

安盟双因素身份认证系统日常维护手册

(Anmeng8.0)

安盟电子信息安全有限责任公司

2023 年 09 月

版本管理

版本	摘要	编 者	时间
1.10	重新编写导入令牌	陈俊	2020/12/14
1.11	设置口令周期	陈俊	2023/09/26
1.12	重现编写令牌本地测试	陈俊	2023/10/16

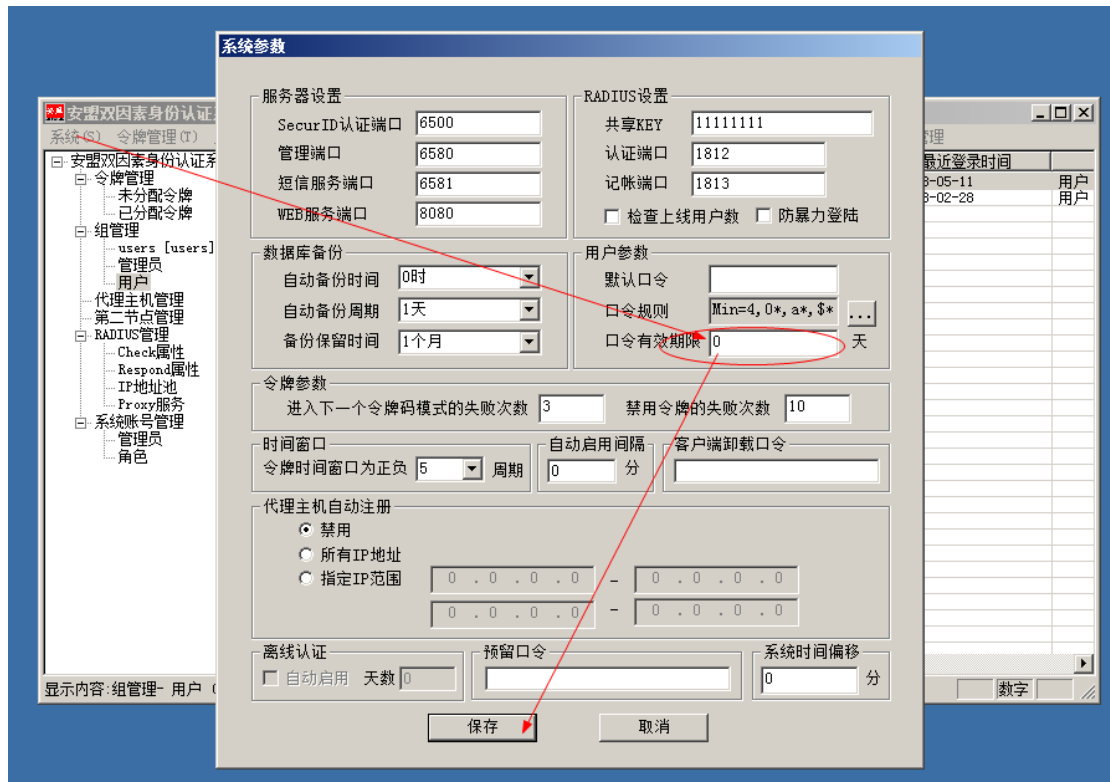
目录

目录

- 1 取消口令周期更改.....4
- 2 令牌管理.....4
 - 2.1 导入令牌.....4
- 3 令牌本地测试.....7
 - 3.1 用户绑定令牌.....8
 - 3.2 直接测试认证.....11
- 4 系统管理.....13
 - 4.1 连接认证服务管理器.....13
 - 4.2 连接认证日志查看器.....15
- 5 常见问题排除方法.....16
 - 5.1 用户登录没有认证日志.....17
 - 5.2 认证日志提示未注册用户.....17
 - 5.3 源地址与目的地址不一致.....17
 - 5.4 清理节点密文.....18
 - 5.5 密码不正确.....18
 - 5.6 用户不在代理主机上.....18
 - 5.7 需要设置新 PIN 码.....19
 - 5.8 需要下一个令牌码.....20
 - 5.9 没有可用的令牌.....21

1 取消口令周期更改

登录服务管理器，在菜单栏打开[系统]，系统参数设置，设置为 0，就可以关闭口令周期更改。



口令周期更改，是面向所有用户，默认值是 90 天，如果设置为 0，表示不在对口令有效期进行限制。

2 令牌管理

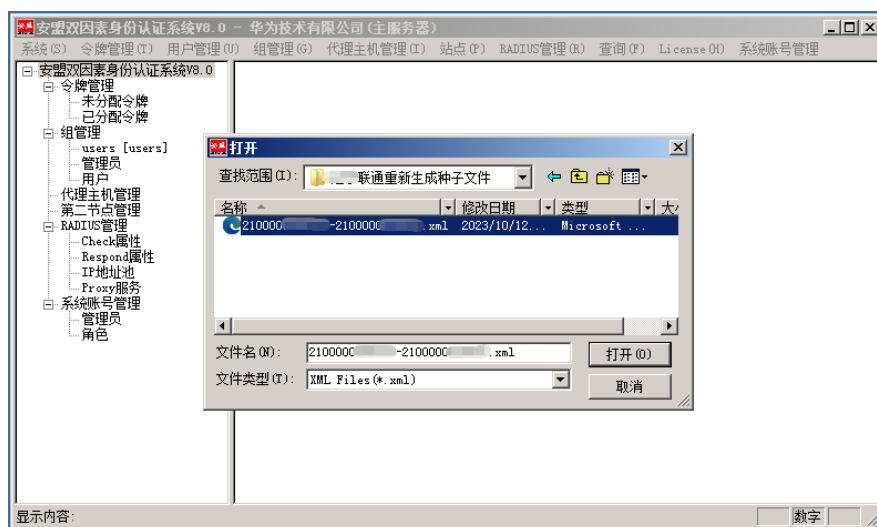
2.1 导入令牌

单击菜单栏**令牌管理**，再点击子菜单项**导入令牌**。可以选择导入不同的令牌。以 ASC 格式的钥匙令牌，以及 XML 格式的刮刮卡令牌的种子文件。



图 1

单击**导入令牌**，会提示导入，以 xml 后缀名的种子文件



提示用户要输入种子密码

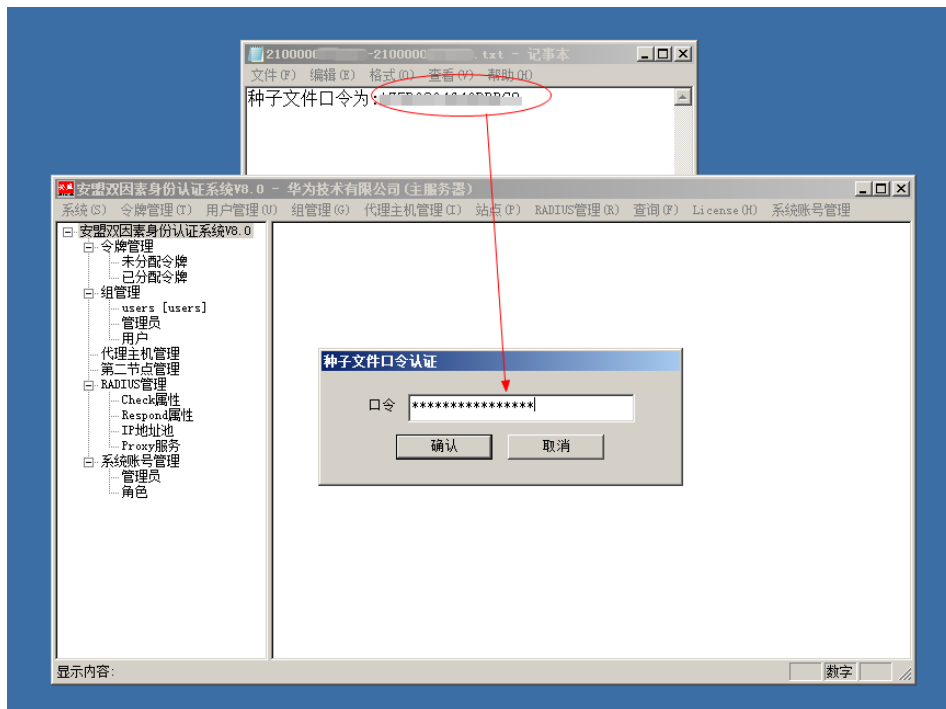


图 2

单击确认后，系统会提示设置令牌工作模式

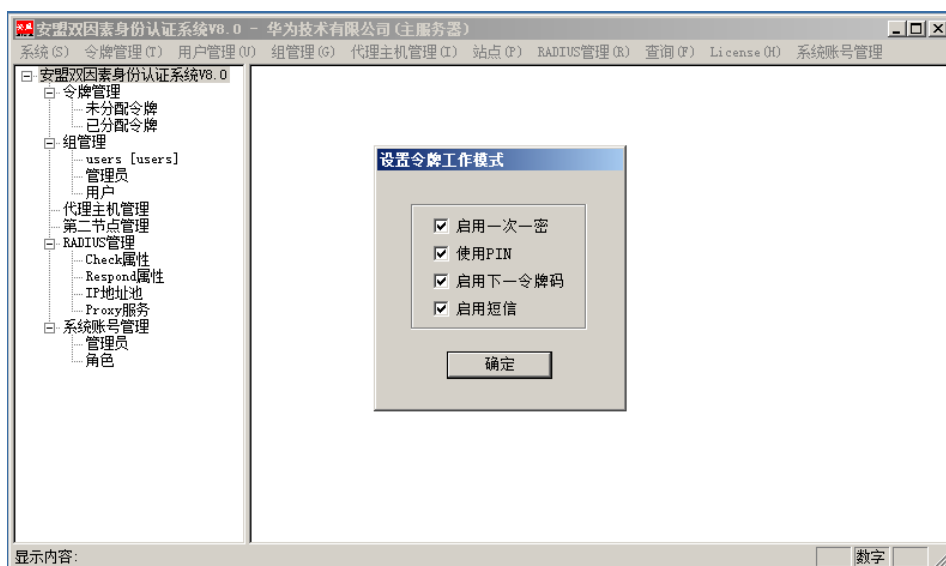


图 3

系统会显示导入令牌的个数。

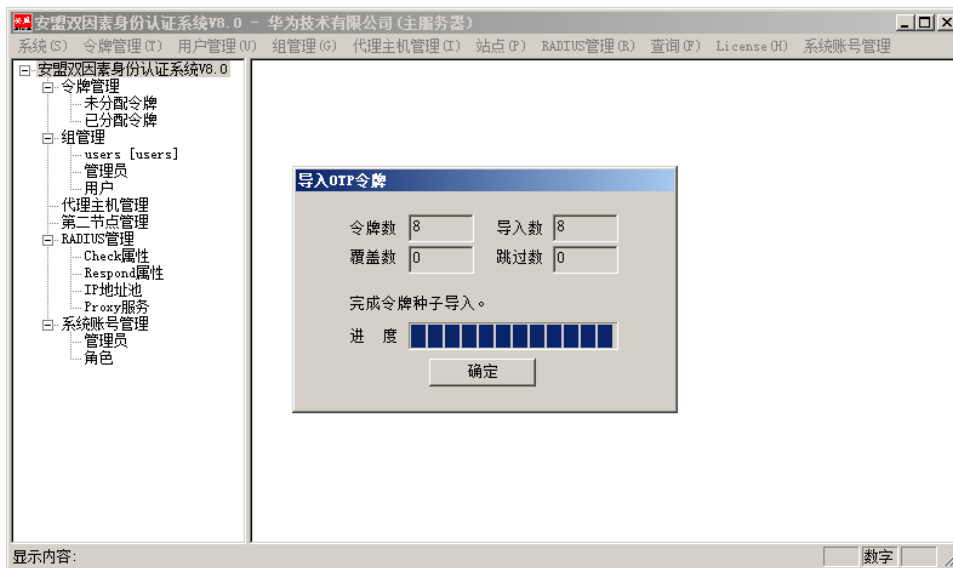


图 4

新导入的令牌在**未分配令牌**一栏中，分配给用户后进入**已分配令牌**一栏。

安盟认证服务管理器

令牌管理

- 未分配令牌
- 已分配令牌

组管理

- 管理员
- 代理主机管理
- 第二节点管理

RADIUS管理

- Check属性
- Respond属性

令牌序列号	开始时间	结束时间
00000078919470	2004-06-08	2010-09-29
00000078919471	2004-06-08	2010-09-29
00000078919472	2004-06-08	2010-09-29
00000078919473	2004-06-08	2010-09-29
00000078919474	2004-06-08	2010-09-29
00000078919475	2004-06-08	2010-09-29
00000078919476	2004-06-08	2010-09-29
00000078919477	2004-06-08	2010-09-29
00000078919478	2004-06-08	2010-09-29
00000078919479	2004-06-08	2010-09-29

图 5

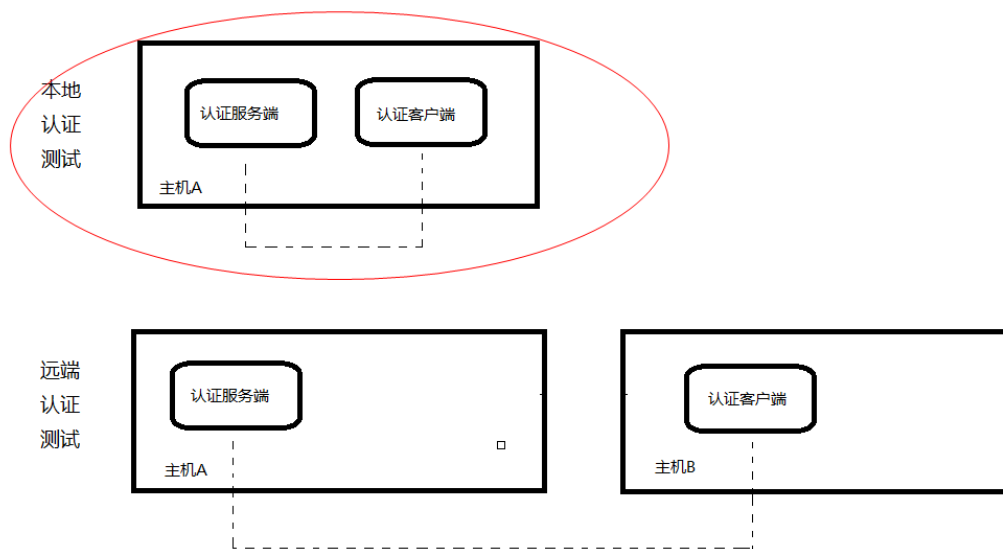
选中某一令牌后双击，可以直接编辑该令牌。

3 令牌本地测试

资源 URL:

<https://www.anmeng.com.cn/ntradping>

本地测试是指服务端和客户端同在一个主机。如果本地认证可以通过，远端认证自然也可以通过。这也是判断认证服务器是否有效的直接方法，当遇到认证异常的时候，首先检查本地认证是否有效。如果有效再排除下一个节点是否有效。当最远端设备和本地认证都有效的时候，两条认证线路经就可以交叉排除故障点位置。



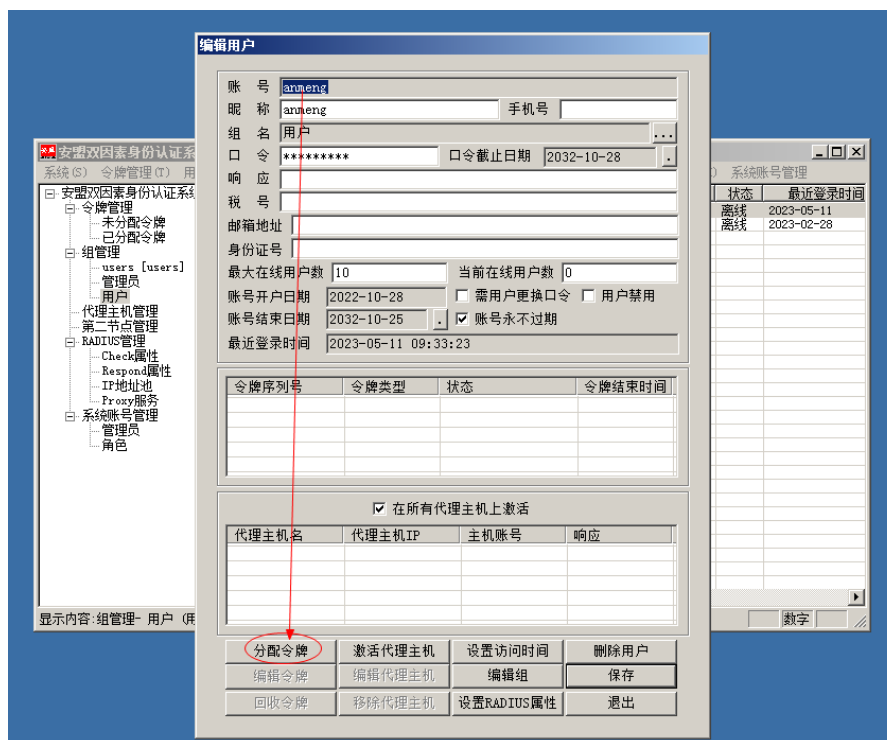
令牌本地测试，先给用户绑定令牌，然后在客户端（NTRadPing）测试。

3.1 用户绑定令牌

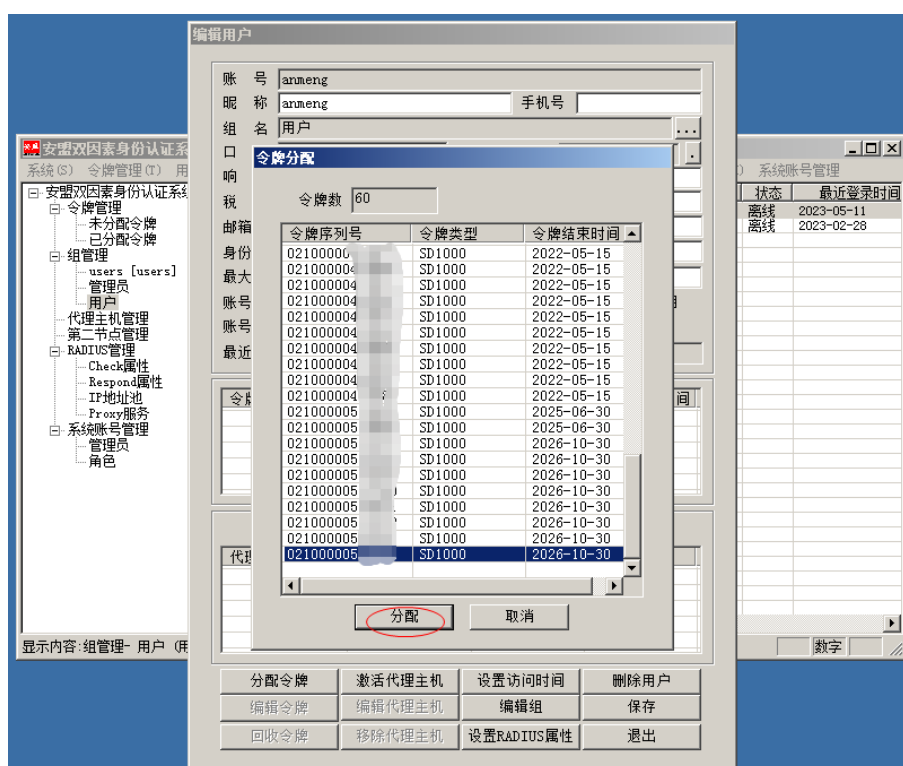
在用户列表中，找到目标用户，例如用户 anmeng，鼠标右键编辑该用户。



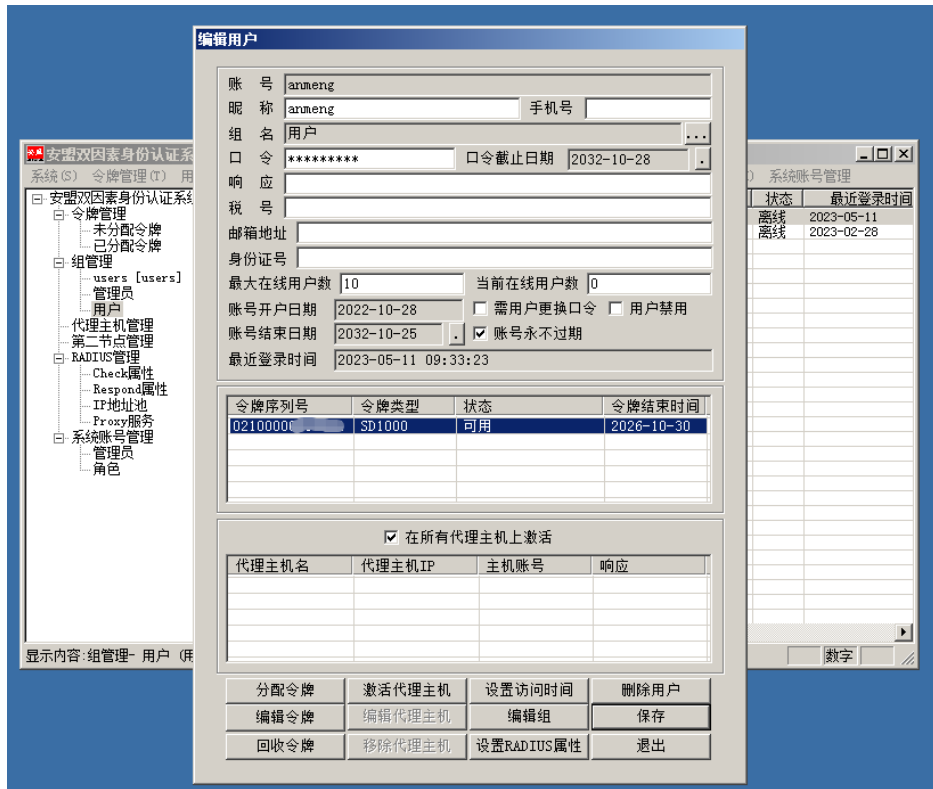
分配令牌



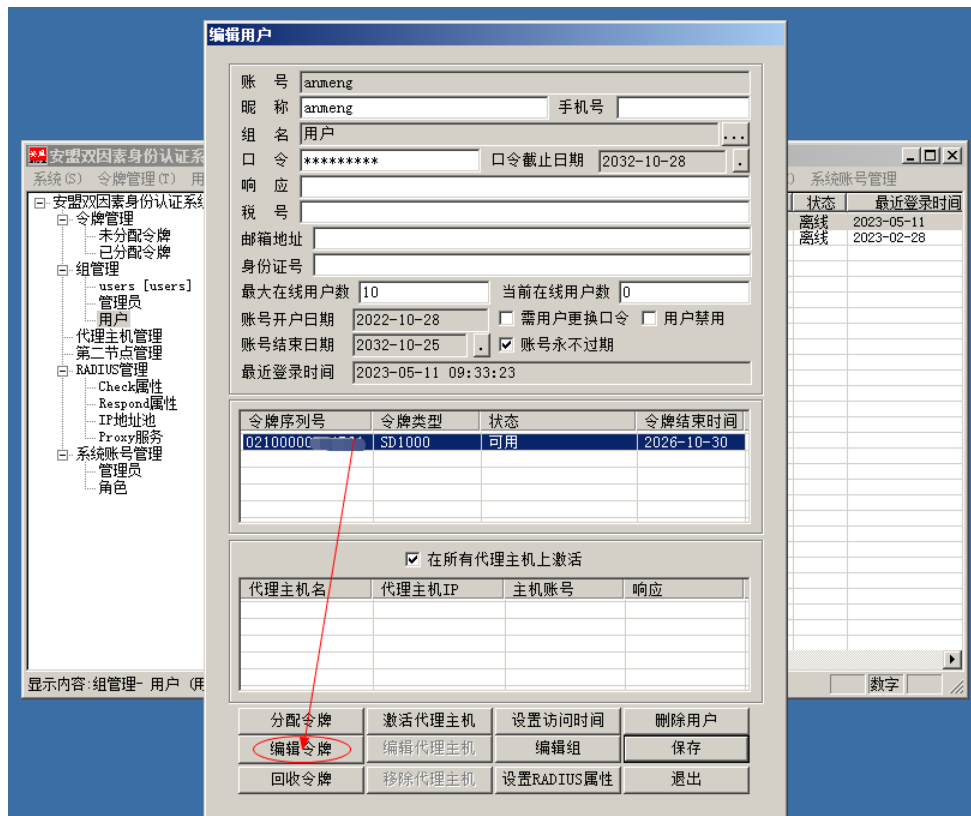
选择刚才导入的新令牌



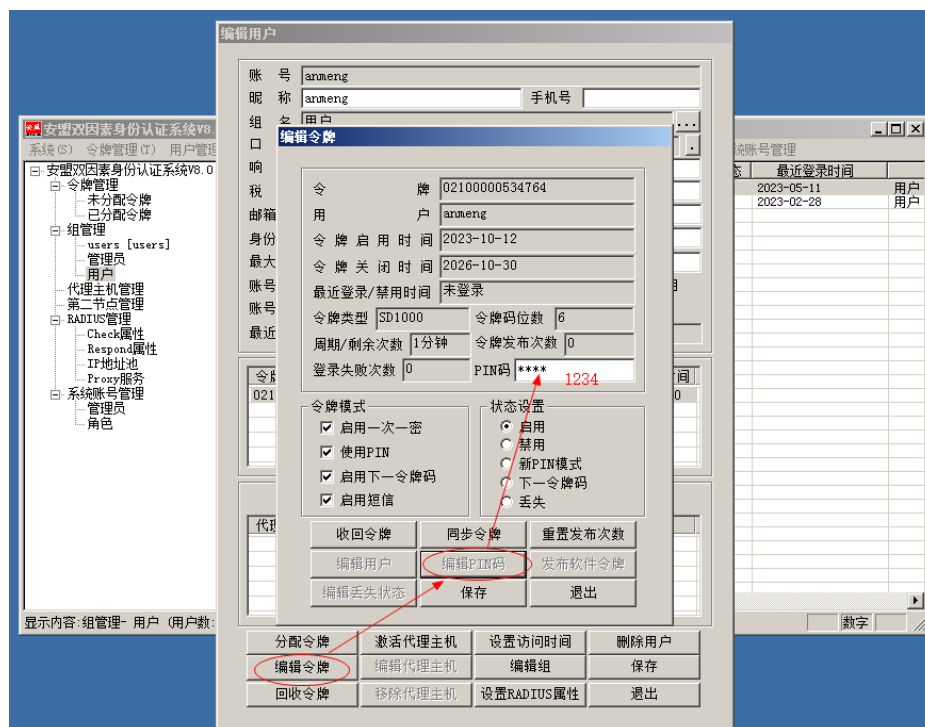
保存配置



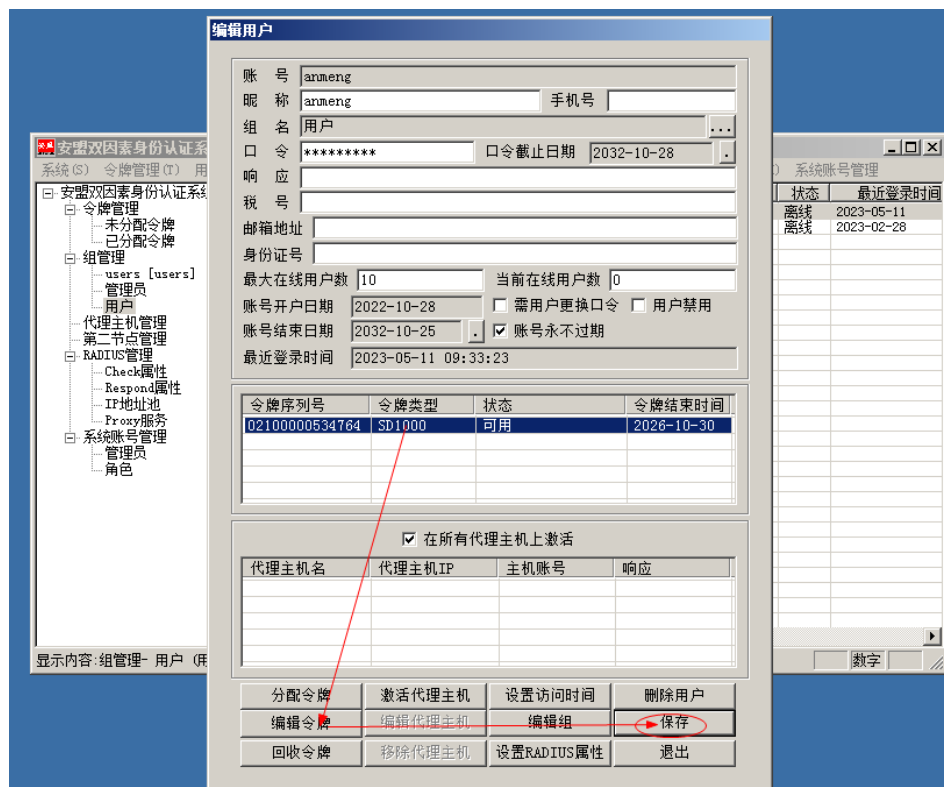
最后设置 PIN 码



为了方便测试假设 PIN 码设置为 1234

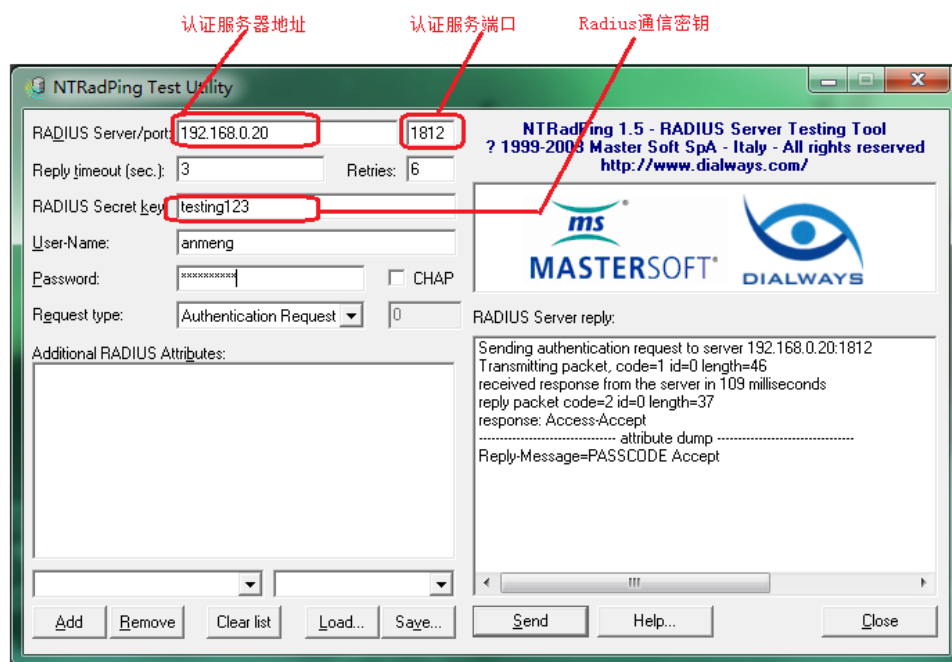


保存所有配置

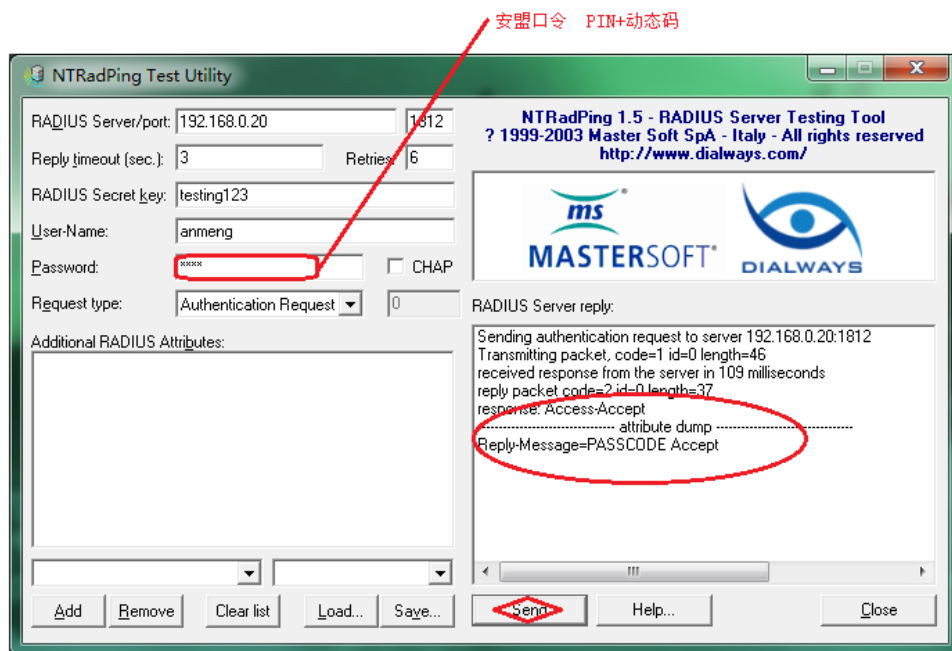


3.2 直接测试认证

假设认证服务器为 192.168.0.20, Radius 公钥为 testing123, 填写用户名和密码, 点击 <Send>按钮, 就可直接看到认证服务器的返回结果。



直接认证测试



如果返回结果是“PASSCODE Accept”，表示认证成功。同时认证日志会记录认证结果。

如果是其它信息，表示可以认证，但用户名或密码是错误的。具体可以参考后文常见问题与

排除方法。

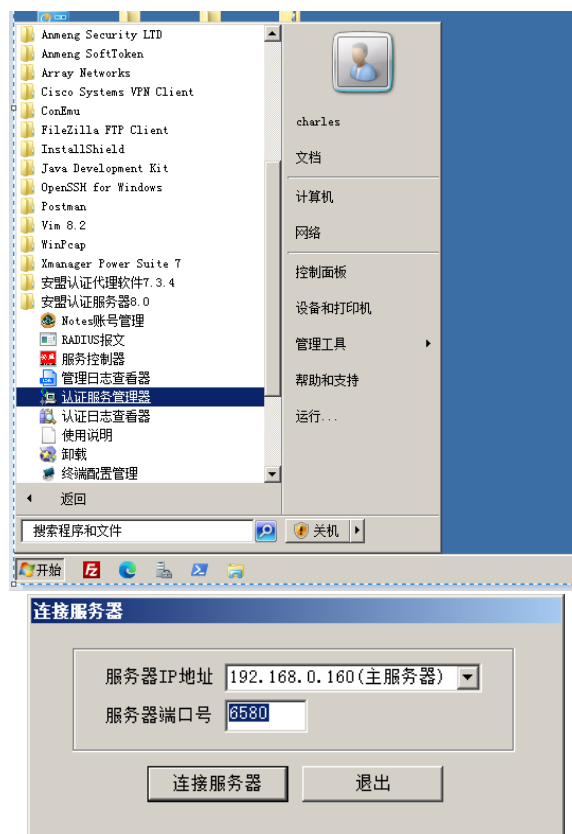
4 系统管理

系统菜单上集成了包括系统设置（对系统进行远程管理的设置、对 PIN 码的设置、对用户静态口令的设置等），用户权限以及配置的操作，可以非常方便对安盟身份认证系统参数进行设置。

安盟公司认证服务器有两种版本，一种是应用于 Windows 系统版本认证系统，另一种是应用 Unix 系统版本的认证系统。

4.1 连接认证服务管理器

服务器软件安装完成后，WINDOWS 开始菜单->所有程序->安盟认证服务器 8.0 -> 服务管理器。出现如下连接服务器对话框。



选择要连接的认证服务器类型，并输入要连接的服务器 IP 地址，点击“连接服务器”。

出现认证服务器登录对话框。

认证服务器管理器登录

用户名

sysadmin

令

确定

退出

登录成功后

安盟双因素身份认证系统V8.0 - 华为技术有限公司(主服务器)

系统(S) 令牌管理(T) 用户管理(U) 组管理(G) 代理主机管理(I) 站点(E) RADIUS管理(R) 查询(Q) License(H) 系统账号管理

安盟双因素身份认证系统V8.0

令牌管理

未分配令牌

已分配令牌

组管理

users [users]

管理员

用户

代理主机管理

第二节点管理

RADIUS管理

Check属性

Respond属性

IP地址池

Proxy服务

系统账号管理

管理员

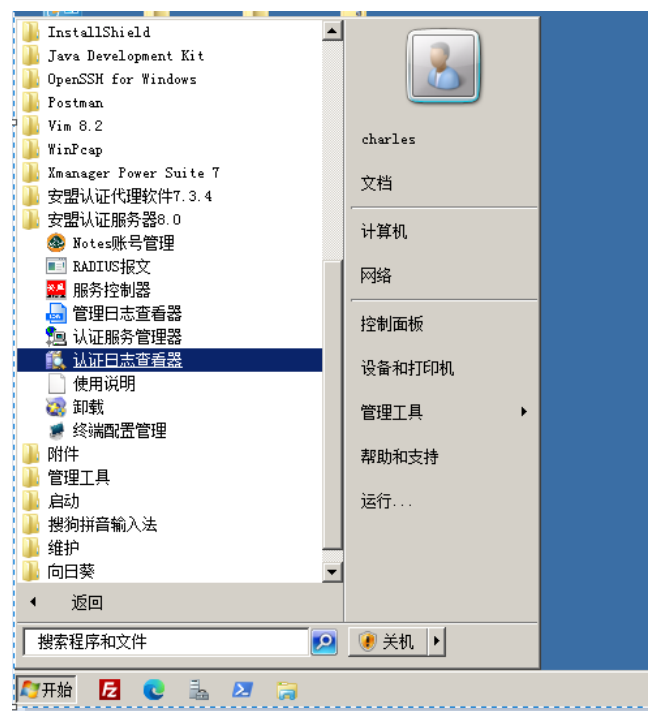
角色

显示内容:

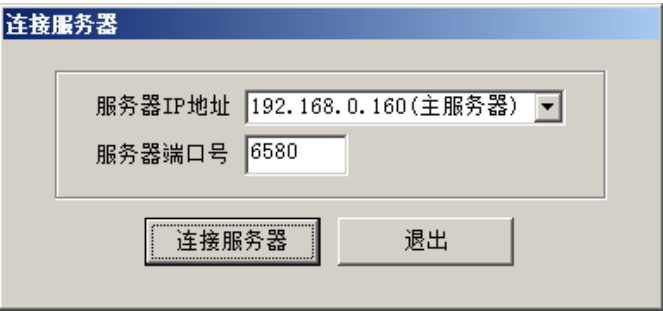
数字

可以完成响应的增删改操作。

4.2 连接认证日志查看器



第一步：点击开始—程序—安盟认证服务器 8.0—认证日志查看器，如图所示。



第二步：在弹出的对话框中，填入主服务器的 IP，选择连接服务器。输入登录名和密码，如图所示：



安盟双因素身份认证系统V8.0—认证日志查看器 - 华为技术有限公司 (主服务器)						
系统 日志管理 报告 (E)						
时间	用户	操作主机	对象	结果		
2023-02-28 15:19:11	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:19:22	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:24:26	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:24:36	xiaolan	192.168.0.37	静态口令	密码不正确		
2023-02-28 15:24:43	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:25:55	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:26:05	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:27:03	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:28:52	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:29:10	xiaolan	192.168.0.37	静态口令	密码不正确		
2023-02-28 15:29:18	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:30:07	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:30:58	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:30:58	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:39:23	xiaolan	192.168.0.37	静态口令	登录成功		
2023-02-28 15:40:59	xiaolan	192.168.0.37	静态口令	登录成功		
2023-05-11 08:49:50	sysadmin	192.168.0.160	管理员登录	密码错误		
2023-05-11 08:49:55	sysadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 08:50:41	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:19:04	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:24:04	sysadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 09:24:34	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:24:48	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:25:12	auditadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 09:25:30	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:25:31	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:31:57	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:32:00	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:33:20	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 09:33:23	anmeng	192.168.0.160	静态口令	登录成功		
2023-05-11 16:44:02	sysadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 16:47:13	auditadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 16:49:20	auditadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 16:50:29	sysadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 16:57:48	auditadmin	192.168.0.160	管理员登录	登录成功		
2023-05-11 17:20:27	sysadmin	192.168.0.160	管理员登录	登录成功		
2023-10-16 11:07:53	sysadmin	192.168.0.160	管理员登录	登录成功		
认证日志 记录数: 183				数字		

各列的具体含义见下表：

列名	含义
时间	用户进行操作的时间
用户	进行操作的用户的帐号
操作主机	用户进行操作时所在主机的标识
对象	被操作的用户帐号
结果	用户进行的具体的操作

5 常见问题排除方法

遇到认证异常，可以通过查看认证日志排错。

选择开始→程序→安盟认证服务器 8.0→认证日志查看器，在经过权限验证后(只有管理员级别的用户方可查看该日志)，可查看认证日志，如下图：



系统 日志管理 报告(R)				
时间	用户	操作主机	对象	结果
2018-03-12 19:52:17	administrator	192.168.1.201	静态口令	管理员登录成功
2018-03-12 22:40:08	administrator	192.168.1.201	静态口令	管理员登录成功
2018-03-12 23:03:28	admin	192.168.1.201		管理员密码不正确
2018-03-12 23:04:52	admin	192.168.1.201		密码不正确
2018-03-12 23:05:43	admin	192.168.1.201		用户已被禁用
2018-03-12 23:06:32	admin	192.168.1.201	静态口令	登录成功
2018-03-12 23:06:47	admin	192.168.1.201		密码不正确

如果用户登录有问题，或者在测试时，都可以通过查看认证日志，找到问题所在。

5.1 用户登录没有认证日志

检查网络是否畅通，从客户端 PING 认证服务器是否能连通。

5.2 认证日志提示未注册用户

检查用户名称是否正确，如果用户名正确，检查认证服务器上边是否有这个用户。

5.3 源地址与目的地址不一致

检查代理主机客户端，添加 IP 地址映射，标明本地主网卡地址。这种情况是由于机器有多个网卡造成，需要指定一个主要网卡。

5.4 清理节点密文

此种情况是，原先可以正常认证，后期变动路由或交换机等网络设备，致使消息包传送路径发生变化，需要执行请节点密文操作。

5.5 密码不正确

认证信息如下：

2018-03-12 23:04:52	admin	192.168.1.201	密码不正确
---------------------	-------	---------------	-------

解决办法：

1. 如果是所有登录某个代理主机的用户均报密码不正确，请确定代理主机对接的协议：
 - a) 如果是 RADIUS 协议，请确保双方的 RADIUS 共享密钥一致。
 - b) 如果是 SECURID 协议，请清除代理主机上的节点密文。
2. 请确保用户的密码类型，
 - a) 如果是静态密码，请确保静态密码没有过期，并重置密码。

账号: admin

用户名: admin 手机号:

组名: 管理员 ...

口令: **** 角色: 管理员

响应:

税号:

最大在线用户数: 10 当前在线用户数: 0

账号开户日期: 2018-03-12 ☐ 需用户更换口令 ☐ 用户禁用

账号开始日期: 2018-03-12 . 口令截止日期: 2017-02-12 .

最近登录时间: 2018-03-12 23:06:32 过期，请延期

- b) 动态密码
 - i. 请确保用户令牌的状态为可用状态；
 - ii. 请确保用户的令牌没有过期；
 - iii. 请重置令牌的 PIN 码，并同步令牌。

5.6 用户不在代理主机上

认证信息如下：

2018-03-09 00:29:03	root	192.168.1.103	用户不在代理主机上
---------------------	------	---------------	-----------

解决办法：

1. 根据日志信息中的操作主机信息，请确保 192.168.1.103 已经添加成为了代理主机，

如果尚未添加，请根据 6.2 添加代理主机中所描述的步骤进行增加。

2. 如果已经把 192.168.1.103 添加成了代理主机，请确保代理主机向 root 用户开放了访问权限，可根据 6.5 激活代理主机小节中所描述的内容进行授权。

5.7 需要设置新 PIN 码

2018-03-13 09:42:05	admin	192.168.1.201	00000046127119	需要设置新PIN码
2018-03-13 09:43:05	test	192.168.1.201	静态口令	需要设置新PIN码

- 1) 当认证对象为令牌序号时，表示用户的令牌模式勾选了使用 PIN，但尚未设置 PIN 码，或者是用户令牌的状态为新 PIN 模式，如下图所示：

编辑令牌

令牌

00000046127119

用户

admin

令牌启用时间

2017-05-09

令牌关闭时间

2018-05-08

最近登录/禁用时间

2018-03-13 10:04:41

令牌类型

128位软件

令牌码位数

6

周期/剩余次数

1分钟

状态

下一令牌模式

登录失败次数

0

PIN码

未设置

令牌模式

☒ 启用一次一密

☒ 使用PIN

☒ 启用下一令牌码

☐ 启用短信

状态设置

☐ 启用

☒ 新PIN模式

☐ 下一令牌码

☐ 丢失

收回令牌

同步令牌

删除令牌

编辑用户

编辑PIN码

发布软件令牌

编辑丢失状态

保存

退出

解决方法：

- a) 在编辑令牌窗口，点击编辑 PIN 码按钮，手动设置 PIN 码，并将令牌的状态设置为启用状态。
- b) 通过认证代理软件或支持 RADIUS 挑战应答的工具，并根据提示设置 PIN 码，如下图所示：

```
Radius客户端: 支持挑战/应答认证模式
请输入用户名: admin
请输入密码: 197518

Response packet:
1 Code = Access-Challenge (11)
1 ID = 0
2 Length = 121
16 Request Authenticator = < 80 42 80 64 1d 62 61 36 8a fb 8c 2f 51 1d 58 e9 >
44 Reply-Message (18) = "Enter a new PIN having from 4 to 8 digits:"
57 State (24) = "AUTH.0=0000c0a801c9ef35dbe1c9be56c997c929300abcacbf53"

Enter a new PIN having from 4 to 8 digits:: abcd1234 ← 设置PIN码

Response packet:
1 Code = Access-Accept (2)
1 ID = 1
2 Length = 37
16 Request Authenticator = < ba 81 56 2c 49 9b 8b 7f f8 19 27 1a 11 f1 44 6d >
17 Reply-Message (18) = "PASSCODE Accept"
```

PIN 设置成功，在认证日志中，将新生成一条设置新 PIN 码成功的日志，如下图所示：

2018-03-13 09:51:08	admin	192.168.1.201	00000046127119	设置新PIN码成功
---------------------	-------	---------------	----------------	-----------

5.8 需要下一个令牌码

2018-03-13 10:03:41	admin	192.168.1.201	00000046127119	需要下一个令牌码
---------------------	-------	---------------	----------------	----------

当用户令牌的模式勾选了启用下一令牌码，且令牌的状态为下一令牌码时，在用户输入正确的 PIN 码+令牌码后，会提示需要下一个令牌码，如下图所示：

编辑令牌

令牌 ID: 00000046127119

用户: admin

令牌启用时间: 2017-05-09

令牌关闭时间: 2018-05-08

最近登录/禁用时间: 2018-03-13 10:04:41

令牌类型: 128位软件 令牌码位数: 6

周期/剩余次数: 1分钟 状态: 下一令牌码模式

登录失败次数: 0 PIN码: 未设置

令牌模式:

- ☒ 启用一次一密
- ☒ 使用PIN
- ☒ 启用下一令牌码
- ☐ 启用短信

状态设置:

- ☐ 启用
- ☐ 禁用
- ☒ 新PIN模式
- ☒ 下一令牌码
- ☐ 丢失

按钮: 收回令牌, 同步令牌, 删除令牌, 编辑用户, 编辑PIN码, 发布软件令牌, 编辑丢失状态, 保存, 退出

解决办法：

- 在编辑令牌窗口，将令牌的状态设置为启用状态，并保存。
- 通过认证代理软件或支持 RADIUS 挑战应答的工具，并根据提示设置 PIN 码，如下图所示：

```
Radius客户端. 支持挑战/应答认证模式
请输入用户名: admin
请输入密码: abcd1234413870 ← PIN码+令牌码

Response packet:
1 Code = Access-Challenge (11)
1 ID = 0
2 Length = 94
16 Request Authenticator = < b6 eb d5 44 a4 c9 dd 09 3a 51 cd ce 54 f7 11 16 >
17 Reply-Message (18) = "Enter Next Code"
57 State (24) = "AUTH.0=0000c0a801c9e6ff4e3f12cdf34fd482a7610584ddfffbac"

Enter Next Code: 785858 ← 输入下一个令牌码，不需要输入PIN码。

Response packet:
1 Code = Access-Accept (2)
1 ID = 1
2 Length = 37
16 Request Authenticator = < eb 96 e2 8f 1c b3 19 4e fe b2 f0 09 fd 4b 26 d9 >
17 Reply-Message (18) = "PASSWORD Accept"
```

所谓的下一个令牌码，是相对于用户登录时，所输入的那个令牌码来讲的，假设有以下

5 个令牌码：

387212	413870	785858	341375	901562
--------	--------	--------	--------	--------

假设，用户在登录时，输入的密码是 abcd1234**413870**，其中，abcd1234 是 PIN 码，413870 是令牌码，那么，等 413870 变化之后的第一个令牌码，就是下一个令牌码，即 785858。

下一个令牌码验证成功之后，在认证日志中，将新生成一条登录成功的日志，如下图所示：

2018-03-13 10:03:41	admin	192.168.1.201	00000046127119	需要下一个令牌码
2018-03-13 10:04:08	admin	192.168.1.201	00000046127119	登录成功

5.9 没有可用的令牌

2019-03-13 10:15:03	admin	192.168.1.201		没有可用的令牌
---------------------	-------	---------------	--	---------

当用户在登录的时候，输入了正确的 PIN 码+正确的令牌码，得到没有可用的令牌时，表示用户的令牌已经过期了。

解决方法：

请为用户重新分配一个没有过期的令牌。