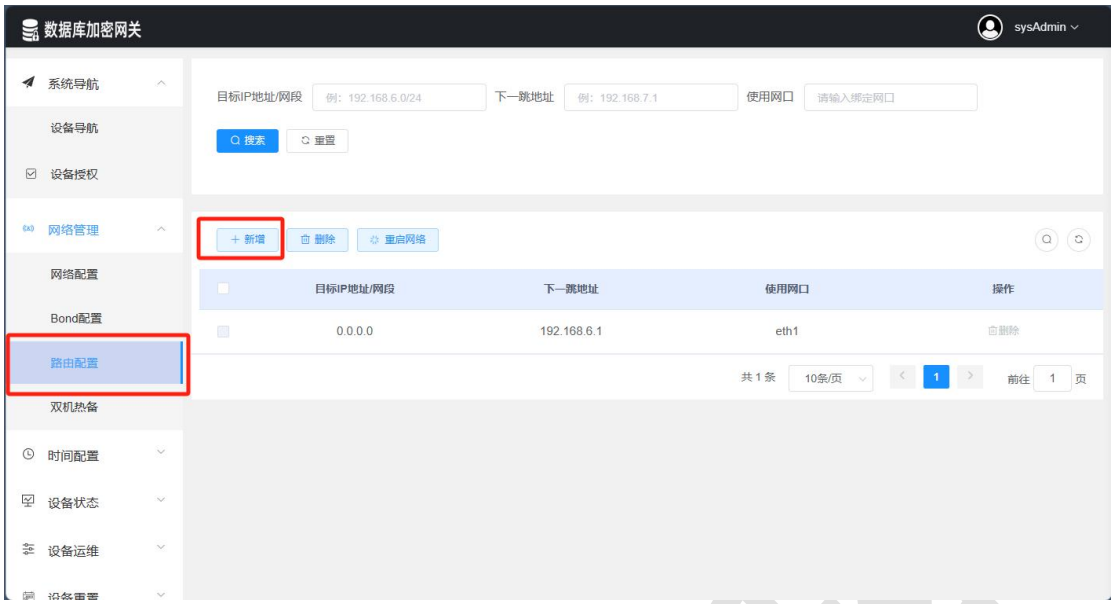
由）。点击【重启网络】后生效。



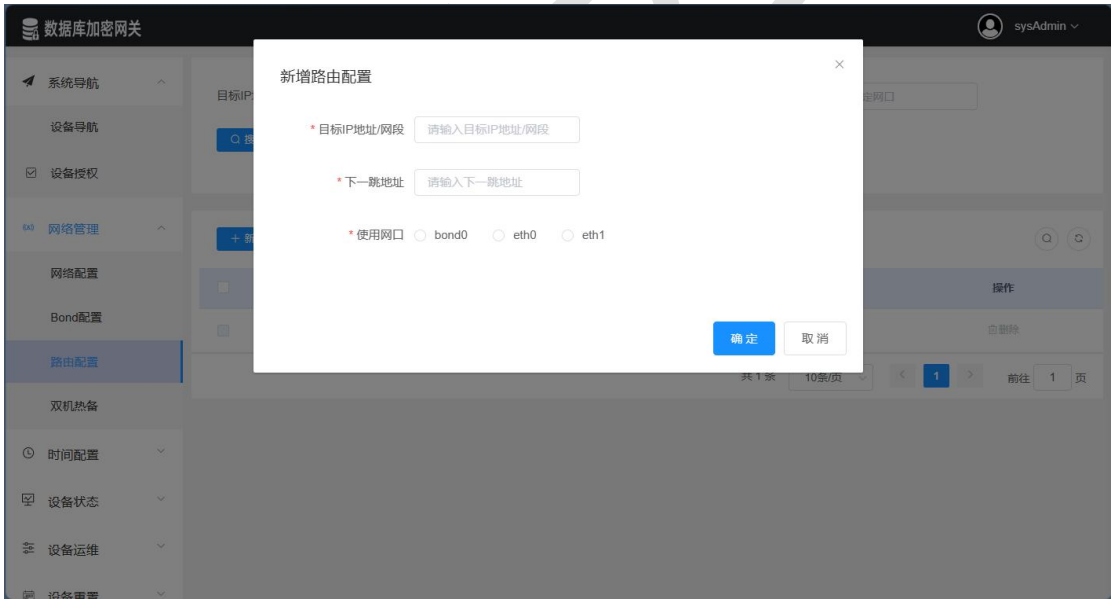


3.2.3 路由配置

点击【网络管理】，点击【路由配置】进入到路由配置页面。

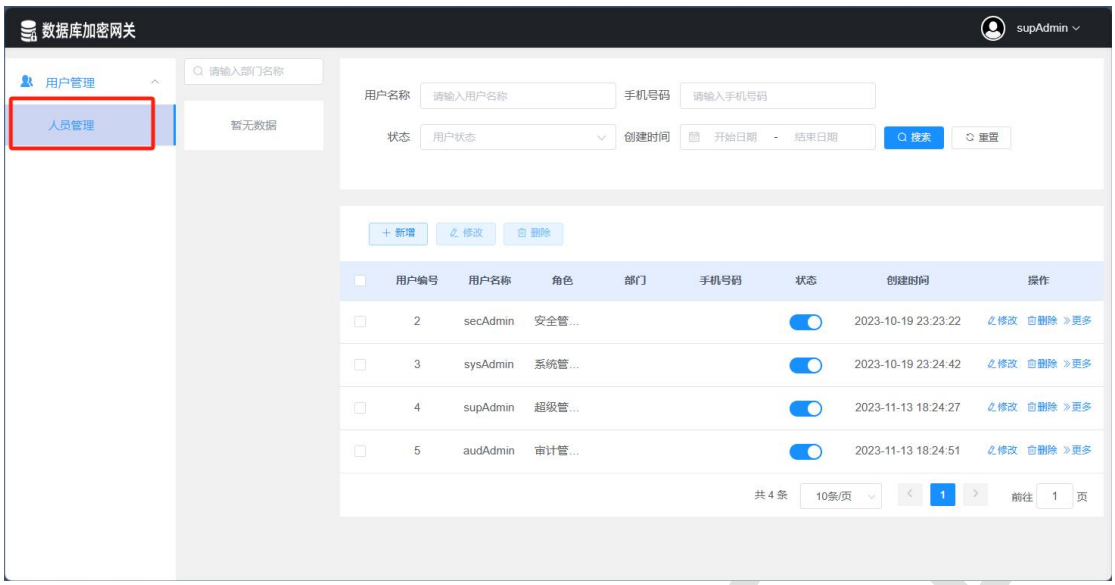


点击【新增】，在弹出的对话框中输入目的 IP 地址/网段、下一跳地址、使用网口，点击【确定】保存配置。注意每个的格式都要填写正确。点击【重启网络】后配置生效。

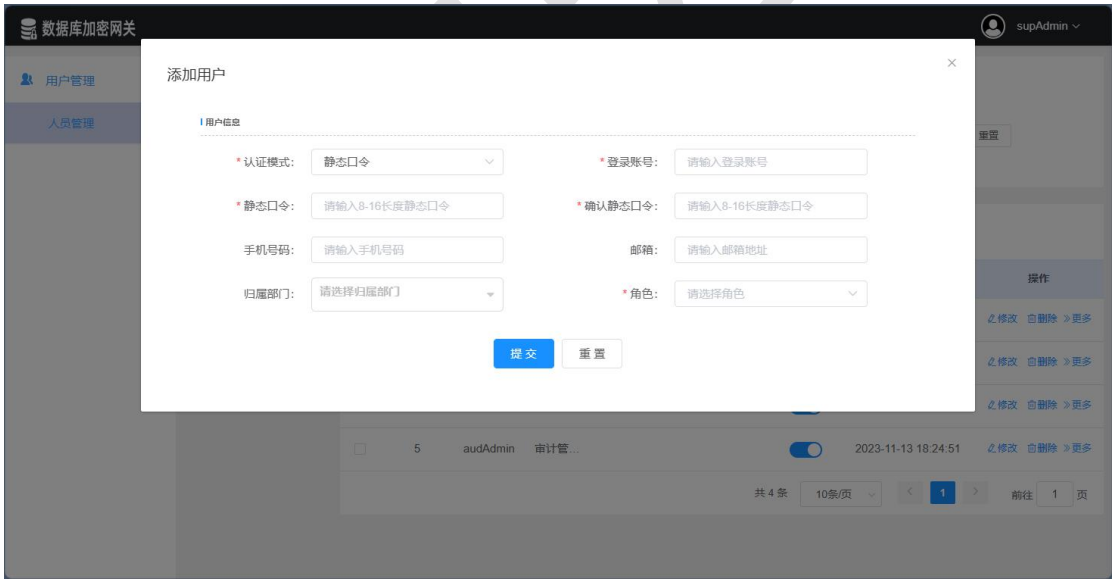


3.2.4 新增管理员

以【系统超级管理员】的身份登录，依次点击【用户管理】->【人员管理】。



管理员类型可以选择系统管理员、系统安全管理员，（注：这里新增管理员的时候，已经插在计算机上的超级管理员的 key 不动，直接将新的 key 插到计算机上即可），插入新的 key，选择要生成的管理员类型，输入口令，点击“提交”按钮，管理员生成成功。

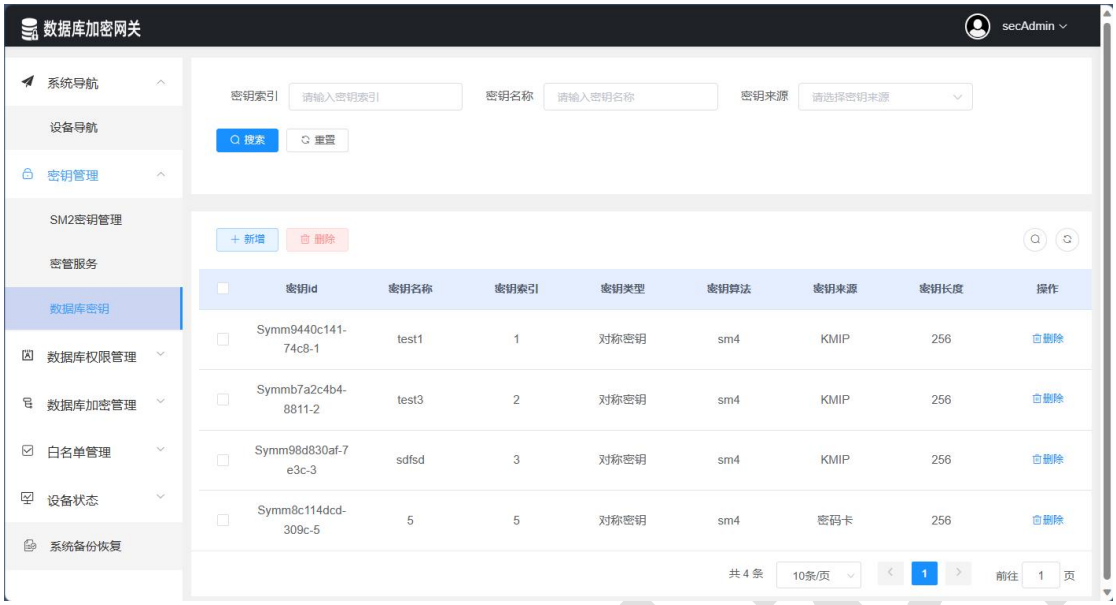


3.3 业务配置

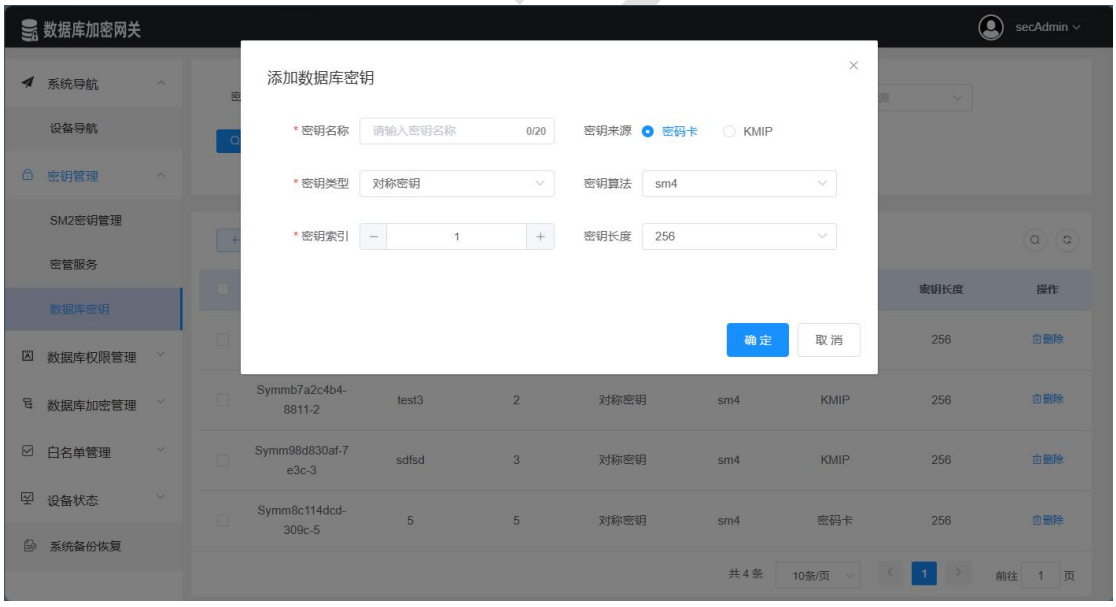
3.3.1 配置数据库密钥

以安全管理员身份登陆 WEB 管理系统，点击【密钥管理】，点击

【数据库密钥】进入数据密钥管理页面。如下图所示：

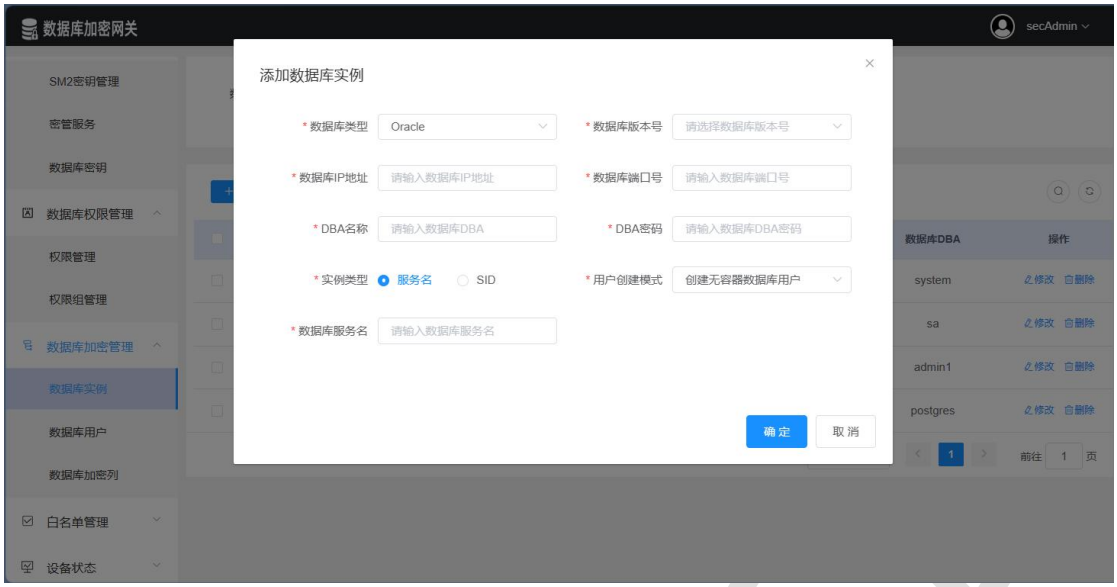


点击“新增”，在弹出窗口中填写密钥信息。



3.3.2 导入数据库实例

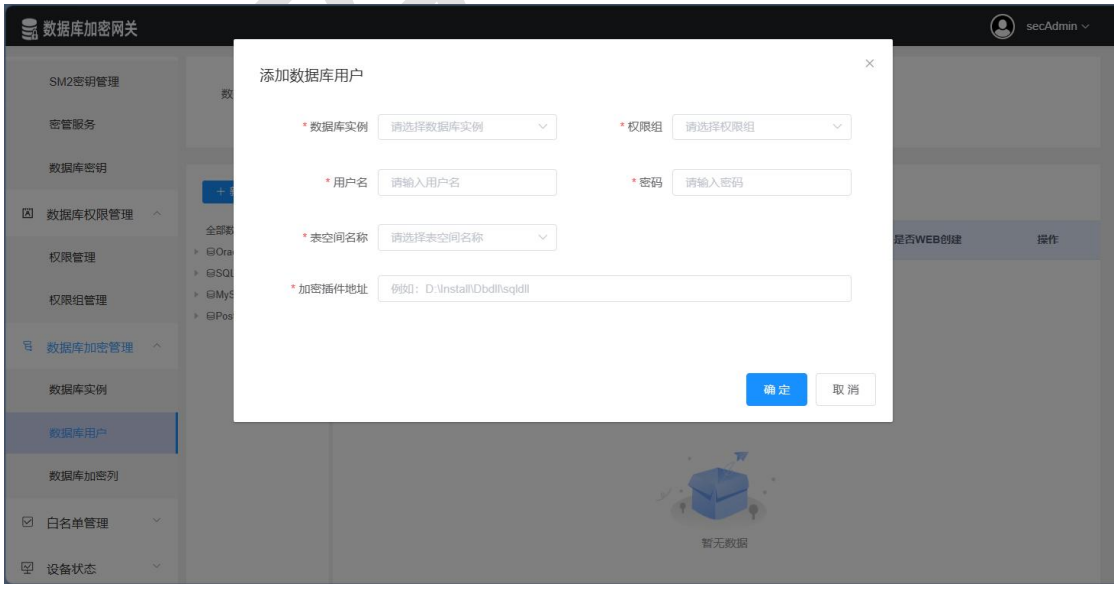
以安全管理员身份登陆 WEB 管理系统，依次打开【数据库加密管理】->【数据库实例】菜单，点击【新增】按钮，打开添加实例对话框，根据界面提示依次输入相关要素，然后点击确定。如下图所示：



3.3.3 数据库加密列配置说明

➢ 新增数据库用户

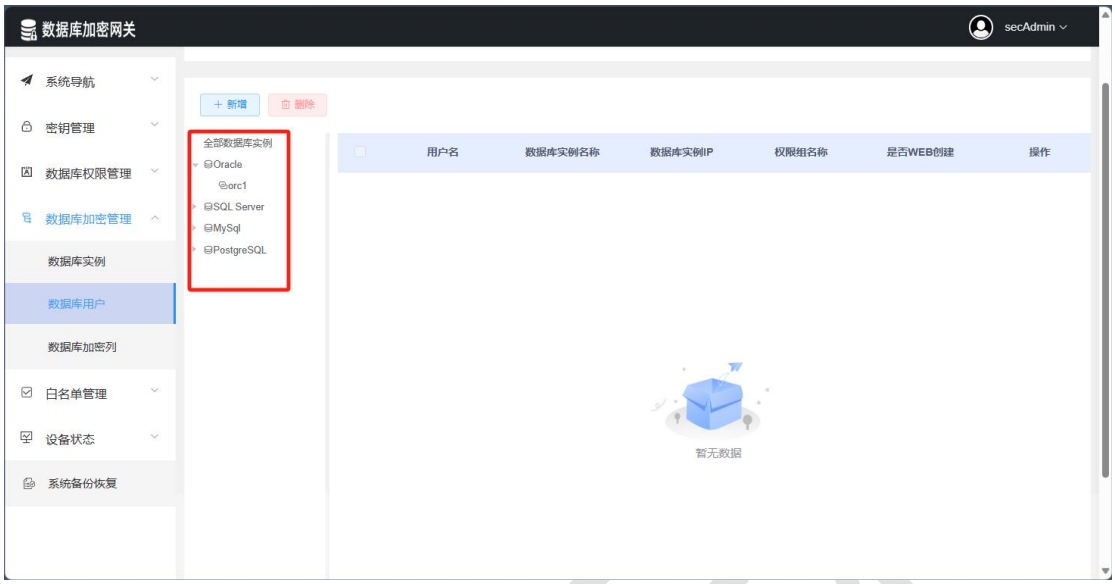
以【安全管理员】身份登陆 WEB 管理系统，依次打开【数据库加密管理】->【数据库用户】，点击【新增】按钮，打开新建数据库加密用户窗口，如下图所示



其中，加密插件地址为数据库加密插件安装的目录，如填写错误可能会导致用户无法加密。

权限组可以下拉选择 3.3.2 章节中添加的数据库权限信息，通常

为所配置的加密表权限。添加完成后，用户将在数据库实例列表中展示：



3.3.4 数据库加密

以【安全管理员】身份登陆 WEB 管理系统，依次打开【数据库加密管理】->【数据库加密列】，在右侧列表中，可查看已添加的数据库实例信息，如下图所示：

点击【配置加密列】，在弹出窗口中设置策略信息。加密列配置的算法类型如下：

SM4_CTR 算法，密文为不可见字符数据，无格式保留功能。

SGD_SM4_FPE_10，限制明文为 10 进制数字类型，加密后密文仍是数字，并且长度与原数据长度定义相同。

SGD_SM4_FPE_62，限制明文为数字+英文字符，加密后密文为英文字符与数字组合，长度与原数据相同；

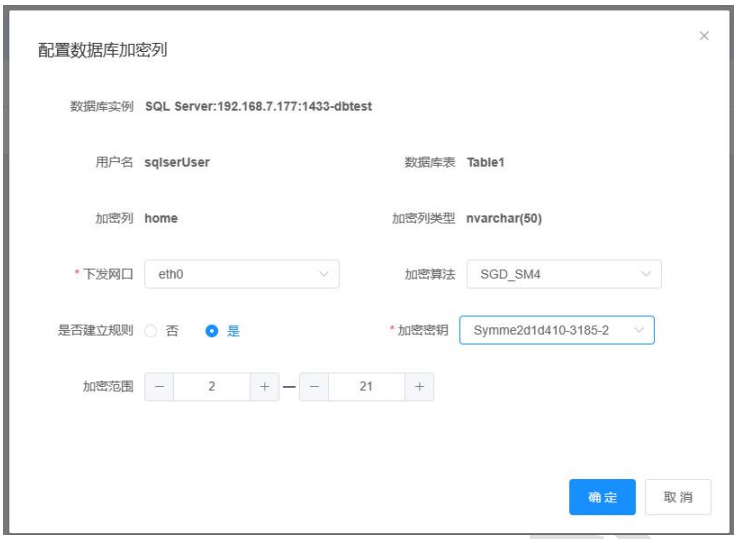
若选择 SGD_SM4_FPE_10（数字）、SGD_SM4_FPE_62 加密类型可选择是否创建加密规则，加密规则为加密该字段数据从第几位开始到第几位结束的数据：

1） Oracle 数据库配置加密列

点击配置加密列按钮，数据库实例选择 Oracle 实例，选择加密策略下发所使用的网口、加密算法、密钥、是否建立规则，点击确定即可。

2）SqlServer 数据库配置加密列

数据库实例选择 SqlServer 实例，选择加密策略下发所使用的网口，以及密钥，点击确定即可。

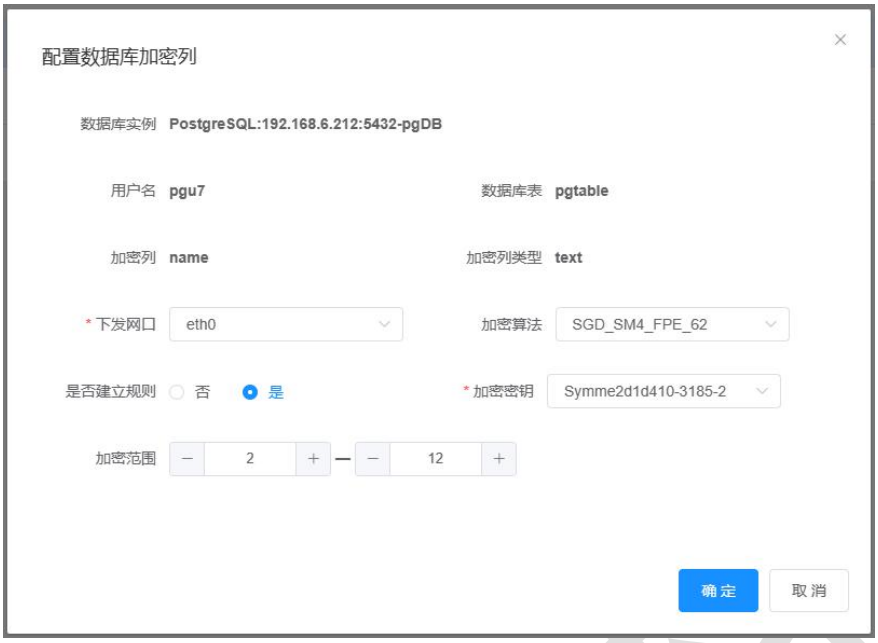


3）MySQL 数据库配置加密列

数据库实例选择 MySQL 实例，选择加密策略下发所使用的网口，以及密钥，点击确定即可。

4）PostgreSQL 数据库配置加密列

数据库实例选择 PostgreSQL 实例，选择加密策略下发所使用的网口，以及密钥，点击确定即可。



数据加密注意事项

1、加密长度不得小于 6 位字符，也不能为空数据。即加密列的所有数据中不能存在小于 6 位字符的数据或空数据

2、设置的偏移量和加密长度总和，不得超出数据长度

3、暂不支持加密中文数据