CKEY 动态认证系统
管理员使用手册

北京中科恒伦科技有限公司

目录

1 项目概述

1.1 编写目的

为了保障双因素认证系统的正常工作与运行，提高系统运维的效率，特编写本操作手册。

1.2 范围

双因素系统管理员维护

2 系统组成

- Jdk-11：${chelen}/iAMS/jdk
- mysql-8：${chelen}/iAMS/mysql
- CKEY DAS 主程序：${chelen}/iAMS
- 数据文件：${chelen}/iAMS/data
- 自助服务主程序：${chelen}/iAUS

3 管理配置

配置流程：

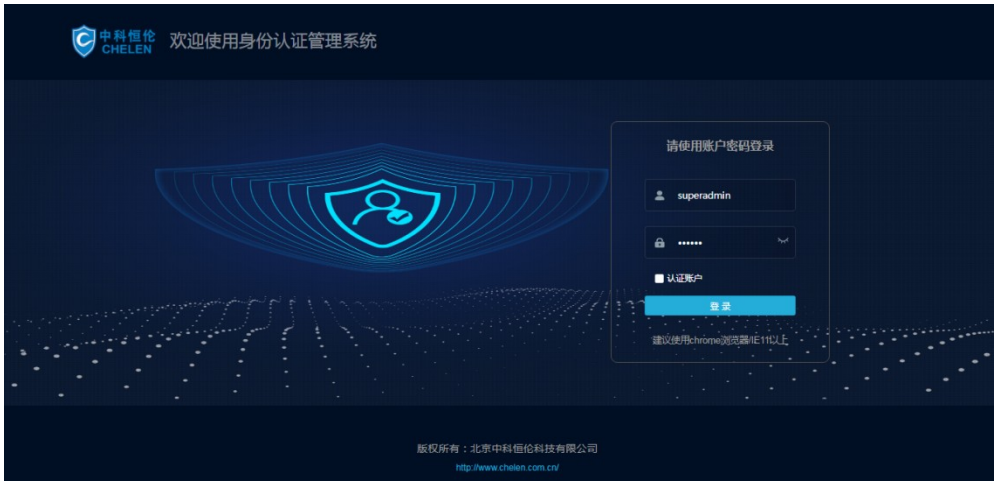
1、网络资源管理-->接入设备管理-->添加认证设备信息

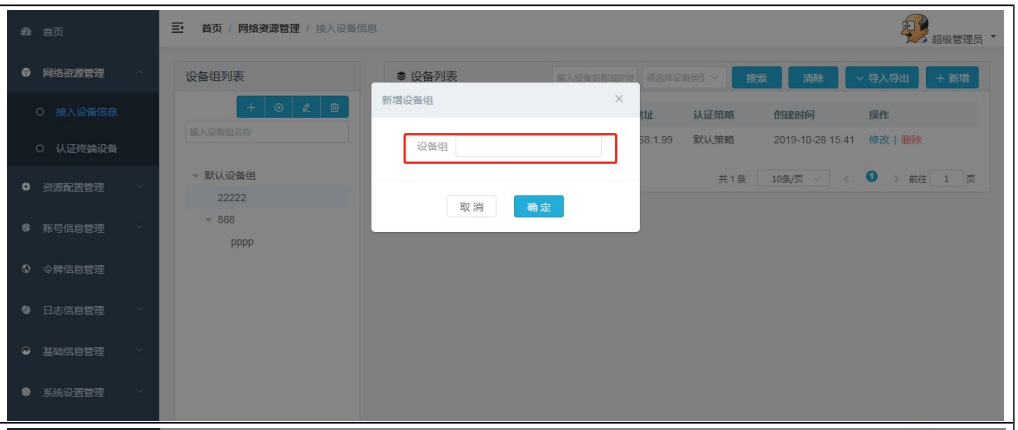
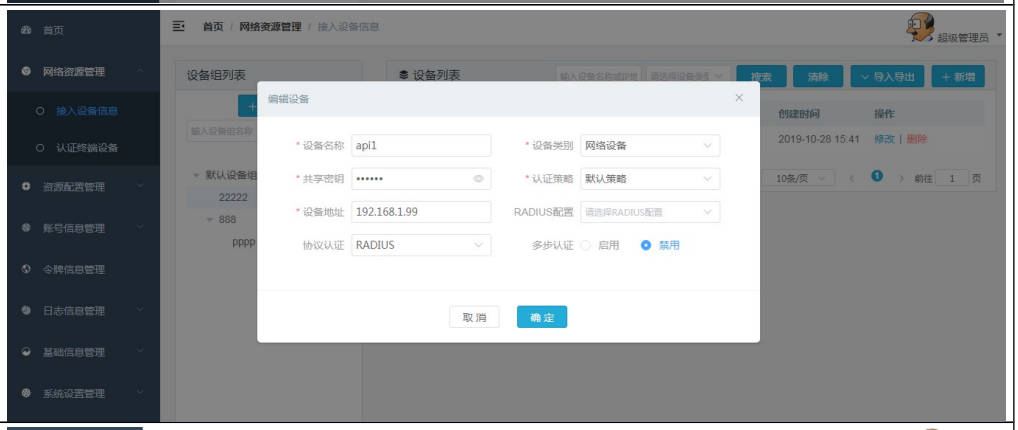
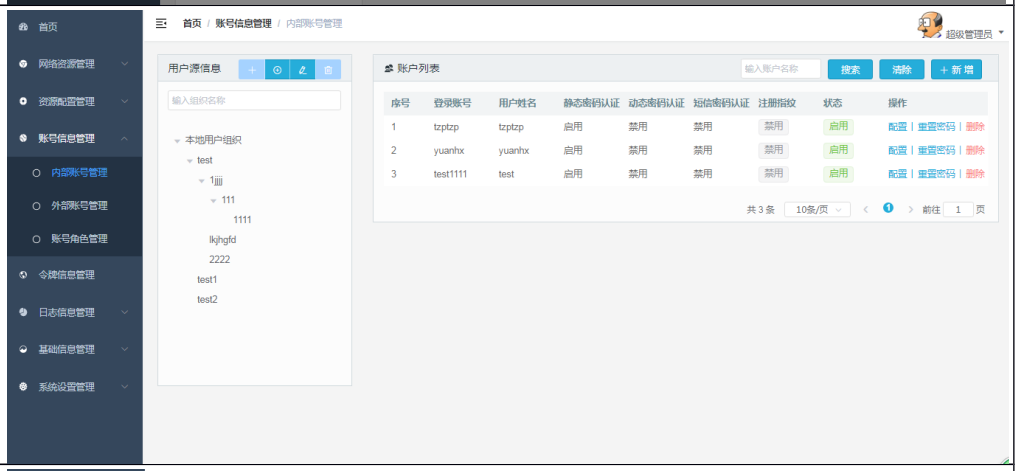
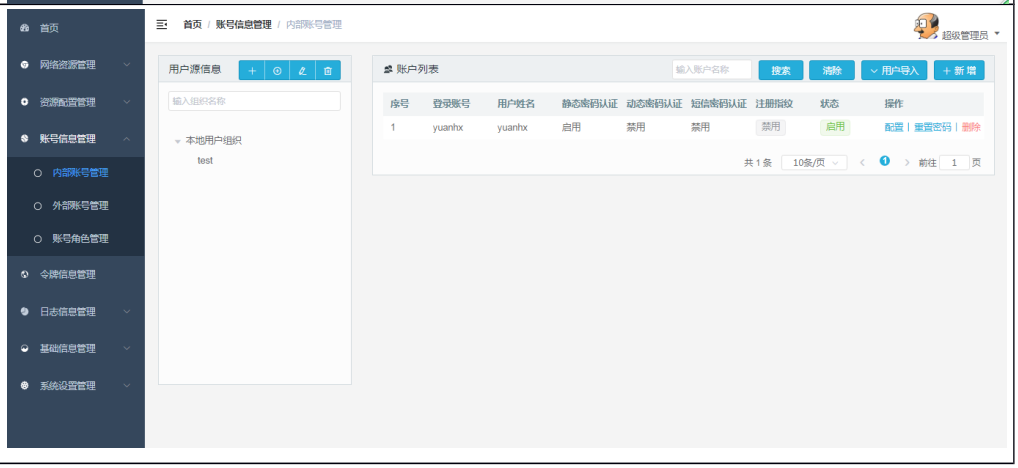
2、资源配置管理-->策略信息管理 -->添加认证策略-->设备加载认证策略

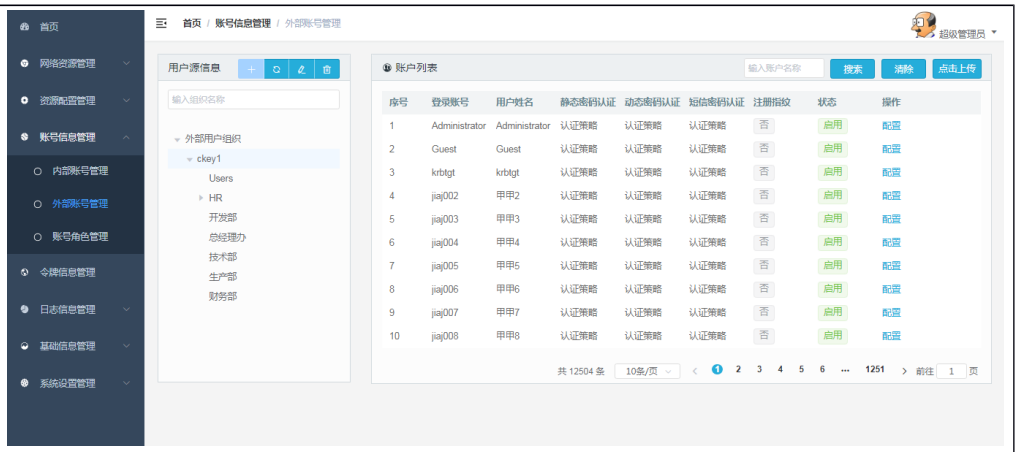
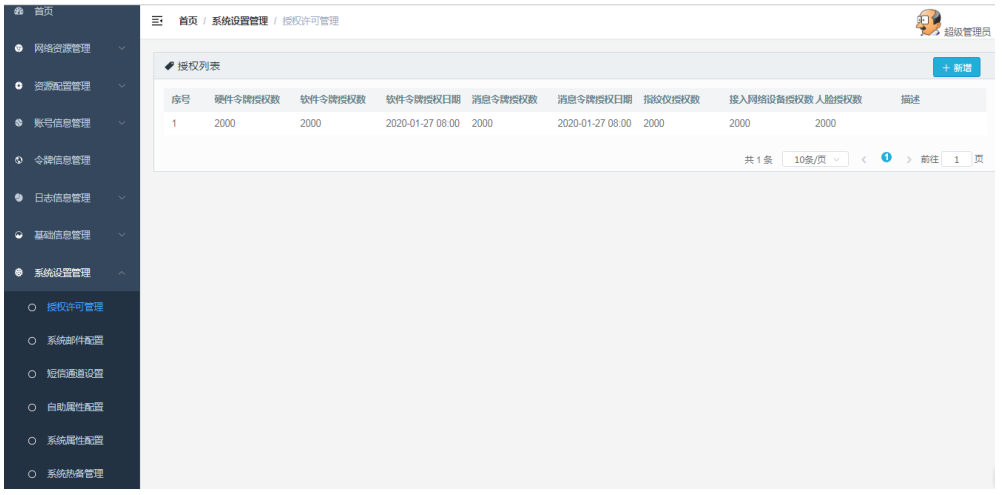
3、帐号信息管理-->内部帐号管理-->添加认证帐号-->或者使用外部帐号管理同步

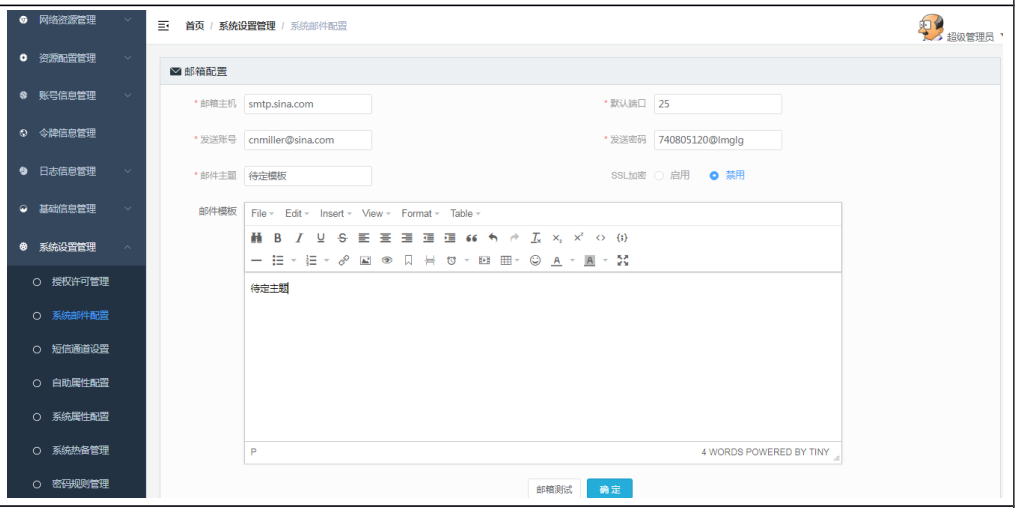
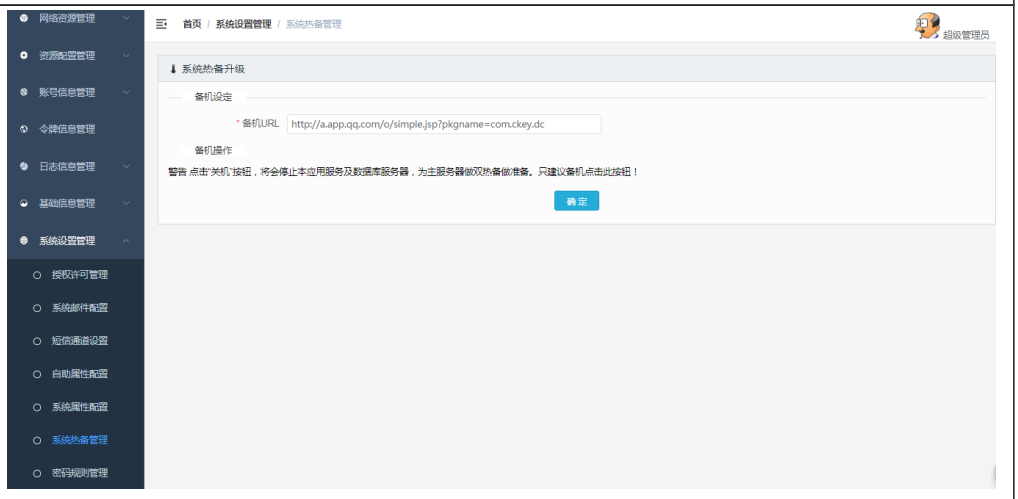
4、编辑帐号信息-->绑定令牌-->激活令牌（软件令牌需要激活，硬件令牌无需激活，绑定后即可使用动态密码）

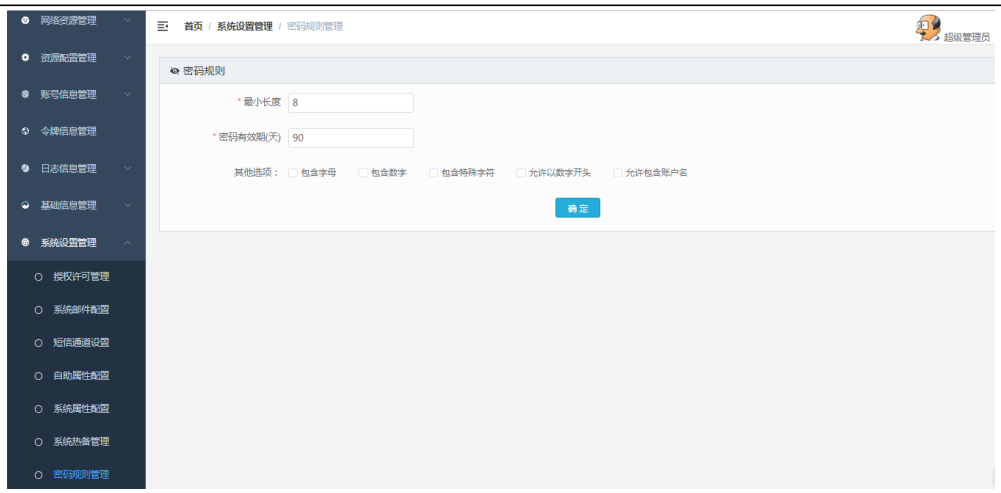
3.1 配置步骤

步骤		
	描述	截图
1	登录 CKEY 认证管理平台，输入默认管理员和密码，superadmin 123456	
2	输入管理帐号和密码，进入管理页面。左侧是导航栏	

4	在网络资源管理-添加需要认证的接入设备组名	
5	在选定组名后-新增对应的认证设备信息，选择对接的认证协议，以及共享密钥（需要对接的设备端保持一致）	
6	本地用户添加在【帐号信息管理】-【内部帐号管理】新添需要认证用户	
7	添加本地用户进行认证	

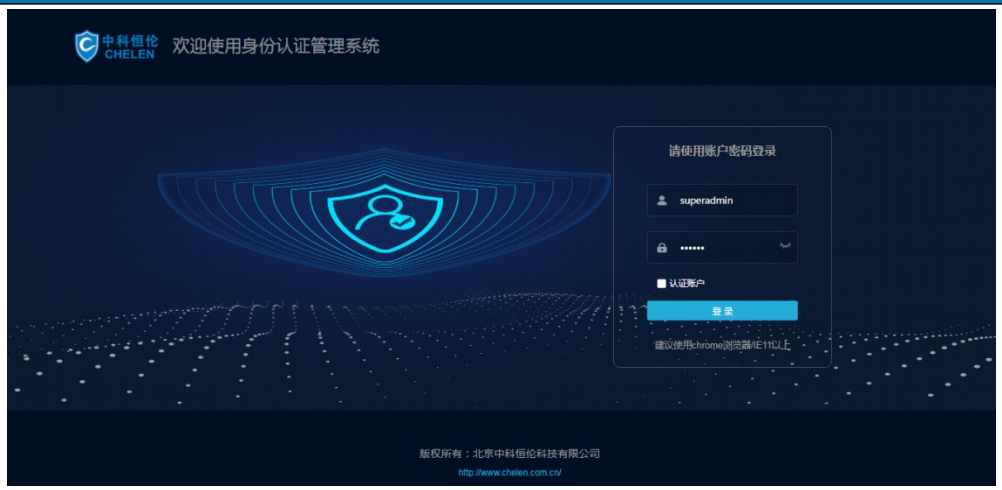
8	添加外部用户数据源（使用第三方的用户帐号做认证。譬如:AD 帐号，LDAP 帐号，数据库存储帐号）详细步骤见 3.2	
9	导入硬件令牌种子文件才能进行硬件令牌绑定，软件令牌系统自动生成。**详细步骤见 3.3**	
10	查看认证日志，可以查看“授权日志”“计费日志”“API 认证日志”“协议认证日志”“终端认证日志”“系统操作日志”	
12	添加授权 【系统设备管理】【系统授权管理】追加授权，详细步骤见“CKEY 动态认证系统授权册.docx”	

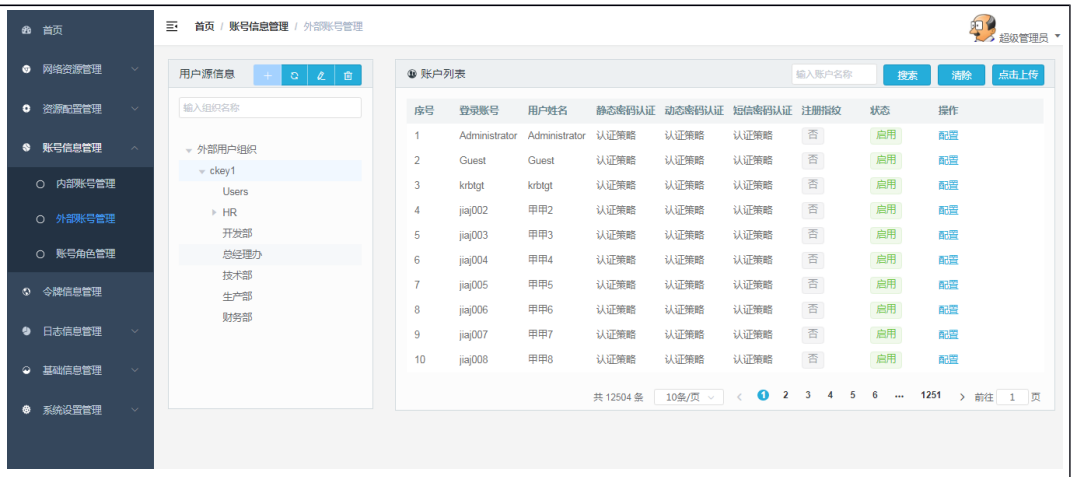
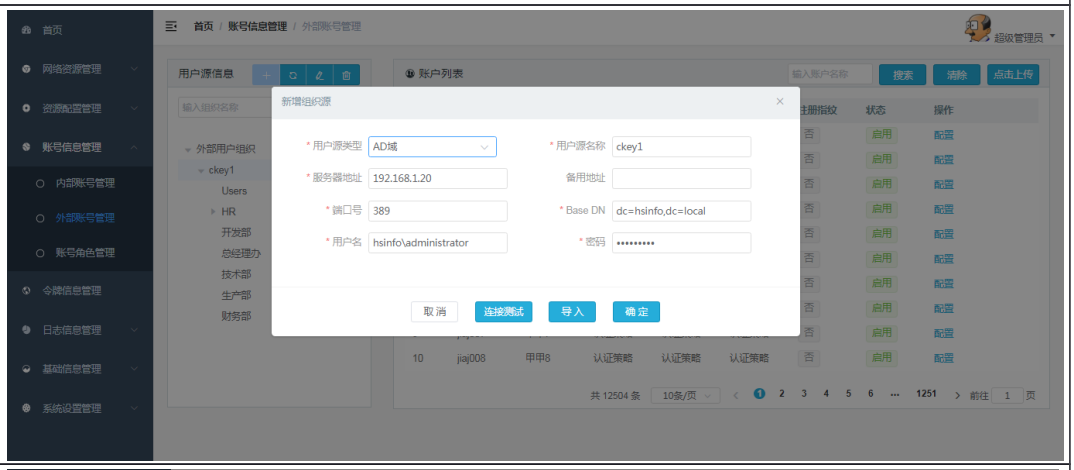
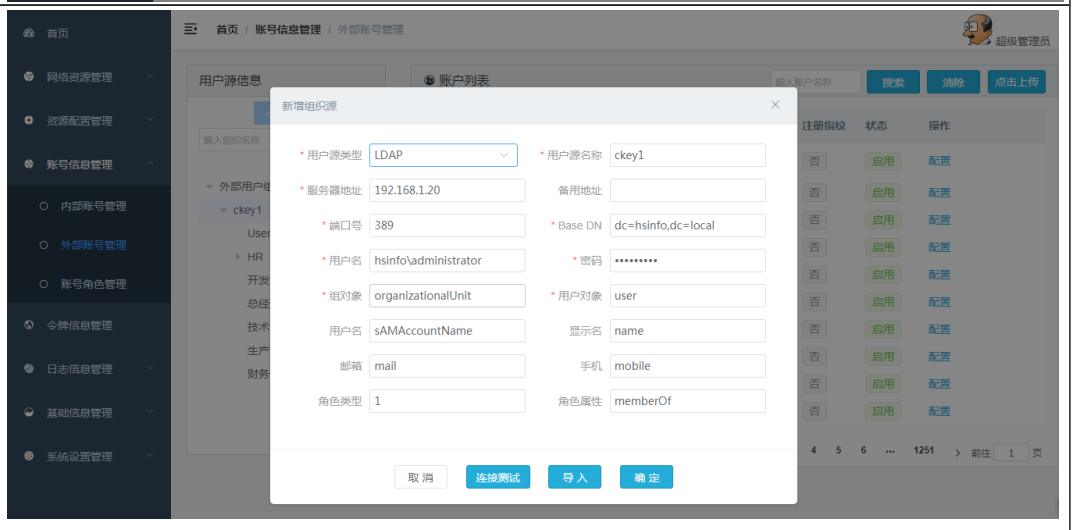
16	令牌管理配置【令牌设置】【消息令牌】如配置 http 类型的短信通道。详细步骤见 3.5.1	
17	邮箱配置 【系统设置管理】【系统邮件配置】配置相应的参数即可。详细步骤见 3.5.3	
18	系统热备 【系统设备管理】【系统热备管理】配置相应备机的 URL 注：热备时要先停备机服务 详细步骤见 3.5.6	

19	【系统设置】【密码规则设置】这个设置对认证用户和系统管理帐号都启作用	

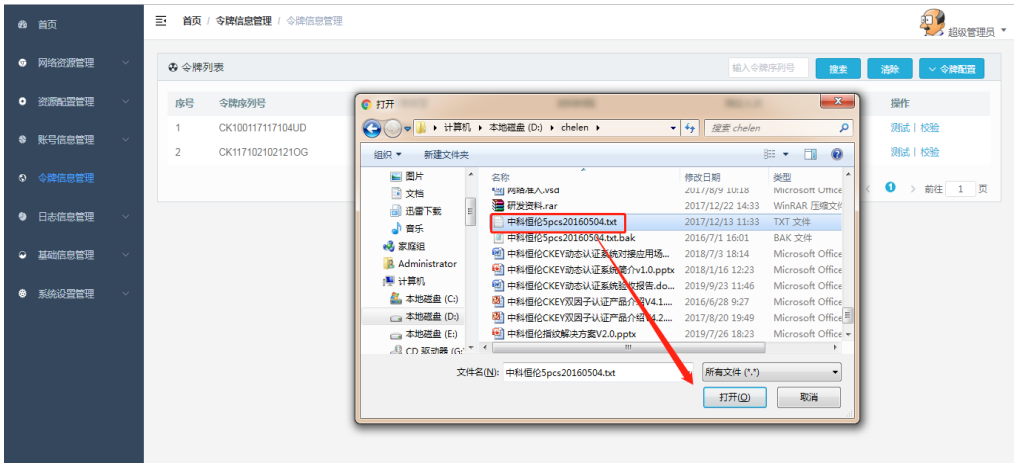
3.2 外部数据源配置和同步

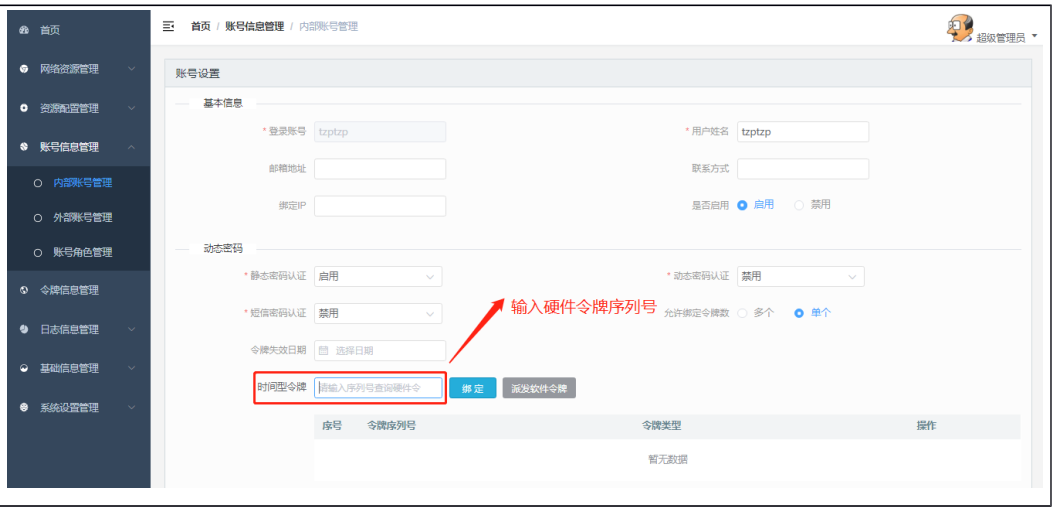
注意：认证帐号如果是采用第三方数据源，如 AD,LDAP，数据库等才需要配置外部数据源。

配置步骤		
	描述	截图
1	登录 CKEY 认证平台，输入管理员和密码	

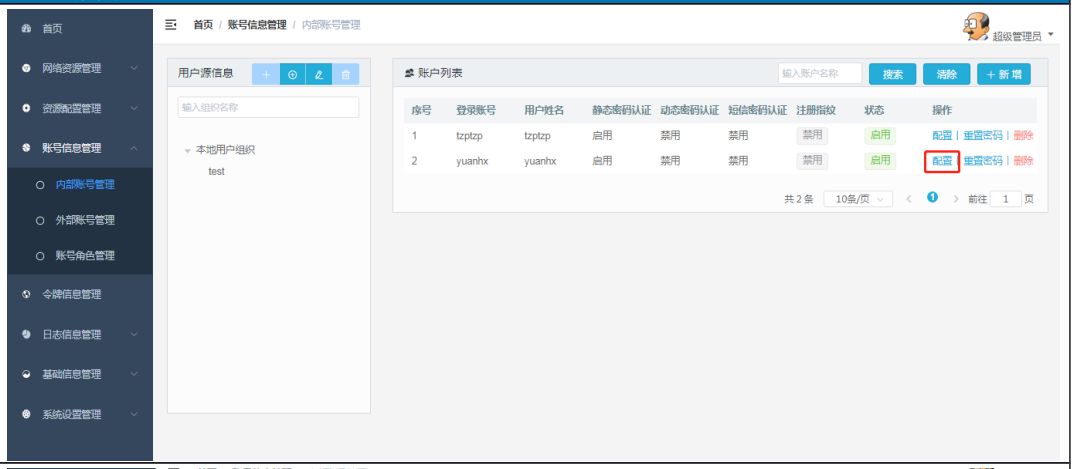
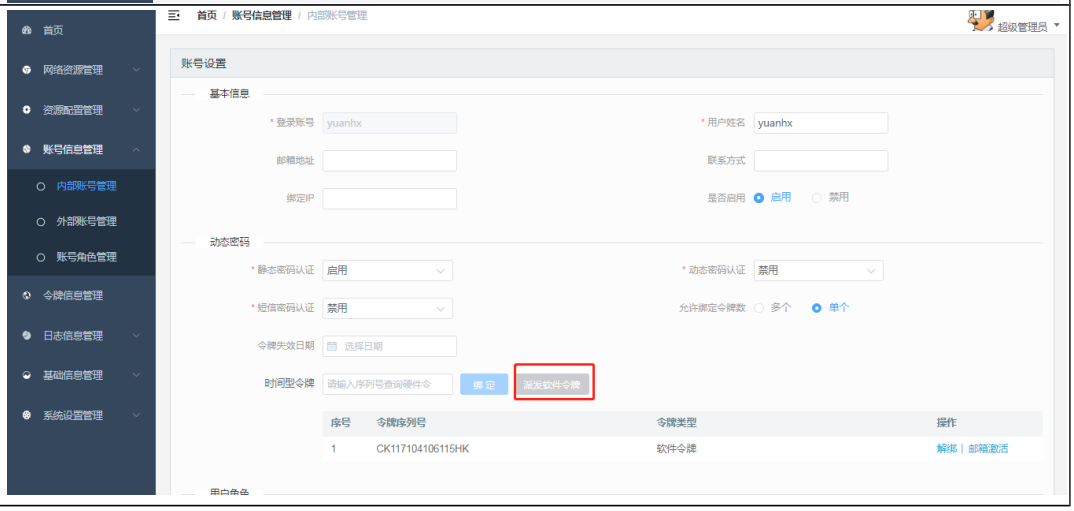
1	配置外部用户数据源（使用第三方的用户帐号做认证。譬如:AD 帐号，LDAP 帐号，数据库存储帐号）	
2	配置 AD 域服务器信息：AD 域服务器地址，组织架构信息，域帐号，密码。按照截图格式填写	
4	配置 LDAP 服务器信息	

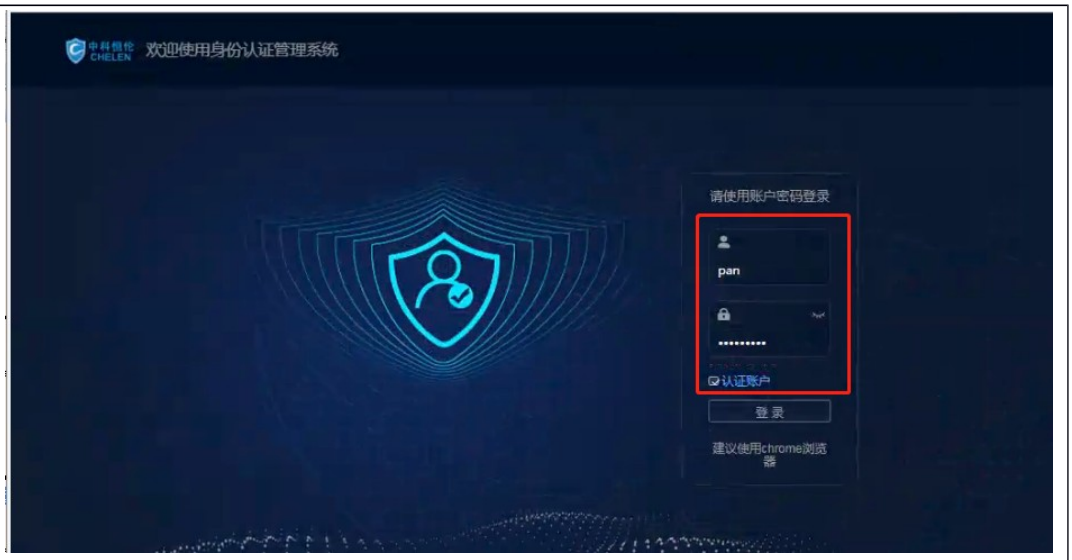
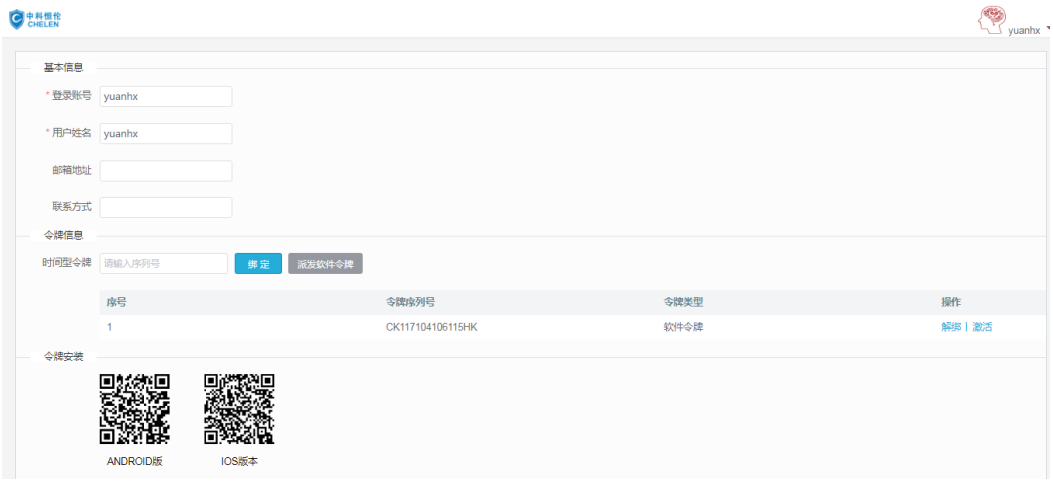
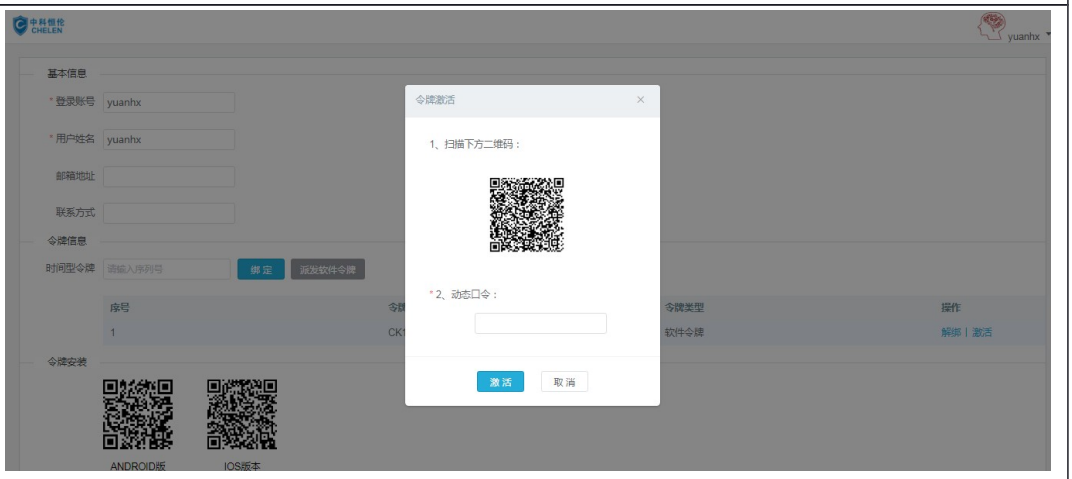
3.3 硬件令牌导入和绑定以及解绑

配置步骤		
	描述	截图
1	【令牌信息管理】，【令牌设置】【上传令牌】注意上传文件为 excel 文件	  

3	选中需要绑定的用户，进行硬件令牌绑定	

3.4 手机令牌派发和激活

配置步骤		
	描述	截图
1	选择要绑定手机令牌的用户点击编辑	
4	选择【派发软件令牌】点击保存并返回	

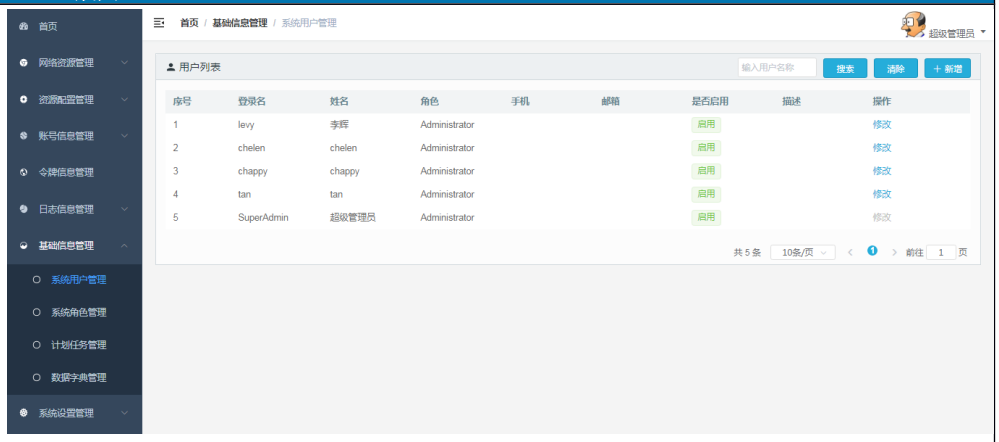
3	手机令牌激活码可以通过登录自助和邮件方式获得 访问认证系统用户自助页面：认证用户勾选上，输入认证用户名和密码	
4	第一次进入需要修改默认密码后，重新登录，进入令牌激活页面	
5	使用手机二维码工具扫描【令牌安装】，根据手机系统扫描对应的二维码安装“ckey 令牌”APP，使用 APP 扫码激活扫描【激活】中的二维码	

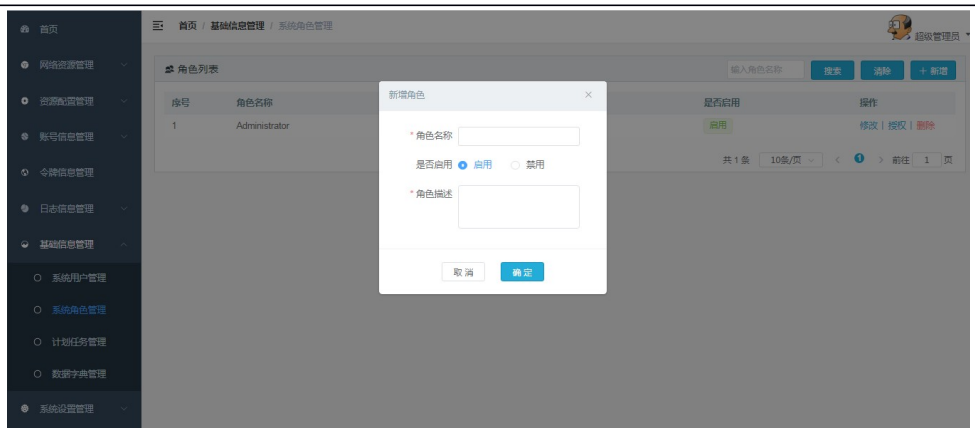
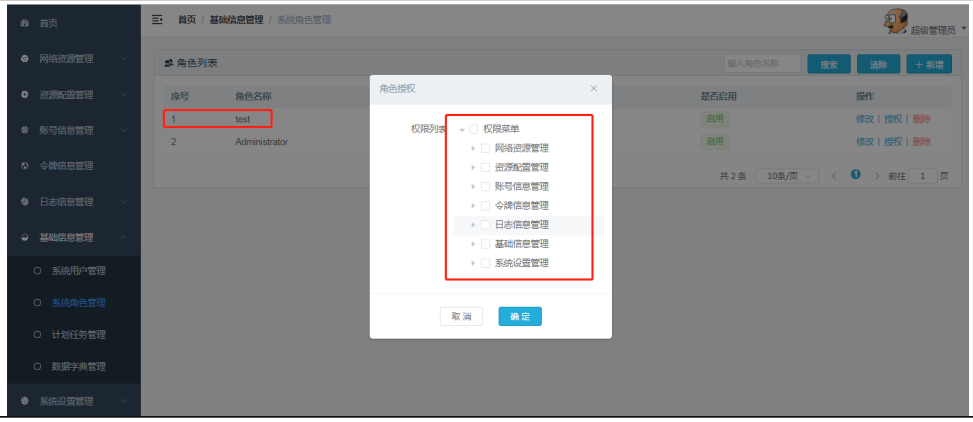
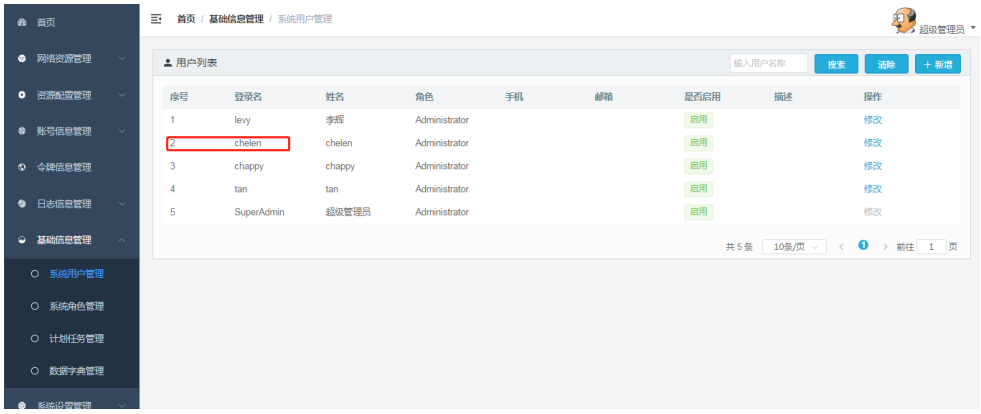
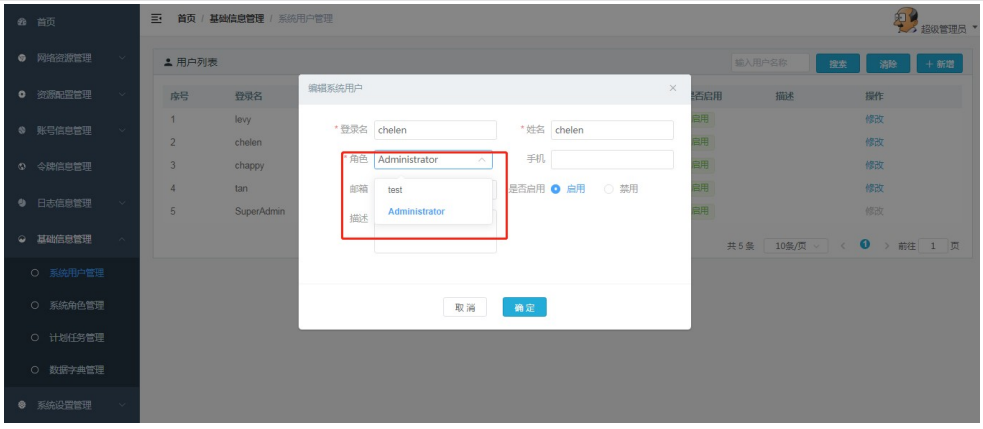
6	手机扫描激活后，显示动态密码，再将显示动态密码输入到自助页面的“输入生成的动态口令”，点“激活”即完成手机令牌激活	

3.5 认证系统设置

3.5.1 基础信息管理

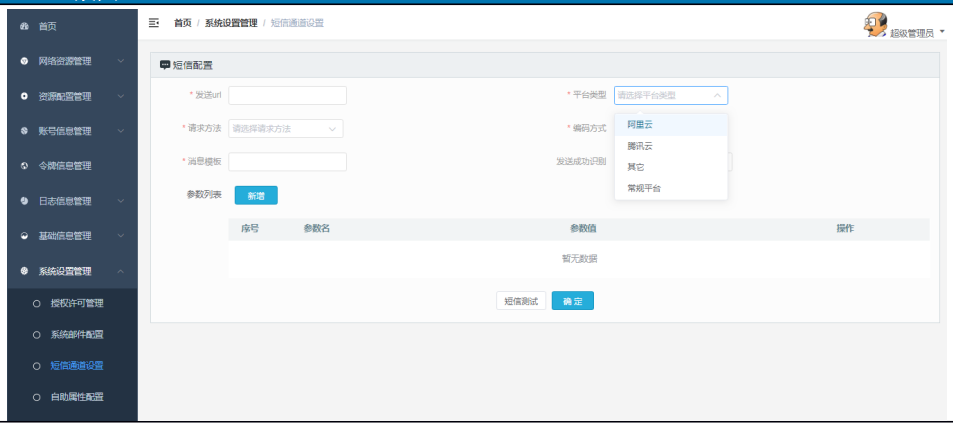
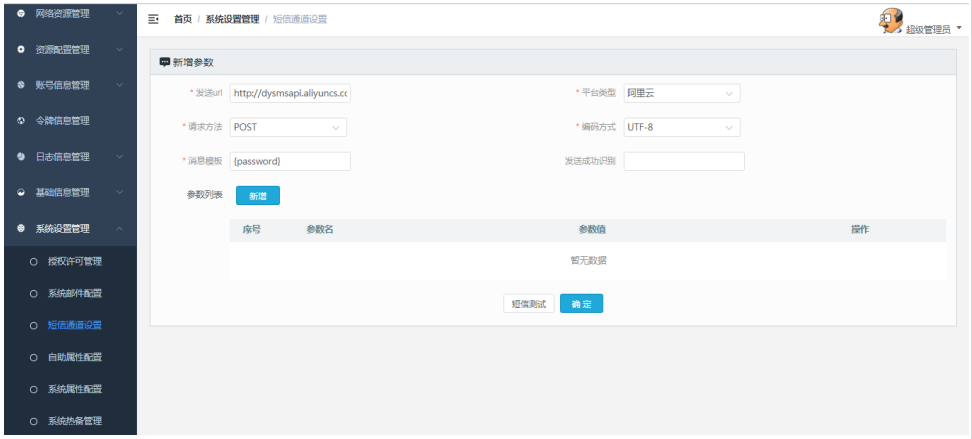
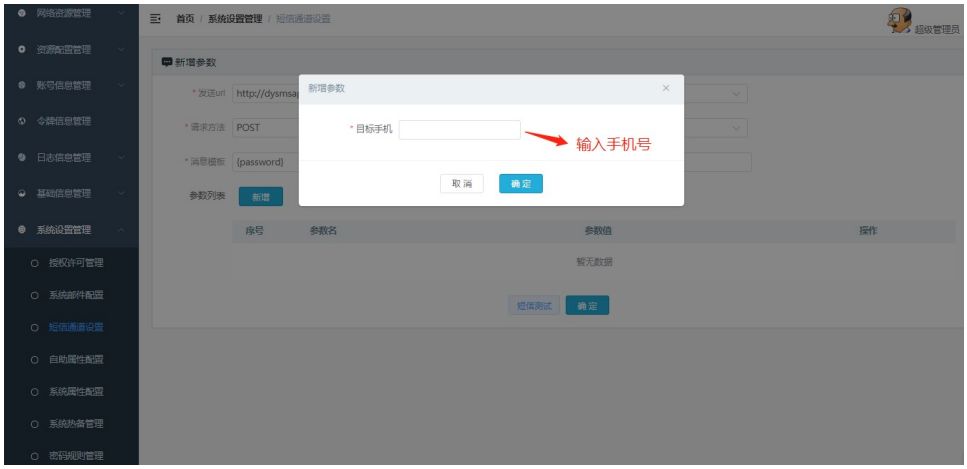
基信息管理用途：可以对认证系统管理用户进行功能权限划分，进行分级管理。

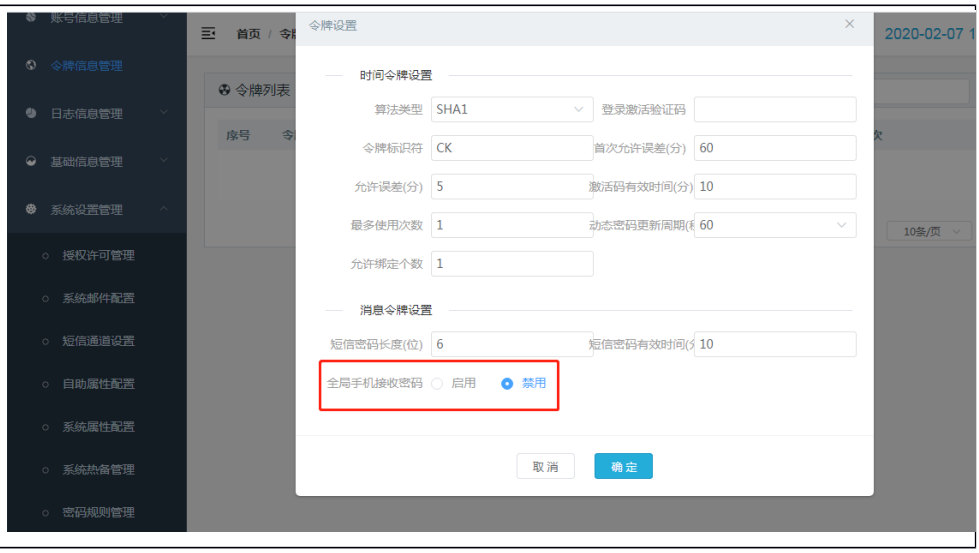
配置步骤		
	描述	截图
1	【基础信息管理】--》【系统用户管理】	

2.	新增一个系统角色，选择对应角色类别。点【确定】	
3	给创建的角色赋权限，选中角色中"授权"，勾选对应的菜单权限	
4	新增系统管理帐号，默认密码为：123456，首次登录会提示修改密码	
5.	将新建系统管理帐号选定对应角色即可使用新管理员进行登录系统	

3.5.2 短信通道配置

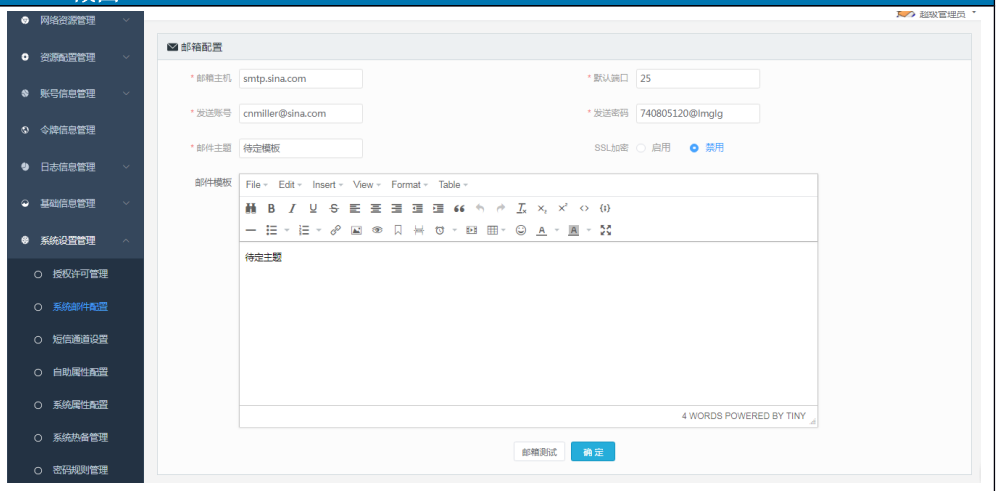
短信配置的用途：可以通过短信的方式将动态口令发到用户的移动设备上步骤如下：

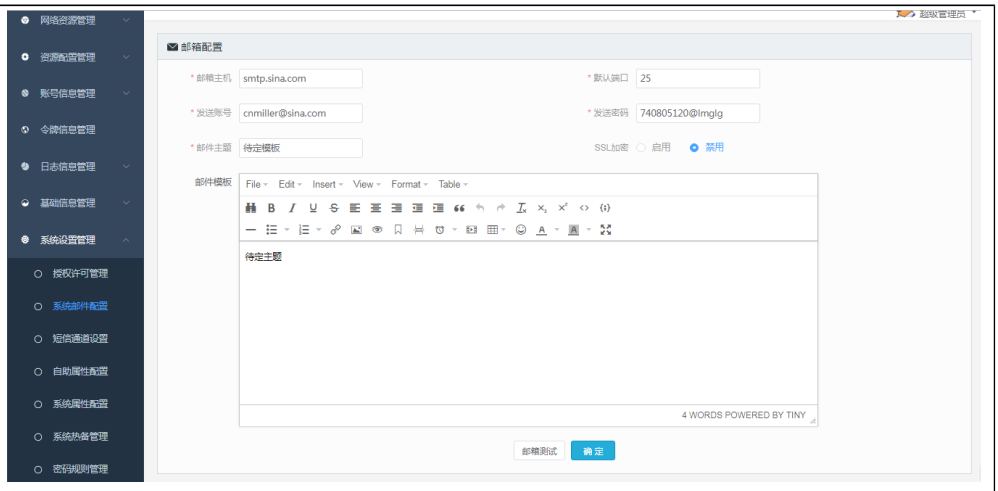
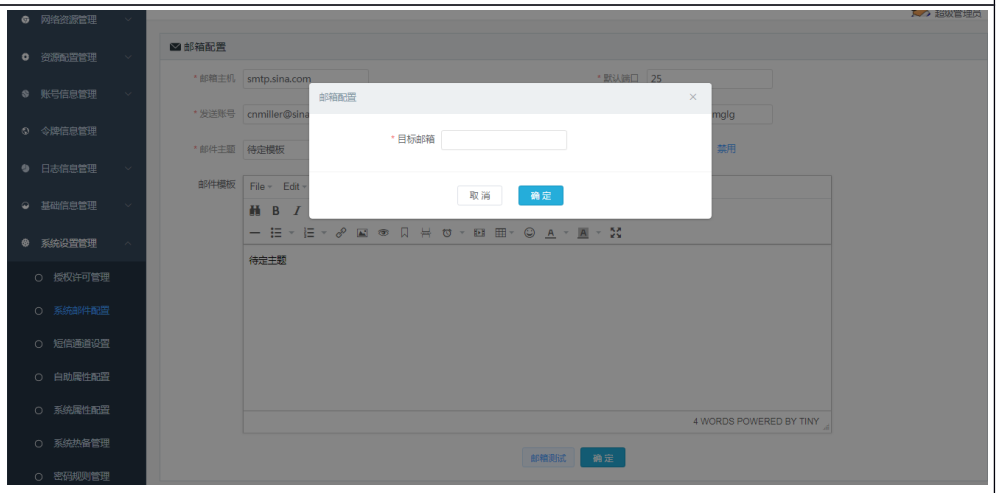
配置步骤		
	描述	截图
1	【系统设置管理】--》【短信通道设置】	
2.	配置短信接口，选定通道类型，短信接口的发送 URL，以及参数请求方法和编码方式，以及发送成功返回值	
3	配置对应参数后，即可进行短信令牌的测试，看是否能够正常收到短信动态口令和验证口令	

4	编辑登录帐号信息维护帐号的对应的手机号码。然后令牌信息管理-令牌设置-消息令牌设置“开启全局接受短信密码”，帐号即可使用短信动态密码	

3.5.3 系统邮件配置

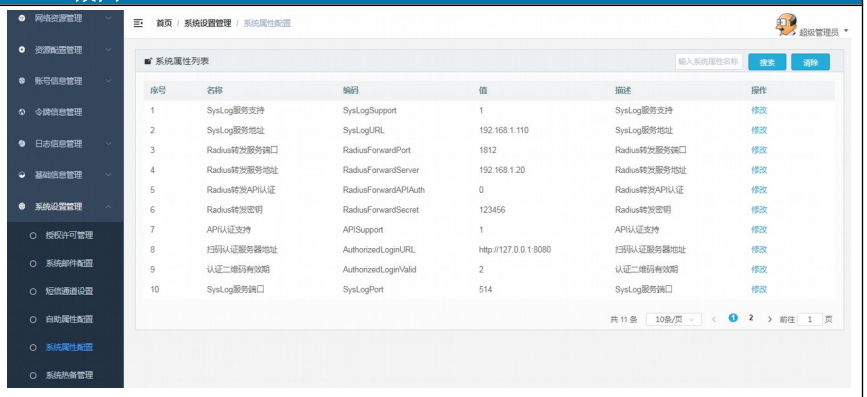
邮件帐号配置的用途：可以通过邮件的方式将手机令牌的激活码和 APP 下载地址发到用户的邮箱中步骤如下：

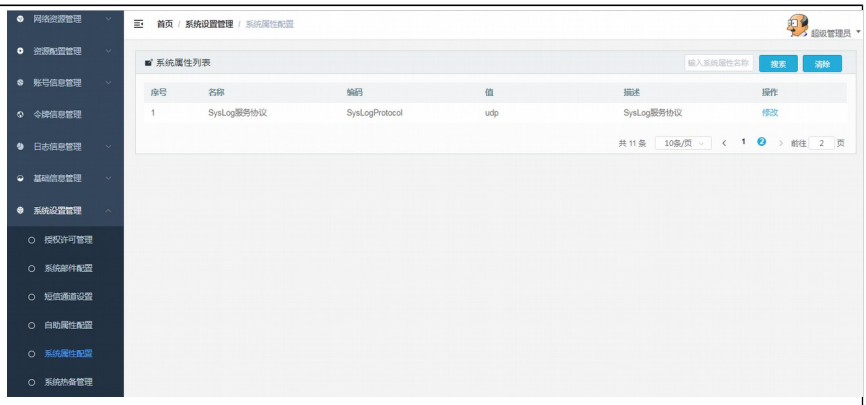
配置步骤		
	描述	截图
1	【系统设置管理】--》【系统邮件设置】	

2.	配置邮箱主机（邮件发送服务器），SSL 是否加密，默认端口，发送邮件帐号，发送的密码，邮件主题，邮件内容模版。	
3	配置对应参数后，即可进行邮件的测试，看是否能够正常收到手机令牌激活码和下载地址	

3.5.4 系统自定义

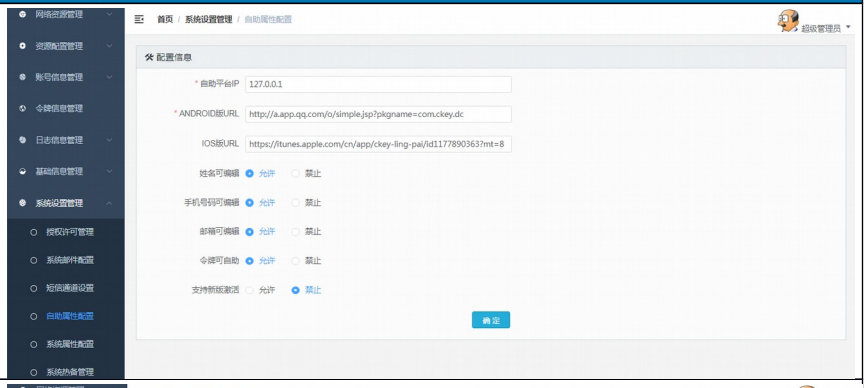
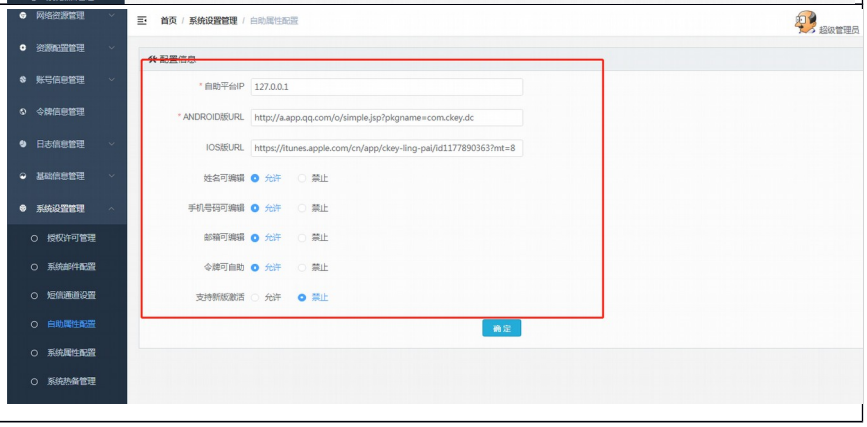
系统自定义的用途：主要是可以提供系统管理参数配置

配置步骤		
	描述	截图
1	【系统设置管理】--》【系统自定义】	

2	可以配置日志上传服务器，radius 设备转发，令牌二维码有效期等系统属性设置	

3.5.5 自助配置管理

自助配置管理用途：定义用户自助页面中用户参数修改权限和手机令牌 APP 下载地址。

配置步骤		
	描述	截图
1	【系统设置管理】--》【自助服务配置管理】	
2	可以配置自助页面 IP：自助页面实现单独部署，也可和认证管理管理在同一台服务器上。	

4 常见问题解决和方法

4.1 用户丢失手机令牌解决

问题定位：用户无法获得动态密码进行认证
解决办法：临时绑定硬件令牌，将动态口令告知用户。操作步骤见 3.2。

4.2 所有移动设备没有收到短信口令

问题定位：检查系统配置的短信通道是否正常发送短信口令
解决办法：【系统设置管理】【短信通道设置】【短信令牌测试】

4.3 用户使用手机令牌口令无法正常登入

问题定位：检查用户手机令牌与用户是否已绑定，令牌是否正常。
解决办法：校验用户手机令牌的动态密码是否正确。【令牌信息管理】【令牌信息管理】【测试】

4.4 在外部数据源中无法找查找到用户的用户名

问题定位：用户是否新建，尚未到自动同步时间。
解决办法：手动同步用户对应的数据源。【用户信息管理】【外部用户管理】选中外部数据员名称，点【操作】【同步】

4.5 出现所有用户都无法认证

问题定位：系统服务器的时间与标准时间偏差值超过的默认设定阀值。
解决办法：手动更新系统服务器的时间或者指定 NTP 时钟服务器即可