



# OTP Server 管理中心用户手册

V4.8

## 章节目录

<b>第 1 章 关于文档</b>	<b>1</b>
1.1 读者对象	1
1.2 反馈意见	1
1.3 基本环境说明	1
1.4 文档约定	1
<b>第 2 章 安装前的准备工作</b>	<b>2</b>
2.1 安装环境检查	2
2.2 授权文件准备	2
2.3 令牌文件准备	2
2.4 数据库管理系统	2
2.5 数据库对应的 ODBC	3
2.6 数据库准备	3
2.7 加密机设备准备	3
2.8 FIDO 认证准备	3
<b>第 3 章 安装</b>	<b>4</b>
<b>第 4 章 系统初始化及登录</b>	<b>5</b>
4.1 系统初始化	5
4.2 登录	9
4.3 找回密码/应急口令	9
4.4 修改密码	10
4.5 编辑个人信息	10
4.6 退出	10
<b>第 5 章 配置管理</b>	<b>11</b>
5.1 系统公共配置	11
5.1.1 数据库	11
5.1.2 数据备份	13
5.1.3 邮件服务器	14
5.1.3.1 添加邮件服务器	14
5.1.3.2 编辑邮件服务器	15
5.1.3.3 设置默认邮箱	15
5.1.3.4 删除邮件服务器	15
5.1.4 短信网关	16
5.1.4.1 添加短信网关	16
5.1.4.2 编辑短信网关	17
5.1.4.3 启用/禁用短信网关	17
5.1.4.4 删除短信网关	18
5.1.5 其它公共配置	18
5.2 认证配置	18
5.2.1 基本配置	18
5.2.2 返回 RADIUS 属性	20
5.2.2.1 添加 RADIUS 配置	20
5.2.2.2 编辑 RADIUS 配置	21
5.2.2.3 RADIUS 配置	21
5.2.2.4 删除 RADIUS 配置	22
5.2.3 无线路由安全保护	22
5.3 用户配置	22

5.3.1	用户-令牌绑定策略.....	22
5.3.2	用户默认属性配置.....	24
5.3.3	用户来源.....	24
5.3.3.1	添加用户来源.....	24
5.3.3.2	配置用户来源.....	28
5.3.3.3	手动更新 .....	28
5.3.3.4	删除用户来源.....	28
5.4	令牌配置 .....	28
5.4.1	软件令牌.....	28
5.4.2	手机令牌.....	28
5.4.3	短信令牌.....	30
5.4.4	应急口令.....	31
5.5	管理中心配置 .....	31
5.5.1	管理员策略.....	31
5.5.2	访问控制策略.....	32
5.5.3	认证服务器选择.....	33
5.5.4	页面配置.....	33
5.6	用户门户配置 .....	33
5.6.1	登录初始密码.....	33
5.6.2	基本策略.....	34
5.6.3	通知公告.....	35
5.6.3.1	添加通知公告.....	35
5.6.3.2	编辑通知公告.....	35
5.6.3.3	查看通知公告.....	35
5.6.3.4	删除通知公告.....	35
5.6.4	页面配置.....	35
5.7	监控预警配置 .....	36
5.7.1	预警配置.....	36
5.7.2	双机运行监控配置.....	36
5.8	密码策略配置 .....	37
5.8.1	管理员密码策略配置.....	37
5.8.2	用户密码策略配置.....	38
5.9	加密机配置 .....	38
5.9.1	加密机配置.....	38
<b>第 6 章</b>	<b>首页.....</b>	<b>40</b>
6.1	快速查询 .....	40
6.2	快速导航 .....	40
6.3	使用向导 .....	40
6.4	系统介绍 .....	41
6.5	授权信息 .....	41
6.5.1	授权信息查看和更新.....	41
6.6	个人中心 .....	41
6.7	用户统计图 .....	42
6.8	令牌统计图 .....	42
<b>第 7 章</b>	<b>组织机构.....</b>	<b>43</b>
7.1	查看企业信息 .....	43
7.1.1	编辑企业信息.....	43
7.1.2	添加子机构.....	43
7.1.3	查看子机构.....	43
7.1.4	编辑子机构.....	43
7.1.5	迁移子机构.....	43
7.1.6	删除组织机构 .....	44

7.1.7 查看企业或子机构下的用户和令牌 .....	44
<b>第 8 章 管理员 .....</b>	<b>45</b>
8.1 管理员 .....	45
8.1.1 添加管理员 .....	45
8.1.2 管理员列表 .....	46
8.1.2.1 查看管理员 .....	46
8.1.2.2 编辑管理员 .....	46
8.1.2.3 启用/禁用管理员 .....	46
8.1.2.4 解锁/锁定管理员 .....	46
8.1.2.5 绑定/解绑令牌 .....	46
8.1.2.6 修改静态密码 .....	47
8.1.2.7 变更创建人 .....	47
8.1.2.8 删除管理员 .....	47
8.2 管理员角色 .....	47
8.2.1 添加管理员角色 .....	47
8.2.2 管理员角色列表 .....	48
8.2.2.1 查看管理员角色 .....	48
8.2.2.2 编辑管理员角色 .....	48
8.2.2.3 变更创建人 .....	49
8.2.2.4 删除管理员角色 .....	49
<b>第 9 章 用户管理 .....</b>	<b>50</b>
9.1 添加用户 .....	50
9.2 导入用户 .....	51
9.3 用户列表 .....	51
9.3.1 查看用户 .....	51
9.3.2 编辑用户 .....	51
9.3.3 设置静态密码 .....	52
9.3.4 锁定/解锁用户 .....	52
9.3.5 启用/禁用用户 .....	52
9.3.6 设置返回 Radius 属性 .....	52
9.3.7 设置后端认证 .....	52
9.3.8 设置本地认证模式 .....	53
9.3.9 变更机构 .....	53
9.3.10 绑定令牌 .....	54
9.3.11 解绑令牌 .....	55
9.3.12 更换令牌 .....	56
9.3.13 令牌同步 .....	57
9.3.14 解绑 .....	57
9.3.15 删除 .....	57
9.3.16 绑定用户组 .....	58
9.3.17 解绑用户组 .....	58
9.3.18 绑定认证代理 .....	59
9.3.19 解绑认证代理 .....	60
9.4 导出用户 .....	61
9.5 批量解绑 .....	61
9.6 批量绑定 .....	61
9.7 变更机构 .....	63
9.8 权限审批 .....	63
9.8.1 查看申请 .....	63
9.8.2 批准申请 .....	63
9.8.3 驳回申请 .....	64
9.8.4 拒绝申请 .....	64

<b>第 10 章 用户组管理</b>	<b>65</b>
10.1 添加用户组	65
10.2 用户组列表	65
10.2.1 查看用户组	65
10.2.2 编辑用户组	65
10.2.3 启用/禁用用户组	65
10.2.4 绑定用户	66
10.2.5 解绑用户	66
10.2.6 绑定认证代理	67
10.2.7 解绑认证代理	67
10.2.8 删除用户组	68
<b>第 11 章 令牌管理</b>	<b>69</b>
11.1 令牌导入	69
11.2 令牌列表	70
11.2.1 查看令牌	70
11.2.2 启用/停用令牌	70
11.2.3 锁定/解锁令牌	71
11.2.4 挂失/解挂令牌	71
11.2.5 作废令牌	71
11.2.6 令牌认证	72
11.2.7 令牌同步	72
11.2.8 设置应急口令	73
11.2.9 软件令牌分发	74
11.2.10 取消分配	74
11.2.11 删除令牌	75
11.3 令牌分配	75
11.4 令牌同步	76
11.5 批量查询	76
11.6 手机令牌分发	76
11.6.1 手机令牌分发查看	76
11.6.2 设定标识码	76
11.6.3 手机令牌分发	77
11.6.4 重置手机令牌	78
11.6.5 重置设备	78
11.6.6 批量重置	78
<b>第 12 章 厂商管理</b>	<b>79</b>
12.1 添加厂商	79
12.2 厂商列表	79
12.2.1 查看厂商信息	79
12.2.2 下载证书	80
12.2.3 编辑厂商信息	80
12.2.4 删除厂商信息	80
<b>第 13 章 设备管理</b>	<b>81</b>
13.1 设备管理	81
13.1.1 受保护地址管理	81
13.1.1.1 添加受保护地址	81
13.1.1.2 受保护地址列表	81
13.1.2 FIDO 日志管理	82
13.1.2.1 FIDO 设备信息列表	82
13.1.2.2 FIDO 设备日志	83

13.1.3 FIDO 配置管理 .....	83
13.1.3.1 FIDO 用户注册策略 .....	83
<b>第 14 章 认证管理 .....</b>	<b>84</b>
14.1 认证服务器 .....	84
14.1.1 添加认证服务器 .....	84
14.1.2 认证服务器列表 .....	85
14.1.2.1 查看认证服务器 .....	85
14.1.2.2 编辑认证服务器 .....	85
14.1.2.3 删除认证服务器 .....	86
14.2 认证代理 .....	86
14.2.1 添加认证代理 .....	86
14.2.2 认证代理列表 .....	87
14.2.2.1 查看认证代理 .....	87
14.2.2.2 编辑认证代理 .....	87
14.2.2.3 下载代理配置文件 .....	87
14.2.2.4 添加认证服务器 .....	87
14.2.2.5 解除代理服务 .....	88
14.2.2.6 删除认证代理 .....	88
14.3 认证代理配置 .....	88
14.3.1 添加认证代理配置 .....	88
14.3.2 认证代理配置列表 .....	89
14.3.2.1 编辑认证代理配置 .....	89
14.3.2.2 删除认证代理配置 .....	90
14.4 后端认证 .....	90
14.4.1 添加后端认证 .....	90
14.4.2 后端认证列表 .....	91
14.4.2.1 编辑后端认证 .....	91
14.4.2.2 启用/禁用后端认证 .....	91
14.4.2.3 删除后端认证 .....	91
<b>第 15 章 日志管理 .....</b>	<b>92</b>
15.1 管理员日志 .....	92
15.2 用户日志 .....	92
<b>第 16 章 报表管理 .....</b>	<b>93</b>
16.1 业务报表 .....	93
16.1.1 认证、同步量统计 .....	93
16.1.2 按时段认证量统计 .....	93
16.1.3 用户门户访问量统计 .....	93
16.2 用户报表 .....	94
16.2.1 数量统计 .....	94
16.2.2 认证方式统计 .....	94
16.3 令牌报表 .....	94
16.3.1 状态统计 .....	94
16.3.2 过期时间统计 .....	94
16.3.3 厂商令牌统计 .....	95

# 第1章 关于文档

## 1.1 读者对象

本文档的读者对象为管理中心的测试人员、技术支持人员（包括售前、售中以及售后技术支持人员）、客户的系统安装、配置、管理和维护人员以及其它相关人员。

## 1.2 反馈意见

为了进一步给读者提供条理清晰、结构完整、内容丰富、简单易懂的文档，我们非常欢迎读者对本文档发表个人意见和建议。如果您愿意，您可以将您的意见和建议告诉我们。

## 1.3 基本环境说明

本文档是在一定的基本环境下编写的，如果用户实际操作时的基本环境与本文档编写时的基本环境不同的话，可能会出现与本文档描述内容不一致的地方。

（1）终端操作系统：Windows7

（2）Web Server：Tomcat7.0

（3）JDK：jdk1.7

## 1.4 文档约定

为了方便用户阅读和理解本文档所描述的内容，对文档中特定类型信息采用特殊的表示方式。下面对本文档中使用的特殊表示方式进行说明。

序号	文档中表示方式	说明
1	→	表示菜单层次
2	#	表示 AS4 系统提示符
3	宋体	表示引用其它文档的名称
4	Consolas	表示用户输入的内容
5	Tohoma	表示系统提示信息或已经存在的信息

## 第2章 安装前的准备工作

为了在安装配置过程中能够顺利进行，考虑到用户的计算机环境和网络环境的差异性，在进行管理中心的实际安装以前，需要进行如下的准备工作。

### 2.1 安装环境检查

管理中心的运行对基础环境有一定的要求，如果基础环境不能满足管理中心的要求，管理中心将不能正常使用。

序号	项目	必要性	说明
1	授权文件	必须	导入令牌时会检查授权文件
2	令牌文件	必须	认证服务器进行认证的基础
3	数据库管理系统	必须	管理中心的运行基础
4	数据库对应的 ODBC	必须	使用 ODBC 方式访问数据库时必须
5	数据库	必须	管理中心的运行基础

### 2.2 授权文件准备

授权文件（.lic 文件）是证明用户合法身份的文件，用户可以从开发商或其代理商处获得。系统在初始化时会自动提供一个评估授权文件，无需导入，若此授权文件不符合公司要求，可进入系统后自行更换授权文件。

### 2.3 令牌文件准备

令牌文件（.tnk 文件）是用于存放令牌信息的文件，用户需要将令牌文件中的令牌信息导入到 OTP Server 系统中，对应的令牌才能用于身份认证。通过管理中心可以将令牌文件中的令牌信息导入到 OTP Server 系统中。

提示：多厂商令牌文件（.xml、.dat 文件）是用于存放对应的厂商令牌信息的文件。

### 2.4 数据库管理系统

管理中心对 OTP Server 系统的管理是通过对数据库的管理来实现的。所以安装管理中心以前需要对数



数据库的选择和相关参数有所准备。比如选择使用何种数据库，选择使用已经存在的数据库还是建立新的数据库，决定使用的数据库和管理中心是否安装在同一计算机上等等。

数据库管理系统的准备工作主要包括以下两个方面：

#### （1）选择数据库类型

OTP Server 支持多种数据库，包括 SQL Server、MySQL、Oracle、PostgreSQL，您可以根据自己的环境和使用习惯任意选择其中的一种。

#### （2）建立访问数据库的账号

您可以选择已经存在的数据库管理系统，也可以选择新建数据库管理系统，不管是哪种方式，您都需要拥有访问数据库的账号和密码，而且该账号必须具有新建数据库的权限。

## 2.5 数据库对应的 ODBC

如果使用 ODBC 访问数据库，需要确认计算机上安装了对应数据库的 ODBC 驱动程序，如果没有安装 ODBC 驱动程序，将无法通过 ODBC 方式连接数据库。

## 2.6 数据库准备

数据库准备包括两个部分，创建数据库和数据库表，当然也可以使用已经创建的数据库。准备数据库时，首先需要在数据库管理系统中创建数据库，然后可以根据 OTP Server 安装程序提供的 SQL 脚本程序创建数据库表，也可以使用 OTP Server 系统初始化过程中的配置数据库连接功能创建数据库表。只有这两个步骤完成，数据库准备才算完成。

## 2.7 加密机设备准备

如果 OTP Server 认证系统运行过程中需要使用到加密机则需要准备加密机，OTP ServerV4.8 产品现支持两种加密机，分别为：“SJJ1310”、“SJJ1309A”。

## 2.8 FIDO 认证准备

客户使用 OTP ServerV4.8 产品是否选择使用 FIDO 认证决定。需要 U2F 设备，使用 U2F 设备目前只支持 Chrome 浏览器、版本 39 以上，需要在浏览器上安装 u2f 插件。把 U2F 设备插入 FIDO 测试程序所在电脑的 USB 口，用户使用 FIDO 登录受保护地址，OTP Server 通过用户信息和 U2F 设备进行身份认证并作出响应。

## 第3章 安装

OTP Server 4.8 采用集成安装包安装，集成安装包中含有：认证服务器、管理中心、用户门户和 MySQL 数据库等的安装，可选择全部安装也可选择部分安装，具体的安装步骤参见《OTP Server 安装配置手册（Windows）v4.8》文档。

## 第4章 系统初始化及登录

管理中心提供组织机构管理、管理员管理、用户管理、用户组管理、令牌管理、厂商管理、设备管理、认证管理、配置管理、日志管理、报表管理等。

使用管理中心进行操作以前，必须先登录管理中心，使用完毕以后应注销登录，防止非法操作和误操作。

### 4.1 系统初始化

(1) 安装 OTP Server4.8 集成安装包成功后，首次使用 OTP Server4.8 时打开浏览器，在浏览器地址栏中输入管理中心地址：<http://ip:18004/otpcenter>，进入到系统初始化语言选择界面，如图表 1 所示：



图表 1 语言选择初始化界面

(2) 在语言选择界面，选择系统使用的语言，点击“下一步”按钮，进入初始化方式界面，如图表 2 所示：



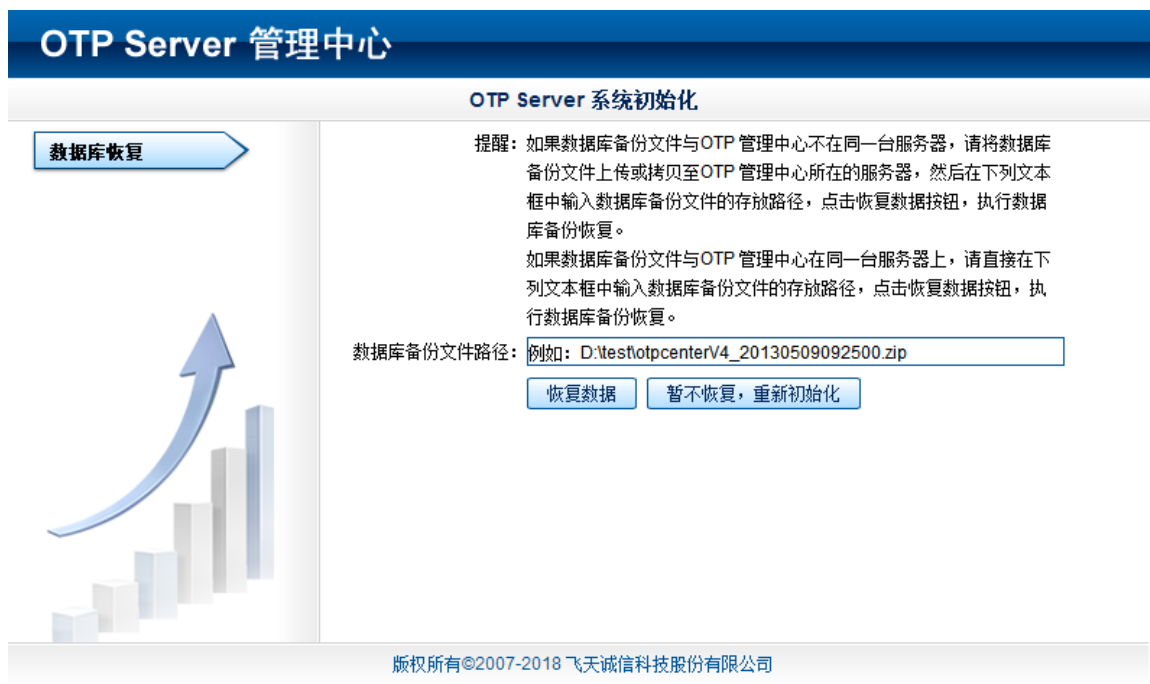
图表 2 初始化方式选择界面

(3) 在初始化界面，选择“创建数据库连接，进行系统初始化配置”，点击“下一步”按钮，若数据库中有授权文件信息，则直接进入“附加模块”界面，如图表 3 所示：



图表 3 附加模块界面

在初始化界面，选择“不需要重新初始化，恢复已经备份的数据库备份文件”，点击“下一步”按钮，进入数据库恢复界面，如错误!未找到引用源。所示：



图表 4 数据库恢复界面

(4) 在附加模块界面，选择需要的附加功能，并点击“下一步”按钮，进入到创建管理员界面，如图表 5 所示：



图表 5 创建管理员界面

(5) 在创建管理员界面，填好管理员信息，并点击“保存”按钮，进入到设置真实 IP 界面，如图表 6 所示：



图表 6 设置真实 IP 界面

(6) 设置好真实 IP 后，点击“下一步”按钮，进入初始化完成界面，如图表 7 所示：



图表 7 初始化完成界面

在数据库恢复界面，输入正确的数据库备份文件路径，点击“恢复数据”按钮，恢复成功后，系统进入到初始化完成界面。

(7) 进入初始化完成界面，完成初始化，若要登录系统则点击界面中的“登录”超链接，进入到登录页面。

## 4.2 登录

(1) 在初始化完成界面点击“登录”超链接或是打开浏览器，在浏览器地址栏中输入管理中心地址：<http://ip:18004/otpcenter>，打开管理中心登录页面。

提示：管理中心地址中“ip”指安装管理中心的机器的 IP 地址，本机为 127.0.0.1 或者 localhost。

(2) 在管理中心登录界面，显示“管理员”，“密码”和“验证码”三个输入框。若管理员登录方式为“只验证静态密码”，则需要依次输入管理员账号，管理员的静态密码和验证码。

若管理员登录方式为“只验证 OTP”，在登录界面“管理员”输入框中输入管理员账号后，界面上只显示一个“OTP 口令”输入框，需要在“OTP 口令”输入框中输入和该管理员账号绑定的令牌产生的 OTP 口令。

若管理员登录方式是“验证静态密码和 OTP”，在“管理员”输入框中输入管理员账号后会显示“密码”和“OTP 口令”两个输入框，在“密码”输入框中输入管理员的静态密码，在“OTP 口令”输入框中输入和该管理员账号绑定的令牌产生的 OTP 口令。

提示：1、超级管理员为初始化时设置的管理员账号，管理员账号不区分大小写。

2、超级管理员创建的管理员账号，管理员账号首次登录时，需要重新设置登录密码。

(3) 当输入的管理员账号、密码（或 OTP）和验证码都正确时，点击“登录”按钮，可以成功登录管理中心。

(4) 成功登录管理中心后，可在管理中心中继续进行其他操作。

## 4.3 找回密码/应急口令

管理员如果忘记静态密码或应急口令无法登录管理中心时，可使用系统的“找回密码”和“应急口令”功能，重置自己的密码或应急口令。

(1) 需要验证“静态密码”的管理员登录界面，密码输入框后会有“找回密码”的超链接，需要验证“OTP 口令”的管理员登录界面，OTP 口令输入框后会有“应急口令”的超链接。

(2) 点击“找回密码”或“应急口令”超链接，切换到找回密码或应急口令界面。

(3) 在“管理员账号”输入框中输入管理员账号，在“邮箱”输入框中输入管理员所对应的邮箱账号，点击“确定”或是“获取应急口令”按钮，可找回该管理员的密码或是应急口令。

提示：“找回密码”或“找回应急口令”是通过邮箱发送的，为保证此处功能正常，需要先在管理中心中配置一个可使用的邮件服务器，另外需要给管理员指定了一个可用的邮箱。

## 4.4 修改密码

管理员如果需要修改自己的密码，登录管理中心后，可以点击页面右上方的“修改密码”超链接，打开修改密码窗口，修改即可。

提示：当管理员再次登录系统时设置的密码生效。

## 4.5 编辑个人信息

管理员如果需要修改自己的个人信息，登录管理中心后，可以点击页面右上方的“编辑个人信息”超链接，修改即可。

## 4.6 退出

登录管理中心后，界面的右上角可以看到“安全退出”超链接，点击该超链接，可安全退出管理中心。

安全退出后系统将自动切换到管理中心登录页面，用户只有重新输入正确的管理员账号、密码和验证码之后才能再次进入管理中心。



## 第5章 配置管理

### 5.1 系统公共配置

#### 5.1.1 数据库

该模块主要是查看系统当前使用的数据库信息，以及重新配置数据库连接的操作，使用此模块功能可以灵活切换数据库，以适应不同需要。具体的设置步骤如下：

- (1) 点击页面上方导航栏中“配置管理”，选择“系统公共配置”下的“数据库”，进入数据库配置界面。
- (2) 界面上显示了当前管理中心连接的数据库信息以及连接状态。
- (3) 点击界面中的“重新配置数据库”按钮，系统弹出确认更换的提示。
- (4) 选择“是”，系统进入到“初始化->语言选择”界面，选择语言，点击“下一步”按钮，进入到“初始化方式”界面。
- (5) 选择“创建数据库连接，进行系统初始化配置”数据库初始化方式，点击“下一步”按钮，进入到“数据库连接”界面。

界面上各字段含义如下：

**数据库类型：**通过下拉选项选择要切换连接的数据库类型。

**数据库名称：**填写新数据库名称。

**数据库 IP：**填写新数据库所在机器的 IP 地址。

**数据库端口：**填写数据库的端口信息。

**数据库用户名：**填写数据库的用户名。

**数据库密码：**填写数据库的密码。

**结果反馈：**显示数据库的测试链接结果。

提示：此处也可选择使用备份数据库，具体操作步骤同初始化界面介绍内容。

- (6) 按要求填写信息，点击“连接测试”按钮，界面显示结果反馈：

**OTP Server 管理中心**

**OTP Server 系统初始化**

语言选择

初始化方式

**数据库连接**

数据库类型: MySQL ✓ OK

数据库名称: otpdb ✓ OK

数据库IP: 127.0.0.1 ✓ OK

数据库端口: 18003 ✓ OK

数据库用户名: root ✓ OK

数据库密码: \*\*\*\* ✓ OK

连接测试

结果反馈: ✓ 数据库连接成功, 请继续下一步操作。

提示: 检测系统已安装以下应用, 是否将数据库连接池配置信息同时更新到以下应用。

☒ 用户门户

☒ 认证服务

上一步 下一步

版权所有©2007-2018 飞天诚信科技股份有限公司

图表 8 切换数据库界面

(7) 在“数据库连接”界面, 若连接的是已有数据库表的数据库, 连接成功时, 系统提示点击“下一步”按钮继续。

连接的数据库没有数据库表, 系统提示先“创建数据库表”, 点击“创建数据库表”按钮, 成功后点击“下一步”按钮继续。

界面上同时还会检查本地是否还安装了“用户门户”和“认证服务器”, 安装了则提示你是否要同时更新这两个系统连接的数据库信息, 勾选上则会同时更新他们的数据库信息, 不勾选则不更新他们的数据库信息。

(8) 点击“下一步”按钮后, 系统提示“数据库连接配置成功, 请重启 web 服务器和 OTP 认证服务器”, 此时需重启 OTPAuthservice 服务和 OTPWebservice 服务。

提示: 若不重启这两个服务, 则会一直停留在初始化的界面。

(9) 重启过服务后, 若切换的新数据库表中无授权信息, 则会跳转到“上传授权文件”的页面, 选择有效的授权文件上传, 成功后点击“下一步”, 进入“附加模块”界面。

(10) 选择需要的附加功能, 点击“下一步”按钮进入“创建管理员”页面, 创建管理员信息, 点击“下一步”, 进入“真实 IP 设置”, 设置成功后, 点击“下一步”, 进入“初始化完成”界面, 完成数据库的切换。

数据库表中若存在初始化的管理员信息, 点击“下一步”, 进入“附加模块”界面, 再点击“下一步”, 直接进入“初始化完成”界面, 完成数据库切换。

## 5.1.2 数据备份

为了提高系统的安全性以及可移植性，管理中心还提供了数据库备份功能，当数据库或程序出现问题时，很容易恢复到原有的系统环境。管理中心提供了本地备份和远程(FTP)备份两种数据库备份方式，接下来详细介绍两种备份的配置。

本地备份：

(1) 点击页面上方导航栏中的“配置管理”，选择“系统公共配置”下的“数据备份”，进入数据库备份界面。

图表 9 备份设置界面

(2) 备份方式选择“本地（服务器）”，在备份地址中填写当前登录的管理中心所安装机器上的指定路径。

备份地址必须满足两个条件：

- 1、必须是管理中心安装在的机器上的地址，而不是访问的客户端地址。
- 2、所指定的路径必须存在，若路径不存在，系统会自动创建（注意：系统必须有该路径的读写权限）。

当勾选上“是否启用定时备份”项时，界面上出现备份时间字段，如图表 1010 所示：

图表 10 启用定时更新界面

远程（FTP）备份：

(1) 在备份设置界面，备份方式选择“远程（FTP）”项，界面上出现远程备份的设置项。

(2) 界面上各项的意义如下：

**远程服务器 IP：**输入远程备份的服务器 IP 地址。

**端口：**输入远程服务器的 FTP 端口，默认为 21。

**用户名：**输入远程服务器 FTP 的用户名。

**密码：**输入远程服务器 FTP 用户名对应的密码。

**备份地址：**输入备份的地址，该地址必须在指定的服务器上存在，若不存在则会自动创建，系统必须对该地址有读写权限。

提示：1) 要保证远程备份成功，首先需远程的机器上有 FTP，否则此处设置无效。

2) FTP 中会设置文件路径，若所设置的文件路径是要备份的准确地址，则远程备份地址中只需输入“/”，若备份的地址是 FTP 上文件路径下的某个文件夹，则备份地址输入为“/文件夹名”。

(3) 填写好远程备份的信息后，系统会将填写的信息组合成 FTP 的地址显示在界面下方，检查是否正确，若正确点击“保存”按钮。

提示：备份设置保存时，会自动检查填写信息是否正确，若不正确无法成功保存。

界面上除了本地备份和远程备份的设置外，还有两个公共设置项：备份日志和定时备份。“备份日志”复选框勾选上，在备份的时候同时也会把日志表内容也一并备份。“定时备份”若勾选上，可启动自动备份，系统将按照设置的备份时间自行备份。

### 5.1.3 邮件服务器

邮件服务器是系统中邮件通知功能的基础，只有配置了正确的邮件服务器，并且为用户配置了正确的邮箱后，才可以接收到邮件通知。如果没有配置邮件服务器，即使为用户填写了正确的邮箱，也无法实现邮件通知。

注意：如果邮件服务器开启了身份认证功能，在管理中心配置邮件服务器时，“验证邮件发送账号身份”必须选择“是”，否则即使其它信息填写正确，也无法实现邮件通知功能。

#### 5.1.3.1 添加邮件服务器

具体的操作步骤如下：

(1) 点击页面上方导航栏中的“配置管理”，选择“系统公共配置”下的“邮件服务器”，进入邮件服务器配置界面。

(2) 点击列表上方的“添加”按钮，切换到添加邮件服务器界面。

(3) 页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**服务器名称：**输入要添加的邮件服务器的名称，长度在 64 字符以内。

**邮件服务器：**输入要添加的邮箱域名，长度在 1 到 64 字符，格式类似为 ftsafe.com。

**发送账号：**在输入框中输入系统发送邮件的账号，长度为 4 到 255 字符，允许输入的内容为字母、数字和 “.-\_@”。

**账号密码：**输入发送邮件账号的密码，长度为 4 到 64 位之间

**确认密码：**在输入框中再次输入账号密码。

**邮件发送者：**给邮件发送者起个名称，长度为 1 到 64 字符，任何可见内容

**发送端口：**输入邮件服务器的端口，只能允许输入数字，默认值为 25

**验证邮件发送账号身份：**选择是，启用邮件发送身份验证，选择否，不启用邮件发送身份验证。

**描述：**在输入框中输入邮件服务器的描述信息。

(4) 按要求填写好信息后，点击界面上的“保存”按钮，系统提示保存成功。

### 5.1.3.2 编辑邮件服务器

如果要修改邮件服务器的信息，在邮件服务器列表页面，点击需修改的服务器“操作”列中的“编辑”图标，打开编辑界面修改信息，点击“保存”按钮，修改成功。

### 5.1.3.3 设置默认邮箱

当邮箱服务器列表中只有一条记录时，该邮箱服务器便为默认邮件服务器，当邮箱服务器列表中的记录为两条或两条以上时，可以手动设置指定的邮件服务器作为默认邮件服务器，系统中需要发送邮件的地方，均使用的是默认邮件服务器。具体的操作步骤如下：

(1) 点击页面上方导航栏中的“配置管理”，选择“系统公共配置”下的“邮件服务器”，进入邮件服务器配置界面。

(2) 在要设置为默认邮件服务器记录后的操作列中，点击“设置为默认邮件服务器”图标。

(3) 系统弹出确认设置的提示信息，选择“是”，设置默认邮件服务器成功。

### 5.1.3.4 删除邮件服务器

若添加的邮件服务器不再使用，可选择删除该邮件服务器。进入邮件服务器列表，选中要删除的邮件

服务器，点击界面上的“删除”按钮，确认后删除成功。

提示：默认邮件服务器不允许删除。

## 5.1.4 短信网关

系统中短信令牌的使用以及短信通知等功能的实现需依赖短信网关的配置，只有配置了正确的短信网关才能使用短信令牌和短信通知。如果短信网关配置不正确，系统中需要发送短信的地方无法发送出短信信息。

### 5.1.4.1 添加短信网关

具体操作步骤如下：

(1) 点击页面上方导航栏中的“配置管理”，选择“系统公共配置”下的“短信网关”，进入短信网关配置页面。

(2) 点击短信网关列表界面中的“添加”按钮，切换到添加短信网关界面，共两个标签页：基本信息配置和短信发送参数配置，默认显示的是基本信息配置界面。

(3) 基本信息配置界面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**配置名称：**在该输入框中输入短信网关的配置名称，作为不同网关之间的区别标识符，不允许重复，输入内容可以为 1-64 字符长度的内容。

**发送方式：**选择短信网关的发送方式。

**发送地址：**在输入框中输入短信网关短信发送地址。

**短信网关账号：**在输入框中输入短信网关账号。

**账号密码：**在输入框中输入短信网关账号对应的密码。

**确认密码：**在输入框中再次输入账号密码。

**重试次数：**在输入框中设置短信发送失败重试次数。

**网关优先级：**选择网关优先级，共 3 种选项：高、中、低，在使用短信令牌和短信通知业务时，会根据优先级高级来应用。

**描述：**在输入框中输入短信网管的描述信息。

(4) 按要求填写内容后，点击界面中的“下一步”按钮，进入短信发送参数配置界面。

(5) 短信发送参数配置界面带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**账号参数：**在输入框中输入短信网关的账号参数名称。

**密码参数：**在输入框中输入短信网关的密码参数名称。

**手机号参数：**在输入框中输入短信网关中手机号参数的名称。

**短信参数：**在输入框中输入短信网关的短信参数名称。

**附加参数：**在输入框中输入短信网关的附加参数名称。

**短信发送结果：**该字段显示网关测试连接结果。

提示：以上各字段输入的值均是参数名称，而非是参数值，例如短信网关的账号参数为 `username=ftotp`，那么在账号参数输入框中输入的值应为 `username`，而非是 `ftotp`。

(6) 按要求填写好短信发送参数配置，点击界面中的“连接测试”按钮，弹出测试短信网关页面。

(7) 在测试短信网关页面的“手机号码”输入框中输入测试的手机号，在短信内容中输入要发送的测试内容，点击“确定”按钮。

(8) 系统弹出测试是否通过的提示信息，根据输入的手机号，查看该手机是否收到测试短信。

若收到，则选择“是”，回到“短信发送参数配置”页面，页面上出现“保存”按钮，未收到，则选择“否”，退出测试页面，回到“测试短信网关”页面，检查填写的手机号是否准确，关闭“测试短信网关”页面，回到“短信发送参数配置”页面，可以修改配置信息重新进行测试，但是不会出现“保存”按钮。

(9) 测试通过，点击按钮“是”后，回到“短信发送参数配置”页面，点击“保存”按钮保存填写的短信网关信息。

提示：保存前可修改短信发送成功标识，若返回的成功标识中含有可变内容，如 ID 号，每次成功后值均不同，应去除可变的返回信息，只保留成功的内容，也许是代码如 0000，也许是字符如 OK，根据不同短信网关返回成功内容不同，适当的进行修改。

#### 5.1.4.2 编辑短信网关

如果要修改短信网关的信息，在短信网关列表页面，点击需修改的短信网关“操作”列中的“编辑”图标，打开编辑界面修改信息，点击“保存”按钮，修改成功。

#### 5.1.4.3 启用/禁用短信网关

当添加的短信网关由于某些原因造成短时期内不能正常使用时，可将该短信网关置为禁用状态。若后



续可以正常使用时，再将其启用。具体的启用/禁用的操作步骤如下：

- (1) 点击页面上方导航栏中的“配置管理”，选择“系统公共配置”下的“短信网关”，进入短信网关配置页面。
- (2) 点击“操作”列中的“启用/禁用”图标。
- (3) 系统弹出确认启用/禁用网关配置的提示信息，选择“是”，则成功启用/禁用所选的短信网关。

#### 5.1.4.4 删除短信网关

如果添加的短信网关不再使用，可选择删除该短信网关。进入短信网关列表，选中要删除的短信网关，点击界面上的“删除”按钮，确认后删除成功。

#### 5.1.5 其它公共配置

该模块列出在 OTP Server 整个产品中设置有效的一些参数。

页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**系统会话有效时间（分）：**必填项，默认值是 120 。是指登录管理中心后，当闲置时间超过此处设置的时长时，会话将失效，再对管理中心操作时需重新登录系统。

**系统默认语言配置：**设置系统中的语言类型，修改后需重新登录系统才能生效。

**启用日志定时删除：**选择“是”，设置日志留存天数，超过留存天数后将被删除。选择“否”，日志不被删除。

**日志存留天数：**当启用了日志定时删除时，该项内容才会出现，用于设置日志保存时间。

### 5.2 认证配置

#### 5.2.1 基本配置

基本配置界面主要用来设置“事件型令牌窗口策略”、“时间型令牌窗口策略”、“窗口调整模式”、“重放检测策略”和“用户和令牌认证失败锁定策略”等。

对于认证窗口设置的值是用来确定一次性都能认证通过的动态口令数量范围的；

调整窗口值是用来调整认证窗口值大小的，以确保在令牌的时钟出现偏差时，能够通过扩大认证窗口值的范围使令牌认证成功。调整窗口需要和窗口调整模式、窗口调整周期配合使用；



同步窗口是用来确定动态口令能够同步成功的数量范围的，可以保证令牌在首次使用或者长时间不使用时仍然能同步成功继续使用。

每个配置项的详细说明如下：

**事件型令牌认证窗口：**设置认证窗口值，默认为 40。

提示：认证时，输入令牌的当前口令以及当前口令之后的 39 个口令均能认证成功。

**事件型令牌调整窗口：**设置调整窗口值，默认为 20。

提示：当窗口调整模式为“进行调整”模式时，该数值才有用，详细使用方法将在窗口调整模式中描述。

**事件型令牌同步窗口：**设置同步窗口，默认值为 200。

提示：认证时，输入的口令在认证窗口值外，同步窗口值内，系统提示该令牌需要进行同步。

同步窗口的值应大于或等于“认证窗口值+调整窗口值”。

**时间型令牌认证窗口：**设置认证窗口值，默认为 3。

提示：认证时，输入当前口令或当前口令前后 3 个口令均能认证成功。

**时间型令牌调整窗口：**设置调整窗口值，默认值为 1。

提示：当窗口调整模式为“进行调整”模式时，该数值才有用，详细使用方法将在窗口调整模式中描述。

**时间型令牌同步窗口：**设置同步窗口值，默认值为 20。

提示：认证时，输入的口令在认证窗口值（前后）外，同步窗口值（前后）内，系统提示该令牌需要进行同步。

同步窗口的值应大于或等于“认证窗口值+调整窗口值”。

**窗口调整模式：**选择“不调整”，事件和时间型令牌的各种窗口保持不变，不随着时间推移而更改；

选择“超过窗口调整周期进行调整，不累计”，在第一个窗口周期之后，事件和时间型令牌首次认证时，认证窗口值调整为“认证窗口+调整窗口”的值，在这个值之内均能认证成功。

选择“超过窗口调整周期进行调整，连续累计”，在每一个窗口周期后，事件和时间型令牌首次认证时，认证窗口值均会调整，直到“认证窗口+调整窗口”值大于同步窗口值，之后的窗口周期便停止调整。

例：

令牌类型	窗口调整模式	窗口调整周期 (默认值)	调整窗口 (默认值)	调整结果
------	--------	-----------------	---------------	------

事件型	不调整	——	20	不调整 认证窗口保持默认值 40
	超过窗口调整周期进行调整，不累计	2	20	调整 认证窗口 2 周后调整为 60，以后保持此值不变
	超过窗口调整周期进行调整，连续累计	2	20	调整 认证窗口 2 周后调整为 60，且以后每隔 2 周在原来的基础上增加 20，调整后的认证窗口值不能大于同步窗口值
时间型	不调整	——	1	不调整 认证窗口保持默认值 3
	超过窗口调整周期进行调整，不累计	2	1	调整 认证窗口 2 周后调整为 4，以后保持此值不变
	超过窗口调整周期进行调整，连续累计	2	1	调整 认证窗口 2 周后调整为 4，且以后每隔 2 周在原来的基础上增加 1，调整后的认证窗口值不能大于同步窗口值

**窗口调整周期（周）：**当窗口调整模式选择为调整时，出现此项，用于指定调整窗口的周期。

**允许重放的时间间隔（秒）：**0 表示不允许重放，其他秒数表示在多少秒内允许重放，允许重放的时间间隔最长为 86400 秒。在重放的时间间隔内，使用同一口令能多次认证成功，直到过了重放时间或在重放时间内使用了新口令进行认证，该口令才会失效。

**临时锁定最大重试次数：**设置用户和令牌的临时锁定最大重试次数。

**自动解锁周期（分钟）：**设置用户或令牌临时锁定后的自动解锁周期。

**永久锁定最大重试次数：**设置用户或令牌的永久锁定最大重试次数。

**启用用户组认证策略：**默认选择“否”，用户认证时，不需要把用户添加到用户组，直接认证即可；选择“是”，用户认证时，如果该用户未添加用户组权限，则认证失败。

## 5.2.2 返回 RADIUS 属性

RADIUS 属性是添加用户时需设置的项，用户若选择了此处配置的 RADIUS 属性值，登录认证请求成功后，将会返回所选配置中的 RADIUS 属性值，可以提高系统登录的安全性。

### 5.2.2.1 添加 RADIUS 配置

具体的操作步骤如下：

(1) 点击页面上方导航栏中的“配置管理”，选择“认证配置”下的“返回 RADIUS 属性”，进入 RADIUS 配置页面。

(2) 点击界面列表上方的“添加”按钮，切换到添加 RADIUS 配置界面。

(3) 页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**RADIUS 配置名称：**在输入框中输入 RADIUS 配置的名称，为 1-64 字符长度的内容。

**RADIUS 配置描述：**在输入框中输入 RADIUS 配置的描述信息，为 0-255 字符长度的内容。

(4) 按要求填写 RADIUS 配置信息后，点击界面中的“保存”按钮，系统提示保存成功。

### 5.2.2.2 编辑 RADIUS 配置

如果要修改 RADIUS 配置信息，在 RADIUS 配置列表页面，点击需修改的 RADIUS 配置“操作”列中的“编辑”图标，打开编辑界面修改信息，点击“保存”按钮，修改成功

### 5.2.2.3 RADIUS 配置

针对每个 RADIUS 配置，可以继续为其添加 RADIUS 配置属性，在添加 RADIUS 配置属性之前，需要先进入 RADIUS 配置界面，操作如下：

点击 RADIUS 配置操作列中的“RADIUS 配置”图标，进入 RADIUS 配置界面。

#### 5.2.2.3.1 添加 RADIUS 配置属性

具体的操作步骤如下：

(1) 如上描述，先进入 RADIUS 配置界面。

(2) 点击列表上方的“添加”按钮，切换到添加 RADIUS 配置属性界面。

(3) 页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**厂商名称：**在下拉列表中选择厂商名称。

提示：除了标准属性外，其他的厂商名称需要进行配置才能显示在厂商名称下拉列表中，具体配置方法可参照非标准 RADIUS 属性配置文档。

**RADIUS 配置属性名称：**在下拉列表中选择 RADIUS 配置属性名称。

**RADIUS 配置属性值类型：**该字段不允许编辑，根据所选择的配置属性名称而自动显示。

**RADIUS 配置属性值：**为所选择的配置属性名称填写一个配置属性值。

提示：配置属性值，大部分需手动输入，有的配置属性名称的属性值是固定的，通过下拉选择就可以。

(4) 按要求填写好 RADIUS 配置属性信息后，点击界面中的“保存”按钮，系统弹出保存成功提示。

#### 5.2.2.3.2 编辑 RADIUS 配置属性

如果要修改 RADIUS 配置属性信息，在 RADIUS 配置属性列表页面，点击需修改的 RADIUS 配置属性“操作”列中的“编辑”图标，打开编辑界面修改信息，点击“保存”按钮，修改成功。

#### 5.2.2.3.3 删除 RADIUS 配置属性

如果加的 RADIUS 配置属性不再需要，可选择删除该 RADIUS 配置属性。进入 RADIUS 配置属性列表，选中要删除的 RADIUS 配置属性，点击界面中的“删除”按钮，确认后删除成功。

#### 5.2.2.4 删除 RADIUS 配置

如果加的 RADIUS 配置不再需要，可选择删除该 RADIUS 配置。进入 RADIUS 配置列表，选中要删除的 RADIUS 配置，点击界面中的“删除”按钮，确认后删除成功。

### 5.2.3 无线路由安全保护

该模块主要是对 PEAP 协议的无线路由保护功能进行设置。启用 PEAP 后只有管理中心的用户才能使用并且可以设置动态口令作为安全密码，可提高无线网络使用的安全性。

**是否启用 PEAP：**勾选“是”，启用 PEAP 无线路由保护，勾选“否”，不启用 PEAP 无线路由保护。

**是否锁定用户：**勾选“是”，当无线路由网络连接错误次数超过设置锁定次数值时锁定用户，勾选“否”，当无线路由网络连接错误次数超过设置锁定次数值时不锁定用户。

提示：只有启用 PEAP 时“是否锁定用户”才显示出来。PEAP 的详细配置参照 PEAP 配置文档中描述。

## 5.3 用户配置

### 5.3.1 用户-令牌绑定策略

用户-令牌绑定策略中主要是配置用户和令牌之间的绑定关系，如“每个用户最大可绑定令牌数”、“每个令牌最大绑定用户数”、“令牌绑定后是否迁移至用户所在的机构”等。下面将详细介绍每一项：

**每个用户最大可绑定令牌数：**可以设置每个用户允许绑定的最多令牌数，绑定超过此处设置的值时，绑定失败并提示已超允许绑定值，系统默认每个用户最多可以绑定 99 个令牌。

**绑定用户时，如果用户不存在，是否新增该用户：**选择“是”，在与别的系统集成，若令牌绑定的用户当前连接的数据库中不存在时，系统将会自动的在本地创建该用户。选择“否”，若令牌绑定的用户当前连接的数据库中不存在时，系统不会在本地创建该用户，绑定失败。

**绑定用户时，是否需要验证令牌的口令：**选择“需要”时，用户门户和认证代理接口中做绑定令牌或者更换令牌时验证令牌口令栏显示，必须要验证令牌的口令，口令正确才能绑定成功；

选择“不需要”时，验证令牌口令栏不显示，绑定令牌或者更换令牌时不需要验证令牌的口令即可绑定成功；

**每个令牌最大可绑定用户数：**每个令牌允许被绑定的最多用户数，绑定超过此处设置的值时，绑定失败并提示已超允许绑定值，系统默认每个令牌最多可以被 99 个用户绑定。

选择“可选”时，验证令牌口令栏显示，绑定令牌或者更换令牌时可以验证令牌口令也可以不验证。

**令牌绑定后是否迁移至用户所在的机构：**选择“是”时，当令牌在企业下被子机构中用户绑定后，令牌的组织机构由“企业”迁移到“用户所在的组织机构”。选择“否”，企业令牌被子机构中的令牌绑定后，令牌的组织机构不发生改变，仍在企业下。

提示：由于绑定多个令牌时每个令牌可能处理情况不同，所以只有“每个用户最大可绑定令牌数”和“每个令牌最大可绑定用户数”都为 1 时，该字段才会显示。当用户绑定的最大令牌数和令牌绑定的最大用户数有一个大于 1 时，该字段便隐藏，同时默认不允许令牌迁移组织机构。

**令牌解绑后是否回到所属的企业：**选择“是”，令牌与用户解绑后回到所属的企业中，选择“否”，则令牌与用户解绑后仍然保留在原来的组织机构中。

提示：

- 1) 只有“每个用户最大可绑定令牌数”和“每个令牌最大可绑定用户数”都为 1 时，该字段才会显示。当“每个用户最大可绑定令牌数”和“每个令牌最大可绑定用户数”有一个大于 1 时，该字段便隐藏，同时默认令牌解绑后不回到企业中。
- 2) 当令牌被多个用户绑定时，只有该令牌绑定的所有用户均被解绑时才会返回到企业中，有一个未解绑则仍然保留在所绑定的用户组织机构中。

**解绑令牌，被解绑令牌是否停用：**选择“是”，则令牌解绑后将被停用，选择“否”，则令牌解绑后仍然是启用状态。

提示：只有“每个令牌最大可绑定用户数”为 1 时才会出现该字段，当“每个令牌最大可绑定用户数”大于 1 时，该字段隐藏，隐藏是该项默认值为否。

**更换令牌，设置被更换令牌的状态：**该处有 3 个选项，当选择“继续使用”时，令牌被更换后不改变状态，继续能被使用；

选择“禁用”时，令牌被更换后将被禁用，若要重新使用，必须先启用令牌；

选择“作废”，则令牌更换后，令牌作废，作废后的令牌若要重新使用，必须删除该令牌后再重新导入。

提示：只有“每个令牌最大可绑定用户数”为 1 时才会出现该字段，当“每个令牌最大可绑定用户数”大于 1 时，该字段隐藏，隐藏时该项默认值为继续使用。

### 5.3.2 用户默认属性配置

用户默认属性配置主要是配置用户门户初始登录密码验证方式设置的是默认密码时的静态密码和用户的默认本地认证模式、后端认证模式。

**默认的用户静态密码：**如果用户门户的初始登录密码验证方式设置的是“默认密码”，而且添加用户时没有对用户设置静态密码，则用户在首次登录用户门户时的密码为此处设置的值。

**默认的本地认证模式：**通过 Excel 模板导入用户或者通过用户来源导入用户时，用户的本地认证模式默认为此处设置的认证模式，避免导入大量用户信息后还要通过手动更改每个用户的本地认证模式。

**默认的后端认证模式：**通过 Excel 模板导入用户或者通过用户来源导入用户时，用户的后端认证模式默认为此处设置的认证模式，避免导入大量用户信息后还要通过手动更改每个用户的后端认证模式。

### 5.3.3 用户来源

管理中心中的用户可通过三种途径添加，一是在用户管理中手动添加，二是使用模板导入用户，三是在用户来源处从 LDAP 或是其它数据库中导入。下面将详细介绍用户来源的使用。

#### 5.3.3.1 添加用户来源

##### 5.3.3.1.1 LDAP

LDAP 添加用户方式可以通过 LDAP 协议，将 LDAP 服务器上使用 Active Directory 等工具维护的用户信息导入到管理中心中。并且可以随时将 LDAP 服务器上的用户信息同步到管理中心中，而不需要重新在管理中心再手动维护。

添加 LDAP 用户来源类型的操作步骤：

- （1）点击页面上方导航栏中的“配置管理”，选择“用户配置”下的“用户来源”，进入用户来源配置页面。
- （2）点击界面中的“添加”按钮，切换到添加用户来源界面。
- （3）默认显示“基本配置”标签页，填写用户来源名称，用户来源类型选择 LDAP，填写用户来源描述信息，点击“下一步”按钮。



(4) 进入详细配置界面，页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**LDAP 服务器 IP：**输入 LDAP 所在机器的 IP 地址。

**LDAP 服务器端口：**输入指定 LDAP 服务器使用的监听端口，默认为 389。

**LDAP 账号：**输入登录 LDAP 服务器的账号，格式为“用户名@域名”。

如：用户账号为 test，域名为 ft.otp.com，则 LDAP 账号应填写 [test@ft.otp.com](mailto:test@ft.otp.com)。

**LDAP 密码：**输入 LDAP 服务器登录账号对应的密码。

提示：LDAP 服务器 IP、端口、账号以及密码用于将本机连接到 LDAP 服务器上，为了提高安全性，“LDAP 密码”项显示为黑点。

**查找 DN：**用来确定在 LDAP 服务器上查找用户时的起始目录，即确定本次操作的起始范围。

如：账号为 test，保存在 Users 目录下，域名为 ft.otp.com，则查找 DN 为 CN=Users,DC=ft,DC=otp,DC=com。

**根 DN：**用来在 LDAP 服务器上对用户进行全局查找。域名为 ft.otp.com，则根 DN 为 DC=ft,DC=otp,DC=com。

**查找条件：**查找用户时所用的查询条件，默认为(&(objectCategory=person)(objectClass=user))，一般不需更改。

**连接超时秒数：**输入连接超时秒数。

(5) 填写好信息，点击“连接测试”按钮，测试成功后，点击“下一步”按钮，进入到“保存配置”界面，各项的输入要求如下：

**组织机构设置方式：**选择“指定本地的组织机构”，不更新 LDAP 服务器上的组织机构信息，使用管理中心的组织机构。选择“更新 AD 的组织机构”，导入用户的时候同时也导入 LDAP 服务器上的组织机构。

**所属机构：**选择用户导入的组织机构。

**是否导入 LDAP 中已被禁用用户：**选择“不导入”，LDAP 服务器上禁用的用户不被导入进来，选择“导入”，LDAP 服务器上的启用和禁用的用户都将导入。

**LDAP 用户被删除时：**选择“不处理”，做同步用户属性时 LDAP 上被删除的用户在本地数据库中不作处理，保持原样；

选择“禁用本地用户”，进行同步用户属性时 LDAP 上被删除的用户在本地数据库中作禁用处理；

**是否同步用户属性：**选择“是”，更新 LDAP 上用户信息时同步用户属性中的信息到本地数据库中，选

择“否”，更新 LDAP 上用户信息时不同步用户属性中的信息到本地数据库中。

**是否支持分页同步用户属性：**选择“是”，更新 LDAP 服务器上用户属性信息时支持分页查询并把用户属性中的信息同步到本地数据库中，选择“否”，则不支持。

**是否使用 LDAP 默认字段配置信息：**选择“是”，使用 LDAP 服务器上配置的字段，选择“否”，则使用页面上配置的各字段信息。

(6) “保存配置”界面上的信息设置好后，点击“保存配置”按钮，系统提示“保存成功，是否设置定时任务”。

选择“否”不启用定时更新，用户来源添加成功并返回用户来源列表。选择“是”启用定时更新，并进入定时更新页面。在定时更新页面设置“执行方式”以及“执行时间点”，点击“保存”按钮，LDAP 用户来源添加成功。

提示：启用定时更新功能，系统将会在指定时间对 LDAP 用户来源中用户进行更新。

#### 5.3.3.1.2 远程数据库

远程数据库方式添加用户是在用户已经使用其他数据库维护了用户信息时使用，可以通过连接远程数据库，将远程数据库上的用户信息直接导入管理中心，不需要用户手动添加。

添加“远程数据库”用户来源类型的操作步骤：

(1) 点击页面上方导航栏中的“配置管理”，选择“用户配置”下的“用户来源”，进入用户来源配置页面。

(2) 点击界面上的“添加”按钮，切换到添加用户来源界面。

(3) 默认显示“基本配置”标签页，填写用户来源名称，用户来源类型选择远程数据库，填写用户来源描述信息，点击“下一步”按钮。

(4) 进入“详细配置”界面，页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**数据库类型：**在数据库类型的下拉选项中选择数据库类型，支持 4 种数据库：Mysql、Oracle、SqlServer、PostgreSQL。

**数据库 IP：**输入数据库所在机器的 IP 地址。

**数据库端口：**该字段填写所选数据库的端口号。

**数据库名称：**输入所要连接的数据库名称。

**数据库用户名：**输入所连接的数据库用户名。



**数据库密码：**输入所连接数据库用户名的密码。

按要求填写信息后，点击“连接测试”按钮，测试成功后，点击“下一步”按钮。

(5) 进入保存配置界面，如图表 111 所示：

图表 11 远程数据库配置界面

**远程数据库表名：**下拉列表中列出所连接的数据库中的所有表名，选择本地数据库中用户表对应的表名。

**本数据库表属性：**下拉列表中列出当前程序所连接的数据库中用户表的用户属性字段信息。

**远程数据库表属性：**下拉列表中列出选择的远程数据库表中的所有字段信息，选择与本数据库表属性选择字段对应的字段信息。

提示：选择了本地数据库表属性、远程数据库表名、远程数据库表属性，点击“添加关系”按钮，将属性对应关系添加到“对应关系”的框中。

**对应关系：**显示添加的本地表属性和远程数据库表属性的对应关系。

提示：若要删除，选中对应关系框中的记录，点击“删除关系”按钮，删除掉指定的对应关系。

**所属机构：**选择用户导入到的组织机构。

(6) “保存配置”界面上的信息设置好后，点击“保存配置”按钮，系统提示“保存成功，是否设置定时任务”。

选择“否”不启用定时更新，用户来源添加成功并返回用户来源列表。选择“是”启用定时更新，并进入定时更新页面。在定时更新页面设置“执行方式”以及“执行时间点”，点击“保存”按钮，远程数据库用户来源添加成功。

提示：启用定时更新功能，系统将会在指定时间对远程数据库中用户进行更新。

### 5.3.3.2 配置用户来源

如果要修改用户来源的信息，在用户来源列表中，点击需修改的用户来源“操作”列中的“配置”图标，进入修改界面。用户来源修改界面上各项要求是添加界面一致，可参考添加界面的说明来配置。

### 5.3.3.3 手动更新

用户来源的更新有两种方式，一种是在添加的时候设置自动更新，另一种是手动更新，自动更新在添加用户来源的时候已描述。手动更新只需在用户来源列表中，点击来源后操作列中的“手动更新”图标。若有新用户便会被更新到系统中来，并给出详细的提示信息。

### 5.3.3.4 删除用户来源

具体操作步骤如下：

- （1）点击页面上方导航栏中的“配置管理”，选择“用户配置”下的“用户来源”，进入用户来源配置页面。
- （2）勾选上要删除的用户来源前的复选框，点击界面上方的“删除”按钮。
- （3）系统弹出确认删除的提示信息，选择是，删除掉所选择的用户来源记录。

## 5.4 令牌配置

### 5.4.1 软件令牌

软件令牌配置界面是用来配置“软件令牌默认 PIN 码”的，系统默认软件令牌 PIN 码为 12345678，可以进行修改。在令牌列表中对软件令牌分发时的 PIN 码可以手动输入，也可以使用默认值，选择使用“默认”时软件令牌的 PIN 码为此处设置的“软件令牌默认 PIN 码”。

### 5.4.2 手机令牌

该模块负责配置手机令牌分发信息、手机令牌推送服务器信息，界面上各项的具体含义如下：

提示：页面上带有星号\*标识项为必填项，不允许为空

**激活密码有效周期（天）：**该字段设置手机令牌激活密码有效周期，在设置时间之后激活密码将失效。

**在线分发激活密码重试次数：**该字段设置在线激活时激活密码重试次数。

**默认激活密码：**手机令牌激活密码有三种方式：随机、手动输入和默认，选择“随机”时手机令牌分发时系统会随机生成激活密码；

选择“手动输入”时在分发手机令牌时由用户手动输入激活密码；

当选择“默认”时，手机令牌分发时将使用此处设置的默认激活密码。

**短信发送离线分发信息：**选“启用”，手机令牌激活时，将通过短信的形式发送激活信息到绑定的用户手机号码上，选“关闭”，手机令牌激活时不给绑定的用户手机发送激活信息。

提示：选“启用”，页面自动加载出“离线激活短信提示信息”项，Token number:[SN],Active password:[AP],Active code:[AC]，[SN]表示令牌号，[AP]表示令牌激活密码，[AC]表示激活码。

**邮件发送分发信息：**选择“启用”，当手机令牌绑定了用户且设置了邮箱时，手机令牌分发信息将以邮件形式通知该用户。选择“关闭”，手机令牌分发时不发送邮件给该用户。

提示：只适用于手机令牌被一个用户绑定的情况。

**是否启用分发站点：**选择“启用”，则启用分发站点，手机令牌在线分发时可以生成二维码；选择“关闭”则停用分发站点，手机令牌在线分发时不能生成二维码。

**分发站点访问类型：**通过下拉选项选择分发站点访问的类型：http、https、http 和 https。

**分发站点访问 URL：**填写分发站点访问的 URL。

提示：1、分发站点访问 URL 中的 IP 地址需输入 web 服务所在机器的 IP 地址。

2、若要保证手机令牌能成功的在线分发，需确保分发站点处于启动状态。

**手机令牌标识码：**选择“必填”，则手机令牌进行分发时，手机令牌标识码项必须填写；选择“可选”，则手机令牌分发时，手机令牌标识码可填可不填。

**是否启用手机令牌推送：**选择“启用”，则启用手机令牌推送策略，页面显示配置推送服务器相关信息；选择“关闭”，则手机令牌不能推送登录，页面不显示配置推送服务器相关信息。

提示：启用手机令牌推送策略，主要体现在“令牌管理→手机令牌分发→二维码”功能模块。

**推送服务器名称：**必填项，输入 1-64 个字符以内的推送服务器名称，默认为 publishServer，也可以改为其它指定的服务器名称。

**推送服务器 IP：**必填项，输入推送服务器的 IP 地址。

提示：推送服务器 IP 地址，页面显示的值是认证服务器所在系统环境的真实 IP 地址。

**推送服务器端口：**必填项，输入推送服务器的端口，默认为 58004，也可以改为其它指定的端口，需要修改“pushserver.properties”文件里面的推送服务器端口（文件路径：/otpservice/otpauthservice/conf/），重

启服务器生效。

“保存”按钮：选择“启用”，推送服务器配置信息填写正确，点击“保存”按钮，手机令牌推送策略配置成功。

提示：

1、开启手机令牌推送策略，需要修改“pushserver.properties”文件里面的认证服务器 IP，文件路径：

/otpserver/otpauthservice/conf/

2、相关文件配置完成，管理中心开启了手机推送策略后，后台需要开启推送服务器，Linux 环境下执行：

./startpushserver.sh，Windows 环境直接双击运行：start\_otp\_push\_server.bat，运行推动服务器脚本路径：

/otpserver/otpauthservice/bin/

**一键激活和一键解绑认证方式：**默认选择的是“后端认证”，在手机端操作手机令牌一键激活功能，管理中心需要配置后端服务器（认证管理→后端认证→添加后端认证），用户需要输入后端服务器密码完成一键激活；“动态口令认证”：用户已绑定令牌，在手机端操作手机令牌一键激活功能时，用户需要输入已绑定令牌的口令完成一键激活；“静态密码认证”：在手机端操作手机令牌一键激活功能时，用户需要输入用户的静态密码完成一键激活；“自定义接口认证”：OTPServer 服务器对接其它认证系统，此功能需要定制开发。

**认证成功自动创建不存在用户：**默认选择“创建”，操作手机端的手机令牌进行一键激活，如果该用户在本地不存在，则会自动创建。选择“不创建”，如果本地不存在该用户，操作手机端的手机令牌进行一键激活，则一键激活失败；如果本地用户存在，操作手机端的手机令牌进行一键激活，则一键激活成功。

提示：此项功能与“一键激活和一键解绑认证方式”结合使用，上述项选择是“后端认证”、“自定义接口认证”，界面自动显示此项。

**解绑一键激活的手机令牌：**该选项与手机令牌一键激活功能有关，选择“启用”，在手机端删除一键激活的令牌时同时解绑该令牌与用户的绑定关系；选择“关闭”，只是把该令牌从手机端删除了，并没有解除与用户的绑定关系。

**手机令牌一键激活二维码：**在手机端操作手机令牌进行一键激活时需要设置推送服务器信息，可直接扫该二维码进行设置推送服务器信息。

### 5.4.3 短信令牌

短信令牌配置主要存储一些短信令牌参数的设置，具体的含义如下：

**短信令牌的 OTP 认证过期时间（秒）：**在短信令牌的口令产生之后，在该设置时间内，口令是有效的，

可以进行认证，当超过该处设置的时间后，当前口令失效，进行认证时提示认证失败，必须重新获取新的口令才能成功认证。

**短信令牌的 OTP 产生过期时间 (秒):** 此处设置短信令牌生成动态口令的时间间隔，系统默认为 60 秒，即每隔 60 秒生成一个新的动态口令，可以进行修改。

提示：短信令牌的“OTP 产生过期时间”应小于“短信令牌的 OTP 认证过期时间”。

**短信 OTP 的提示信息:** 用来设置获取短信令牌时收取到的短信内容，默认显示“Your SMS OTP is [SMSOTP], Order is [SMSORDER]”，[SMSOTP]为短信令牌当前生成的动态口令，不可修改，[SMSORDER]为短信序列号：1-99，不可修改，其他内容可以进行修改。

RADIUS 请求短信配置主要配置 RADIUS 请求短信的属性设置，具体配置信息如下：

**RADIUS 请求短信 OTP 附加属性名称:** 默认名称为 State。

**RADIUS 请求短信 OTP 附加属性值:** 默认值是 get。

**发送短信 OTP 前身份认证方式:** 默认选择“静态密码认证”，在发送短信 OTP 之前需要输入静态密码进行认证。选择“不认证”，在发送短信 OTP 之前不需要认证。选择“后端认证”，在发送短信 OTP 之前需要进行后端认证。

**短信 OTP 发送成功后的相应包属性 Code 值:** 默认值为 11。

## 5.4.4 应急口令

用来设置应急口令的默认有效时长和最大有效时长，具体每项的意义如下：

**应急口令默认有效时长 (小时):** 默认值为 2 小时，可手动修改，但必须小于或等于“应急口令最大有效时长”。

提示：为令牌设置应急口令时，默认的有效期截止时间为“Web 服务所在机器时间+默认有效时长”。

**应急口令最大有效时长 (小时):** 为令牌设置应急口令时，有效时长不能大于此处设置的值，应急口令最大有效时长由用户自己来设置，可以满足不同的工作需要。

## 5.5 管理中心配置

### 5.5.1 管理员策略

此处主要控制管理员登录认证策略和超级管理员权限控制策略，界面上各项的意义如下：

**临时锁定最大重试次数：**该字段设置的是管理员临时锁定的最大重试次数，当登录时输入密码错误次数超过此处设置的值时，管理员账户将被临时锁定。

提示：临时锁定的管理员账户解锁方法有两种，一种是在自动解锁周期后成功认证一次后账户将自动解锁，一种是请上级管理员在管理中心中解锁。

**永久锁定最大重试次数：**该字段设置的是管理员永久锁定的最大重试次数，当登录时输入密码错误次数超过此处设置的值时，管理员账户将被永久锁定。

提示：永久锁定的管理员账户只有一种解锁方法，就是请上级管理员在管理中心解锁。

**自动解锁周期（分钟）：**该字段是针对临时锁定设置的，当管理员被临时锁定后，在该处设置的时间之后成功认证一次将自动解锁。

**提示管理员修改密码周期（天）：**该字段设置某个数值，在该处设置的天数后，管理员登录系统时系统会给出提示，请重新设置密码。

**是否禁止使用超级管理员：**选择“是”，则禁止超级管理账户，使用超级管理员登录提示已被禁用，选择“否”，则允许使用超级管理员账户。超级管理员不能禁用自己。

## 5.5.2 访问控制策略

访问控制策略主要用来指定哪些机器允许访问管理中心，极大的提高了产品的安全性。详细的配置步骤如下：

（1）点击页面上方导航栏中的“配置管理”，选择“管理中心配置”下的“访问控制策略”，进入访问控制策略配置页面。

（2）页面上各项的输入要求如下：

**启用 IP 访问控制策略：**选择“否”，则不启用此处设置的策略，不管“允许访问的 IP 列表”中是否有值，管理中心均允许所有的客户端访问。选择“是”，则启用此处设置的策略，只有在“允许访问的 IP 列表”中的 IP 地址或 IP 号段的客户端才能访问管理中心。

**允许访问的 IP 列表：**存放已添加的 IP 地址和 IP 号段，在该列表中显示的 IP 地址或 IP 号段均是允许访问管理中心的。

（3）点击“添加”按钮，弹出添加信任 IP 的对话框。

添加允许访问的 IP 地址，在“允许访问的 IP 地址”框中输入要添加的 IP 地址，点击添加按钮，IP 地址被添加到允许访问的 IP 列表中。



添加允许访问的 IP 号段，勾选上“IP 号段”，在“允许访问的 IP 地址”中输入 IP 号段，点击“添加”按钮，IP 号段被添加到允许访问的 IP 列表中。

提示：若删除 IP 地址或 IP 号段时，选中某个或某些 IP 地址或 IP 号段，点击“移除”按钮，删除 IP 或 IP 号段。

(4) 点击“保存”按钮，成功设置访问控制策略。

### 5.5.3 认证服务器选择

该模块主要为当前管理中心选择主备认证服务器，下拉列表中列出的是“认证管理->认证服务器列表”中的所有记录。

提示：当选择的主认证服务器出现问题时，系统会自动转换到备用认证服务器进行认证操作。

### 5.5.4 页面配置

管理员可以自主配置管理中心系统主题、LOGO、预览信息。页面配置操作步骤如下：

(1) 点击页面上方导航栏中的“配置管理”，选择“管理中心配置”下的“页面配置”，进入页面配置页面。

(2) 各字段的填写规则如下：

**系统主题：**输入系统主题内容，内容为 0-64 个字符长度。

**登录页 LOGO：**选择登录页 LOGO，图片大小不允许超过 100KB，尺寸：215x30，格式：png、jpg。

**预览：**展示登录页 LOGO。

**主页 LOGO：**选择主页 LOGO，图片大小不允许超过 100KB，尺寸：260x30，格式：png、jpg。

**预览：**展示主页 LOGO。

(3) 点击“保存”按钮，管理中心页面配置成功。

## 5.6 用户门户配置

### 5.6.1 登录初始密码

登录初始密码主要用来设置用户首次登录用户门户时使用的密码验证方式，共有四种方式：默认密码、邮件发送激活密码、短信发送验证码、AD 密码验证，用户可以按照自己的需求选择相应的密码验证方式，

既能满足使用要求也可以提高系统使用的安全性。下面分别介绍：

**默认密码：**选择“默认密码”时，会显示出默认的用户静态密码，即配置管理->用户配置->用户默认属性中设置的“默认的用户静态密码”，用户首次登录用户门户时登录密码为此处显示的密码。

**邮件发送激活密码：**选择“邮件发送激活密码”时，会显示出激活密码验证有效期设置栏，可以设置验证码的有效时间，用户首次登录用户门户时，密码验证方式为邮件发送激活密码，点击获取按钮可以获取激活密码。

**短信发送验证码：**选择“短信发送验证码”时，会显示出短信码验证有效期设置栏，可以设置验证码的有效时间，用户首次登录用户门户时，密码验证方式为短信发送验证，点击获取按钮可以获取激活验证码。

提示：选择“邮件发送激活密码”或者“短信发送验证码”时，若邮件服务器或者短信网关未配置或者用户信息中没有填写邮箱地址或手机号，用户会收不到发送的验证码信息。

**AD 密码验证：**选择“AD 密码验证”时，会显示出服务器 IP、服务器端口、域名设置栏，各项填写说明如下：

服务器 IP：填写 AD 所在服务器的 IP 地址；

服务器端口：填写 AD 所在服务器的端口号；

域名：AD 上设置的域名；

用户登录用户门户时，密码验证方式为 AD 密码验证，用户在进行登录时使用在 AD 中所设置的密码进行登录。

## 5.6.2 基本策略

该模块主要设置是否允许使用用户门户，以及将开放哪些用户门户功能模块，具体的每项内容如下：

**启用用户门户：**选择“是”，允许用户使用用户门户产品，选择“否”，禁止用户使用该产品。

**用户门户开启功能：**该项列出了用户门户中的所有功能模块，管理员根据需要选择给用户开放那些功能。

**密码找回邮件链接有效周期（小时）：**用户找回密码时，发送到邮箱中的链接时间有效性设置，超过此处设置的时间，链接将失效，必须重新发送。

提示：勾选用户门户开启功能处的全选复选框，则选中所有模块，选中再取消勾选，则不选中任何模块。在未保存前，点击“重置”按钮时，“开启功能”恢复到刚进入页面时的初始状态。



### 5.6.3 通知公告

通知公告模块是为了实现管理员与各客户端用户门户之间的快速通讯，当管理员有重要事情通知各用户门户时，不需发送邮件或者别的通讯连接，只需在通知公告中填写通告内容并设置等级，在用户门户登录页面会显示通告内容，当用户在客户端登录用户门户时，会看到管理员添加的通知内容，方便快捷。

#### 5.6.3.1 添加通知公告

在通知公告列表，点击“添加”按钮切换到添加通知公告界面，输入主题、过期时间和通知内容，选择通知级别，点击“保存”按钮，添加成功。成功后在每一个用户门户客户端的登录界面均可以看到通知公告列表，点击链接可查看相应的通知公告内容。

#### 5.6.3.2 编辑通知公告

如果要修改通知公告的内容，点击需修改的通知公告“操作”列中的“编辑”图标，进入修改界面，修改信息，点击“保存”按钮。

#### 5.6.3.3 查看通知公告

通知公告内容较多时，可通过设置查询条件，查看指定的通知内容。点击查询到公告的“标题”超链接，能查看到全部的通知公告内容。

#### 5.6.3.4 删除通知公告

通知公告过期作废时，可进行删除。选中要删除的通知公告，点击界面上“删除”按钮，删除掉指定的通知公告。

### 5.6.4 页面配置

管理员可以自主配置用户门户系统主题、LOGO、预览信息。页面配置操作步骤如下：

(1) 点击页面上方导航栏中的“配置管理”，选择“用户门户配置”下的“页面配置”，进入页面配置页面。

(2) 各字段的填写规则如下：

**系统主题：**输入系统主题内容，内容为 0-64 个字符长度。

**登录页 LOGO：**选择登录页 LOGO，图片大小不允许超过 100KB，尺寸：315x29，格式：png、jpg。

**预览：**展示登录页 LOGO。

**主页 LOGO：**选择主页 LOGO，图片大小不允许超过 100KB，尺寸：315x29，格式：png、jpg。

**预览：**展示主页 LOGO。

(3) 点击“保存”按钮，用户门户页面配置成功。

## 5.7 监控预警配置

该模块主要对令牌使用和服务器运行情况进行设置预警值和预警方式，方便在超过预警值时，系统及时通知管理员。

### 5.7.1 预警配置

令牌监控配置主要对令牌将要过期天数、未绑定的令牌比例和 1 小时内令牌同步比例等内容设置预警值和预警方式，页面上各设置项的意义如下：

**是否启用预警：**勾选上，启用预警配置，不勾选，不启用预警配置。

**预警方式：**选择“邮件”，则达到预警值时使用邮件方式通知，选择“短信”，则达到预警值时将使用短信方式通知。

**预警接收人：**选择预警通知的管理员账号。

提示：若选择的管理员没有配置邮箱和手机号，或者配置的邮箱和手机号不准确，则不能正常接收邮箱预警或短信预警。

**令牌将要过期天数（天）：**设置令牌要过期天数的预警值，当系统中有令牌的过期天数小于此处设置的值时，将会给出预警通知。

**未绑定的令牌比例（%）：**设置未绑定令牌比例的预警值，当未绑定令牌的比例低于此处设置的值时，将会给出预警通知。

**1 小时内令牌同步比例（次数/用户数）（%）：**设置 1 小时内令牌同步比例的预警值，当 1 小时内令牌同步比例超过此处设置的值时，系统将会给出预警通知。

按要求设置预警基本配置，点击“保存”按钮，配置生效。

### 5.7.2 双机运行监控配置

双机运行监控在双机热备的环境下可以对主从服务器的运行情况进行监控并设置预警方式，主服务器

和从服务器相互监控，其中一台出现故障时另一台就会自动启用，不影响用户使用，同时向预警接收人发送邮件或者短信进行通知。页面上各设置项的意义如下：

**是否启用预警：**勾选上，启用预警配置，不勾选，不启用预警配置。

**主服务器真实 IP 地址：**填写主服务器的 IP 地址，若是 heartbeat 环境，则填写虚拟 IP 地址，若非 heartbeat 环境，则直接填写所在服务器的真实 IP 地址。格式要求：http://ip 或者 https://ip。

**从服务器真实 IP 地址：**填写从服务器的 IP 地址，若是 heartbeat 环境，则填写虚拟 IP 地址，若非 heartbeat 环境，则直接填写所在服务器的真实 IP 地址。格式要求：http://ip 或者 https://ip。

提示：若是非 heartbeat 环境，主从服务器需共用同一数据库。

**预警方式：**勾选“邮件”时，则主服务器或者从服务器出现故障时使用邮件方式通知，选择“短信”，则主服务器或者从服务器出现故障时将使用短信方式通知。

**预警接收人：**选择预警通知的管理员账号。

提示：若选择的管理员没有配置邮箱和手机号，或者配置的邮箱和手机号不准确，则不能正常接收邮箱预警或短信预警。

**定时器时间间隔（分）：**设置对主从服务器进行监控的时间间隔。

## 5.8 密码策略配置

### 5.8.1 管理员密码策略配置

对管理员密码进行加强。页面上各设置项的意义如下：

**是否启用管理员密码策略：**勾选上，启用密码策略配置，不勾选，不启用密码策略配置。

**启用密码最短长度：**默认选择“是”，最短密码长度项默认是 6；选择“否”，最短密码长度项不显示，长度为系统默认密码长度 4。

**密码组成方式：**默认选择“是”，显示密码组合方式项，展示了各种组合方式：密码应为数字和字母的组合、允许使用特殊字符（空格除外）、不允许使用重复字符等；选择“否”，密码组合方式项不显示。

**是否禁止使用历史密码：**默认选择“否”，选择“是”，显示不允许使用历史密码个数项，默认为 3。

**是否启用密码更改频率：**默认选择“否”，选择“是”，显示密码更改频率项，一天一次。

**是否定期更改密码：**默认选择“否”，选择“是”，显示定期更改时间 90 天。

按要求配置管理员密码策略，点击“保存”按钮，配置生效。

## 5.8.2 用户密码策略配置

对用户密码进行加强。页面上各设置项的意义如下：

**是否启用用户密码策略：**勾选上，启用密码策略配置，不勾选，不启用密码策略配置。

**启用密码最短长度：**默认选择“是”，最短密码长度项默认是 6；选择“否”，最短密码长度项不显示，长度为系统默认密码长度 4。

**密码组成方式：**默认选择“是”，显示密码组合方式项，展示了各种组合方式：密码应为数字和字母的组合、允许使用特殊字符（空格除外）、不允许使用重复字符等；选择“否”，密码组合方式项不显示。

**是否禁止使用历史密码：**默认选择“否”，选择“是”，显示不允许使用历史密码个数项，默认为 3。

**是否启用密码更改频率：**默认选择“否”，选择“是”，显示密码更改频率项，一天一次。

**是否定期更改密码：**默认选择“否”，选择“是”，显示定期更改时间为 90 天。

**是否禁用不活跃用户：**默认选择“否”，选择“是”，显示不活跃用户的最小期限为 90 天。

按要求配置用户密码策略，点击“保存”按钮，配置生效。

## 5.9 加密机配置

该模块主要是通过连接不同型号的加密机，对导入成功的令牌文件的种子进行加密。

提示：在系统初始化的“附加模块”，选择了“加密机”，管理中心才会显示该功能。

### 5.9.1 加密机配置

**加密机型号：**必选项，选择对应的加密机型号。

提示：

配置加密机相关信息，需要修改 cacipher.ini 文件，配置文件信息如下：

hsmModel = SJJ1310 //加密机型号

host = 192.168.16.112 //加密机 IP

port = 8018 //加密机端口

OTPServer 管理中心配置加密机信息，文件路径：

/otpserver/otpwebservice/tomcat/webapps/otpcenter/WEB-INF/hsmllib/

OTPServer 认证服务器配置加密机信息，文件路径：/otpserver/otpauthservice/lib/hsmlib/

**加密机状态：**绿色对勾，表示选择的加密机连接成功，红色预警标识，表示选择的加密机不可用。

**认证密钥索引值：**填写加密机型号对应的密钥索引值，认证密钥索引值范围为 1-2048。

**提示：**密钥索引值对应加密机中的密钥索引号下的密钥，此密钥对种子数据进行加解密操作。

**OTPCenter 加密机配置文件：**显示 Web 端配置加密机信息的文件路径。

**OTPServer 加密机配置文件：**显示服务端配置加密机信息的文件路径。

## 第6章 首页

登录系统后默认显示的是首页，展现了快速查询、系统介绍、使用向导、授权信息、个人中心及用户和令牌的统计信息。

### 6.1 快速查询

快速查询为用户提供了方便快捷的查询用户和令牌的通道，无需进入到令牌列表或用户列表，就能查询出想要的用户信息或令牌信息。

在输入框中输入想要查询的用户或令牌信息，选择要查询的类型，点击“快速查询”按钮，便可查询到符合条件的数据信息。

提示：选择“用户或令牌”查询类型，如果输入的信息只在用户列表中存在，则打开用户列表列出查询到的用户信息；如果输入的信息只在令牌列表中存在，则打开令牌列表列出查询到的令牌信息；如果输入的信息既存在于用户列表中也存在于令牌列表中时，则只打开用户列表列出查询到的用户信息；如果输入的信息既不存在于用户列表中也不存在于令牌列表中时，查询结果为空。

### 6.2 快速导航

快速导航功能，帮助用户设置个性的快捷操作链接，在快速导航树中直接点击模块名称，便可打开相关模块的页面，更方便的使用系统。具体的操作如下：

- (1) 根据页面上方的导航栏或者左侧的导航栏进入到有添加至快速导航栏的界面。
- (2) 点击界面上右侧的“收藏至常用”图标，系统弹出收藏成功的提示信息。
- (3) 查看首页的快速导航栏菜单，收藏的页面添加到快速导航的树节点下。

提示：添加到快速导航下的链接也可以删除，只要将鼠标放置在链接上，后面便出现红色叉号图标，点击图标，便删除掉该链接。

### 6.3 使用向导

在系统首页，点击页面上的“使用向导”图标，页面上展示出系统中主体功能的一些介绍，并提供快速链接功能，点击文字中有下划线的超链接，便可切换到相应的模块页面去。

## 6.4 系统介绍

在系统首页，点击页面上的“系统介绍”图标，列出当前系统的一些介绍信息，方便对产品整体有所了解。

## 6.5 授权信息

### 6.5.1 授权信息查看和更新

在系统首页，点击页面上的“授权信息”图标，可查看系统当前所使用的授权文件信息。

系统初始化的时候会自动提供一个“评估授权”文件，由于“认证服务器节点”和“令牌总量”限制，可能达不到企业的使用要求，需对授权文件进行及时更新。具体的操作步骤如下：

- (1) 使用有“更新授权”权限的管理员登录到系统中。
- (2) 点击首页界面上“授权信息”图标，可看到“更新授权”按钮。
- (3) 点击界面上出现的“更新授权”按钮，切换到更新授权界面。
- (4) 选择要更新的授权文件，点击“上传”按钮，系统提示上传成功。

提示：更新授权文件时，若使用的是“评估授权文件”，可被更换成任意的正常的授权文件，不管客户标识是否相同，不管授权类型是评估、企业还是高级，均允许被更换；

若当前使用的是“企业授权文件”，只能更换成与当前授权文件客户标识相同的企业或者高级授权文件；

若当前使用的是“高级授权文件”，只能更换成与当前授权文件客户标识相同的企业或者高级授权文件。

若授权文件已失效，与授权相关的功能都不能正常使用，操作相关功能给予信息提示。

## 6.6 个人中心

在系统首页的个人中心中列出当前登录的管理员一些简单的信息，除了可以查看管理员的信息外，还可以查看管理的角色权限，点击“个人中心->管理员角色/权限”后的超链接，弹出当前管理员的角色权限界面，界面上列出当前管理员的所拥有的权限节点。



## 6.7 用户统计图

系统首页的用户统计图显示的是“报表管理->用户报表->数量统计”的信息，可直观的查看当前系统的用户总数、锁定用户数和绑定用户数。

提示：统计图中的数据不是实时更新的，而是一小时一更新。

## 6.8 令牌统计图

系统首页的用户统计图显示的是“报表管理->令牌报表->状态统计”的信息，可直观的查看当前系统的令牌总数、各种状态下的令牌数量。

提示：统计图中的数据不是实时更新的，而是一小时一更新。

## 第7章 组织机构

组织机构模块主要用来管理企业及企业中的各职能机构关系，是系统中的基础模块，系统中的用户和令牌都是基于组织机构存在的，管理员与组织机构则是管理与被管理的关系，详细的关联关系将在后续章节详细介绍，本章主要介绍对组织机构的管理和维护。

### 7.1 查看企业信息

点击上方导航栏中的“组织机构”，打开企业信息查看页面，系统提供个默认的企业名称“default domain”。针对默认的企业信息，管理员通过编辑功能，自行修改成符合实际的信息。

#### 7.1.1 编辑企业信息

在企业信息查看界面，点击“编辑本机构”按钮，进入编辑界面，修改信息，保存成功。

提示：界面上有红色星号的为必填内容。管理员与组织机构是管理与被管理的关系，管理员只能对自己所管理的组织机构及其下的子组织机构、用户或令牌进行管理操作。

#### 7.1.2 添加子机构

该功能实现在企业下添加更小单位的组织机构，具体操作步骤如下：

- （1）在企业信息查看界面，点击“添加子机构”图标，切换到添加子机构界面。
- （2）按要求填写信息，点击“保存”按钮，保存成功

#### 7.1.3 查看子机构

查看子机构信息，点击左侧组织机构树上对应子机构名称，打开子机构信息查看界面。

#### 7.1.4 编辑子机构

在打开的子机构信息查看界面，点击“编辑本机构”按钮，切换到编辑子机构界面，修改子机构信息，点击“保存”按钮。

#### 7.1.5 迁移子机构

企业中若出现部门调整和变动，管理中心组织机构树也得相应进行调整，为了方便处理这种情况，

提供了迁移机构的功能，可快速的调整组织机构树的层级关系，以及对组织机构下的用户和令牌的处理，具体的操作步骤如下：

- （1）点击页面左侧导航栏中的要迁移的子机构名称，进入该机构信息查看界面。
- （2）点击界面上“迁移本机构”按钮，切换到迁移机构界面。
- （3）页面上带有星号\*标识项为必填项，不允许为空，页面上各项的含义如下：

**组织机构：**该字段不允许编辑，显示的是所选的要迁移的子机构名称。

**新父机构：**点击输入框，打开选择机构对话框，勾选上新的父机构前的选择框，此处是单选。

**同步迁移子机构：**勾选上，迁移机构时将带走该机构下的所有子机构，不勾选上，迁移时只迁移走当前所选的机构，其下的子机构将变为当前子机构的父机构下的子机构。

**同步迁移用户和令牌：**勾选上，迁移机构时，将同时迁移走该机构下的用户和令牌，不勾选上，则迁移机构时，只迁移走机构，该机构下用户和令牌归属于当前企业。

- （5）按要求填写好内容后，点击界面上的“保存”按钮，系统弹出迁移成功的提示信息。

### 7.1.6 删除组织机构

点击左侧导航栏中组织机构树上要删除的组织机构名称，进入到该机构的查看界面，点击界面上的“删除本机构”按钮，弹出确认删除的提示信息，选择是，删除掉该机构。

提示：当前所选子机构下若存在子组织机构或令牌或用户，均不允许被删除。

### 7.1.7 查看企业或子机构下的用户和令牌

在组织机构信息的查看界面，可查看到该机构下的用户数以及令牌数，同时点击后面的“用户列表”或“令牌列表”超链接，可直接跳转到用户列表页面和令牌列表页面查看具体的用户信息和令牌信息。

## 第8章 管理员

管理员模块包括与管理员、管理员角色以及管理员相关的各项操作，例如查看管理员、添加管理员、编辑管理员、变更管理员创建人、删除管理员、查看管理员角色、添加管理员角色、编辑管理员角色、变更管理员角色创建人、删除管理员角色等。

其中，管理员角色限定了属于该角色下的管理员的权限。

### 8.1 管理员

#### 8.1.1 添加管理员

添加管理员的步骤如下：

(1) 点击页面上方导航栏中的“管理员”，选择“管理员”下的“添加管理员”，进入添加管理员页面。

(2) 页面上带有红色星号\*标识项为必填项，不允许为空，各字段的填写规则如下：

**管理员账号：**输入管理员登录系统的账号，账号内容 1-64 字符长度的字母、数字、“\_”的任意组合。

**真实姓名：**在输入框中输入管理员的真实姓名，可以为 0-64 字符长度的内容。

**密码验证方式：**有 3 种登录方式：只验证静态密码、只验证 OTP 和验证静态密码和 OTP。选择只验证静态密码，则管理员登录的时候只需验证其静态密码；选择只验证 OTP，管理员登录的时候需验证其绑定令牌的动态口令；选择验证静态密码和 OTP，管理员登录的时候即需验证静态密码，也需验证绑定令牌的 OTP。

**静态密码：**密码验证验证方式选择“只验证静态密码”或“验证静态密码和 OTP”时，该字段才会出现，用于输入管理员静态密码。

**确认静态密码：**确认所输入的静态密码。

**选择角色：**选择界面列出当前管理员所创建的所有管理员角色。

**选择机构：**非必填项，为管理员选择所管理的组织机构，允许多选。

**邮箱：**输入管理员的邮箱地址，输入内容只能为空或 4-255 字符长度的字母、数字和“-\_@”等组合，填写的邮箱需符合邮箱账号规则。

**手机：**在输入框中输入管理员的手机号码，内容为 0-64 字符长度的数字、加号、减号、英文括号任意组合。

**描述：** 在输入框中输入 0-255 字符长度的字符内容。

(4) 点击“保存”按钮，管理员添加成功。

## 8.1.2 管理员列表

管理员列表包括查询、查看管理员、编辑管理员、变更创建人、删除管理员等操作。

### 8.1.2.1 查看管理员

当管理员的数量比较多时，可以通过查询功能来查看特定管理员的信息。输入要查询的内容，查询出符合条件的信息，点击“管理员名称”超链接，打开管理员详细信息界面。

提示：在管理中心中，不同权限的管理员可以查看到的管理员信息不同。普通管理员只能查看到其自身及自身所添加的管理员信息。初始化时添加的超级管理员，能查看到系统中所有的管理员。

### 8.1.2.2 编辑管理员

若要修改管理员的信息，在管理员列表页面点击操作列中的“编辑”图标，进入编辑界面，修改信息后，点击“保存”按钮。

### 8.1.2.3 启用/禁用管理员

管理员默认为“启用”状态，可通过“操作”列中的“启用/禁用”图标来更改状态。

### 8.1.2.4 解锁/锁定管理员

管理员默认为“未锁定”状态，可通过“操作”列中的“锁定/解锁”图标来更改状态。

### 8.1.2.5 绑定/解绑令牌

管理员为“只验证 OTP”时，需给管理员绑定指定的令牌，具体操作步骤如下：

(1) 点击页面上方导航栏中的“管理员”，选择“管理员”下的“管理员列表”，进入管理员列表页面。

(2) 点击要绑定令牌的管理员“操作”列中的“绑定令牌”图标，进入令牌查询界面。

(3) 设置查询条件，查询到要绑定的令牌，勾选前面的复选框，然后点击界面中的“绑定”按钮，系统提示绑定成功。

若要解绑令牌，直接点击对应管理员“操作”列中的“解绑”图标，系统弹出确认提示信息，确认后解绑管理员与令牌的绑定关系。

提示：管理员绑定的令牌只能是在企业下的令牌，而非是子机构下的令牌。

#### 8.1.2.6 修改静态密码

若要修改管理员的静态密码，点击管理员“操作”列中的“重置密码”图标，弹出修改对话框，修改静态密码。

#### 8.1.2.7 变更创建人

管理员不能直接对系统中非自己创建的管理员进行编辑和删除操作，为了应对某管理员离职或出差等原因造成其创建的子管理员的后期维护中断问题，提供了变更创建人的功能。具体操作步骤如下：

（1）点击页面上方导航栏中的“管理员”，选择“管理员”下的“管理员列表”，进入管理员列表页面。

（2）勾选要变更的管理员前的复选框，然后点击“变更创建人”按钮，确认变更后，进入变更创建人界面。

（3）选择指派人，系统会列出该创建人创建的所有角色，为变更的管理员选择对应的角色，点击“确定”按钮，系统提示变更成功。

提示：被变更的管理员选择的指派变更人不能为管理员自身，否则不会改变。超级管理员默认就有变更创建人的权限，而其他管理员则需要通过创建的时候添加该权限。

#### 8.1.2.8 删除管理员

当创建的管理员不再使用时，可以选择删除管理员。在管理中心中删除管理员的具体操作步骤如下：

（1）点击页面上方导航栏中的“管理员”，选择“管理员”下的“管理员列表”，进入管理员列表页面。

（2）选择要删除的管理员前面的复选框，然后点击“删除”按钮，出现确认删除提示框，确认后删除。

提示：

- 1) 超级管理员不允许删除
- 2) 管理员不能删除自身账号

## 8.2 管理员角色

### 8.2.1 添加管理员角色

拥有添加角色权限的管理员可在此模块添加角色，添加的角色权限只能小于或等于当前管理员权限，

具体操作步骤如下所示：

(1) 点击页面上方导航栏中的“管理员”，选择“管理员角色”下的“添加角色”，进入添加管理员角色页面。

(2) 填写角色信息，图中带有星号\*标识项为必填项，不允许为空，添加界面中的填写项的具体要求如下：

**角色名称：**在“角色名称”输入框中输入要添加的角色名，允许输入长度为 4 到 64 个字符。

**选择角色拥有的权限：**必填项，在“选择角色拥有的权限”中，根据实际情况，选择该角色的授权节点。

**描述：**在描述输入框中输入该角色的描述信息，长度为 0-255 之间的所有可见字符。

(3) 完成必要的信息输入后，点击“保存”按钮，系统会弹出保存成功提示。

提示：超级管理员添加角色的界面，列出了所有的权限节点。而其它管理员的添加角色界面，只列出它自己所拥有的权限节点。

## 8.2.2 管理员角色列表

### 8.2.2.1 查看管理员角色

当管理员角色的数量比较多时，可以通过查询功能来查看特定管理员角色的信息，具体的操作步骤如下：

(1) 点击页面上方导航栏中的“管理员”，选择“管理员角色”下的“角色列表”，进入管理员角色列表页面。

(2) 输入相应的查询条件，然后点击“查询”按钮，符合查询条件的管理员角色记录就会显示出来。

### 8.2.2.2 编辑管理员角色

如果需要修改管理员角色信息，可以按照以下步骤进行操作：

(1) 点击页面上方导航栏中的“管理员”，选择“管理员角色”下的“角色列表”，进入管理员角色列表页面。

(2) 在管理员角色列表页面，点击需要修改的管理员角色操作列中的编辑图标，可以对管理员角色名称、权限、描述信息进行修改。

(3) 修改管理员角色之后，点击“保存”按钮，系统提示修改成功。



### 8.2.2.3 变更创建人

由于管理员并不能直接对系统中非自己创建的角色进行编辑和删除操作，为了应对某管理员离职或出差等原因造成其创建的管理员角色的后期维护中断问题，提供了变更创建人的功能。具体操作步骤如下：

- （1）点击页面上方导航栏中的“管理员”，选择“管理员角色”下的“角色列表”，进入管理员角色列表页面。
- （2）勾选上要变更的角色，然后点击“变更创建人”按钮，确认变更后，进入变更创建人界面。
- （3）选择指派人，点击“确定”按钮，系统提示变更成功。

提示：所选择的角色权限，超出指派人所拥有的权限时，将无法变更角色，系统会给出相应提示信息。

### 8.2.2.4 删除管理员角色

当创建的管理员角色不再使用时，可以选择删除管理员角色。在管理中心中删除管理员角色的具体操作步骤如下：

- （1）点击页面上方导航栏中的“管理员”，选择“管理员角色”下的“角色列表”，进入管理员角色列表页面。
- （2）选择要删除的管理员角色前面的复选框，然后点击“删除”按钮，将出现确认删除提示框。
- （3）如果确认要删除选中的管理员角色，可以单击“确定”按钮；如果要取消删除操作，可以点击“取消”按钮。

提示：删除某个管理员角色以后会使属于该管理员角色的管理员的权限发生变化，所以删除以前需要确认该管理员角色确实已经没有用以及对属于该组的管理员进行更换角色或删除等处理以后才进行删除操作。

## 第9章 用户管理

该模块主要处理与用户相关的各种操作，例如查看用户、添加用户、批量绑定、批量解绑、导入用户、导出用户、编辑用户、删除用户、绑定令牌、设置 PIN 等。

### 9.1 添加用户

拥有添加用户权限的管理员才可以添加用户，具体操作步骤如下所示：

(1) 点击页面上方导航栏中的“用户管理”，选择“添加用户”，进入添加用户页面。

(2) 在添加页面输入用户信息，页面上带有星号\*标识项为必填项，不允许为空，其中一些添加项的输入要求如下：

**选择机构：**将光标定位在选择机构输入框，会弹出选择机构对话框，选择指定的组织机构。

提示：在弹出的选择机构界面列出当前登录管理员管理的所有组织机构节点。

**用户账号：**输入创建的用户账号。

**真实姓名：**输入创建的用户真实姓名。

**本地认证模式：**本地认证模式用于设置在飞天服务器认证时的认证模式。

共 3 种选择，选择只验证 OTP，则在本地认证时，只需输入用户的动态口令认证；选择只验证静态密码，在本地认证时，只需输入用户的静态密码认证；选择验证静态密码和令牌，在本地认证时，即对用户的静态密码验证也对用户的动态口令验证。

**后端认证模式：**该项用于设置认证请求是否通过飞天认证服务器端转发至第三方服务器端进行认证。

共 3 种选择。选择需要，认证时会符合后端策略的请求发送到指定的第三方服务器认证。选择不需要，只需对该用户进行本地认证，不进行第三方认证。选择默认，当后端认证列表中存在可用的认证服务器，且发送请求满足后端认证服务器的转发策略，便使用后端认证，若不满足两个条件中的任意一个，则不使用后端认证。

**返回 Radius 配置：**下拉列表中列出“配置管理->认证配置->返回 RADIUS 属性”中的所有配置项，选择用户所要返回的 RADIUS 属性。

**邮箱：**设置用户的邮箱信息。

**手机：**设置用户的手机信息。

(3) 完成必要的信息输入后，点击“保存”按钮，系统弹出保存成功是否要绑定令牌的提示，选择“是”，则继续为用户绑定令牌，详细操作见 9.3.10 节的步骤，选择“否”则回到添加用户界面。

提示：当用户初始密码验证方式设置为邮件发送激活密码时，若用户的邮箱账号未填写在保存时会弹出提示框；

当用户初始密码验证方式设置为短信发送验证码时，若用户的手机号未填写在保存时会弹出提示框。

## 9.2 导入用户

系统中用户除了通过添加操作，将用户一个个添加到系统中外，还可以通过导入文件来实现批量的添加用户，具体操作步骤如下：

- (1) 点击页面上方导航栏中的“用户管理”，选择“导入用户”，进入导入用户页面。
- (2) 点击“下载导入模板”按钮，弹出下载模板界面。
- (3) 根据需要勾选用户和令牌的属性字段，点击“确定”按钮，下载模板到本地。
- (4) 根据模板内容，填写模板，并保存。
- (5) 在导入用户界面选择填写好的模板文件，然后点击“导入”按钮。

## 9.3 用户列表

### 9.3.1 查看用户

当用户的数量比较多时，可以通过查询功能来查看特定用户的信息，在查询条件中根据实际情况输入单个或者组合的查询条件，点击“查询”，查询出用户信息，点击用户账号超链接，弹出用户信息界面，可查看用户的详细信息和绑定令牌状况。

提示：初始化的管理员可查看到系统中所有机构下的所用用户，其它普通的管理员只能查看到自己管理的所有组织机构下的用户。

### 9.3.2 编辑用户

若要修改用户的信息，点击用户列表操作列中“编辑”图标，进入编辑界面，修改信息后，点击“保存”按钮。

提示：当用户初始密码验证方式设置为邮件发送激活密码时，若用户的邮箱账号未填写在保存时会弹出提示框；

当用户初始密码验证方式设置为短信发送验证码时，若用户的手机号未填写在保存时会弹出提示框。

### 9.3.3 设置静态密码

若要修改用户的静态密码，点击用户列表“操作”列中的“设置静态密码”图标，弹出设置静态面对话框，设置静态密码。

### 9.3.4 锁定/解锁用户

用户默认为“未锁定”状态，可通过“操作”列中的“锁定/解锁”图标来更改状态，也可以通过“操作”项下拉列表的“锁定/解锁”来更改状态。

### 9.3.5 启用/禁用用户

用户默认为“启用”状态，可通过“操作”项下拉列表的“启用/禁用”来更改状态。

### 9.3.6 设置返回 Radius 属性

编辑用户可设置 RADIUS 属性，也可以通过操作项下拉列表中的“设置 RADIUS 配置”进行设置，具体操作步骤如下：

（1）点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

（2）操作对象选择“本页选中的记录”，操作选择“设置 RADIUS 配置”，选中要设置的用户，点击“执行”按钮，弹出“设置 RADIUS 配置”对话框。

操作对象选择“本次查询所有记录”，操作选择“设置 RADIUS 配置”，点击“执行”按钮，弹出“设置 RADIUS 配置”对话框。

（3）选择返回的 RADIUS 属性，点击“确定”按钮，设置成功。

### 9.3.7 设置后端认证

编辑用户可设置后端认证，也可以通过操作项下拉列表中的“设置后端认证”进行设置，具体操作步骤如下：

（1）点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选

择查询条件，进入指定的用户列表标签页。

(2) 操作对象选择“本页选中的记录”，操作选择“设置后端认证”，选中要设置的用户，点击“执行”按钮，弹出“选择后端认证设置”对话框。

操作对象选择“本次查询所有记录”，操作选择“设置后端认证”，点击“执行”按钮，弹出“选择后端认证设置”对话框。

(3) 选择后端认证模式，点击“确定”按钮，设置成功。

### 9.3.8 设置本地认证模式

编辑用户可设置本地认证模式，也可以通过操作项下拉列表中的“设置本地认证模式”进行设置，具体操作步骤如下：

(1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

(2) 操作对象选择“本页选中的记录”，操作选择“设置本地认证模式”，选中要设置的用户，点击“执行”按钮，弹出“选择本地认证模式设置”对话框。

操作对象选择“本次查询所有记录”，操作选择“设置本地认证模式”，点击“执行”按钮，弹出“选择本地认证模式设置”对话框。

(3) 选择本地认证模式，点击“确定”按钮，设置成功。

### 9.3.9 变更机构

企业中常出现不同部门间人员调动的情况，由于每个管理员只能对自己管理的机构下用户及令牌进行管理，为了应对人员调动后的用户管理，现提供了对用户变更机构的功能。具体使用步骤如下：

(1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

(2) 点击需变更的用户“操作”列中的“变更机构”图标，切换到“变更机构->选择机构”界面。

(3) 在“变更到的组织机构”中选择要变更的目标机构，点击“下一步”按钮，进入到“机构变更”标签页。

(4) 用户未绑定令牌，或者绑定的令牌全为域下令牌时，机构变更的操作项只列出“该用户下没有绑定令牌或令牌为域下令牌，没有可变更的绑定令牌”，

提示：用户组织机构发生变更，但令牌组织机构不变，且绑定关系也未解除。

用户绑定的令牌均是独自使用的组织机构令牌，变更方式为“不变更绑定令牌的组织机构，但解除绑定关系”和“变更绑定的独自使用的组织机构令牌，解除共同使用的绑定令牌的绑定关系”。

提示：选择“不变更绑定令牌的组织机构，但解除绑定关系”，用户变更，用户绑定的所有令牌均不变更，仍留在原来的组织机构中，用户与令牌间绑定关系解除；

选择“变更绑定的独自使用的组织机构令牌，解除共同使用的绑定令牌的绑定关系”，用户变更，所有绑定的令牌也变更组织机构。

用户绑定的令牌均是公用的组织机构令牌，变更方式为“不变更绑定令牌的组织机构，但解除绑定关系”和“变更绑定的所有组织机构令牌，解除公共绑定令牌中其它的绑定关系”。

提示：选择“不变更绑定令牌的组织机构，但解除绑定关系”，用户变更，用户绑定的所有令牌均不变更，仍留在原来的组织机构中，用户与令牌间的绑定关系解除；

选择“变更绑定的所有组织机构令牌，解除公共绑定令牌中其它的绑定关系”，用户变更组织机构，令牌也变更组织机构，与用户的绑定关系未解除，但其他与选中共用令牌绑定的未变更的用户解除绑定关系。

用户绑定的令牌既有公用令牌也有单用的组织机构令牌，变更方式为“不变更绑定令牌的组织机构，但解除绑定关系”、“变更绑定的独自使用的组织机构令牌，解除共同使用的绑定令牌的绑定关系”和“变更绑定的所有组织机构令牌，解除公共绑定令牌中其它的绑定关系”。

提示：选择“不变更绑定令牌的组织机构，但解除绑定关系”，用户变更，用户绑定的所有令牌均不变更，仍留在原来的组织机构中，用户与令牌间的绑定关系解除；

选择“变更绑定的独自使用的组织机构令牌，解除共同使用的绑定令牌的绑定关系”，用户变更，绑定的令牌中为独用的令牌将被变更组织机构，绑定关系仍在，其它共用的令牌不变更，与用户的绑定关系解除；

选择“变更绑定的所有组织机构令牌，解除公共绑定令牌中其它的绑定关系”，用户变更组织机构，所有令牌也变更组织机构，与用户的绑定关系未解除，但其他与选中令牌绑定的未变更的用户将解除绑定关系。

(5) 在机构变更界面，根据需要选择变更方式，点击“变更”按钮，进入变更结果界面，结果界面列出本次变更的详细信息，点击“完成”按钮，完成变更。

### 9.3.10 绑定令牌

成功添加用户的时候可以选择继续为用户绑定令牌，如果添加用户时没进行绑定令牌操作，还可以进入到用户列表中，通过点击操作列中的绑定令牌图标进行绑定令牌。详细的操作步骤如下：

(1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

(2) 点击需绑定令牌的用户“操作”列中的“绑定令牌”图标，进入令牌查询界面。

(3) 设置查询条件，查询到要绑定的令牌，勾选前面的复选框，然后点击界面中的“下一步”按钮，进入令牌绑定界面。

(4) 在令牌绑定界面，根据选择的令牌数，选择适当的绑定方式，点击“绑定”按钮，弹出确认绑定的提示信息，选择是，继续进行绑定，绑定成功进入绑定结果界面。

提示：用户只能与所在组织机构中的令牌或者所在企业下的令牌进行绑定，不能跨组织机构进行绑定。

(5) 若导出用户和令牌的绑定信息，点击界面中的“导出绑定明细”按钮，导出用户和令牌的绑定信息。若不导出用户和令牌的绑定信息，则点击返回，回到用户列表页面。

### 9.3.11 解绑令牌

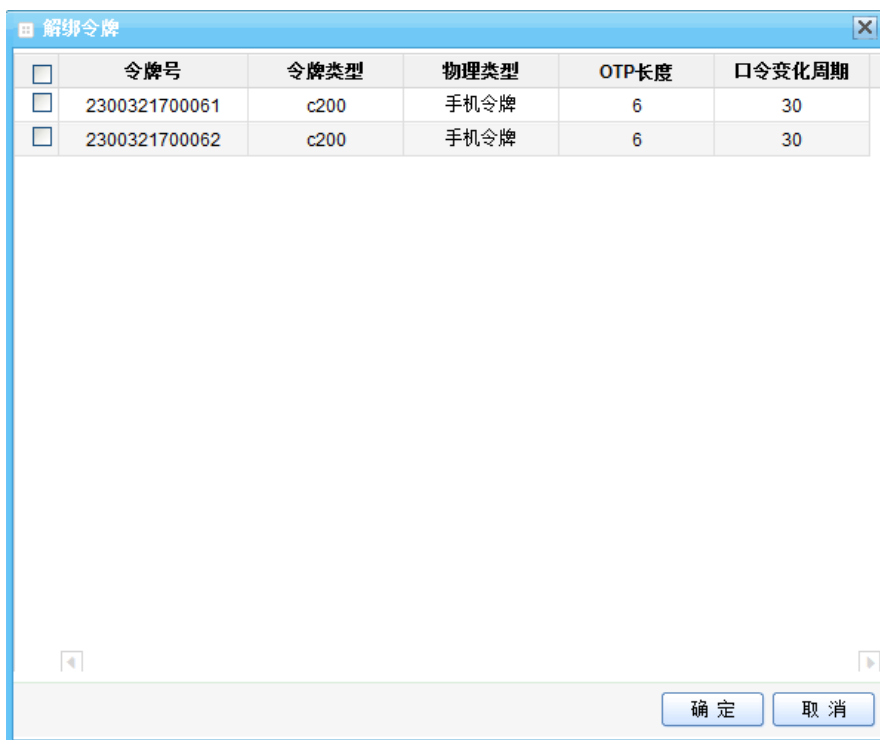
当用户绑定了令牌后，在用户的“操作”列中会出现“解绑令牌”的图标，可实现用户与令牌的快速解绑，具体操作步骤如下：

(1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

(2) 用户只绑定一个令牌时，点击需解绑令牌的用户“操作”列中的“解绑令牌”图标，弹出确认解绑的提示信息，选择是，解绑用户和令牌。

用户若绑定多个令牌，点击需解绑令牌的用户“操作”列中的“解绑令牌”图标，系统弹出解绑令牌界面，如图表 12 所示：





图表 12 解绑令牌界面

界面上列出当前用户所绑定的所有令牌，选择要解除绑定的令牌，点击“确定”按钮，系统弹出确认解除的提示信息，选择是则解除绑定关系。

提示：只有绑定令牌的用户操作列中才会出现解绑图标。

### 9.3.12 更换令牌

当用户想更换已绑定的令牌时，可通过操作列中的更换令牌来实现，用户列表中只有绑定了令牌的用户，操作列中才会出现更换令牌的操作，具体操作步骤如下：

- （1）点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。
- （2）在用户列表界面设置查询条件，点击“查询”按钮，查询到要更换令牌的用户。
- （3）点击需更换令牌的用户“操作”列中的“更换令牌”图标，进入“更换令牌->选择预更换的令牌”界面，选择该用户要更换的令牌，点击“下一步”按钮，进入“选择新令牌”标签页。
- （4）选择与被更换令牌数量相等的新令牌，点击界面中的“下一步”按钮，进入到“更换令牌”标签，点击“更换”按钮，更换用户绑定的令牌。

提示：只有绑定令牌的用户操作列中才会出现“更换令牌”的图标。

### 9.3.13 令牌同步

同步令牌是指当令牌处于异步状态或超异步状态时，通过同步操作，将其恢复到同步状态。只有处于同步状态的令牌才能用于身份认证。具体的操作步骤如下：

- (1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。
- (2) 点击需同步令牌的用户“操作”列中的“令牌同步”图标，弹出令牌同步对话框。
- (3) 除短信令牌外的其它类型的令牌，同步时在“动态口令”输入框中输入令牌生成的第一个动态口令，在“下一次动态口令”输入框中输入令牌连续生成的下一个动态口令，点击“同步”按钮进行同步操作。

提示：如果令牌处于超异步状态，则需要修改同步窗口的默认值，根据令牌的具体情况，增大同步窗口的值，直到同步成功为止。

### 9.3.14 解绑

对绑定令牌的用户除了提供对某一个用户进行解绑令牌功能（9.3.11 节）外，还提供对批量用户进行解绑操作，具体步骤如下：

- (1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。
- (2) 在用户列表界面设置查询条件，点击“查询”按钮，查询到要解绑的用户。
- (3) 若查询出的用户不是全部要解绑，需在要解绑的用户前复选框中勾选上。
- (4) 在“操作对象”中选择“本页选中的记录”，“操作”选择“解绑”，点击“执行”按钮，确认解绑后，系统提示解绑成功。

提示：若对本次查询出的所有用户进行批量解绑，则可在第 3 步骤中，“操作对象”选择“本次查询的所有记录”，然后执行批量解绑的操作。

### 9.3.15 删除

当用户离职或其它原因导致用户账号不再使用时，可通过批量删除来删除列表中的用户账号，具体操作步骤如下：

- (1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

(2) 在用户列表界面设置查询条件，点击“查询”按钮，查询到要删除的用户。

(3) 若查询出的用户不是全部要删除，需在要删除的用户前复选框中勾选上。

(4) 在“操作对象”中选择“本页选中的记录”，“操作”选择“删除”，点击“执行”按钮，确认删除后，系统提示删除成功。

提示：若对本次查询出的所有用户进行批量删除，则可在第 3 步骤中，“操作对象”选择“本次查询的所有记录”，然后执行批量删除的操作。

### 9.3.16 绑定用户组

在用户列表中，通过点击操作列中的绑定用户组图标进行绑定用户组。详细的操作步骤如下：

(1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

(2) 点击用户“操作”列中的“绑定用户组”图标，系统弹出绑定用户组界面。

(3) 设置查询条件，查询到要绑定的用户组，勾选前面的复选框，然后点击界面中的“确定”按钮，系统弹出确认绑定的提示信息，选择是进行绑定关系。

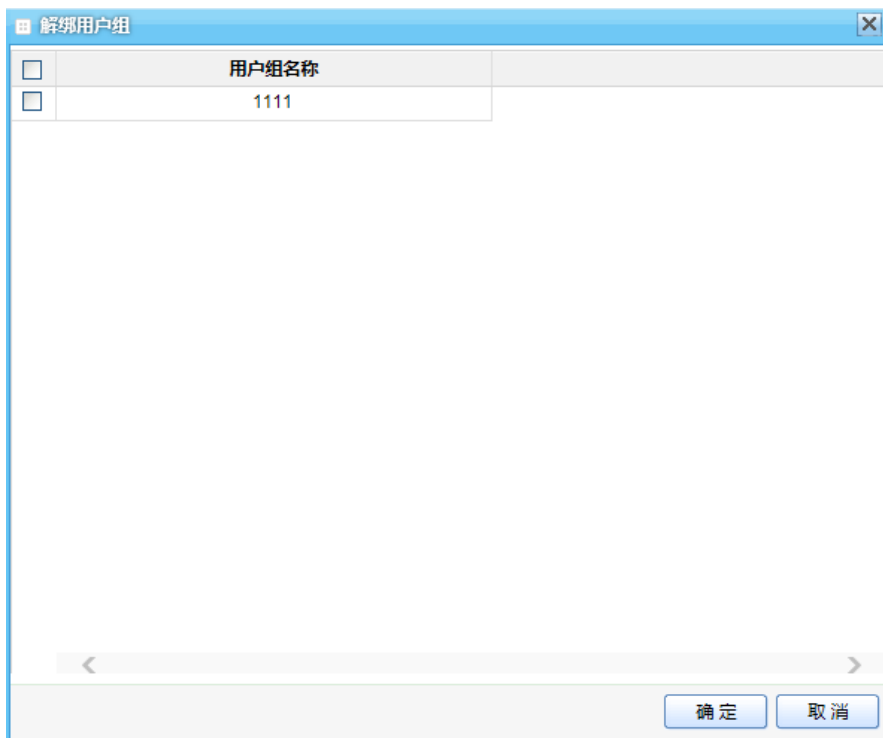
提示：若对查询出的所有用户进行批量绑定用户组，则可在“操作对象”选择“本次查询的所有记录”，然后执行批量绑定用户组的操作。

### 9.3.17 解绑用户组

当用户绑定了用户组后，在用户的“操作”列中会出现“解绑用户组”的图标，可实现用户与用户组的快速解绑，具体操作步骤如下：

(1) 点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

(2) 用户已绑定了用户组时，点击用户“操作”列中的“解绑用户组”图标，系统弹出解绑用户组界面，如图表 12 所示：



图表 13 解绑用户组界面

界面上列出当前用户所绑定的所有用户组信息，选择要解除绑定的用户组，点击“确定”按钮，系统弹出确认解除的提示信息，选择是则解除绑定关系。

提示：1、只有绑定了用户组的用户操作列中才会出现解绑用户组的图标。

2、若对查询出的已绑定用户组的用户进行批量解绑用户组操作，则可在“操作对象”选择“本次查询的所有记录”，然后执行批量解绑用户组的操作。

### 9.3.18 绑定认证代理

在用户列表中，通过点击操作列中的绑定认证代理图标进行绑定认证代理。详细的操作步骤如下：

（1）点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

（2）点击用户“操作”列中的“绑定认证代理”图标，系统弹出绑定认证代理界面。

（3）设置查询条件，查询到要绑定的认证代理，勾选前面的复选框，然后点击界面中的“确定”按钮，系统弹出确认绑定的提示信息，选择是进行绑定关系。

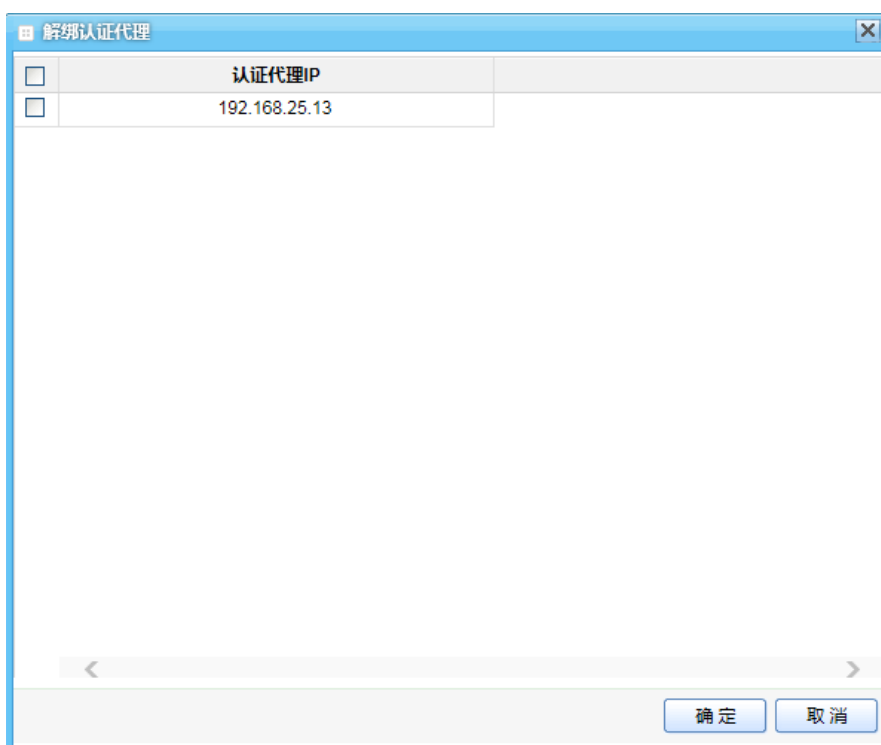
提示：若对查询出的所有用户进行批量绑定认证代理，则可在“操作对象”选择“本次查询的所有记录”，然后执行批量绑定认证代理的操作。

### 9.3.19 解绑认证代理

当用户绑定了认证代理后，在用户的“操作”列中会出现“解绑认证代理”的图标，可实现用户与认证代理的快速解绑，具体操作步骤如下：

（1）点击页面上方导航栏中的“用户管理”，选择“用户列表”，进入用户列表的用户查询标签页，选择查询条件，进入指定的用户列表标签页。

（2）用户已绑定了认证代理时，点击用户“操作”列中的“解绑认证代理”图标，系统弹出解绑认证代理界面，如图表 12 所示：



图表 14 解绑认证代理界面

界面上列出当前用户所绑定的所有认证代理信息，选择要解除绑定的认证代理，点击“确定”按钮，系统弹出确认解除的提示信息，选择是则解除绑定关系。

提示：1、只有绑定了认证代理的用户操作列中才会出现解绑认证代理的图标。

2、若对查询出的已绑定了认证代理的用户进行批量解绑认证代理操作，则可在“操作对象”选择“本次查询的所有记录”，然后执行批量解绑认证代理的操作。

## 9.4 导出用户

为了方便管理员对系统中用户信息的统计，系统提供了导出用户的功能，具体操作步骤如下：

- (1) 点击页面上方导航栏中的“用户管理”，选择“导出用户”，进入导出用户页面。
- (2) “选择机构”输入框中选择要导出哪个组织机构下的用户，选择要导出的用户类型，选择用户和令牌的属性字段，然后点击“导出用户”按钮。
- (3) 系统弹出文件下载页面，为文件指定存放路径，导出文件将会存放到指定的路径下。

## 9.5 批量解绑

系统中除了在用户列表中提供了解绑的功能外，在用户管理的下拉菜单中也提供了批量解绑的模块，该处批量解绑是通过上传用户和令牌绑定关系的模板文件来实现令牌批量解绑，具体操作步骤如下：

- (1) 点击页面上方导航栏中的“用户管理”，选择“批量解绑”，进入批量解绑页面。
- (2) 点击界面上的“下载模板文件”超链接，下载模板文件，并依照模板填写内容并保存。
- (3) 在批量解绑文件后点击“选择”按钮，上传填写好的模板文件，然后点击“批量解绑”按钮。
- (4) 解绑成功，提示“批量解绑成功!”；解绑失败，给予相应的错误信息提示。

## 9.6 批量绑定

用户与令牌的绑定，除了在用户列表的操作列中对单一的用户进行令牌绑定外，还可以对批量的用户进行令牌绑定，具体的操作步骤如下：

- (1) 点击页面上方导航栏中的“用户管理”，选择“批量绑定”，进入批量绑定页面。
- (2) 通过设置各种查询条件，查出要批量绑定的用户。
- (3) 操作对象选择“本页选中的记录”，在当前页选择要批量绑定的用户，点击“下一步”按钮，进入“令牌查询/选择”标签页。

操作对象选择“本次查询的所有记录”，将对查询出的所有用户进行批量绑定操作，点击“下一步”按钮，进入“令牌查询/选择”标签页。

- (4) 在“令牌查询/选择”界面，设置查询条件，查询出要绑定的令牌，勾选上要绑定的令牌前复选框，然后点击“下一步”操作按钮，进入到令牌绑定标签页。

(5) 根据“配置管理->用户配置->用户-令牌绑定策略”设置不同、选定的用户和令牌的数量不同，令牌绑定结果界面的提供的绑定方式也不同。

用户、令牌最大绑定数均为 1:

- 1) 选定一个用户，一个令牌，令牌绑定界面绑定方式为“一个用户绑定一支令牌”
- 2) 选定“多个用户，一个令牌”，或“一个用户，多个令牌”，提示超过限制
- 3) 选定多个用户，多个令牌，令牌绑定方式为“每一个用户对应只绑定一支令牌，多选的用户或令牌放弃绑定”

用户最大绑定数大于 1，令牌最大绑定数为 1:

- 4) 选定一个用户，一个令牌，令牌绑定界面绑定方式为“一个用户绑定一支令牌”
- 5) 选定多个用户，一个令牌，提示超过绑定上限
- 6) 选定一个用户，多个令牌（小于等于用户最大绑定数），令牌绑定方式为“一个用户绑定一支令牌”、“一个用户绑定多支令牌，绑定令牌上线不能超过 X 支”
- 7) 选定多个用户，多个令牌，令牌绑定方式为“每一个用户对应只绑定一支令牌，多选的用户或令牌放弃绑定”、“每一个用户分别绑定多支令牌，绑定令牌上限不能超过 X 支”

用户最大绑定数为 1，令牌最大绑定数大于 1:

- 1) 选定一个用户，一个令牌，令牌绑定界面绑定方式为“一个用户绑定一支令牌”
- 2) 选定多个用户（小于等于令牌绑定上限），一个令牌，令牌绑定方式为“多个用户共同绑定一支令牌”
- 3) 选定一个用户，多个令牌，提示超过绑定上限
- 4) 选定多个用户，多个令牌，令牌绑定方式为“每一个用户对应只绑定一支令牌，多选的用户或令牌放弃绑定”

用户最大绑定数大于 1，令牌最大绑定数大于 1:

- 1) 选定一个用户，一个令牌，令牌绑定界面绑定方式为“一个用户绑定一支令牌”
- 2) 选定多个用户（小于等于令牌绑定上限），一个令牌，令牌绑定方式为“每个用户共同绑定一支令牌”
- 3) 选定一个用户，多个令牌（小于等于用户绑定上限），令牌绑定方式为“一个用户绑定一支令牌”、“一个用户绑定多支令牌，绑定令牌上线不能超过 X 支”



4) 选定多个用户，多个令牌，令牌绑定方式为“每一个用户对应只绑定一支令牌，多选的用户或令牌放弃绑定”、“每一个用户分别绑定多支令牌，绑定令牌上限不能超过 x 支”

(6) 根据实际情况选择绑定方式，然后点击界面中的“绑定”按钮，系统弹出确认绑定的提示信息，选择是，进入到绑定结果的标签页。

(7) 在绑定结果界面显示用户和令牌之间的绑定结果，当用户、令牌绑定关系较多时，可点击“导入绑定明细”按钮，将绑定的用户和令牌导出成 excel 表。

## 9.7 变更机构

变更机构为了应对企业中不同部门之间的人事变动，不需要删除并重新添加账号，直接通过变更，将用户以及用户绑定的令牌按要求变更到新的组织机构下。

设置查询条件，查询出要变更的用户信息，选择要变更的操作对象，为选择的用户指定目标机构，然后根据用户绑定令牌的情况，选择变更的方式，点击“变更”按钮，完成用户及绑定令牌的变更。

## 9.8 权限审批

管理员审批用户提交的权限申请。

### 9.8.1 查看申请

当用户的申请数据比较多时，可以通过查询功能来查看特定用户的申请信息，在查询条件中根据实际情况输入单个或者组合的查询条件，点击“查询”，查询出用户申请信息，点击操作列的放大镜图标，弹出用户申请信息界面，可查看用户申请的详细信息。

提示：初始化的管理员可查看到系统中所有机构下的所有用户申请，其它普通的管理员只能查看到自己管理的所有组织机构下的用户申请。

### 9.8.2 批准申请

若用户提交的权限申请符合要求，管理员可通过点击操作列中的批准图标进行批准。详细操作步骤如下：

(1) 点击导航菜单中的“权限审批”，进入用户申请查询标签页，选择查询条件，进入申请列表标签页。

(2) 点击用户申请“操作”列中的“批准”图标，系统弹出批准界面。

(3) 填写备注信息，点击“确定”按钮，系统弹出批准成功的提示信息。

提示：若对查询出的已提交的申请进行批量批准操作，则可在“操作对象”选择“本次查询的所有记录”，然后执行批量批准的操作。

### 9.8.3 驳回申请

若用户提交的权限申请没有达到要求，管理员可通过点击操作列中的驳回图标进行驳回。详细操作步骤如下：

(1) 点击导航菜单中的“权限审批”，进入用户申请查询标签页，选择查询条件，进入申请列表标签页。

(2) 点击用户申请“操作”列中的“驳回”图标，弹出驳回弹出框提示，点击“是”驳回成功，点击“否”不驳回。

提示：若对查询出的已提交的申请进行批量驳回操作，则可在“操作对象”选择“本次查询的所有记录”，然后执行批量驳回的操作。

### 9.8.4 拒绝申请

管理员审核时，用户提交的申请信息不符合要求的，管理员可通过点击操作列中的拒绝图标进行拒绝用户提交的申请。详细操作步骤如下：

(1) 点击导航菜单中的“权限审批”，进入用户申请查询标签页，选择查询条件，进入申请列表标签页。

(2) 点击用户申请“操作”列中的“拒绝”图标，系统弹出拒绝申请界面。

(3) 填写拒绝原因，点击“确定”按钮，系统弹出拒绝审核成功的提示信息。

提示：若对查询出的已提交的申请不符合要求的，需要进行批量拒绝操作，则可在“操作对象”选择“本次查询的所有记录”，然后执行批量拒绝的操作。

## 第10章 用户组管理

该模块主要处理与用户组相关的各种操作，例如查看用户组、添加用户组、绑定/解绑用户、绑定/解绑认证代理、编辑用户组、启用/禁用用户组、删除用户组等。

### 10.1 添加用户组

拥有添加用户组权限的管理员才可以添加用户组，具体操作步骤如下所示：

(1) 点击页面上方导航栏中的“用户组管理”，选择“添加用户组”，进入添加用户组页面。

(2) 在添加页面输入用户组信息，页面上带有星号\*标识项为必填项，不允许为空，添加项的输入要求如下：

**用户组名称：**输入创建的用户组名称。

**描述：**在输入框中输入 0-255 字符长度的字符内容。

(3) 点击“保存”按钮，用户组添加成功。

### 10.2 用户组列表

#### 10.2.1 查看用户组

当用户组的数量比较多时，可以通过查询功能来查看特定的用户组信息，在查询条件中根据实际情况输入单个或者组合的查询条件，点击“查询”，查询出用户组信息，点击用户组名称超链接，弹出用户组信息界面，可查看用户组的详细信息和绑定用户、认证代理的信息。

#### 10.2.2 编辑用户组

若要修改用户组的信息，点击用户组列表操作列中“编辑”图标，进入编辑界面，修改信息后，点击“保存”按钮。

#### 10.2.3 启用/禁用用户组

用户组默认为“启用”状态，可通过点击“操作”列的“启用/禁用”图标更改用户组状态。

## 10.2.4 绑定用户

在用户组列表中，通过点击操作列中的绑定用户图标进行绑定用户。详细的操作步骤如下：

（1）点击页面上方导航栏中的“用户组管理”，选择“用户组列表”，进入用户组列表界面。

（2）点击用户组“操作”列中的“绑定用户”图标，系统弹出绑定用户界面。

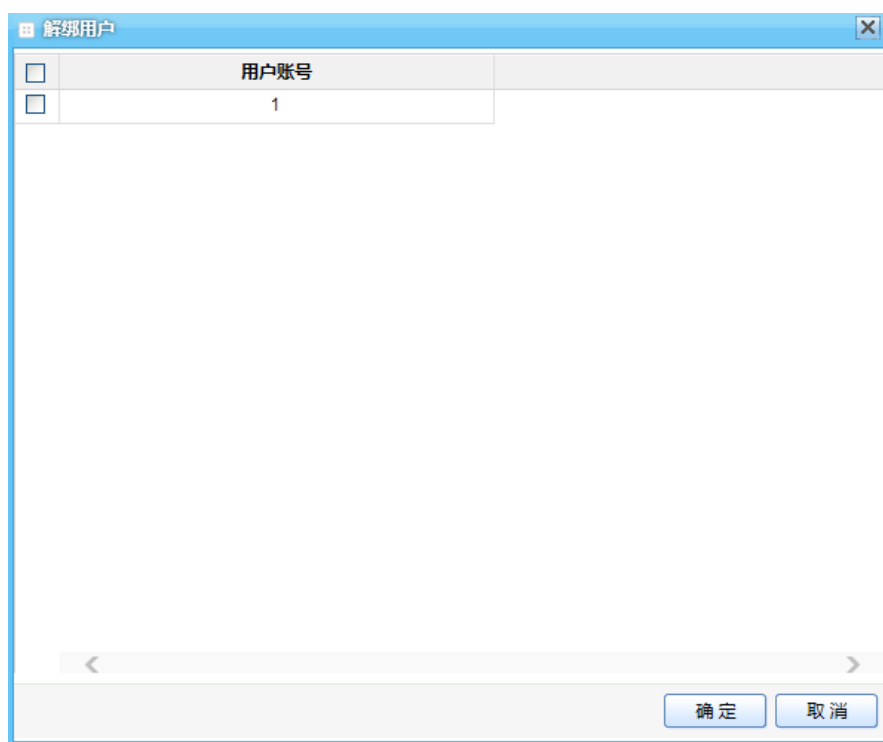
（3）设置查询条件，查询到要绑定的用户，勾选前面的复选框，然后点击界面中的“确定”按钮，系统弹出确认绑定的提示信息，选择是进行绑定关系。

## 10.2.5 解绑用户

当用户组绑定了用户后，在用户组的“操作”列中会出现“解绑用户”的图标，可实现用户与用户组的快速解绑，具体操作步骤如下：

（1）点击页面上方导航栏中的“用户组管理”，选择“用户组列表”，进入用户组列表界面。

（2）用户已绑定了用户组时，点击用户“操作”列中的“解绑用户”图标，系统弹出解绑用户界面，如图表 12 所示：



图表 15 解绑用户界面

界面上列出当前用户组绑定的所有用户信息，选择要解除绑定的用户，点击“确定”按钮，系统弹出确认解除的提示信息，选择是则解除绑定关系。

提示：只有绑定了用户的用户组操作列中才会出现解绑用户的图标。

## 10.2.6 绑定认证代理

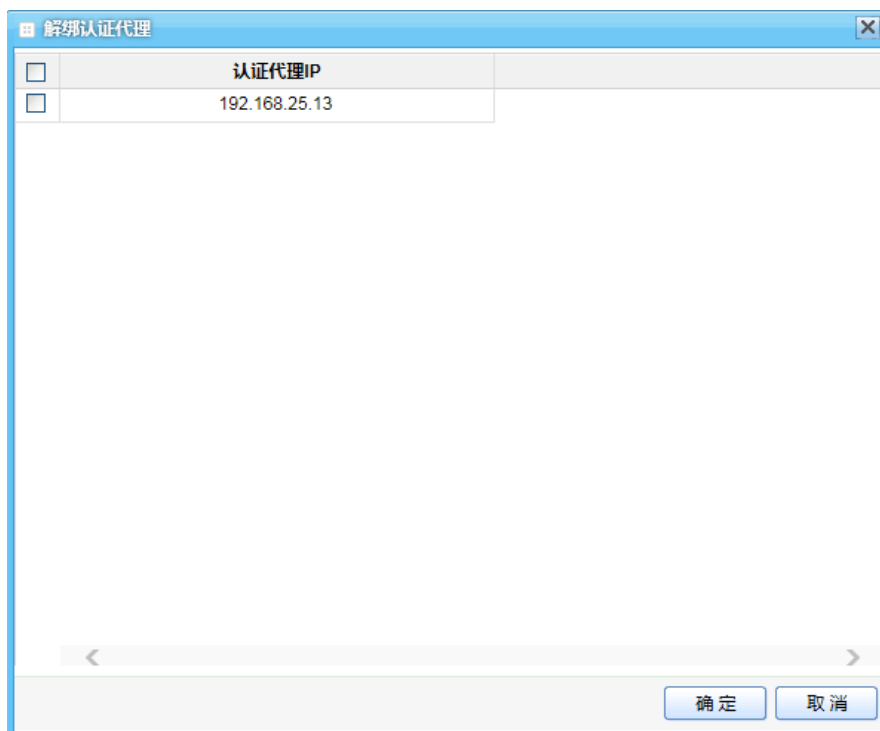
在用户组列表中，通过点击操作列中的绑定认证代理图标进行绑定认证代理。详细的操作步骤如下：

- (1) 点击页面上方导航栏中的“用户组管理”，选择“用户组列表”，进入用户组列表界面。
- (2) 点击用户组“操作”列中的“绑定认证代理”图标，系统弹出绑定认证代理界面。
- (3) 设置查询条件，查询到要绑定的认证代理，勾选前面的复选框，然后点击界面上的“确定”按钮，系统弹出确认绑定的提示信息，选择是进行绑定关系。

## 10.2.7 解绑认证代理

当用户组绑定了认证代理后，在用户组的“操作”列中会出现“解绑认证代理”的图标，可实现用户组与认证代理的快速解绑，具体操作步骤如下：

- (1) 点击页面上方导航栏中的“用户组管理”，选择“用户组列表”，进入用户列表界面。
- (2) 用户组已绑定了认证代理时，点击用户“操作”列中的“解绑认证代理”图标，系统弹出解绑认证代理界面，如图表 12 所示：



图表 16 解绑认证代理界面

界面上列出当前用户组绑定的所有认证代理信息，选择要解除绑定的认证代理，点击“确定”按钮，系统弹出确认解除的提示信息，选择是则解除绑定关系。

提示：只有绑定了认证代理的用户组操作列中才会出现解绑认证代理的图标。

### 10.2.8 删除用户组

当用户组被禁用、用户组不再使用时，可通过删除来删除列表中的用户组信息，具体操作步骤如下：

- （1）点击页面上方导航栏中的“用户组管理”，选择“用户组列表”，进入用户组列表界面。
- （2）在用户组列表界面设置查询条件，点击“查询”按钮，查询到要删除的用户组。
- （3）若查询出的用户组不是全部要删除，需在要删除的用户组前复选框中勾选上。
- （4）在“用户组列表”界面点击“删除”按钮，进行删除。

提示：删除用户组之前，该用户组内不能存在绑定的用户和认证代理，如果存在，需要先解除绑定关系，才能删除成功，否则不能删除。

## 第11章 令牌管理

令牌管理是 OTP Server 系统的一个重要组成部分，用户进行身份认证时需要使用自己的令牌生成动态口令，才能通过认证。

令牌管理包括令牌列表、令牌导入、令牌分配、令牌同步、批量查询和手机令牌分发等几个部分，下面将针对每个子模块进行详细的介绍。

### 11.1 令牌导入

管理中心安装完成以后，需要将令牌信息导入到管理中心的数据库中，才能将软件系统和令牌结合起来，提供身份认证功能。

管理中心支持的令牌文件有：Tnk、PSKC、Xml、Dat 格式令牌文件，其中 Dat、Xml 文件格式，在初始化“附加模块”勾选了“多厂商”，才显示的两种令牌文件格式。具体的操作步骤如下：

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌导入”，进入令牌导入页面。

(2) 页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**导入至组织机构：**选择令牌要导入到的组织机构，单选。

**令牌文件格式：**支持 Tnk、PSKC、Dat 和 Xml，其中 Dat、Xml 文件格式，在初始化“附加模块”勾选了“多厂商”，才显示的两种令牌文件格式。

**令牌文件：**上传.tnk、PKSC、.xml 和.dat 格式的令牌文件，且该文件的客户标识应和系统中在用的授权类型的客户标识一致，否则提示导入失败。

**令牌所属厂商：**根据导入的令牌文件，选择对应的厂商。在初始化“附加模块”勾选了“多厂商”，才显示“令牌所属厂商”。

**启用令牌：**选择是，则导入的令牌状态为启用状态，选择否，导入的令牌为禁用状态。

提示：点击界面上的重置按钮，则清空界面上所填写的信息。

(3) 选择好界面上各字段内容后，点击“导入令牌”按钮，系统提示导入成功。

提示：

1、如果导入的令牌文件是 OTP Server 密钥管理系统提供的令牌文件，需要初始化系统时，在“附加模块”

选择“加密机”，并在管理中心→配置管理→加密机配置，填写对应的加密机信息。否则，导入时系统提示“令牌导入失败，种子密钥是经过加密的，需要有加密机的支持！”

2、多厂商令牌不支持标准 Radius 协议中除 PAP 外其它协议。

3、如果在系统初始化之前，修改“vendorconf.properties”配置文件，开启了“是否校验令牌种子头信息厂商编号”，那么，在导入多厂商令牌文件时，必须选择对应的令牌所属的厂商，否则，导入失败，系统给予相应的错误提示。vendorconf.properties 路径：

../otpservice/otpwebsevice/tomcat/webapps/otpcenter/WEB-INF/conf

4、令牌导入的数量受系统在用的授权类型限制。授权类型为评估授权，导入的令牌最大总量为 10；授权类型为企业授权，导入的令牌最大数量为 5 万个；授权类型为高级授权，导入的令牌最大数量将不受限制。

## 11.2 令牌列表

### 11.2.1 查看令牌

查看令牌是令牌管理中的一项常用功能，可根据不同的令牌信息查询指定的某个令牌或某些令牌。具体的操作步骤如下：

提示：查询条件不设置任何内容时，显示当前登录管理员权限下的所有令牌信息。

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。

(2) 在“令牌查询”标签页，可设置单个查询条件或者组合的查询条件，点击“查询”按钮。

(3) 系统由“令牌查询”标签页跳转到“令牌列表”标签页，列出符合查询条件的令牌信息。点击令牌号的超链接，弹出令牌的详细信息。

提示：在令牌详细信息界面的绑定用户标签页，可点击用户名称的超链接去查看令牌所绑定的用户信息。

### 11.2.2 启用/停用令牌

启用/停用令牌的操作步骤如下：

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。

(2) 设置查询条件，点击“查询”按钮，查询出要启用/停用的令牌号。

(3) 操作对象选择“本页选中的记录”，操作选择“启用/停用”，在本页选中要启用/停用的令牌，点击“执行”按钮，对所选择的令牌进行“启用/停用”操作。



操作对象选择“本次查询所有记录”，操作选择“启用/停用”，点击“执行”按钮，对本次查询出的所有令牌进行“启用/停用”操作。

### 11.2.3 锁定/解锁令牌

为了防止他人或各种网络攻击利用令牌进行损害用户利益的操作，当令牌认证的错误次数超过了允许重试的最大次数时，令牌将自动锁定登录。

锁定/解锁令牌的操作步骤如下：

- (1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。
- (2) 设置查询条件，点击“查询”按钮，查询出要锁定/解锁的令牌号。
- (3) 操作对象选择“本页选中的记录”，操作选择“锁定/解锁”，在本页选中要锁定/解锁的令牌，点击“执行”按钮，对所选择的令牌进行“锁定/解锁”操作。

操作对象选择“本次查询所有记录”，操作选择“锁定/解锁”，点击“执行”按钮，对本次查询出的所有令牌进行“锁定/解锁”操作。

### 11.2.4 挂失/解挂令牌

当令牌遗失或被盗时，为了防止别人利用丢失的令牌进行损害用户利益的操作，用户可以通过令牌挂失来保护自己的利益。

挂失/解挂令牌的操作步骤如下：

- (1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。
- (2) 设置查询条件，点击“查询”按钮，查询出要挂失/解挂的令牌号。
- (3) 操作对象选择“本页选中的记录”，操作选择“挂失/解挂”，在本页选中要挂失/解挂的令牌，点击“执行”按钮，对所选择的令牌进行“挂失/解挂”操作。

操作对象选择“本次查询所有记录”，操作选择“挂失/解挂”，点击“执行”按钮，对本次查询出的所有令牌进行“挂失/解挂”操作。

### 11.2.5 作废令牌

当确认令牌已经损坏需要返厂维修时，可以将其作废，作废之后该令牌还存在数据库中，但无法对其进行除删除操作以外的其它操作，且该操作是单项不可恢复的。

作废令牌的操作步骤如下：

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。

(2) 设置查询条件，点击“查询”按钮，查询出要作废的令牌号。

(3) 操作对象选择“本页选中的记录”，操作选择“作废”，在本页选中要作废的令牌，点击“执行”按钮，对所选择的令牌进行“作废”操作。

操作对象选择“本次查询所有记录”，操作选择“作废”，点击“执行”按钮，对本次查询出的所有令牌进行“作废”操作

提示：作废后的令牌将不能再恢复，如果要接着使用，则必须删除掉该令牌，并重新进行导入，但需激活的 c300 令牌作废后再导入将无法正常使用。

### 11.2.6 令牌认证

认证测试是指可以在管理中心中对指定的令牌进行认证测试，验证该令牌的有效性。具体的操作步骤如下：

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。

(2) 设置查询条件，点击“查询”按钮，查询出相应的令牌，点击要认证的令牌后“操作”列中的“认证”图标，弹出令牌认证对话框。

(3) 在动态口令框中输入正确的口令，点击“确定”按钮进行认证。

c300 类型令牌认证测试界面上多出个“获取挑战值”按钮。其口令测试分两种，一种是时间型的口令，直接将获取到的口令输入动态口令框中认证；另一种是挑战应答型口令的认证，点击界面上的“获取挑战值”按钮，按钮后出现挑战值，将该值输入到令牌中获取应答值，将应答值输入到认证界面上的“动态口令”输入框中，点击“确定”按钮进行验证应答测试。

### 11.2.7 令牌同步

同步令牌是指当令牌处于异步状态或超异步状态时，通过同步操作，将其恢复到同步状态。只有处于同步状态的令牌才能用于身份认证。具体的操作步骤如下：

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。

(2) 设置查询条件，点击“查询”按钮，查询出相应的令牌，点击要同步的令牌后“操作”列中的令牌同步图标，弹出令牌同步对话框

(3) 除短信令牌外的其它类型令牌，同步时在“动态口令”输入框中输入令牌生成的第一个动态口令，在“下一次动态口令”输入框中输入令牌连续生成的下一个动态口令。

(3) 点击“同步”按钮进行同步操作。

提示：如果令牌处于超异步状态，则需要修改同步窗口的默认值，根据令牌的具体情况，增大同步窗口的值，直到同步成功为止。

## 11.2.8 设置应急口令

当用户令牌忘记携带时，可设置个应急口令以便于能登录到身份认证的系统中，具体的操作步骤为：

提示：1) 设置的应急口令有个时效限制，在设置的时间内允许使用应急口令登录，超过设置的时间后需重新申请。

2) 用户绑定的令牌设置了应急口令后，若用户在应急口令时效内使用了绑定的令牌动态口令登录后，设置的应急口令便失效。

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。

(2) 在“令牌号”输入框中输入要设置应急口令的令牌号，然后点击“查询”按钮，找到该令牌。

(3) 点击要设置应急口令的令牌序列号后面的“设置应急口令”图标，弹出设置应急口令的对话框。

(4) 页面上带有星号\*标识项为必填项，不允许为空，各项的输入要求如下：

**令牌：**该字段显示所选的令牌号，不允许手动修改。

**认证方式：**该字段的下拉选项包括应急口令认证和动态口令认证。选择“应急口令”认证，为令牌设置应急口令，选择“动态口令”认证方式，用户登录认证时启用动态口令认证。

提示：该字段的动态口令认证方式可实现对启用应急口令令牌绑定的用户，强制其停用应急口令。

**应急口令：**只有认证方式选择“应急口令”时才出现该项，输入用户的应急口令。

提示：设置的应急口令长度需和所选令牌的动态口令长度一致。

**确认应急口令：**只有认证方式选择“应急口令”时才出现该项，再次输入用户应急口令。

**应急口令过期时间：**默认显示的时间为“配置管理->令牌配置->应急口令”中设置的应急口令默认有效时长。

提示：应急口令过期时间不能超过“配置管理->令牌配置->应急口令”中设置的应急口令最大有效时长。

(4) 按要求设置了应急口令后，点击界面上的“确定”按钮，保存设置，应急口令设置完成。

### 11.2.9 软件令牌分发

具体操作步骤如下：

- (1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。
- (2) 在查询条件中物理类型一项选择“软件令牌”，点击“查询”按钮，进入令牌列表标签页。
- (3) 点击要分发的软件令牌后面“操作”列中的“软件令牌分发”图标，弹出软件令牌分发对话框，对话框中有“软件令牌分发”和“绑定管理员/用户”两个标签页，默认显示的是“软件令牌分发”标签页。
- (4) 界面上的各项内容的含义如下：

**令牌号：**该字段不允许编辑，显示的是所选的令牌号。

**软件令牌的 PIN 码：**此 PIN 码用于软件令牌生成动态口令时输入。PIN 码产生有两种方式：“默认”和“手动输入”。选择“默认”，则 PIN 码为“配置管理->令牌配置->软件令牌”配置界面上设置的默认 PIN 码；选择手动输入，在界面下方出现“PIN 码”项，可手动设置 PIN 码。

**分发结果：**令牌未被用户绑定，分发结果只有“页面下载”一项，若令牌被用户绑定，分发结果界面有“页面下载”和“邮件发送”两项。选择页面下载，分发生成的.stf 文件在页面上直接下载，选择邮件发送，分发生成的.stf 文件通过邮件方式发送给用户。

提示：选择邮件方式发送给用户，需要先在配置管理->系统公共配置->邮件服务器中进行邮件服务器配置，并且绑定的用户需要填写邮箱信息，否则无法收到邮件。

- (4) 按各项要求，设置分发条件后，点击界面中的“确定”按钮，显示分发结果。

### 11.2.10 取消分配

如果导入到系统中的令牌已经分配到企业的某个组织机构下或进入系统后被分配到企业的某个组织机构后，想对已分配的令牌重新分配时，可采用取消分配操作，让令牌回归到企业中，然后再重新分配，具体操作如下：

- (1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。
- (2) 设置查询条件，点击“查询”按钮，查询到要取消分配的令牌信息。
- (3) 操作对象选择“本页选中的记录”，操作选择“取消分配”，选中要取消的令牌，点击“执行”按钮，对所选令牌执行取消分配操作。

操作对象选择“本次查询处的所有记录”，操作选择“取消分配”，点击“执行”按钮，对本次查询出的所有令牌执行取消分配操作。

### 11.2.11 删除令牌

当令牌作废后不再使用时，可以将其删除，具体的操作步骤如下：

提示：列表中的令牌只有处于作废状态的令牌才允许删除，其它状态下的令牌不允许删除。

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌列表”，进入令牌列表的令牌查询标签页。

(2) 设置查询条件，点击“查询”按钮，查询到要删除的令牌信息。

(3) 操作对象选择“本页选中的记录”，操作选择“删除”，选中要删除的令牌，点击“执行”按钮，删除所选的令牌。

操作对象选择“本次查询处的所有记录”，操作选择“删除”，点击“执行”按钮，对本次查询出的所有令牌执行删除操作。

## 11.3 令牌分配

导入进系统的令牌根据实际情况进行令牌分配，分配到企业下不同的子机构中，具体操作步骤如下：

(1) 点击页面上方导航栏中的“令牌管理”，选择“令牌分配”，进入令牌分配页面下的选择令牌标签页。

(2) 在选择令牌标签页，设置查询条件，点击“查询”按钮，查询出要分配的令牌。

提示：已与用户绑定的令牌，将不会出现在该令牌中。

(3) 操作对象选择“本页选中的记录”，勾选要分配的令牌，将会对选择的令牌进行分配操作，点击“下一步”按钮进入到“令牌分配”标签页。

操作对象选择“本次查询的所有记录”，将对查询出的所有令牌进行分配操作，点击“下一步”按钮进入到“令牌分配”标签页。

(4) 在“令牌分配”标签页，选择令牌要分配到的组织机构，然后点击“分配”按钮，令牌分配标签页显示分配到的组织机构信息和被分配的令牌数，还显示了分配的结果信息，成功的个数和失败的个数，点击界面中的“确定”按钮，完成令牌分配。

提示：若想继续分配令牌，可点击“继续分配”按钮，回至前面页面进行继续分配。

## 11.4 令牌同步

同步令牌是指当令牌处于异步状态或超异步状态时，通过同步操作，将其恢复到同步状态。只有处于同步状态的令牌才能用于身份认证。具体的操作步骤如下：

- (1) 点击页面上方导航栏中的“令牌管理”，选择“令牌同步”，进入令牌同步页面。
- (2) 在“令牌号”输入框中输入令牌号，在“动态口令”输入框中输入令牌生成的第一个动态口令，在“下一次动态口令”输入框中输入令牌连续生成的下一个动态口令。
- (3) 点击“同步”按钮进行同步操作。

提示：如果令牌处于超异步状态，则需要修改同步窗口的默认值，根据令牌的具体情况，增大同步窗口的值，直到同步成功为止。

## 11.5 批量查询

当用户对一批令牌进行操作，而这一批令牌散乱分布在令牌列表中，为了方便操作，可通过上传“.txt”文件对令牌进行批量查询，然后对查询出的令牌进行进一步的操作，具体操作步骤如下：

- (1) 点击页面上方导航栏中的“令牌管理”，选择“批量查询”，进入批量查询页面。
- (2) 点击“选择”按钮，上传 txt 格式批量查询文件。
- (3) 点击“批量查询”按钮，进入到令牌列表界面，查询出指定的令牌。

## 11.6 手机令牌分发

### 11.6.1 手机令牌分发查看

当手机令牌的数量比较多时，可以通过查询功能来查看特定令牌信息，在查询条件中根据实际情况输入单个或者组合的查询条件，点击“查询”，查询出手机令牌信息。

### 11.6.2 设定标识码

设定标识码是将手机令牌与手机进行一次绑定操作，具体操作步骤如下：

- (1) 点击页面上方导航栏中的“令牌管理”，选择“手机令牌分发”，进入手机令牌分发页面。
- (2) 点击手机令牌操作列中的“设置标识码”图标，切换到手机令牌标识码界面。



(3) 令牌号字段不允许编辑，显示的是所选择的令牌号，在“标识码”输入框中输入所选手机令牌的标识码，点击“设定”按钮，令牌与手机绑定成功。

### 11.6.3 手机令牌分发

手机令牌分发有两种方式，一种是二维码分发，一种是离线分发。如“配置管理→令牌管理→手机令牌”开启手机令牌推送策略，那么，手机令牌二维码分发成功的手机令牌就会有推送功能。

**二维码分发具体操作步骤如下：**

(1) 点击页面上方导航栏中的“令牌管理”，选择“手机令牌分发”，进入手机令牌分发页面。

(2) 点击需分发的手机令牌“操作”列中的“分发”图标，切换到手机令牌分发界面，页面有二维码和离线分发两个标签页，默认显示的是二维码。

(3) 界面上的各项内容的含义如下：

**用户名：**若令牌被用户绑定，则会显示该字段，不可编辑，若令牌未被绑定，则不显示该字段。

**令牌号：**该字段不允许编辑，显示的是所选的令牌号。

**手机令牌标识码：**该字段显示的为手机令牌标识码，可在此页面直接填写，也可如 11.6.2 节描述，单独分发标识码。

**分发方式：**勾选在线分发，令牌生成在线激活二维码。在线分发更安全，但是要求用来激活令牌的手机必须能联网。勾选离线分发，进行离线分发令牌生成离线激活二维码，此时激活手机不需要联网。

**是否需要激活密码：**用于激活令牌时使用，激活密码的来源有三种：随机、默认和手动输入。选择“随机”，激活密码系统给随机分配，选择“默认”，激活密码使用“配置管理->令牌配置->手机令牌”中设置的默认激活密码，选择“手动输入”，激活密码采用手动设置的值。

(4) 按各项要求，设置分发条件后，点击界面上的“分发”按钮，生成二维码。

(5) 如开启手机令牌推送策略，手机令牌激活成功后，手机令牌分发列表的“设备类型”列，显示 android 手机图标或者 Iphone 手机图标。

**离线分发具体操作步骤如下：**

(1) 点击页面上方导航栏中的“令牌管理”，选择“手机令牌分发”，进入手机令牌分发页面。

(2) 点击需分发的手机令牌“操作”列中的“分发”图标，切换到手机令牌分发界面，默认显示的是二维码，切换到离线分发。

(3) 界面上的各项内容的含义如下：

**用户名：**若令牌被用户绑定，则会显示该字段，不可编辑，若令牌未被绑定，则不显示该字段。

**令牌号：**该字段不允许编辑，显示的是所选的令牌号。

**手机令牌标识码：**该字段显示的为手机令牌标识码，可在此页面直接填写，也可如 11.6.2 节描述，单独进行分发标识码。

**激活密码：**用于激活令牌时使用，激活密码的来源有三种：随机、默认和手动输入。选择“随机”，在激活密码系统给随机分配，选择“默认”，激活密码使用“配置管理->令牌配置->手机令牌”中设置的默认激活密码，选择“手动输入”，激活密码采用手动设置的值。

(4) 按各项要求，设置在线分发条件后，点击界面上的“分发”按钮，显示分发结果。

## 11.6.4 重置手机令牌

手机令牌分发成功后，若想重新分发，可点击“重置”按钮，恢复到初始状态，再重新分发。

提示：如果手机令牌是在“开启手机令牌推送策略”的情况下，进行分发成功的，那么，点击该“重置”图标，只是把手机令牌的激活状态进行了改变，推送关系并没有改变。

## 11.6.5 重置设备

开启手机令牌推送策略，分发成功的手机令牌，若想重置推送关系，可点击“操作”列的“重置设备”图标，“设备类型”列的图标就会消失，手机令牌的推送关系取消。但是，手机令牌的激活状态不变。

## 11.6.6 批量重置

若想对查询出的已分发成功的手机令牌进行批量重置操作，则可勾选行首的复选框，然后点击“批量重置”按钮，进行批量重置操作。



## 第12章 厂商管理

在厂商管理模块主要是解决除了能导入飞天的令牌外，其它的厂商令牌也可以导入；通过添加厂商提供的动态库和厂商信息，把某厂商的令牌导入到 OTP Server 管理中心后，可以对某厂商的令牌进行相应的操作。有关厂商信息的配置，请参考《OTP Server V4.8 多厂商配置文档》。

提示：在系统初始化的“附加模块”，选择了“多厂商集成”，管理中心才会显示该功能。

### 12.1 添加厂商

添加厂商信息具体操作步骤如下所示：

- （1）点击页面上方导航栏中的“厂商管理”，选择“厂商管理”下的“添加厂商”，进入添加厂商页面。
- （2）页面上带有星号\*标识项为必填项，不允许为空，各添加项的输入要求如下：

**厂商编号：**必填项，唯一值，由 4-32 个数字、字母和下划线组成。

**厂商名称：**必填项，唯一值，长度要求 1-64 位字符。

**描述：**非必填项，长度要求不能超过 255 个字符。

### 12.2 厂商列表

主要用来展示厂商信息，在列表操作项还包括了编辑厂商信息功能和下载厂商证书功能。

#### 12.2.1 查看厂商信息

查看厂商信息是厂商管理管理中的一项常用功能，可根据不同的厂商名称或厂商编号查询相关厂商信息。具体的操作步骤如下：

提示：查询条件不设置任何内容时，显示当前登录管理员权限下的所有厂商信息。

- （1）点击页面上方导航栏中的“厂商管理”，选择“厂商列表”，进入厂商列表页面。
- （2）根据查询条件，输入相应的厂商编号、厂商名称信息，点击“查询”按钮，进行查询。

提示：在查出的厂商信息结果中“厂商编号”列的数据带有超链接，可点击查看厂商的详细信息。

## 12.2.2 下载证书

从管理中心下载相应的厂商证书，主要是在种子管理系统中生产对应厂商的种子文件。

下载相应的厂商证书的操作步骤如下：

（1）点击页面上方导航栏中的“厂商管理”，选择“厂商列表”，进入厂商列表信息页面，显示当前登录管理员权限下的所有厂商信息。

（2）在厂商列表信息的“操作”列中显示证书下载功能图标，可点击图标进行证书下载。

## 12.2.3 编辑厂商信息

如果要修改厂商的信息，在厂商列表页面，点击厂商列表的“操作”列中的“编辑”图标，打开编辑界面修改信息，点击“保存”按钮，修改成功。

## 12.2.4 删除厂商信息

若添加的厂商不再使用，可选择删除该厂商。进入厂商列表，选中要删除的厂商，点击界面上的“删除”按钮，确认后删除成功。

## 第13章 设备管理

### 13.1 设备管理

OTP Server4.8 集成 FIDO 身份认证的功能，主要处理与 FIDO 设备相关的各种操作，例如查看 FIDO 设备信息、FIDO 设备日志信息、添加受保护地址等。用户使用 FIDO 登录受保护地址，OTP Server 通过用户信息和 U2F 设备进行身份认证并作出响应。

提示：在系统初始化的“附加模块”，选择了“FIDO 认证”，管理中心才会显示该功能。

#### 13.1.1 受保护地址管理

##### 13.1.1.1 添加受保护地址

添加受保护地址步骤如下：

（1）点击页面上方导航栏中的“设备管理”，选择“设备管理→受保护地址管理→添加受保护地址”，进入添加受保护地址页面。

（2）页面上带有红色星号\*标识项为必填项，不允许为空，各字段的填写规则如下：

**受保护的地址：**必填项，长度为 10-128 个字符。

**描述：**在输入框中输入 0-255 字符长度的字符内容。

（3）点击“保存”按钮，受保护地址添加成功。

提示：受保护的地址是访问 FIDO 客户端的 URL 地址，URL 地址是截止到端口号，例如：<http://localhost:8080>

##### 13.1.1.2 受保护地址列表

受保护地址列表包括查看受保护地址、编辑受保护地址、删除受保护地址的操作。受保护地址指的是访问 FIDO 客户端的 URL 地址。

###### 13.1.1.2.1 编辑受保护地址信息

若要修改受保护地址的信息，在受保护地址列表页面点击操作列中的“编辑”图标，进入编辑界面，

修改信息后，点击“保存”按钮。

#### 13.1.1.2.2 删除受保护地址信息

当创建的受保护地址不再使用时，可以选择删除受保护地址。在管理中心删除受保护地址的具体操作步骤如下：

（1）点击页面上方导航栏中的“设备管理”，选择“设备管理”下的“受保护地址列表”，进入受保护地址列表页面。

（2）选择要删除的受保护地址前面的复选框，然后点击“删除”按钮，出现确认删除提示框，确认后删除。

### 13.1.2 FIDO 日志管理

管理 FIDO 设备信息和 FIDO 设备日志。

#### 13.1.2.1 FIDO 设备信息列表

FIDO 设备信息列表包括查询、查看 FIDO 设备详细信息、删除 FIDO 设备信息等操作。通过调用飞天 FIDO 接口，FIDO 设备注册的信息和 FIDO 设备认证的信息显示在设备信息列表。

##### 13.1.2.1.1 查看 FIDO 设备信息

当 FIDO 设备信息的数量比较多时，可以通过查询功能来查看特定 FIDO 设备的信息。输入要查询的内容，查询出符合条件的 FIDO 设备信息，在 FIDO 设备信息列表页面点击操作列中的“放大镜”图标，打开 FIDO 设备详细信息界面。

##### 13.1.2.1.2 删除 FIDO 设备信息

当 FIDO 设备不再使用时，可以选择删除对应的 FIDO 设备信息。在管理中心删除 FIDO 设备信息的具体操作步骤如下：

（1）点击页面上方导航栏中的“设备管理”，选择“设备管理”下的“FIDO 设备信息列表”，进入 FIDO 设备信息列表页面。

（2）选择要删除的 FIDO 设备信息前面的复选框，然后点击“删除”按钮，出现确认删除提示框，确认后删除。

### 13.1.2.2 FIDO 设备日志

FIDO 设备日志主要记录操作 FIDO 设备时的相关日志信息。

#### 13.1.2.2.1 查看 FIDO 设备信息

当 FIDO 设备日志的数量比较多时，可以通过查询功能来查看特定 FIDO 设备的日志信息。输入要查询的内容，查询出要查看的 FIDO 设备日志信息。

### 13.1.3 FIDO 配置管理

用于配置 FIDO 用户注册策略。

#### 13.1.3.1 FIDO 用户注册策略

“FIDO 用户注册时，如果用户不存在，是否新增用户”：选择“是”，在注册 FIDO 设备时，“用户管理→用户列表”不存在该用户也可以注册成功，注册成功的用户信息，就会体现在用户列表；选择“否”，“用户管理→用户列表”必须存在该用户才能注册成功，否则失败。

## 第14章 认证管理

### 14.1 认证服务器

#### 14.1.1 添加认证服务器

添加认证服务器具体操作步骤如下所示：

(1) 点击页面上方导航栏中的“认证管理”，选择“认证服务器”下的“添加认证服务器”，进入添加认证服务器页面。

(2) 页面上带有星号\*标识项为必填项，不允许为空，各添加项的输入要求如下：

**服务器名称：**在输入框中输入认证服务器的名称，允许输入 1-64 字符的内容。

**服务器 IP：**在输入框中输入认证服务器所在的 IP 地址。

**优先级：**选择认证服务器的优先级，有 3 种选项：高级、普通、低级。当认证代理选择多个认证服务器，认证时将优先使用优先级别高的认证服务器。

**授权类型：**显示当前系统所使用的授权类型。

**启用扩展 Radius 服务：**选择是，启用扩展 Radius 服务，选择否，禁用扩展 Radius 服务。

**扩展 Radius 认证端口：**在输入框中设置扩展 Radius 的认证端口，默认为 1915，也可以改为其它指定的端口。

提示：扩展 Radius 服务为启用状态时，才出现此设置项。

**扩展 Radius 同步端口：**输入框中设置扩展 Radius 的同步端口，默认为 1916，也可以改为其它指定的端口。

提示：扩展 Radius 服务为启用状态时，才出现此设置项。

**协议类型：**必选项，支持 UDP 协议（必选协议）、TCP 协议。

提示：扩展 Radius 服务为启用状态时，才出现此设置项。

**启用标准 Radius 服务：**选择是，启用标准 Radius 服务，选择否，禁用标准 Radius 服务。

**标准 Radius 认证端口：**在输入框中填写标准 Radius 认证的端口，默认为 1812，也可以改为其它指定的端口。

提示：当“启用标准 Radius 服务”选择是时，出现此设置项。

**启用 HTTP 服务：**选择是，启用 HTTP 服务，页面显示配置“HTTP 服务端口”信息，默认为 18080；选择否，不启用 HTTP 服务，页面不显示配置“HTTP 服务端口”信息。

**SOAP 服务端口：**在输入框中输入 SOAP 服务的端口，默认为 18081，可修改为其它指定的服务端口。

**WebService 名称：**在输入框中输入客户端访问的 Webservice 名称，默认为：otpservice。

**描述：**在输入框中输入当前认证服务器的描述信息。

(3) 按要求填写认证服务器信息，点击“保存”按钮，系统提示保存成功。

提示：添加的服务器数量受所使用的授权文件制约。使用评估授权，只允许添加一个认证服务器；使用企业授权，允许添加两个认证服务器；使用高级授权，添加的认证服务器不受限制，可以任意添加。

## 14.1.2 认证服务器列表

### 14.1.2.1 查看认证服务器

当认证服务器数量比较多时，可以通过查询功能来查看特定认证服务器的信息，设置查询条件，点击“查询”按钮，查询出指定的认证服务器，点击列表中“服务器 IP”超链接，可以查看到服务器的详细信息。

提示：认证服务器绑定了认证代理，在查看信息时也能链接到代理的详细页面。

### 14.1.2.2 编辑认证服务器

如果需要修改认证服务器信息，可以按照以下步骤进行操作：

(1) 点击页面上方导航栏中的“认证管理”，选择“认证服务器”下的“认证服务器列表”，进入认证服务器列表页面。

(2) 在“操作”列点击要编辑的认证服务器“编辑”图标，对认证服务器相关信息进行修改，修改项的要求和添加界面的一致，可参考添加界面的详细描述。

(3) 修改认证服务器信息之后，点击“保存”按钮，系统弹出修改成功的提示信息。



### 14.1.2.3 删除认证服务器

当创建的认证服务器不再使用时，可以选择删除，在管理中心中删除认证服务器的具体操作步骤如下：

（1）点击页面上方导航栏中的“认证管理”，选择“认证服务器”下的“认证服务器列表”，进入认证服务器列表页面。

（2）选择要删除的认证服务器前面的复选框，然后点击“删除”按钮，将出现确认删除提示框，点击“确定”按钮删除认证服务器。

提示：被认证代理选中绑定的认证服务器无法删除，需先解绑后才能删除。

## 14.2 认证代理

### 14.2.1 添加认证代理

添加认证代理具体操作步骤如下所示：

（1）点击页面上方导航栏中的“认证管理”，选择“认证代理”下的“添加认证代理”，进入添加认证代理页面。

（2）页面上带有星号\*标识项为必填项，不允许为空，各添加项的输入要求如下：

**认证代理名称：**在输入框中输入认证代理的名称。

**认证代理 IP：**在输入框中输入认证代理所在机器的 IP 地址。

**共享密钥：**在输入框中输入认证代理和认证服务器的共享密钥。

**服务器列表：**选择当前认证代理对应的认证服务器，允许多选。

**认证代理类型：**选择当前认证代理的代理类型，允许多选。

提示：1、Windows 登录保护认证代理和 Linux 登录保护认证代理，只能选择其一，不能同时被选中。

2、选择“普通认证代理”，页面自动显示“高级配置-（CISCO、VPN 配置项）”配置，挑战应答认证项选择是，该功能支持标准 Radius 认证协议的终端（VPN、CISCO），集成动态口令双因子认证模式。

**认证代理配置：**只有选择了“Windows 登录保护认证代理”或“Linux 登录保护认证代理”，才会出现该项。下拉选项中列出“认证代理配置列表”中的所有记录，选择适当的代理配置。

**登录保护认证代理宽限期：**只有选择了“Windows 登录保护认证代理”时，才会出现登录保护认证代理宽限期。在 Windows 登录保护代理端登录认证时，在宽限期内，可不需输入绑定令牌的动态口令登录。

**描述：** 在输入框中输入当前认证代理的描述信息。

(3) 按要求填写认证代理信息，点击“保存”按钮，系统提示保存成功。

## 14.2.2 认证代理列表

### 14.2.2.1 查看认证代理

当认证代理数量比较多时，可以通过查询功能来查看特定认证服务器的信息，输入想要查询的代理端 IP，点击“查询”按钮，查询出指定的认证代理，点击列表中“认证代理 IP”超链接，可以查看到认证代理的详细信息。

提示：认证代理绑定了认证服务器，在查看信息时也能链接到服务器的详细页面。

### 14.2.2.2 编辑认证代理

如果需要修改认证代理信息，可以按照以下步骤进行操作：

(1) 点击页面上方导航栏中的“认证管理”，选择“认证代理”下的“认证代理列表”，进入认证代理列表页面。

(2) 在“操作”列点击要编辑的认证代理“编辑”图标，对认证代理相关信息进行修改，修改项的要求和添加界面的一致，可参考添加界面的详细描述。

(3) 修改认证代理信息之后，点击“保存”按钮，系统弹出修改成功的提示信息。

### 14.2.2.3 下载代理配置文件

用户使用认证代理（如域代理和 IIS 代理）时，安装过程中需提供对应的代理配置文件，代理配置文件由管理员通过管理中心生成。在代理列表中选择需要生成代理配置文件的记录，点击“操作”列中的“下载代理配置文件”图标，指定保存路径保存。

### 14.2.2.4 添加认证服务器

为代理指定认证服务器，可以通过在添加或编辑界面直接选择，若添加时未选择，也可以通过“操作”列中的“添加认证服务器”来实现，具体步骤如下：

(1) 点击页面上方导航栏中的“认证管理”，选择“认证代理”下的“认证代理列表”，进入认证代理列表页面。

(2) 在“操作”列点击要添加认证服务器的认证代理的“添加认证服务器”图标，弹出认证服务器对

话框。

(3) 认证服务器对话框中列出认证服务器列表中的所有记录，选择指定的服务器，可多选，点击“确定”按钮，为认证代理添加服务器成功。

#### 14.2.2.5 解除代理服务器

当代理选择了认证服务器后，若解除代理与认证服务器之间的绑定关系，可以在编辑界面的服务器列表中删除掉要解除的服务器 IP，也可以直接在列表的操作列中执行解除代理服务器操作，步骤如下：

(1) 点击页面上方导航栏中的“认证管理”，选择“认证代理”下的“认证代理列表”，进入认证代理列表页面。

(2) 在“操作”列点击要解除认证服务器的认证代理的“解除认证服务器”图标，代理只绑定了一个认证服务器，系统弹出确认解除的提示信息，选择“是”解除代理和服务器的绑定关系。

代理绑定了多个服务器，系统弹出认证服务器对话框，列出代理绑定的所有认证服务器，选择要解除的记录，点击“确定”解除代理与选择的认证服务器之间的绑定关系。

#### 14.2.2.6 删除认证代理

当创建的认证代理不再使用时，可以选择删除，在管理中心中删除认证代理的具体操作步骤如下：

(1) 点击页面上方导航栏中的“认证管理”，选择“认证代理”下的“认证代理列表”，进入认证代理列表页面。

(2) 选择要删除的认证代理前面的复选框，然后点击“删除”按钮，将出现确认删除提示框，点击“确定”按钮删除认证代理。

提示：绑定了认证服务器的认证代理无法删除，需先解绑后再删除

### 14.3 认证代理配置

#### 14.3.1 添加认证代理配置

添加认证代理配置具体操作步骤如下所示：

(1) 点击页面上方导航栏中的“认证管理”，选择“认证代理配置”下的“添加认证代理配置”，进入添加认证代理配置页面。

(2) 页面上带有星号\*标识项为必填项，不允许为空，各添加项的输入要求如下：

**配置名称：**在输入框中输入认证代理的配置名称。

**代理配置类型：**在登录保护代理配置类型的下拉选择项中选择指定的配置类型，若是 windows 操作系统的代理端，选择“Windows 登录保护代理”，若代理端为 Linux 操作系统，则选择“Linux 登录保护代理”。

**用户名格式：**选择当前代理配置的用户名格式，共三种格式：user、user@IP、user@domain。

**本地登录：**只有代理配置类型为 Windows 登录保护代理才出现此项，用来选择当前代理配置的本地登录保护类型，共四种类型：不保护、保护本地账号、保护域账号、保护本地账号和域账号。

提示：不保护，则对代理端不进行本地登录保护；保护本地账号，对代理端的本地账号本地登录的时候进行保护；保护域账号，对代理端域账号的本地登录进行保护；保护本地账号和域账号，对代理端本地账号和域账号的本地登录进行保护。

**远程登录：**只有代理配置类型为 Windows 登录保护代理才出现此项，用来选择当前代理配置的远程登录保护类型，共四种类型：不保护、保护本地账号、保护域账号、保护本地账号和域账号。

提示：不保护，则对代理端不进行远程登录保护；保护本地账号，对代理端的本地账号远程登录的时候进行保护；保护域账号，对代理端域账号的远程登录进行保护；保护本地账号和域账号，对代理端本地账号和域账号的远程登录进行保护。

**UAC 登录：**只有代理配置类型为 Windows 登录保护代理才出现此项，用来选择当前代理配置的 UAC 登录保护类型，共四种类型：不保护、保护本地账号、保护域账号、保护本地账号和域账号。

提示：不保护，则对代理端不进行 UAC 登录保护；保护本地账号，对代理端的本地账号进行 UAC 保护；保护域账号，对代理端域账号进行 UAC 保护；保护本地账号和域账号，对代理端本地账号和域账号进行 UAC 保护。

UAC 保护只存在于 vista 之后的 Windows 操作系统。

**是否允许未绑定令牌的用户登录：**选择是，允许未绑定令牌用户登录，选择否，则不允许未绑定令牌的用户登录。

**描述：**在输入框中输入认证代理配置的描述信息。

(3) 按要求填写认证代理配置信息，点击“保存”按钮，系统提示保存成功。

## 14.3.2 认证代理配置列表

### 14.3.2.1 编辑认证代理配置

如果需要修改认证代理配置信息，点击代理配置列表操作列中的“编辑”图标，修改信息后，点击“保存”按钮，修改成功。

### 14.3.2.2 删除认证代理配置

当创建的认证代理配置不再使用时，可以选择删除，在代理配置列表中选中要删除的记录，点击“删除”按钮，删除代理配置。

提示：已被代理使用的代理配置不允许被删除，若要删除需先取消代理处的选择。

## 14.4 后端认证

### 14.4.1 添加后端认证

添加后端认证具体操作步骤如下所示：

（1）点击页面上方导航栏中的“认证管理”，选择“后端认证”下的“添加后端认证”，进入添加后端认证页面。

（2）页面上带有星号\*标识项为必填项，不允许为空，各添加项的输入要求如下：

**配置名称：**在输入框中输入后端认证配置名称，不允许重复。

**后端认证类型：**选择后端认证类型，选择 Radius，则当前的后端认证服务器为 Radius 后端认证，选择 AD 则该服务器为 AD 后端认证。

**后端服务器 IP：**在输入框中输入后端认证服务器的 IP 地址。

**备后端服务器 IP：**输入备用的后端认证服务器 IP 地址，不允许与主服务器 IP 地址重复。

提示：主备后端认证服务器使用的其它参数必须相同。

**端口：**在输入框中输入后端认证的端口。

**转发策略：**该字段设置何种情况下转发认证请求至后端认证服务器。

选择“本地用户不存在或未绑定令牌(不进行本地认证)”，代理端登录认证时符合这个条件时便会将请求转发到后端认证服务器上来认证，若不满足转发条件，则不转发认证请求。

选择“本地认证成功”，代理端登录认证时当本地认证成功时，便将请求发送到后端认证服务器上认证，若不满足条件，则不转发认证请求。

提示：此处允许多选。

**域名：**后端认证类型为“AD”时，才会出现此项，勾选上，为 AD 后端类型所在机器指定域名，不勾选

上，AD 后端认证服务器不需要域名。

**共享密钥：**只有后端认证类型为 Radius 时才会出现此字段，在输入框中输入共享密钥，此共享密钥是飞天认证服务器与后端认证服务器之间的共享密钥。

**连接超时时间(秒)：**在输入框中设置连接超时时间，在此时间后还未连接上则提示连接超时。

**连接超时重试次数：**在输入框中设置连接超时重试次数。

(3) 按要求填写后端认证信息，点击“保存”按钮，系统提示保存成功。

提示：系统中只能添加一个后端认证服务器，若要切换 RADIUS 后端服务器和 AD 后端服务器，需编辑修改服务器类型来进行切换。

## 14.4.2 后端认证列表

### 14.4.2.1 编辑后端认证

如果需要修改后端认证信息，进入后端认证列表，点击记录“操作”列中的编辑图标，进入编辑后端认证页面，修改信息，点击“保存”按钮，保存修改后的信息。

### 14.4.2.2 启用/禁用后端认证

添加的后端服务器默认状态为启用，可通过“操作”列中的“启用/禁用”图标来更改状态。

### 14.4.2.3 删除后端认证

当创建的后端认证不再使用时，可以选择删除，在后端认证列表中选中要删除的记录，点击“删除”按钮，删除后端认证。

## 第15章 日志管理

### 15.1 管理员日志

管理员日志模块只记录管理中心中管理员账号的操作内容，不同权限管理员查看到内容也不同，没有管理员日志权限的管理员登录后看不到管理员日志模块，只拥有查看个人的管理日志权限的管理员登录后，只能查看到自己的操作记录；拥有查看个人及个人创建的管理员日志权限的管理员登录后能查看到自己及自己创建的管理员日志内容；拥有查看所有管理员日志权限的管理员登录后能查看到所有管理员的日志。

查看具体的某个日志内容的操作步骤如下：

（1）点击页面上方导航栏中的“日志管理”，选择“管理员日志”，进入管理员日志页面。

（2）设置查询条件，然后点击“查询”按钮。

（3）查询出符合查询条件的管理员操作记录，要进一步看详细的内容时，点击对应的日志记录“详细信息”列中的“明细”图标，打开日志详细信息的界面。

### 15.2 用户日志

用户日志记录管理中心中所有用户的操作内容，只有拥有查看用户日志权限的管理员登录系统后才能看到用户日志模块，管理员只能查看自己所管理的组织机构下的用户日志，未管理的组织机构下用户日志是查看不到的。

查看具体的某个日志内容的操作步骤如下：

（1）点击页面上方导航栏中的“日志管理”，选择“用户日志”，进入用户日志页面。

（2）设置查询条件，然后点击“查询”按钮。

（3）查询出要查看的用户操作记录，要查看详细的内容时，点击对应的日志记录后“详细信息”列中的“明细”图标，打开日志详细信息的界面。



## 第16章 报表管理

报表管理模块主要用来查看系统中一些数据的统计信息，主要包括业务报表、用户报表和令牌报表 3 个方面。

### 16.1 业务报表

#### 16.1.1 认证、同步量统计

“认证服务器认证、同步量统计”界面显示当前系统中的某一时间段下认证服务器接收到的认证和同步请求数，以柱状图形式展现。可以设置查询条件，查看指定的某个机构某个时间段下的统计数据。除了查看外，系统还提供了导出统计表的功能，方便使用图中的统计数据。

提示：若不设置任何查询条件，则统计图中列出当前登录管理员权限下的所有机构所有时间段的统计信息。

#### 16.1.2 按时段认证量统计

“认证服务器时间段认证量统计”界面显示当前系统中的某一时间段下认证服务器接收到的认证量统计，以线形图形式直观的展现不同时间段的曲线。可以设置查询条件，查看指定的某个机构某个时间段下的统计数据。除了查看外，系统还提供了导出统计表的功能，方便使用图中的统计数据。

提示：1) 若不选择机构，则统计图中列出当前登录管理员权限下的所有机构指定时间段的统计信息。

2) 查询条件“时间段”中不允许为空，最大时间段长为 12 个月，默认时长为 30 天。

#### 16.1.3 用户门户访问量统计

“用户门户访问量统计”界面显示当前系统中某一时间段下用户门户的访问量，以线性的方式展现不同时间段下的访问曲线。可以设置查询条件，查看指定的某个机构某个时间段下的统计数据。除了查看外，系统还提供了导出统计表功能，方便使用图中的统计数据。

提示：1) 若不选择机构，则统计图中列出当前登录管理员权限下的所有机构指定时间段的统计信息。

2) 查询条件“时间段”中不允许为空，最大时间段长为 12 个月，默认时长为 30 天。

## 16.2 用户报表

### 16.2.1 数量统计

“用户数量统计”模块按“新增”、“锁定”、“绑定”类别统计了某组织机构某时间段下的用户数。让管理员更直观的看到目前系统中用户的使用情况。通过查询条件的设置，可看到指定的组织机构和指定时间段的用户统计信息。除了查看外，系统还提供了导出统计表和导出详细报表功能，方便使用图中的统计数据。

提示：若不选择机构，不设定时间段，则统计图中列出当前登录管理员权限下的所有机构所有时间段的统计信息。

### 16.2.2 认证方式统计

“用户认证方式统计”模块按“静态密码”、“OTP”和“静态密码+OTP”类别统计了组织机构下的不同认证方式的用户数量分布。通过查询条件，可以查看指定的组织机构下认证方式的统计信息。除了查看外，系统还提供了导出统计表和导出详细报表功能，方便使用图中的统计数据。

提示：若不选择机构，则统计图中列出当前登录管理员权限下的所有机构的统计信息。

## 16.3 令牌报表

### 16.3.1 状态统计

“令牌状态统计”根据令牌的不同状态，统计了系统中的令牌数。通过查询条件，可以查看指定的组织机构下的不同状态的令牌数。除了查看外，系统还提供了导出统计表和导出详细报表功能，方便使用图中的统计数据。

提示：若不选择机构，则统计图中列出当前登录管理员权限下的所有机构不同状态下的令牌统计信息。

### 16.3.2 过期时间统计

“令牌过期时间统计”模块按照“令牌总量”、“一周内过期”、“一个月内过期”、“一个季度内过期”和“大于三个月过期”等分类统计了当前系统中令牌过期时间分布。通过设置查询条件，可以查看指定的组织机构下令牌过期时间分布图。除了查看外，系统还提供了导出统计表和导出详细报表功能，方便使用图中的统计数据。

提示：若不选择机构，则统计图中列出当前登录管理员权限下的所有机构下的令牌过期统计信息。

### 16.3.3 厂商令牌统计

“厂商令牌统计”模块是用来统计不同厂商、不同组织机构中各种状态的令牌数量，共有两个功能页签“厂商令牌供货统计”和“组织机构令牌数据统计”。

厂商令牌供货统计：该模块是按照不同厂商的实际供货量、已绑定、已过期、已作废和结存的令牌数量来进行统计的。

组织机构令牌数据统计：该模块是按照不同的组织机构下导入的各厂商的令牌数据，也包括供货量、已绑定、已过期、已作废和结存这几个方面。

具体统计方法可使用“厂商令牌统计”模块中的“手动统计”按钮进行手动统计，也可以使用“配置管理—>其他公共配置”中的“启用令牌统计定时任务”设置定时统计。“统计时间”显示为最近一次统计的时间。

提示：在初始化 OTP Server 管理中心的“附加模块”勾选了“多厂商集成”，在“报表管理”模块显示“厂商令牌统计”，否则，不显示。

## 图目录

图表 1 语言选择初始化界面.....	5
图表 2 初始化方式选择界面.....	6
图表 3 附加模块界面 .....	6
图表 4 数据库恢复界面 .....	7
图表 5 创建管理员界面 .....	7
图表 6 设置真实 IP 界面 .....	8
图表 7 初始化完成界面 .....	8
图表 8 切换数据库界面 .....	12
图表 9 备份设置界面 .....	13
图表 10 启用定时更新界面 .....	13
图表 11 远程数据库配置界面.....	27
图表 12 解绑令牌界面 .....	56
图表 13 解绑用户组界面 .....	59
图表 14 解绑认证代理界面 .....	60
图表 15 解绑用户界面 .....	66
图表 16 解绑认证代理界面 .....	67