



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.....	3
1.1 编写目的.....	3
1.2 范围.....	3
2 系统组成.....	3
3 管理配置.....	3
3.1 配置步骤.....	3
3.2 外部数据源配置和同步.....	7
3.3 硬件令牌导入和绑定以及解绑.....	9
3.4 手机令牌派发和激活.....	10
3.5 认证系统设置.....	12
3.5.1 基础信息管理.....	12
3.5.2 短信通道配置.....	14
3.5.3 系统邮件配置.....	15
3.5.4 系统自定义.....	16
3.5.5 自助配置管理.....	17
4 常见问题解决和方法.....	18
4.1 用户丢失手机令牌解决.....	18
4.2 所有移动设备没有收到短信口令.....	18
4.3 用户使用手机令牌口令无法正常登入.....	18
4.4 在外部数据源中无法找查找到用户的用户名.....	18
4.5 出现所有用户都无法认证.....	18



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

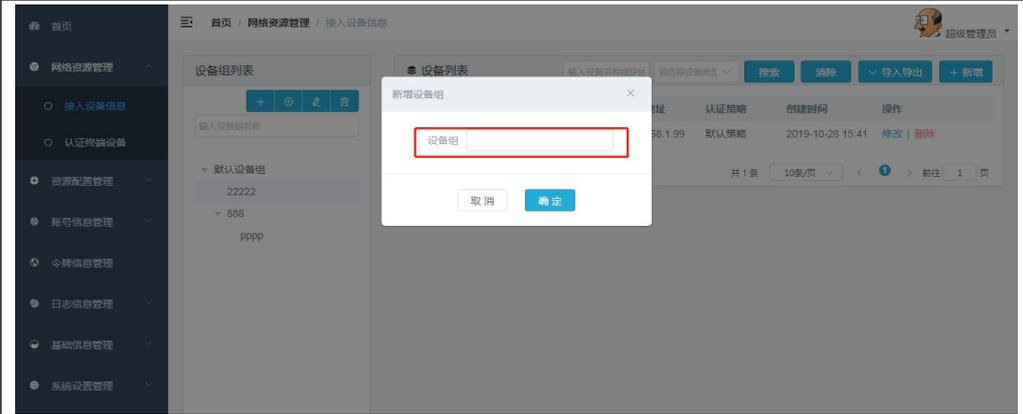
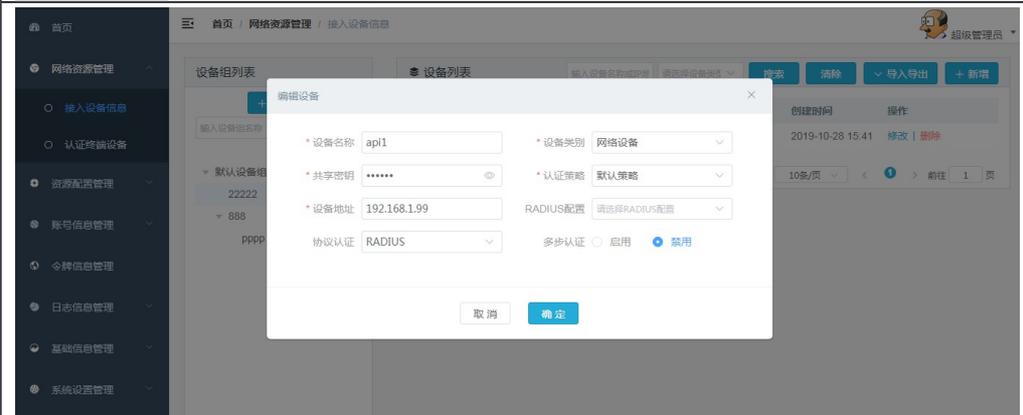
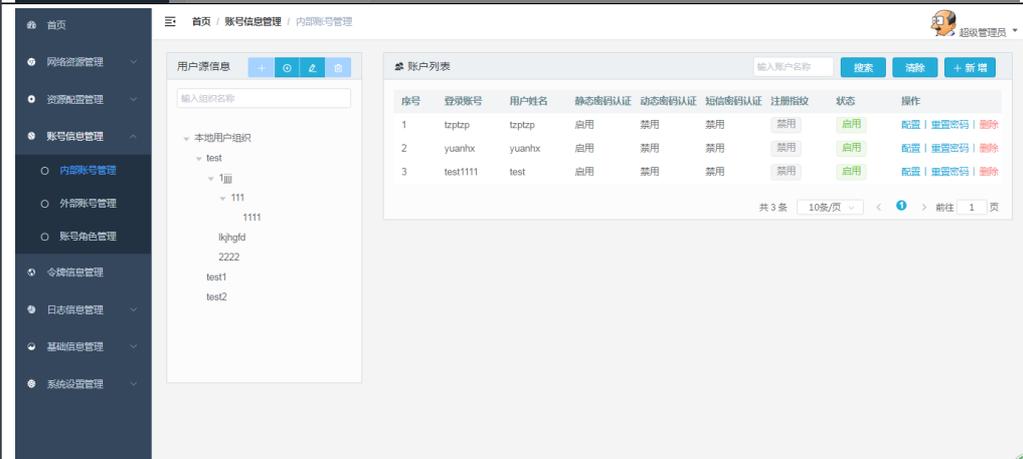
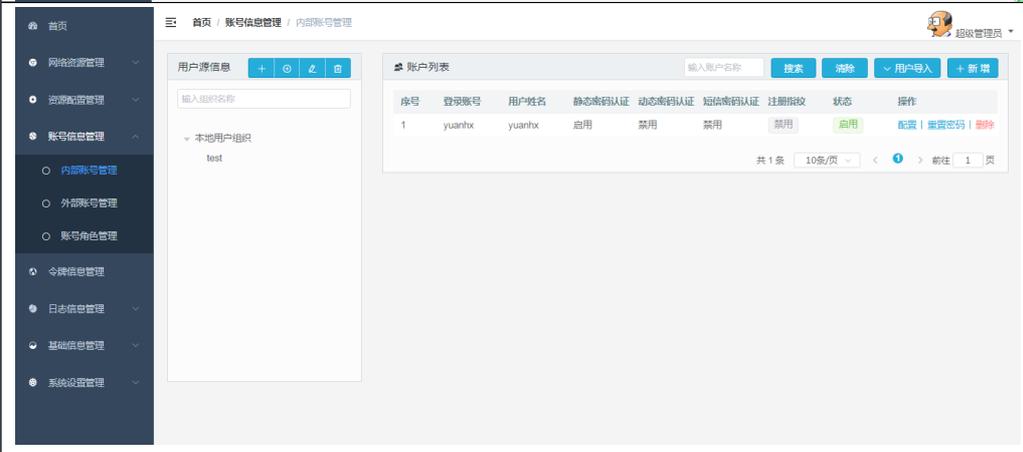
配置流程：

- 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）

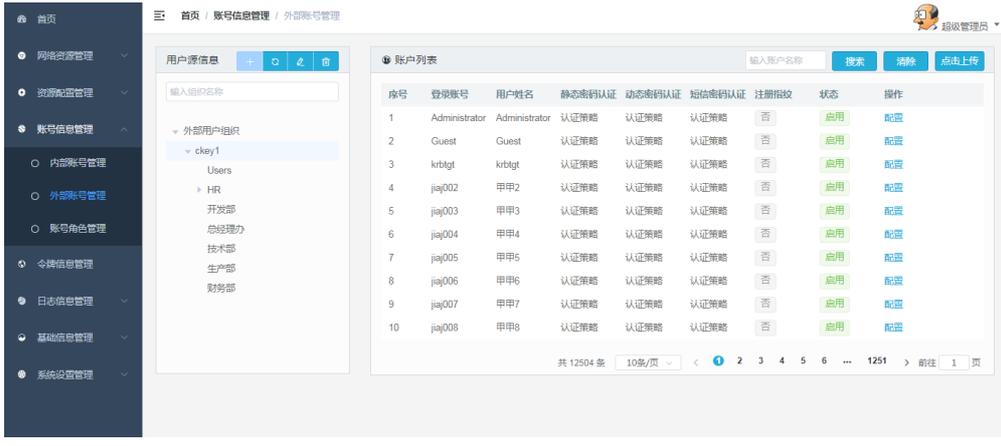
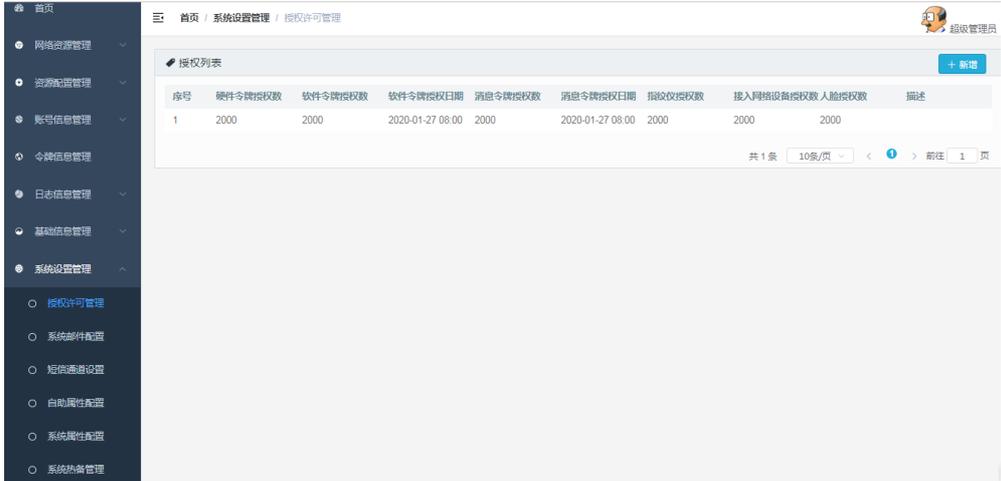
3.1 配置步骤

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	

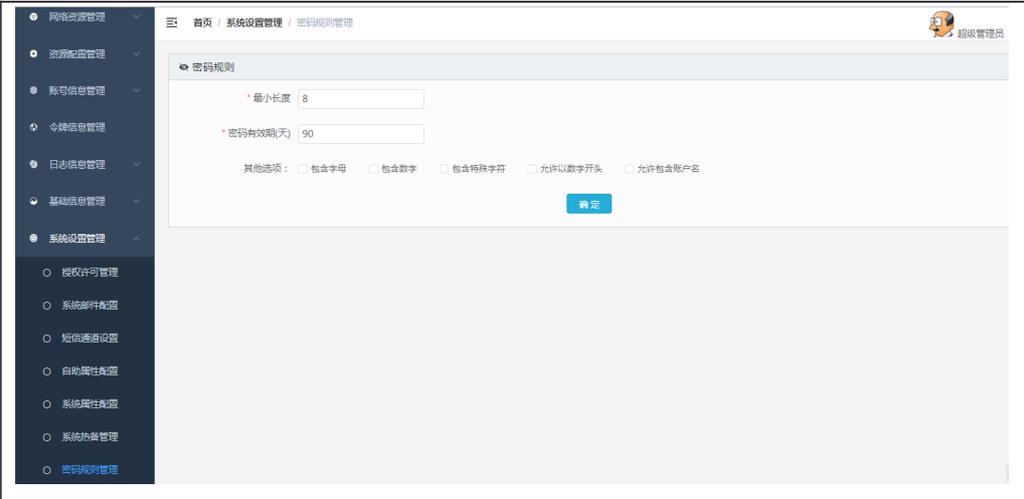


8	<p>添加外部用户数据源（使用第三方的用户帐号做认证。譬如:AD帐号，LDAP帐号，数据库存储帐号）详细步骤见 3.2</p>	 <p>用户源列表</p> <table border="1"> <thead> <tr> <th>序号</th> <th>登录账号</th> <th>用户名</th> <th>静态密码认证</th> <th>动态密码认证</th> <th>短信密码认证</th> <th>注册指纹</th> <th>状态</th> <th>操作</th> </tr> </thead> <tbody> <tr><td>1</td><td>Administrator</td><td>Administrator</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>2</td><td>Guest</td><td>Guest</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>3</td><td>krbtgt</td><td>krbtgt</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>4</td><td>jjaj002</td><td>甲甲2</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>5</td><td>jjaj003</td><td>甲甲3</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>6</td><td>jjaj004</td><td>甲甲4</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>7</td><td>jjaj005</td><td>甲甲5</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>8</td><td>jjaj006</td><td>甲甲6</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>9</td><td>jjaj007</td><td>甲甲7</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> <tr><td>10</td><td>jjaj008</td><td>甲甲8</td><td>认证策略</td><td>认证策略</td><td>认证策略</td><td>否</td><td>启用</td><td>配置</td></tr> </tbody> </table>	序号	登录账号	用户名	静态密码认证	动态密码认证	短信密码认证	注册指纹	状态	操作	1	Administrator	Administrator	认证策略	认证策略	认证策略	否	启用	配置	2	Guest	Guest	认证策略	认证策略	认证策略	否	启用	配置	3	krbtgt	krbtgt	认证策略	认证策略	认证策略	否	启用	配置	4	jjaj002	甲甲2	认证策略	认证策略	认证策略	否	启用	配置	5	jjaj003	甲甲3	认证策略	认证策略	认证策略	否	启用	配置	6	jjaj004	甲甲4	认证策略	认证策略	认证策略	否	启用	配置	7	jjaj005	甲甲5	认证策略	认证策略	认证策略	否	启用	配置	8	jjaj006	甲甲6	认证策略	认证策略	认证策略	否	启用	配置	9	jjaj007	甲甲7	认证策略	认证策略	认证策略	否	启用	配置	10	jjaj008	甲甲8	认证策略	认证策略	认证策略	否	启用	配置
序号	登录账号	用户名	静态密码认证	动态密码认证	短信密码认证	注册指纹	状态	操作																																																																																													
1	Administrator	Administrator	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
2	Guest	Guest	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
3	krbtgt	krbtgt	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
4	jjaj002	甲甲2	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
5	jjaj003	甲甲3	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
6	jjaj004	甲甲4	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
7	jjaj005	甲甲5	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
8	jjaj006	甲甲6	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
9	jjaj007	甲甲7	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
10	jjaj008	甲甲8	认证策略	认证策略	认证策略	否	启用	配置																																																																																													
9	<p>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</p>	 <p>令牌列表</p> <table border="1"> <thead> <tr> <th>序号</th> <th>令牌序列号</th> <th>令牌类型</th> <th>时间间隔</th> <th>绑定次数</th> <th>操作</th> </tr> </thead> <tbody> <tr><td>1</td><td>CK100117117104UD</td><td>软件令牌</td><td>60</td><td>0</td><td>测试 绑定 令牌设置</td></tr> <tr><td>2</td><td>CK11710210211206</td><td>软件令牌</td><td>60</td><td>0</td><td>测试 绑定 令牌设置</td></tr> </tbody> </table>	序号	令牌序列号	令牌类型	时间间隔	绑定次数	操作	1	CK100117117104UD	软件令牌	60	0	测试 绑定 令牌设置	2	CK11710210211206	软件令牌	60	0	测试 绑定 令牌设置																																																																																	
序号	令牌序列号	令牌类型	时间间隔	绑定次数	操作																																																																																																
1	CK100117117104UD	软件令牌	60	0	测试 绑定 令牌设置																																																																																																
2	CK11710210211206	软件令牌	60	0	测试 绑定 令牌设置																																																																																																
10	<p>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”</p>	 <p>协议认证日志列表</p> <table border="1"> <thead> <tr> <th>序号</th> <th>账号</th> <th>设备名称</th> <th>令牌序列号</th> <th>接入IP</th> <th>认证详情</th> <th>认证状态</th> <th>记录时间</th> </tr> </thead> <tbody> <tr><td>1</td><td>test111</td><td>api1</td><td>认证成功</td><td>192.168.1.99</td><td></td><td>认证成功</td><td>2019-10-29 09:10</td></tr> <tr><td>2</td><td>test111</td><td>api1</td><td>认证成功</td><td>192.168.1.99</td><td></td><td>认证成功</td><td>2019-10-29 08:50</td></tr> <tr><td>3</td><td>test111</td><td>api1</td><td>认证成功</td><td>192.168.1.99</td><td></td><td>认证成功</td><td>2019-10-29 08:50</td></tr> <tr><td>4</td><td>test111</td><td>api1</td><td>认证成功</td><td>192.168.1.99</td><td></td><td>认证成功</td><td>2019-10-29 08:26</td></tr> <tr><td>5</td><td>test111</td><td>api1</td><td>认证成功</td><td>192.168.1.99</td><td></td><td>认证成功</td><td>2019-10-29 08:26</td></tr> <tr><td>6</td><td>test111</td><td>api1</td><td>认证成功</td><td>192.168.1.99</td><td></td><td>认证成功</td><td>2019-10-29 08:26</td></tr> <tr><td>7</td><td>test111</td><td>api1</td><td>认证成功</td><td>192.168.1.99</td><td></td><td>认证成功</td><td>2019-10-29 08:26</td></tr> </tbody> </table>	序号	账号	设备名称	令牌序列号	接入IP	认证详情	认证状态	记录时间	1	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 09:10	2	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:50	3	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:50	4	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26	5	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26	6	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26	7	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26																																			
序号	账号	设备名称	令牌序列号	接入IP	认证详情	认证状态	记录时间																																																																																														
1	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 09:10																																																																																														
2	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:50																																																																																														
3	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:50																																																																																														
4	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26																																																																																														
5	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26																																																																																														
6	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26																																																																																														
7	test111	api1	认证成功	192.168.1.99		认证成功	2019-10-29 08:26																																																																																														
12	<p>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”</p>	 <p>授权列表</p> <table border="1"> <thead> <tr> <th>序号</th> <th>硬件令牌授权数</th> <th>软件令牌授权数</th> <th>软件令牌授权日期</th> <th>消息令牌授权数</th> <th>消息令牌授权日期</th> <th>指纹授权数</th> <th>接入网络设备授权数</th> <th>人脸授权数</th> <th>描述</th> </tr> </thead> <tbody> <tr><td>1</td><td>2000</td><td>2000</td><td>2020-01-27 08:00</td><td>2000</td><td>2020-01-27 08:00</td><td>2000</td><td>2000</td><td>2000</td><td></td></tr> </tbody> </table>	序号	硬件令牌授权数	软件令牌授权数	软件令牌授权日期	消息令牌授权数	消息令牌授权日期	指纹授权数	接入网络设备授权数	人脸授权数	描述	1	2000	2000	2020-01-27 08:00	2000	2020-01-27 08:00	2000	2000	2000																																																																																
序号	硬件令牌授权数	软件令牌授权数	软件令牌授权日期	消息令牌授权数	消息令牌授权日期	指纹授权数	接入网络设备授权数	人脸授权数	描述																																																																																												
1	2000	2000	2020-01-27 08:00	2000	2020-01-27 08:00	2000	2000	2000																																																																																													



<p>16</p>	<p>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</p>	
<p>17</p>	<p>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</p>	
<p>18</p>	<p>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</p>	



19	<p>【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起作用</p>	
----	--	--

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	<p>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)</p>	
2	<p>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</p>	
4	<p>配置 LDAP 服务器信息</p>	

3.3 硬件令牌导入和绑定以及解绑



配置步骤																																																		
	描述	截图																																																
1	<p>【令牌信息管理】， 【令牌设置】 【上传令牌】 注意上传文件为 excel 文件</p>	<p>The screenshots illustrate the process of uploading a token file. The first screenshot shows the '令牌列表' (Token List) interface with a table containing two entries. A red arrow points to the '上传令牌' (Upload Token) button in the '操作' (Action) column. The second screenshot shows a file explorer window where the file '中标恒伦5pcs20160504.txt' is selected. The third screenshot shows the updated '令牌列表' table with three new entries highlighted in red, indicating the successful upload of the file.</p> <table border="1"> <thead> <tr> <th>序号</th> <th>令牌序列号</th> <th>令牌类型</th> <th>时间间隔</th> <th>绑定人次</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>CK100117117104UD</td> <td>软件令牌</td> <td>60</td> <td>0</td> <td>测试 校验</td> </tr> <tr> <td>2</td> <td>CK1171021021210G</td> <td>软件令牌</td> <td>60</td> <td>0</td> <td>测试 校验</td> </tr> <tr> <td>3</td> <td>CK117104106115HK</td> <td>软件令牌</td> <td>60</td> <td>1</td> <td>测试 校验</td> </tr> <tr> <td>4</td> <td>CK99981041130J</td> <td>软件令牌</td> <td>60</td> <td>1</td> <td>测试 校验</td> </tr> <tr> <td>5</td> <td>DAS123456</td> <td>硬件令牌</td> <td>1</td> <td>0</td> <td>测试 校验</td> </tr> <tr> <td>6</td> <td>DAS123457</td> <td>硬件令牌</td> <td>1</td> <td>0</td> <td>测试 校验</td> </tr> <tr> <td>7</td> <td>DAS123458</td> <td>硬件令牌</td> <td>1</td> <td>0</td> <td>测试 校验</td> </tr> </tbody> </table>	序号	令牌序列号	令牌类型	时间间隔	绑定人次	操作	1	CK100117117104UD	软件令牌	60	0	测试 校验	2	CK1171021021210G	软件令牌	60	0	测试 校验	3	CK117104106115HK	软件令牌	60	1	测试 校验	4	CK99981041130J	软件令牌	60	1	测试 校验	5	DAS123456	硬件令牌	1	0	测试 校验	6	DAS123457	硬件令牌	1	0	测试 校验	7	DAS123458	硬件令牌	1	0	测试 校验
序号	令牌序列号	令牌类型	时间间隔	绑定人次	操作																																													
1	CK100117117104UD	软件令牌	60	0	测试 校验																																													
2	CK1171021021210G	软件令牌	60	0	测试 校验																																													
3	CK117104106115HK	软件令牌	60	1	测试 校验																																													
4	CK99981041130J	软件令牌	60	1	测试 校验																																													
5	DAS123456	硬件令牌	1	0	测试 校验																																													
6	DAS123457	硬件令牌	1	0	测试 校验																																													
7	DAS123458	硬件令牌	1	0	测试 校验																																													



3 选中需要绑定的用户，进行硬件令牌绑定

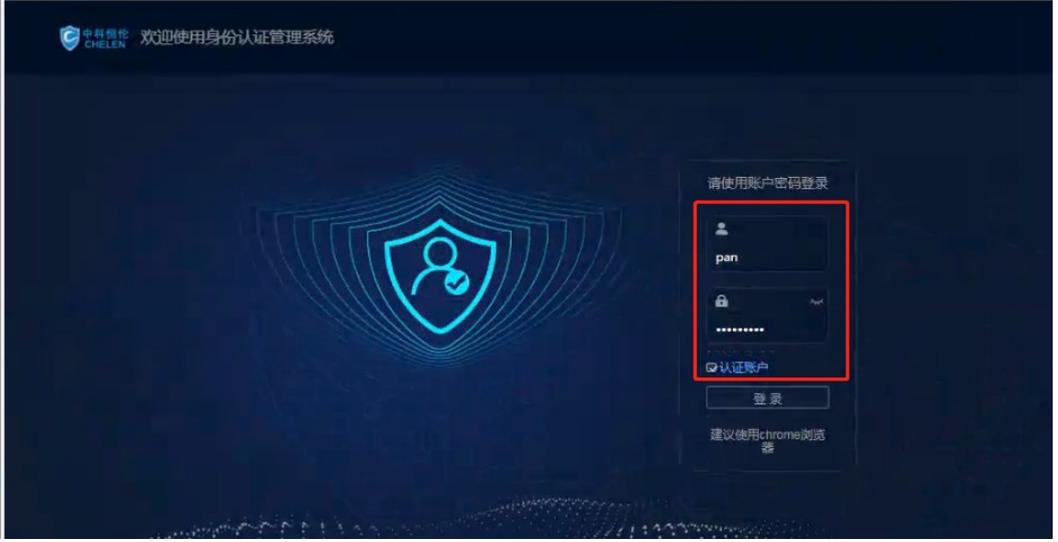
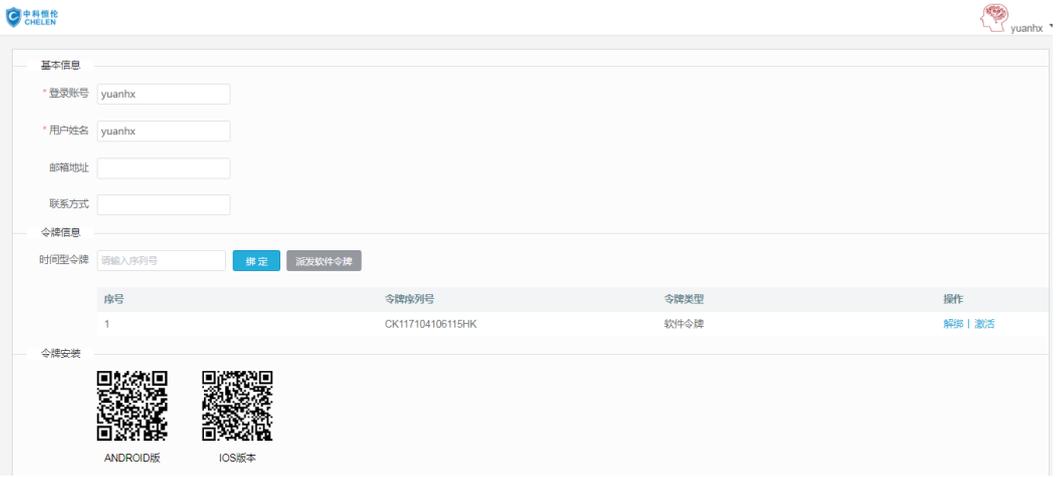
The screenshot shows the '账号设置' (Account Settings) page for user 'tzptzp'. Under the '动态密码' (Dynamic Password) section, the '时间型令牌' (Time-based token) is selected. A red box highlights the input field for the hardware token serial number, with a red arrow pointing to it and the text '输入硬件令牌序列号'. Below this, there is a table for token management.

序号	令牌序列号	令牌类型	操作
暂无数据			

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	<p>The screenshot shows the '用户列表' (User List) page. A table lists users with columns for '序号', '登录账号', '用户姓名', '静态密码认证', '动态密码认证', '短信验证码', '注册指纹', '状态', and '操作'. The '操作' column for user 'yuanhx' has a red box around the '配置' (Configure) button.</p>
4	选择【派发软件令牌】点击保存并返回	<p>The screenshot shows the '账号设置' (Account Settings) page for user 'yuanhx'. In the '动态密码' (Dynamic Password) section, the '时间型令牌' (Time-based token) is selected. A red box highlights the '派发软件令牌' (Dispatch Software Token) button.</p>



<p>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</p>	
<p>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</p>	
<p>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</p>	

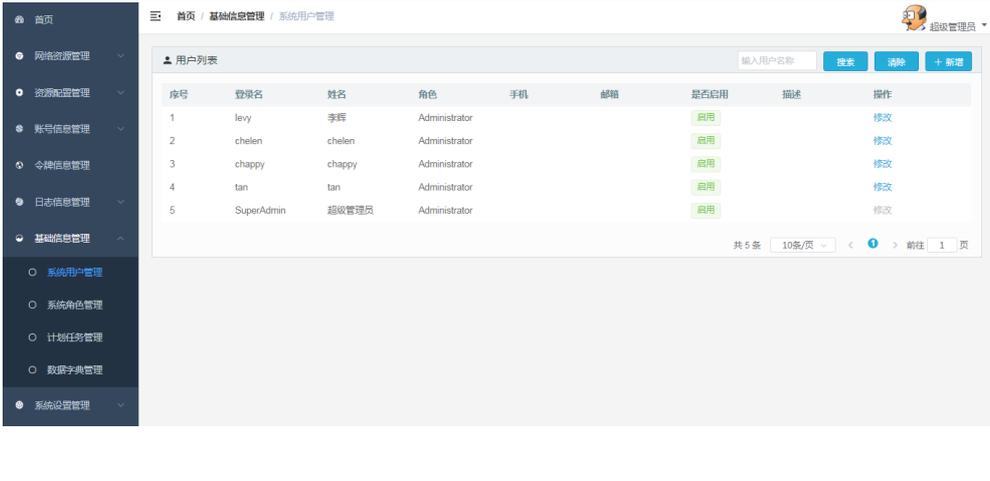


6	手机扫描激活后，显示动态密码，再将显示动态密码输入到自助页面的“输入生成的动态口令”，点“激活”即完成手机令牌激活	
---	---	---

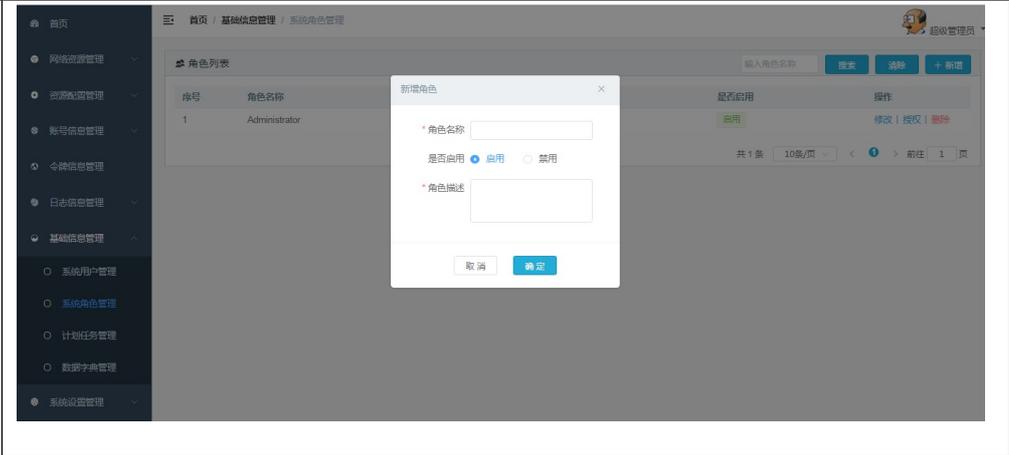
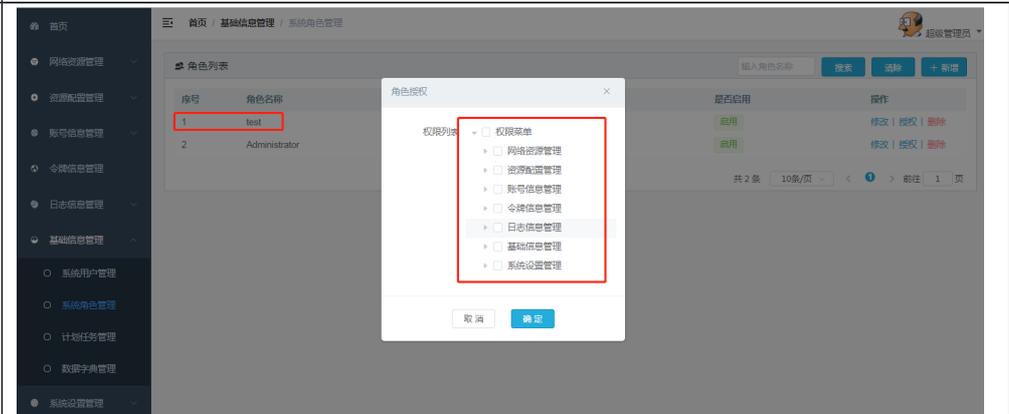
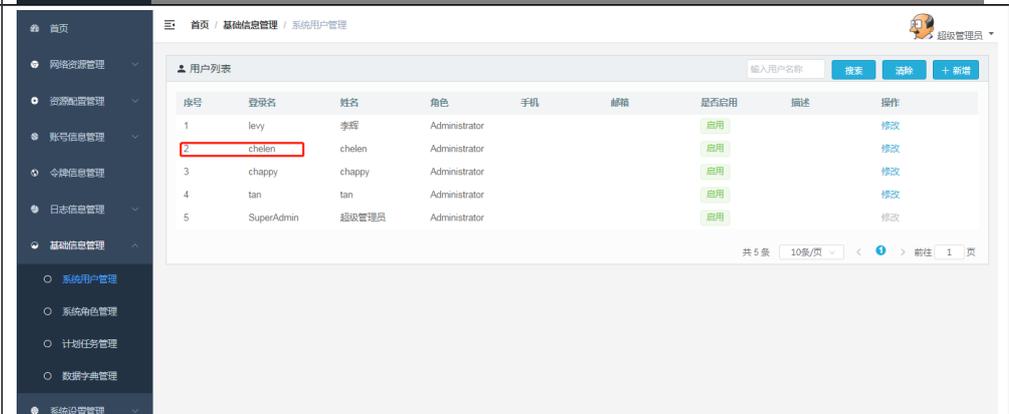
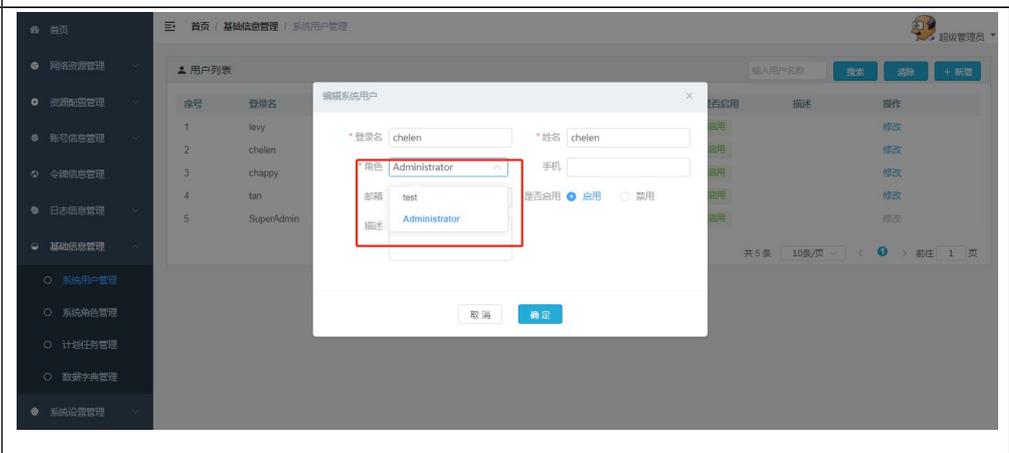
3.5 认证系统设置

3.5.1 基础信息管理

基础信息管理用途：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】	



<p>2. 新增一个系统角色，选择对应角色类别。点【确定】</p>	
<p>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</p>	
<p>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</p>	
<p>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</p>	



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	



<p>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</p>	
---	--

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	<p>【系统设置管理】-->【系统邮件设置】</p>	



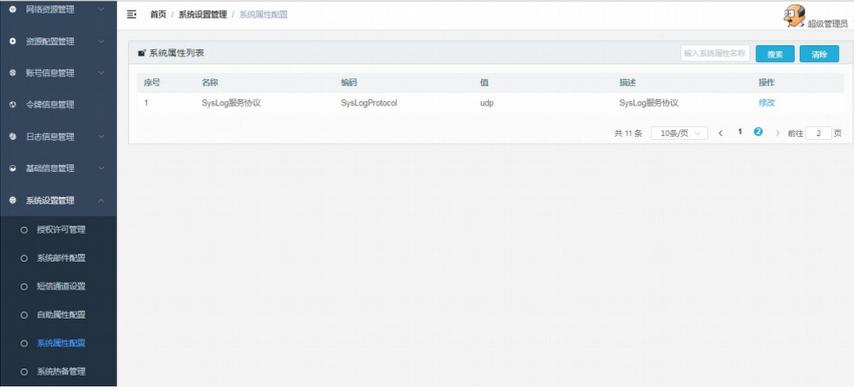
<p>2. 配置邮箱主机（邮件发送服务器），SSL 是否加密，默认端口，发送邮件帐号，发送的密码，邮件主题，邮件内容模版。</p>	
<p>3 配置对应参数后，即可进行邮件的测试，看是否能够正常收到手机令牌激活码和下载地址</p>	

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

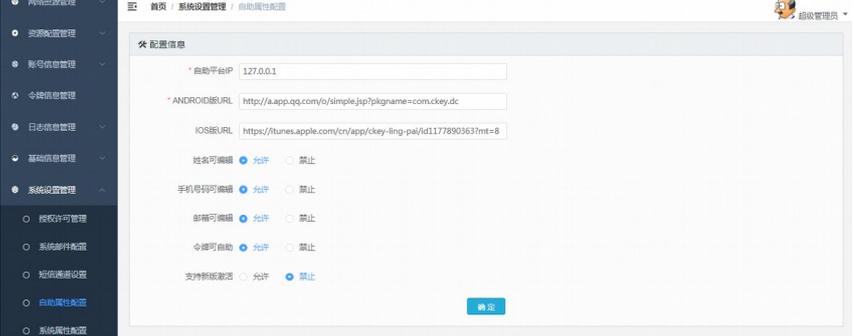
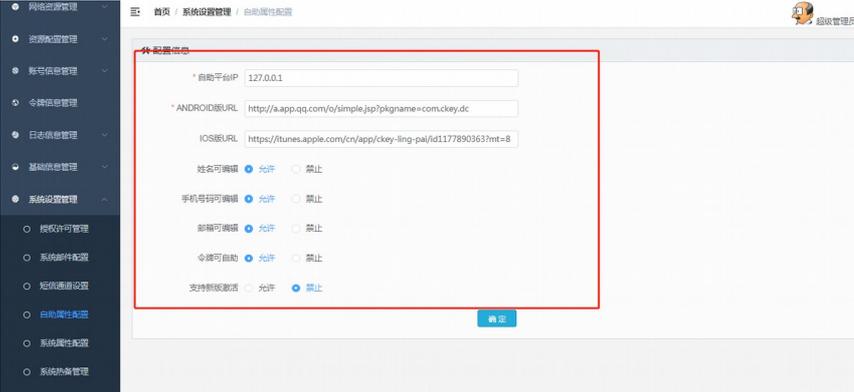
配置步骤																																																																				
	描述	截图																																																																		
1	【系统设置管理】--》 【系统自定义】	<table border="1"> <thead> <tr> <th>序号</th> <th>名称</th> <th>编码</th> <th>值</th> <th>描述</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>SysLog服务支持</td> <td>SysLogSupport</td> <td>1</td> <td>SysLog服务支持</td> <td>修改</td> </tr> <tr> <td>2</td> <td>SysLog服务地址</td> <td>SysLogURL</td> <td>192.168.1.110</td> <td>SysLog服务地址</td> <td>修改</td> </tr> <tr> <td>3</td> <td>Radius转发服务端口</td> <td>RadiusForwardPort</td> <td>1812</td> <td>Radius转发服务端口</td> <td>修改</td> </tr> <tr> <td>4</td> <td>Radius转发服务地址</td> <td>RadiusForwardServer</td> <td>192.168.1.20</td> <td>Radius转发服务地址</td> <td>修改</td> </tr> <tr> <td>5</td> <td>Radius转发API认证</td> <td>RadiusForwardAPIAuth</td> <td>0</td> <td>Radius转发API认证</td> <td>修改</td> </tr> <tr> <td>6</td> <td>Radius转发密码</td> <td>RadiusForwardSecret</td> <td>123456</td> <td>Radius转发密码</td> <td>修改</td> </tr> <tr> <td>7</td> <td>API认证支持</td> <td>APISupport</td> <td>1</td> <td>API认证支持</td> <td>修改</td> </tr> <tr> <td>8</td> <td>扫码认证服务器地址</td> <td>AuthorizedLoginURL</td> <td>http://127.0.0.1:8080</td> <td>扫码认证服务器地址</td> <td>修改</td> </tr> <tr> <td>9</td> <td>认证二维码有效期</td> <td>AuthorizedLoginValid</td> <td>2</td> <td>认证二维码有效期</td> <td>修改</td> </tr> <tr> <td>10</td> <td>SysLog服务端口</td> <td>SysLogPort</td> <td>514</td> <td>SysLog服务端口</td> <td>修改</td> </tr> </tbody> </table>	序号	名称	编码	值	描述	操作	1	SysLog服务支持	SysLogSupport	1	SysLog服务支持	修改	2	SysLog服务地址	SysLogURL	192.168.1.110	SysLog服务地址	修改	3	Radius转发服务端口	RadiusForwardPort	1812	Radius转发服务端口	修改	4	Radius转发服务地址	RadiusForwardServer	192.168.1.20	Radius转发服务地址	修改	5	Radius转发API认证	RadiusForwardAPIAuth	0	Radius转发API认证	修改	6	Radius转发密码	RadiusForwardSecret	123456	Radius转发密码	修改	7	API认证支持	APISupport	1	API认证支持	修改	8	扫码认证服务器地址	AuthorizedLoginURL	http://127.0.0.1:8080	扫码认证服务器地址	修改	9	认证二维码有效期	AuthorizedLoginValid	2	认证二维码有效期	修改	10	SysLog服务端口	SysLogPort	514	SysLog服务端口	修改
序号	名称	编码	值	描述	操作																																																															
1	SysLog服务支持	SysLogSupport	1	SysLog服务支持	修改																																																															
2	SysLog服务地址	SysLogURL	192.168.1.110	SysLog服务地址	修改																																																															
3	Radius转发服务端口	RadiusForwardPort	1812	Radius转发服务端口	修改																																																															
4	Radius转发服务地址	RadiusForwardServer	192.168.1.20	Radius转发服务地址	修改																																																															
5	Radius转发API认证	RadiusForwardAPIAuth	0	Radius转发API认证	修改																																																															
6	Radius转发密码	RadiusForwardSecret	123456	Radius转发密码	修改																																																															
7	API认证支持	APISupport	1	API认证支持	修改																																																															
8	扫码认证服务器地址	AuthorizedLoginURL	http://127.0.0.1:8080	扫码认证服务器地址	修改																																																															
9	认证二维码有效期	AuthorizedLoginValid	2	认证二维码有效期	修改																																																															
10	SysLog服务端口	SysLogPort	514	SysLog服务端口	修改																																																															



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	 <p>The screenshot shows the 'System Attribute List' (系统属性列表) interface. It contains a table with columns: 序号 (Serial Number), 名称 (Name), 输入 (Input), 值 (Value), 描述 (Description), and 操作 (Action). One entry is visible: 1, SysLog服务协议, SysLogProtocol, udp, SysLog服务协议, 修改. The left sidebar shows '系统设置管理' (System Settings Management) as the active menu item.</p>
---	---	---

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】	 <p>The screenshot shows the '自助配置信息' (Self-Service Configuration Information) form. It includes fields for: 自助平台IP (Self-Service Platform IP), ANDROID版URL (Android Version URL), and IOS版URL (iOS Version URL). Below these are several toggle switches for permissions: 姓名可编辑 (Name Editable), 手机号码可编辑 (Mobile Number Editable), 邮箱可编辑 (Email Editable), 令牌可自助 (Token Self-Service), and 支持新版激活 (Support New Version Activation).</p>
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。	 <p>This screenshot is identical to the one above, but a red rectangular box highlights the '自助平台IP' (Self-Service Platform IP) field, which contains the value '127.0.0.1'.</p>



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阈值。

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