安盟双因素身份认证系统日常维护手册
（Anmeng7.0）

安盟电子信息安全有限责任公司

2015 年 5 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	重现编写令牌本地测试；降级处理手机令牌管理	陈俊	2023/10/16

目录

1 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。

1.1 连接服务管理器

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 7.0 -> 服务管理器。出现如下连接服务器对话框。

图 1

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。

图 2

首次登录，用户名为安装认证服务管理软件的 WINDOWS 用户的登录名，口令默认为

1111。

注意：首次登录后应立即修改默认口令，我们建议最好将登陆用户名使用动态口令保护。安盟建议您最少设定两个以上管理员，一个用于日常使用，一个用于紧急情况下登录使用。最少每三个月使用备用管理员登陆一次，保证备用管理员的系统时间和令牌码保持同步。

进入到管理画面后，主要三个部分组成，分别是菜单栏，树列表区和信息列表区。

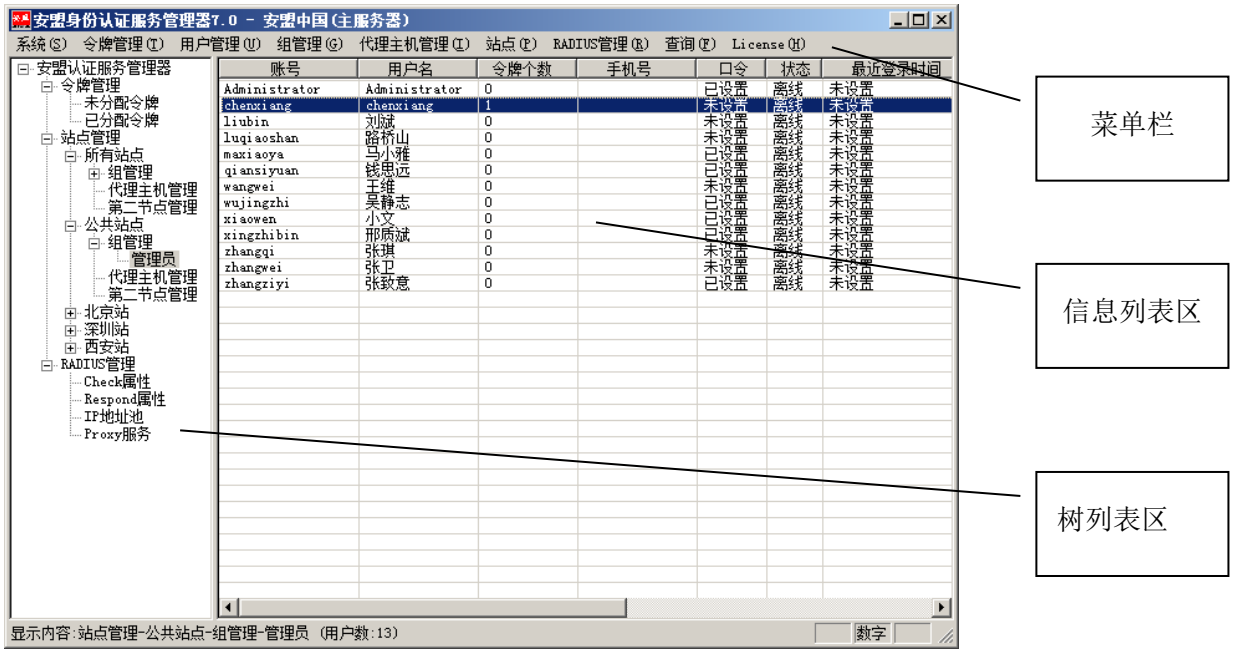


图 3

1.2 查看认证日志

连接日志管理器

第一步：点击开始－程序－安盟认证服务器 7.0－认证日志查看器，如图所示。

图 4

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：

图 5

用户名为安装认证服务管理软件的 WINDOWS 用户的登录名，口令默认为 1111。登录成功显示安盟认证服务器日志查看器，如图所示：

时间	用户	操作主机	对象	结果
2009-05-29 10:42:30	mj	192.168.0.161	静态口令	管理员登录成功
2009-05-29 11:27:44	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:27:44	test	mj	192.168.0.161	发送节点密文
2009-05-29 11:29:01	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:38:20	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:40:38	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:40:38	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:40:39	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:43:59	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:48:25	test	192.168.0.161	静态口令	登录成功
2009-05-29 11:57:57	test	192.168.0.161		不正确
2009-05-29 11:58:02	mj	192.168.0.161		密码不正确
2009-05-29 11:58:03	mj	192.168.0.161		密码不正确
2009-05-29 11:58:11	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:58:18	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:21	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:24	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:25	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:25	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:25	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:26	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:26	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:26	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:26	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:26	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:26	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:27	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:27	mj	192.168.0.161	静态口令	登录成功
2009-05-29 11:59:27	mj	192.168.0.161	静态口令	登录成功
2009-05-29 12:00:32	mj	192.168.0.161	静态口令	登录成功
2009-05-29 12:00:33	mj	192.168.0.161	静态口令	登录成功
2009-05-29 12:00:33	mj	192.168.0.161	静态口令	登录成功

图 6

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

2 令牌管理

首次安装安盟双因素身份认证管理系统时，系统内部是没有令牌。管理员需要导入令牌。导入成功后，会在信息列表区显示导入令牌详细的信息。依次是令牌序列号、开始时间、结束时间、令牌类型、位数和周期。

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 7

在弹出的文件对话框中，选择.ASC 文件,即令牌种子文件，然后打开。弹出导入情况明细对话框。

单击**导入令牌**，会提示导入，以 xml 后缀名的种子文件

首先提示用户要输入种子密码

图 8

单击确认后，系统会提示设置令牌工作模式

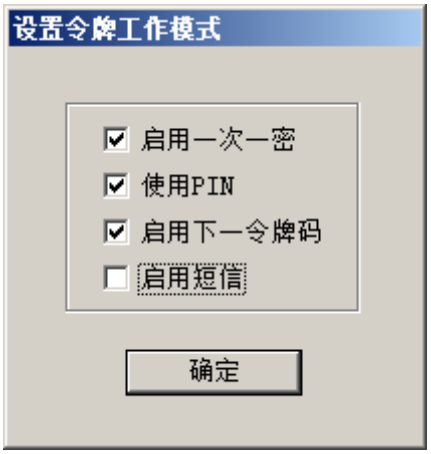


图 9

系统会显示导入令牌的个数。

图 10

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。

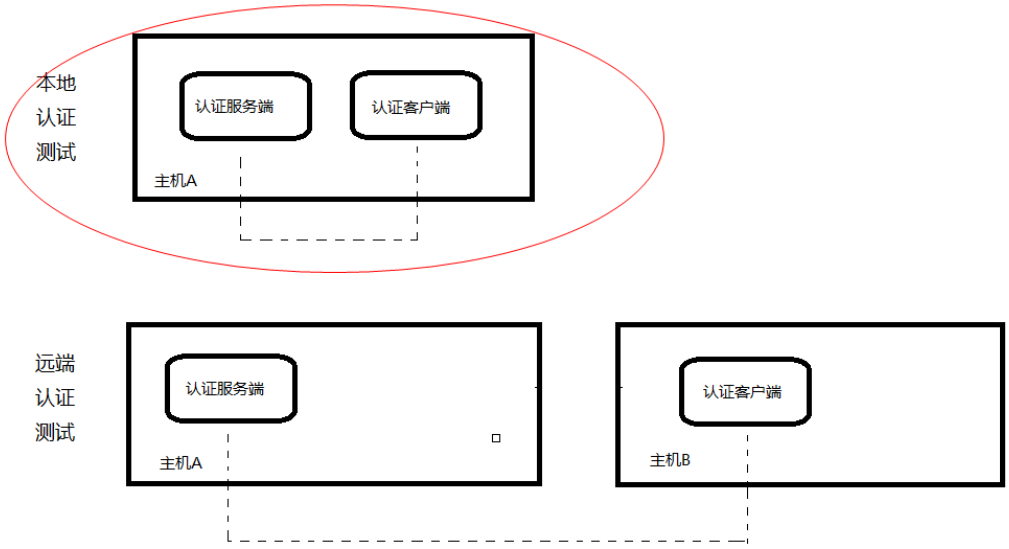
图 11

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

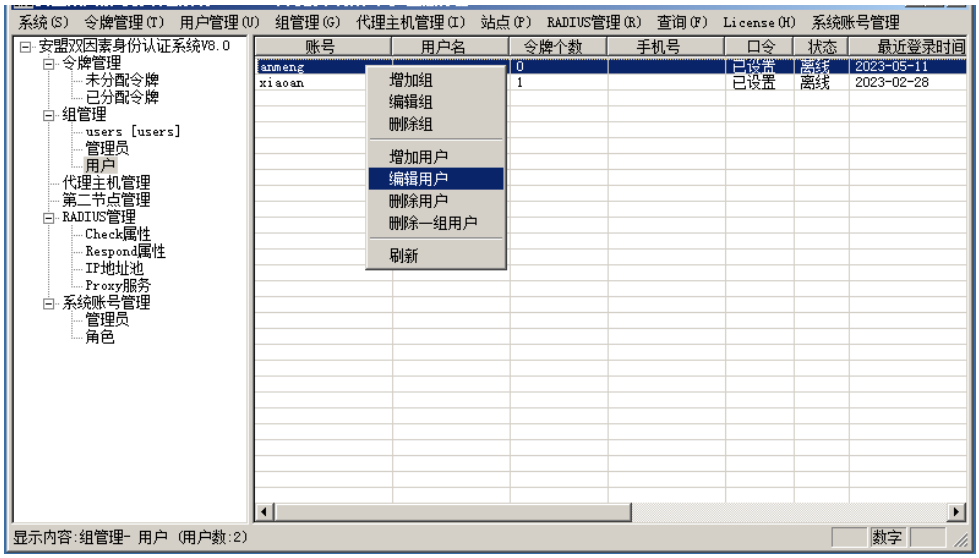
本地测试是指服务端和客户端同在一个主机。如果本地认证可以通过，远端认证自然也可以通过。这也是判断认证服务器是否有效的直接方法，当遇到认证异常的时候，首先检查本地认证是否有效。如果有效再排除下一个节点是否有效。当最远端设备和本地认证都有效的时候，两条认证线路经就可以交叉排除故障点位置。



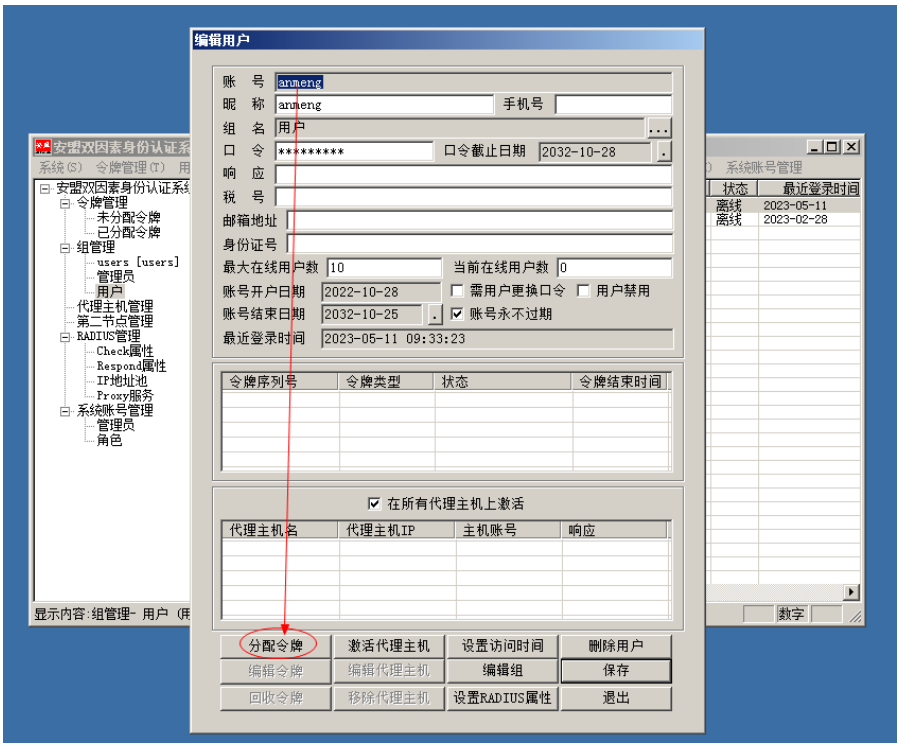
令牌本地测试，先给用户绑定令牌，然后在客户端（NTRadPing）测试。

3.1 用户绑定令牌

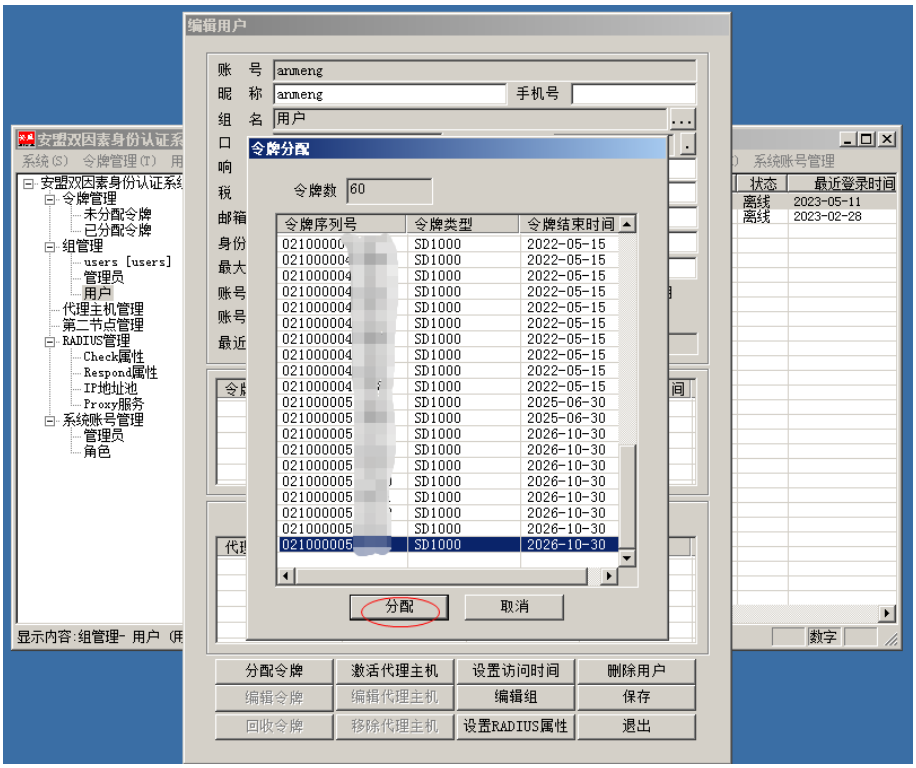
在用户列表中，找到目标用户，例如用户 anmeng，鼠标右键编辑该用户。



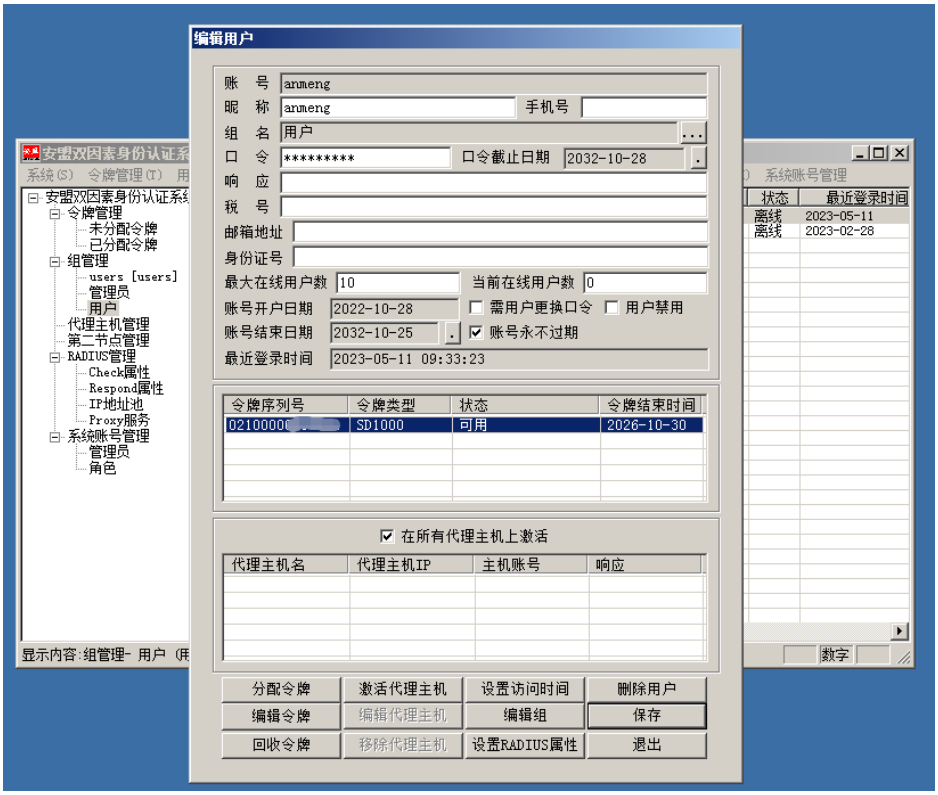
分配令牌



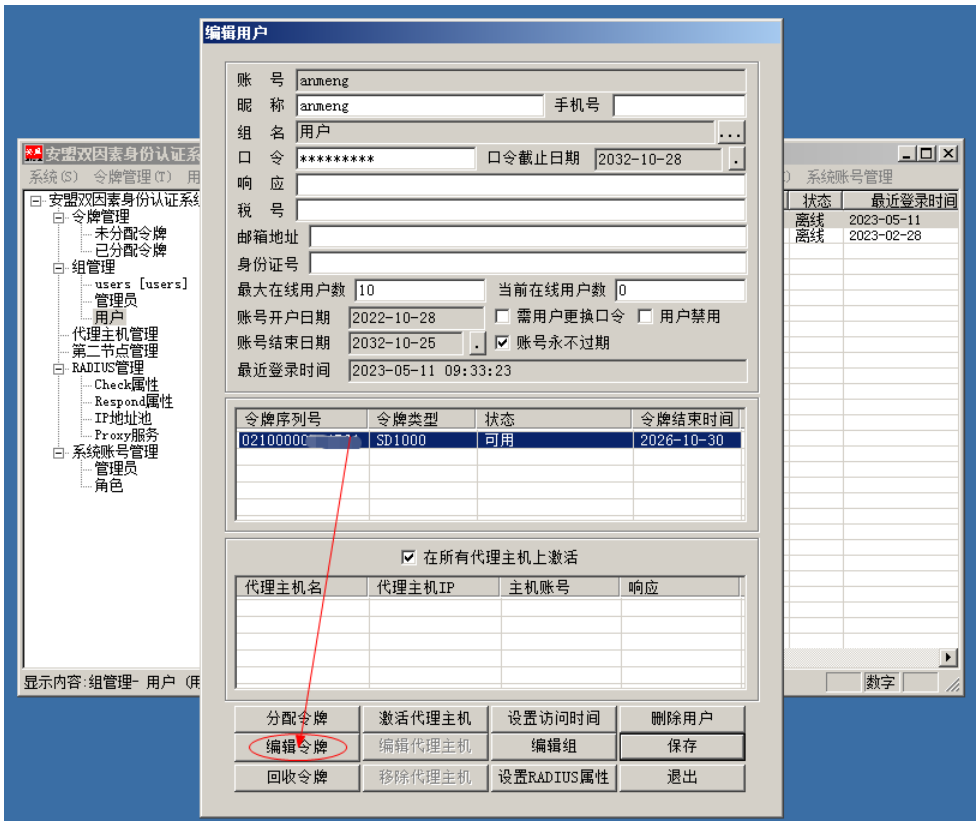
选择刚才导入的新令牌



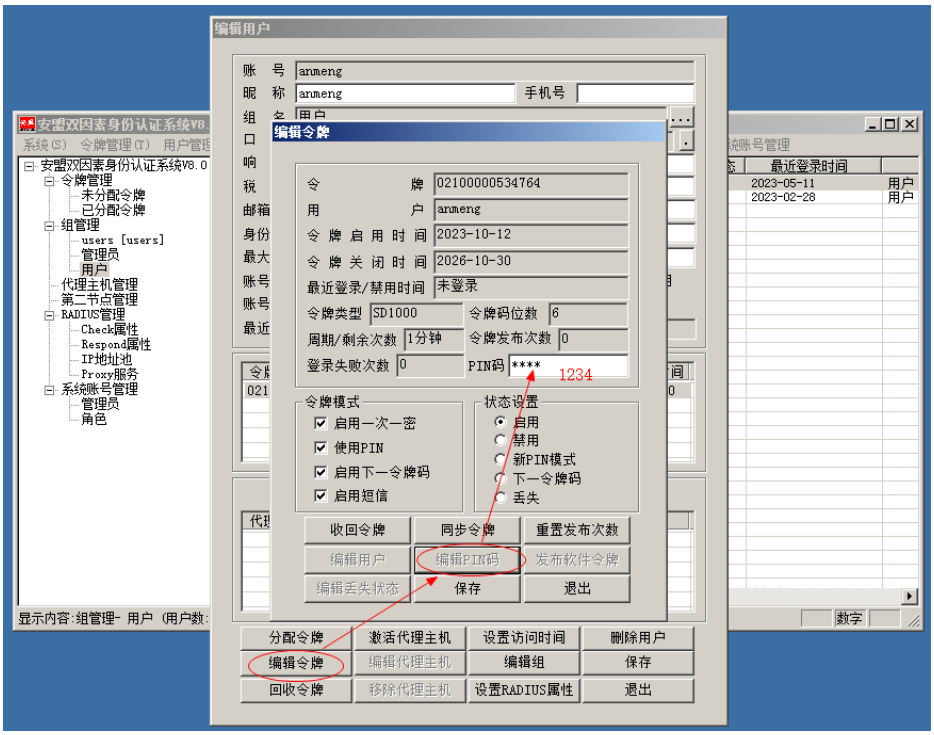
保存配置



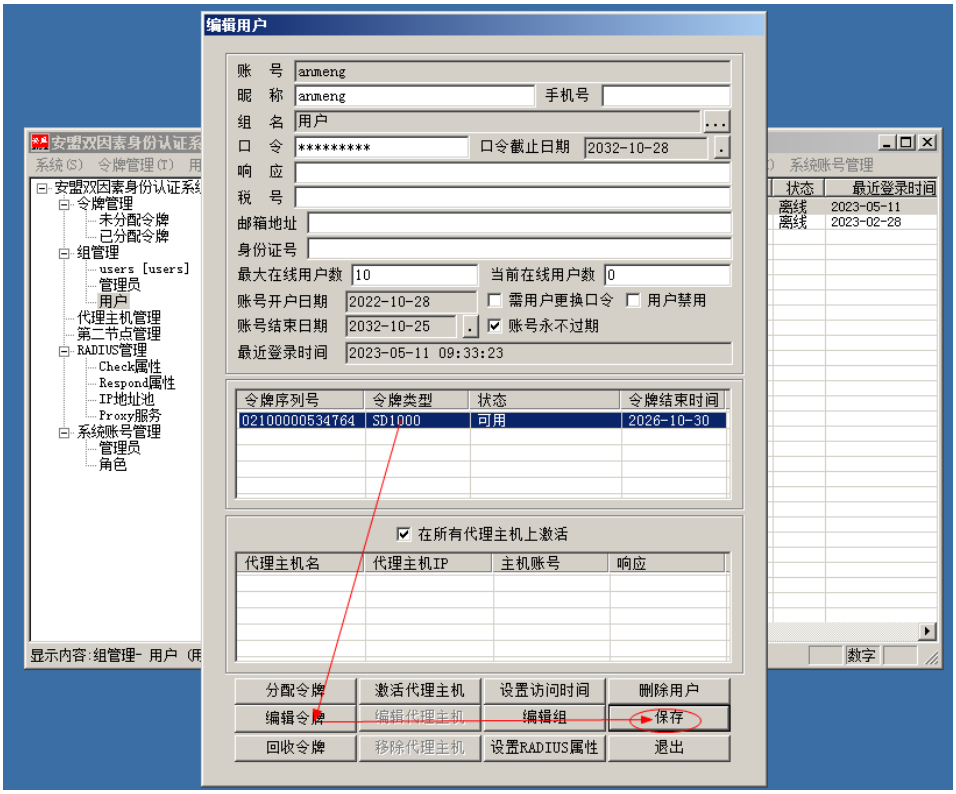
最后设置 PIN 码



为了方便测试假设 PIN 码设置为 1234

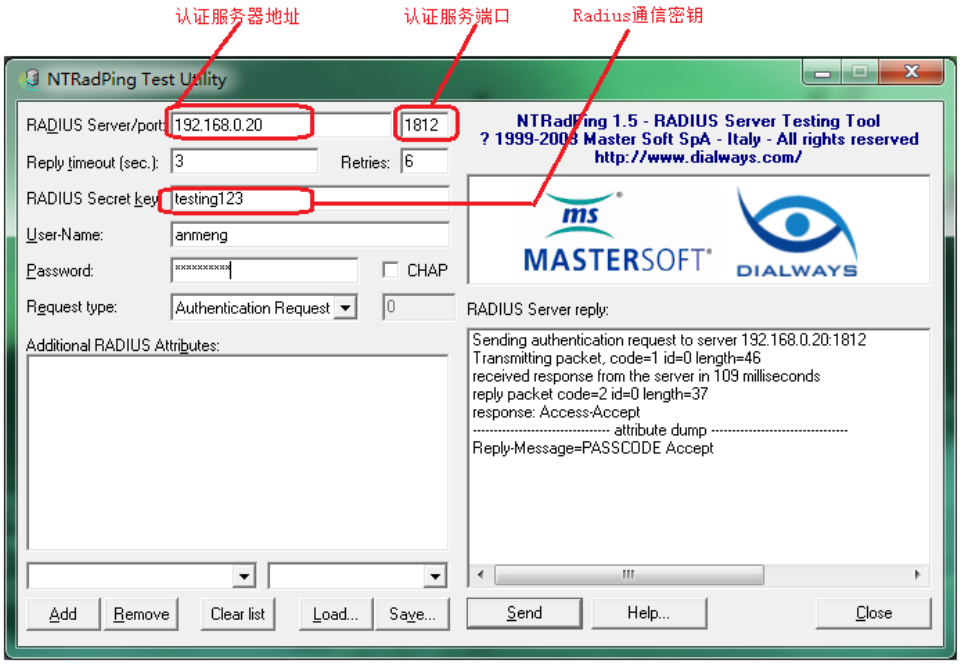


保存所有配置

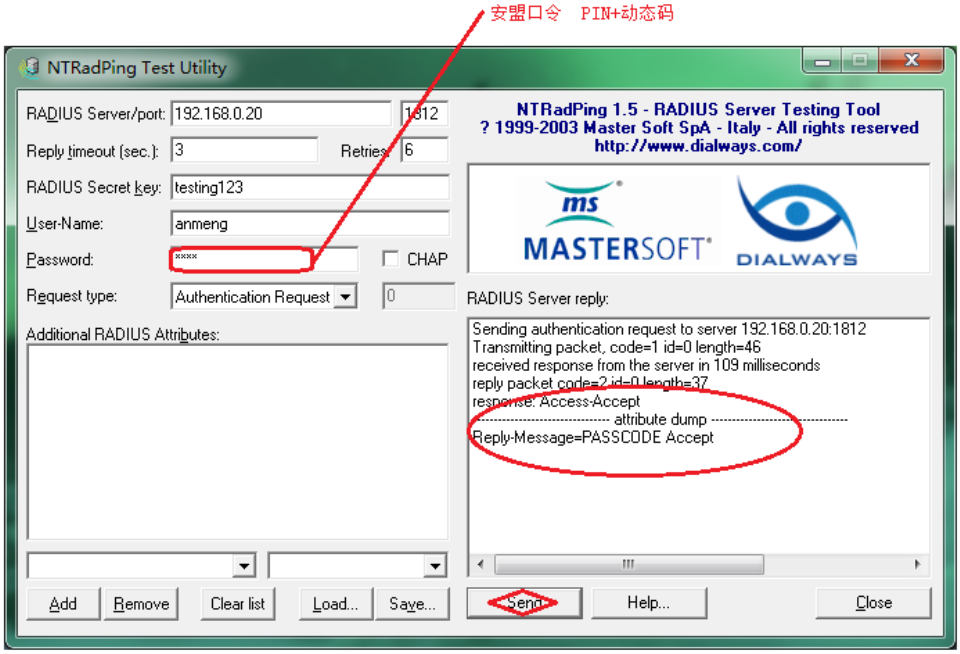


3.2 直接测试认证

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。

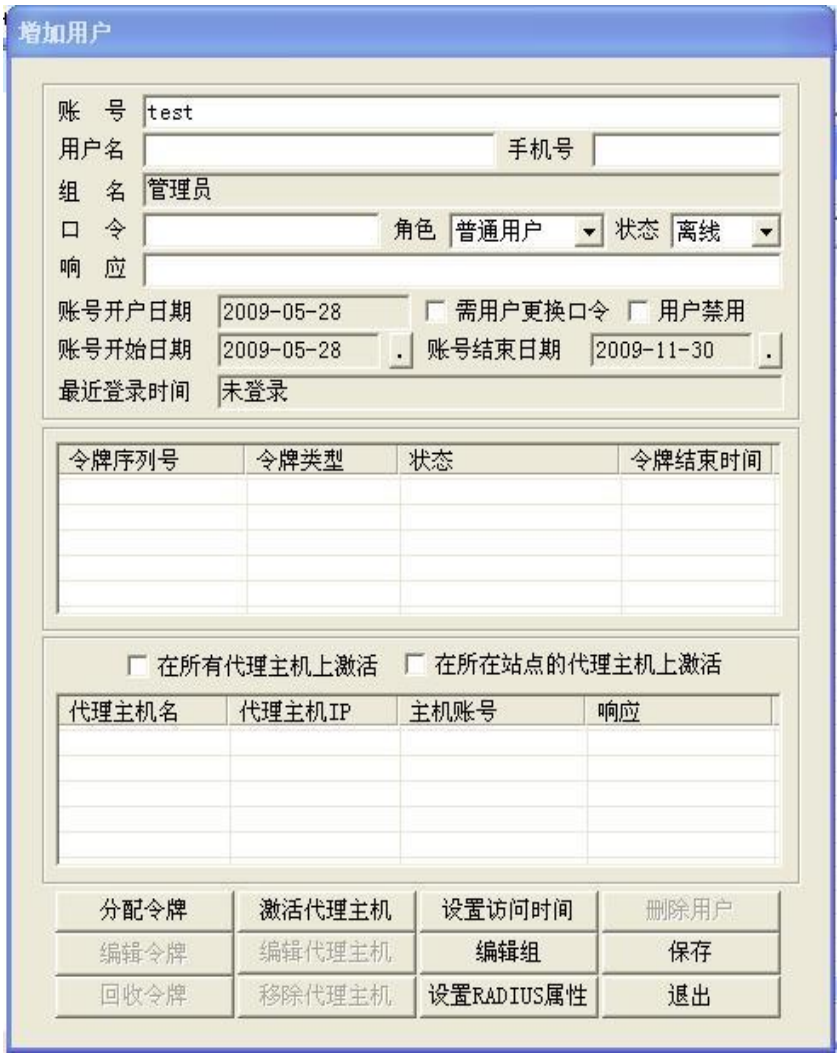
4 用户管理

在安盟认证服务器上注册的用户，默认都是普通用户。

4.1 增加用户

在左侧树列表窗口中选择要增加用户的组，单击鼠标右键/增加用户。或者点击菜单栏上边的用户管理/增加用户。

在弹出的增加用户对话框里输入用户帐号，还可设定密码和用户类型等，再点击**确定**按钮。



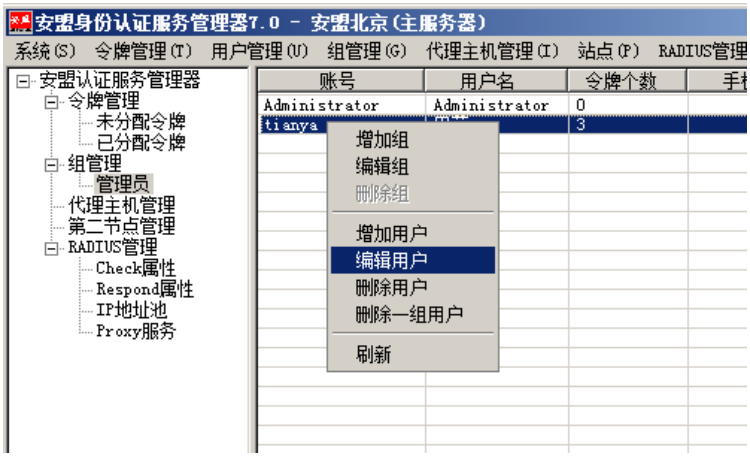
输入用户名“test”，点击保存按钮，可以在右侧信息区看到新添加的用户“test”，用户组为“管理员”。

账号	用户名	令牌个数	手机号	口令	状态	最近登录时间
test		0	18912345678	未设置	离线	未设置

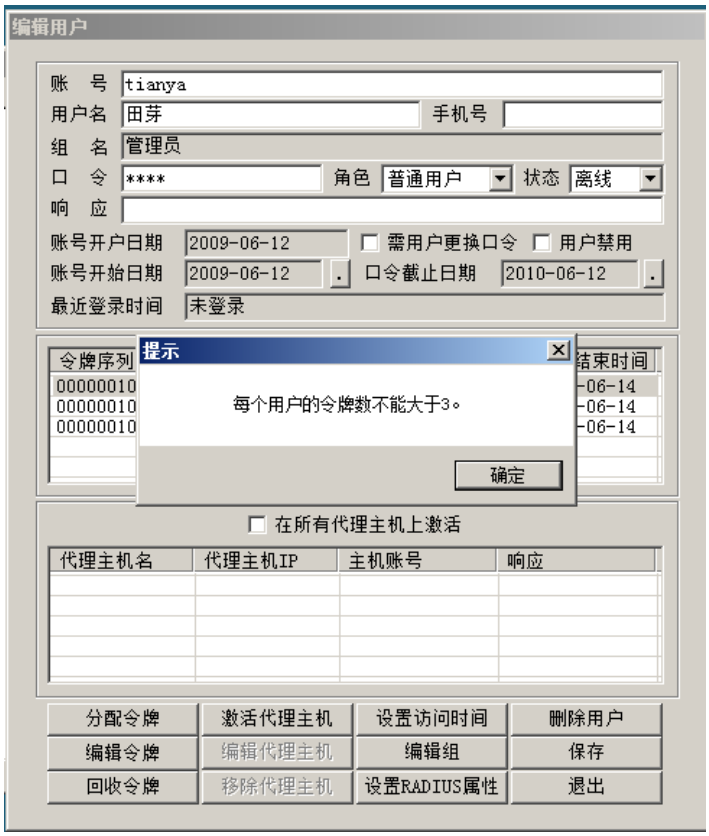
4.2 编辑用户

在树列表中选中要编辑用户的所在组，例如“管理员”，右侧信息区列出该组下所有用户的信息。

选中要编辑的用户，直接双击该用户，或者单击鼠标右键。



弹出编辑用户对话框。假如编辑用户“田芽”，给她分配令牌。



此处就是前边小结提到过的，每个用户只能分配三个令牌。如果大于三个安盟认证系统会给出提示。

4.3删除用户

通过左侧树列表中选择用户所在的组。

在右侧信息列表里选择待删除的用户，单击鼠标右键，在弹出的快捷菜单里点击菜单项

删除用户。

选择**是**，test 用户从数据库中删除。次过程不可恢复，管理员慎重操作。

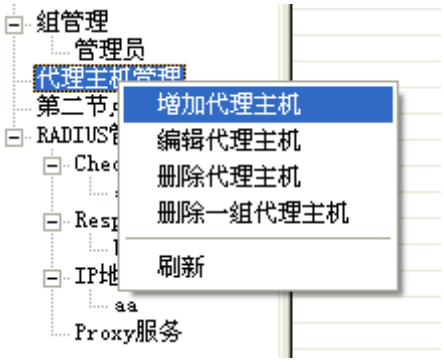
5 代理主机

安盟认证服务器可以使用令牌保护 TCP/IP 网络下的大量资源。安盟身份认证系统保护的计算机和其它设备需要安装安盟代理软件，或者进行特殊配置，使得安盟双因素身份认证服务替代原有的静态口令认证。这些设备称为代理主机。

5.1 增加代理主机

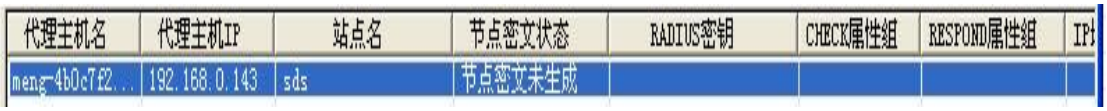
一个代理主机记录必须被添加到为每一个在域中的代理主机的安盟认证服务器软件的数据库。

第一步：在左侧窗口，要增加代理主机的站点>代理主机管理，在右侧窗口右键>增加代理主机。



弹出编辑代理主机对话框，输入代理主机的机器名和 IP 地址。

点击保存。



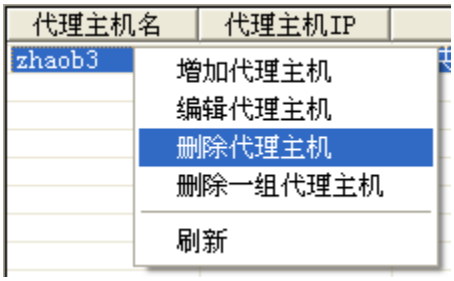
5.2 编辑代理主机

选中要编辑的代理主机，右键>编辑代理主机。

5.3删除代理主机

第一步：在左侧窗口，站点管理>代理主机管理。

第二步：在右侧窗口选中所要删除的主机，右键>删除代理主机。



6 手机令牌管理

6.1 手机令牌安装

6.1.1 安装前准备

6.1.1.1导入安盟软件令牌

管理员登录安盟认证服务器，单击令牌管理，导入安盟软件令牌。

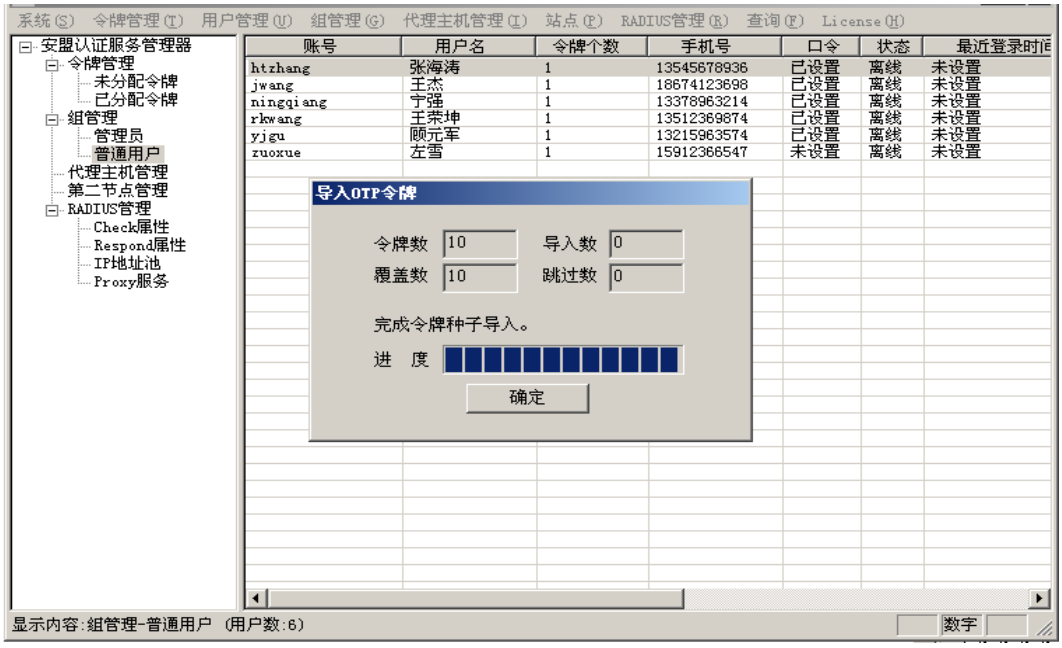


图 6-1 导入令牌

6.1.1.2给用户分配软件令牌

任意选择一个用户，例如用户左雪，双击该用户。

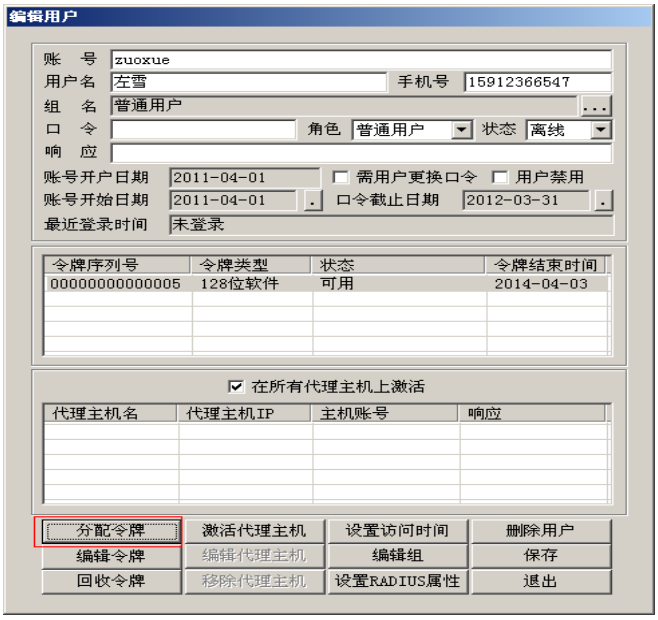


图 6-2 编辑用户

单击<分配令牌>

图 6-3 分配令牌

选择 128 位软件令牌，单击<分配>，回到编辑用户画面。

6.1.1.3发布软件令牌

回到编辑用户画面图 1-2 处，单击<编辑令牌>按钮，此时可以看到安盟令牌状态信息，

然后再点击发布软件令牌

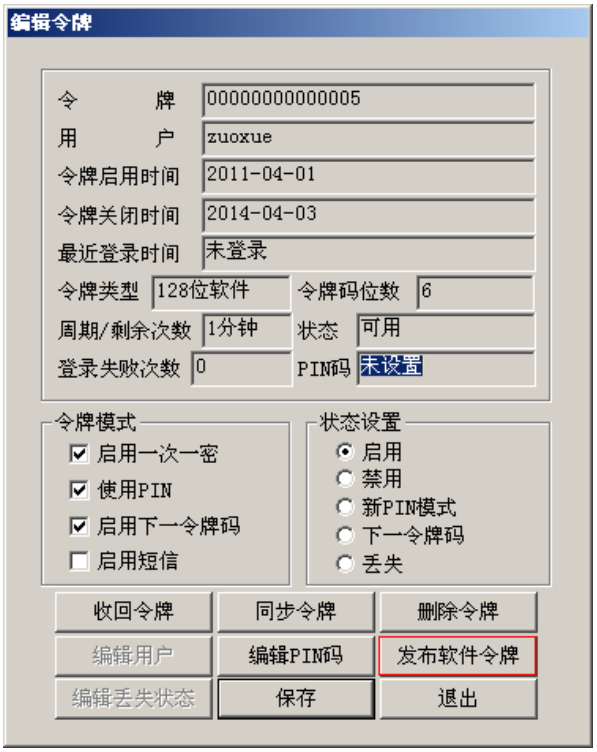


图 6-4 发布软件令牌

单击<发布软件令牌>后，会提示管理员“是否使用口令保护？”此处选择“是”。

图 6-5 设置口令保护

单击<是>。

6.1.2　手机客户端准备

6.1.2.1安盟手机令牌（Android 版）

主界面

安盟手机令牌-Android 版提供了 3 种导入令牌种子文件的方式，方便用户选择：

6.1.2.2安盟手机令牌（IOS 版）

安盟手机令牌 2.0-IOS 版提供了 2 种导入令牌种子文件的方式，方便用户选择：

- 网络激活：导入令牌种子文件时，需要指定令牌种子文件的 URL 地址和导入密码，如下图所示：

此种方式所指的令牌文件（.xml）需要用附件中的“GenMobileTokenFile.exe”对从安盟认证服务器中发布的软件令牌种子进行重新封装，且导入密码也是由 GenMobileTokenFile.exe 生成，详情请参考 GenMobileTokenFile 使用方法。

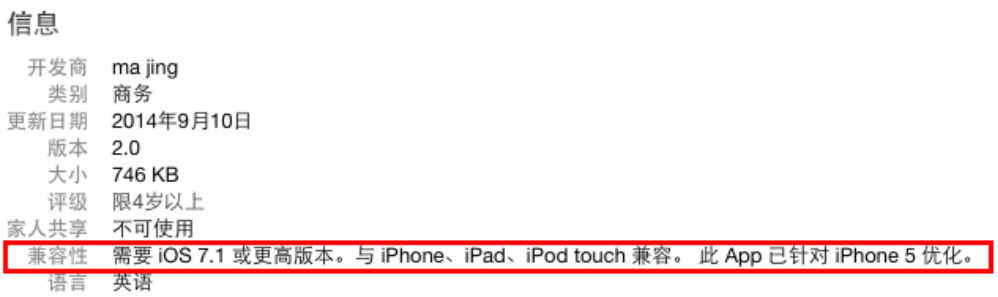
- 本地激活：即将令牌种子文件的内容复制到手机上，如下图所示：

此种方式所指的令牌文件（.xml）也需要用附件中的“GenMobileTokenFile.exe”对从安盟认证服务器中发布的软件令牌种子进行重新封装，且导入密码也是由 GenMobileTokenFile.exe 生成.

6.1.2.3安装安盟 iPhone 手机令牌

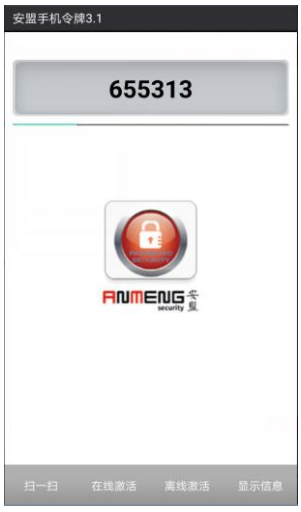
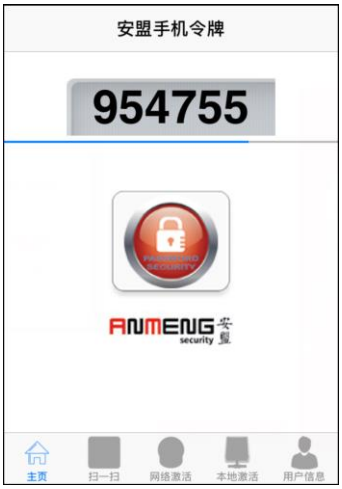
如需安装安盟手机令牌，请到 App Store 上查找安盟手机令牌 2.0,如下图所示:

安盟手机令牌需要 iOS7.1 或更高版本才能安装,因此,如果您的手机不能升级到 iOS7.1 的话,可以安装安装手机令牌老版本,即上图中没有被红框框住的那个版本,使用方法请参考<<安盟 iphone 手机令牌_管理员手册 v1.2.pdf>>.



6.1.2.4安装安盟 Android 手机令牌

6.2手机令牌使用

Android 版本主界面	iOS 版本主界面
	

手机所显示的密码，就是安盟软件动态码，在登录系统时，输入该动态码完成登录认证。

7 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 7.0→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：

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。

7.1 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。

7.2 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。

7.3 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。

7.4清理节点密文

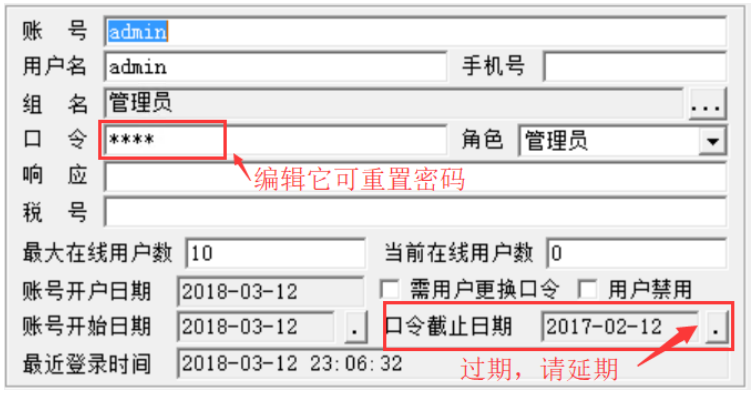
此种情况是，原先可以正常认证，后期变动路由或交换机等网络设备，致使消息包传送路径发生变化，需要执行请节点密文操作。

7.5密码不正确

认证信息如下：

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。



   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。

7.6用户不在代理主机上

认证信息如下：

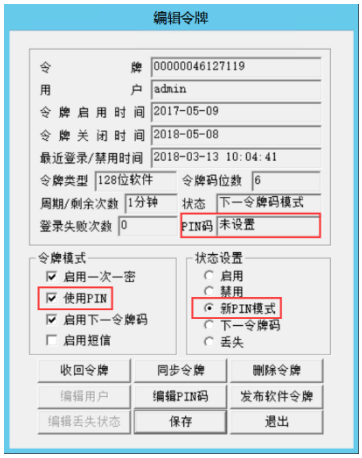
解决办法：

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。

7.7 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

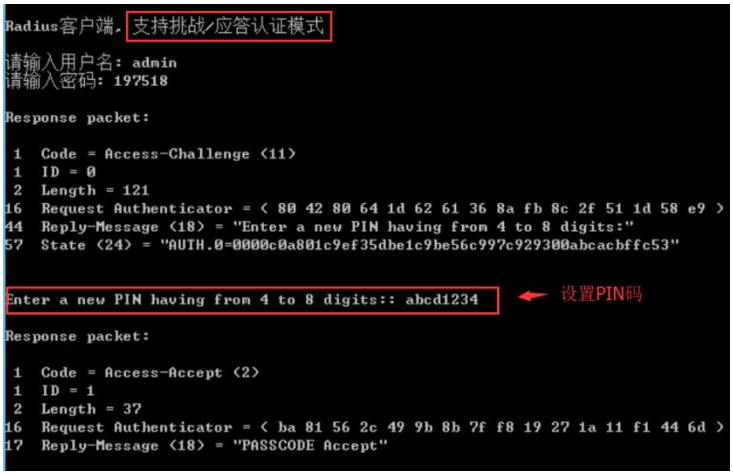
1) 当认证对象为令牌序号时，表示用户的令牌模式钩选了使用 PIN，但尚未设置 PIN 码，或者是用户令牌的状态为新 PIN 模式，如下图所示：



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：



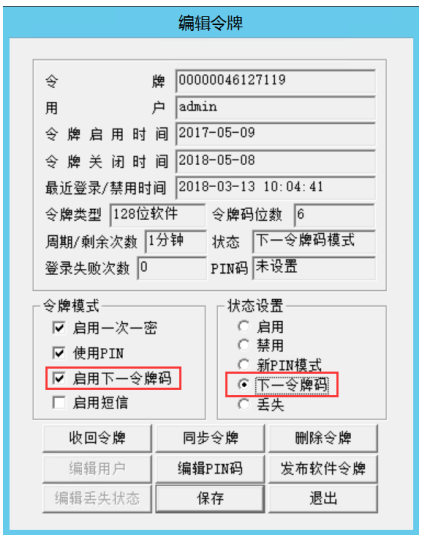
PIN 设置成功，在认证日志中，将新生成一条设置新 PIN 码成功的日志，如下图所示：

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

7.8 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

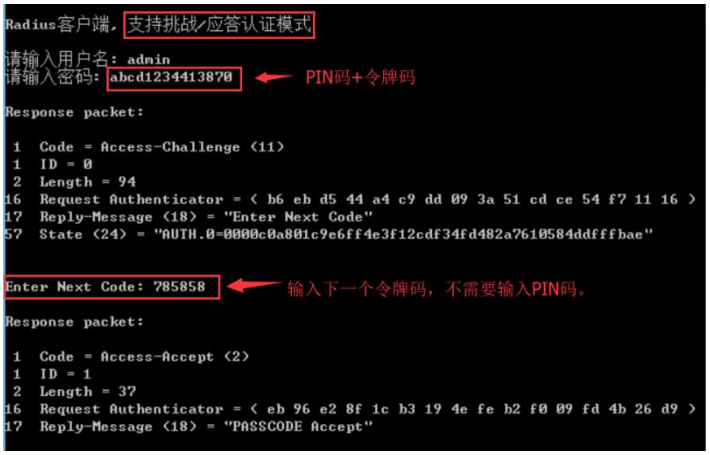
当用户令牌的模式钩选了启用下一令牌码，且令牌的状态为下一令牌码时，在用户输入正确的 PIN 码+令牌码后，会提示需要下一个令牌码，如下图所示：



解决办法：

a) 在编辑令牌窗口，将令牌的状态设置为启用状态，并保存。

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：

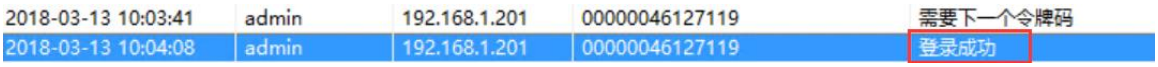


所谓的下一个令牌码，是相对于用户登录时，所输入的那个令牌码来讲的，假设有以下 5 个令牌码：

387212	413870	785858	341375	901562

假设，用户在登录时，输入的密码是 abcd1234413870，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：



7.9 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。