“易安全动态密码系统”服务器管理员手册

深圳市海月通信技术有限公司

一、软件安装的安装与备份

1. 安装“易安全动态密码服务器管理系统”的机器最低配置要求：CPU 800M，硬盘空间：1G，内存 256M，操作系统为 Windows 2000 Server 或 windows 2003 Server，安装本软件前需要先安装 Microsoft SQL Server 2000。
2. 打开光盘，双击“易安全动态密码服务器管理系统.exe”进行安装，安装目录可以自行设定，按照系统提示进行安装。
3. 安装完毕后， 利用本软件建立一个数据库。方法：开始→程序→易安全动态密码服务器管理系统→设置数据库连接，点击<新建>建立数据库。
4. 如果需要重新安装本软件，直接安装本软件，不需要重新恢复数据库。
5. 数据资料的备份，可以通过 Microsoft SQL Server 的企业管理器把你建立的数据库备份或者利用本软件主窗口的“系统”→“数据备份”菜单功能进行备份。
6. 如果需要恢复数据，通过 Microsoft SQL Server 的企业管理器把备份的数据库直接恢复到数据库中。
7. 本软件为 C/S 模式，可以在多台机器上安装，配置数据库服务器的相关信息，即可使用。用户登录密码安全管理系统的密码默认为空。注意：在多台机器上面“易安全动态密码服务器管理系统”时，必须保证安装的机器时间的准确性。

二、软件主要功能介绍

1. **导入 SN**，导入供应商提供的密码卡的 SN 号，包含了购买的密码卡的信息。
2. **删除 SN**，删除导入密码卡的信息。
3. **用户组管理,**对用户进行分组管理，用户组可以新增、修改、删除。
4. **导入用户**，导入指定格式的用户到系统
5. **增加用户**，指的新开通一个用户，这里指的用户是需要登录客户应用软

件系统的用户，并非登录本软件的用户。用户应用软件的用户想通过动态密码管理，必须增加这个用户后，才能使用。

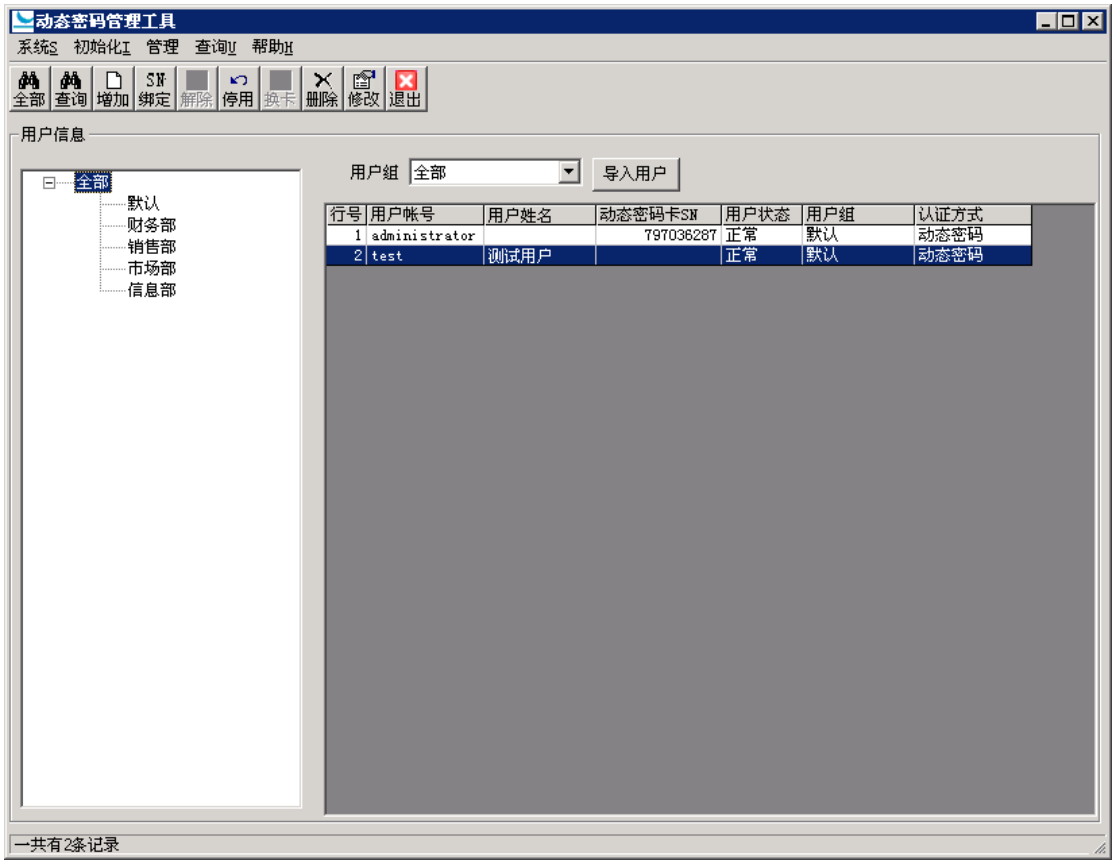
6. **绑定 SN**，把用户与一个 SN 号进行绑定。
7. **取消绑定,**把用户与绑定的 SN 进行取消。
8. **停用**，当用户的密码卡丢失后，可以通过停用处理，让用户的密码卡暂时不能使用。
9. **恢复**，把已经挂失的密码卡恢复到可以使用状态
10. **删除**，把已经开通使用安全密码的用户进行删除，使该用户不可登录客户的应用软件系统。
11. **换卡**，主要是把用户当前使用的密码卡更换成另外一个密码卡。
12. **解 PIN 码**，当用户使用密码卡时，连续 6 次输入错误的 PIN 时，密码卡会被锁定，此时可以通过此功能来进行解锁。
13. **同步服务器密码**，当用户连续生成 19~21 个密码(或者更多的密码)，而不登录客户应用软件的时候，这时密码卡再生成的密码不可用。密码卡需要与服务器进行同步后才能正常使用。
14. **管理员操作日志**，查看管理员操作系统的日志，系统记录的操作内容包括：新增用户、挂失用户，恢复挂失用户、修改用户信息、注销用户，以及换卡操作。
15. **用户登录日志分析**，可以统计分析某一时间段内用户成功或错误登录系统的数据。同时可以对应用安全策略的用户解除禁止登录系统的限制。
16. **安全策略**，安全策略是设置用户登录系统尝试次数达到规定次数时，系统中止用户与系统之间的会话。防止用户受到恶意攻击。系统默认设置为：用户连续登录 10 次失败时，系统将该用户锁定 10 分钟，用户不能在 10 分钟内不能登录系统。该值可以配置。通过“管理→安全策略”进行配置。

三、软件使用方法

1. 配置数据库服务器，选择“开始”→程序→“易安全动态密码服务器管

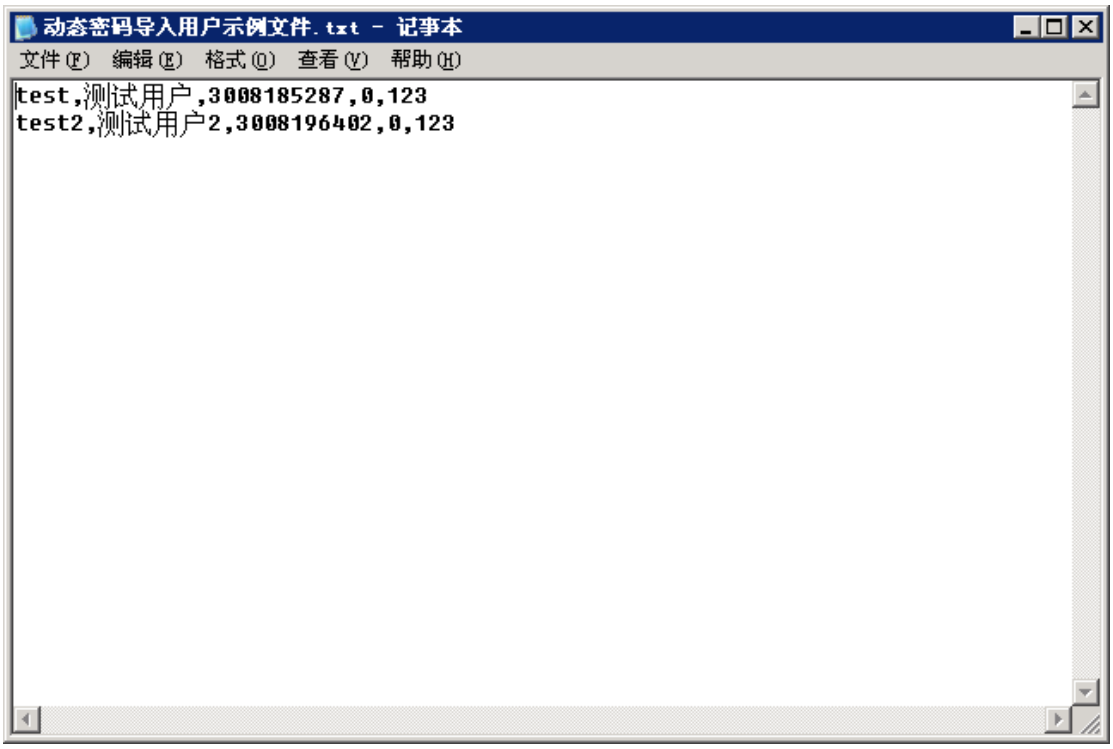
理系统”→“设置数据库连接”，然后输入数据库用户名、密码、服务器、并且选择数据库，点击“保存” 如下图所示

2. 登录后，是系统的主界面，可以在上面进行各种操作，如下图所示：



3. 修改登录密码，通过“系统”→“修改密码”菜单进行操作。
4. 备份用户数据，通过“系统”→“数据备份”菜单进行操作。备份后的文件为数据库备份文件，必要时可以恢复数据。
5. 导出数据，把当前的用户信息导出到 Excel。通过“系统”→“导出数据”菜单进行操作。
6. 导入 SN，把供应商提成的密码卡信息导入到系统中。
7. 删除 SN，可以把导入的 SN 进行删除。
8. 用户组管理，可以对用户组进行增加，修改，删除，查询等操作，通过“初始化”→“用户组管理”进行操作。用户组管理的界面如下：

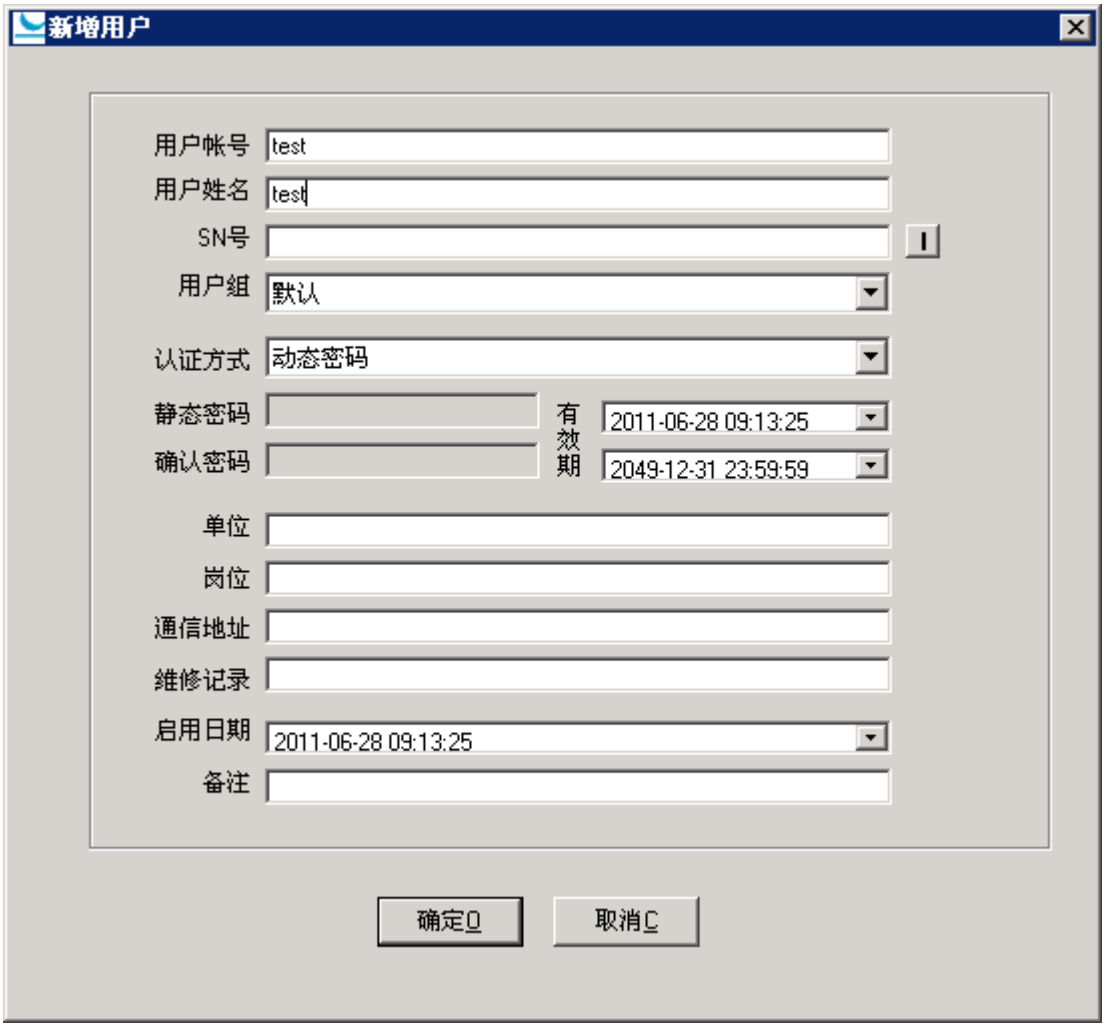
9. 导入用户，导入用户的格式为文本格式，每一个用户作为文本文件的一行。如下图所示：



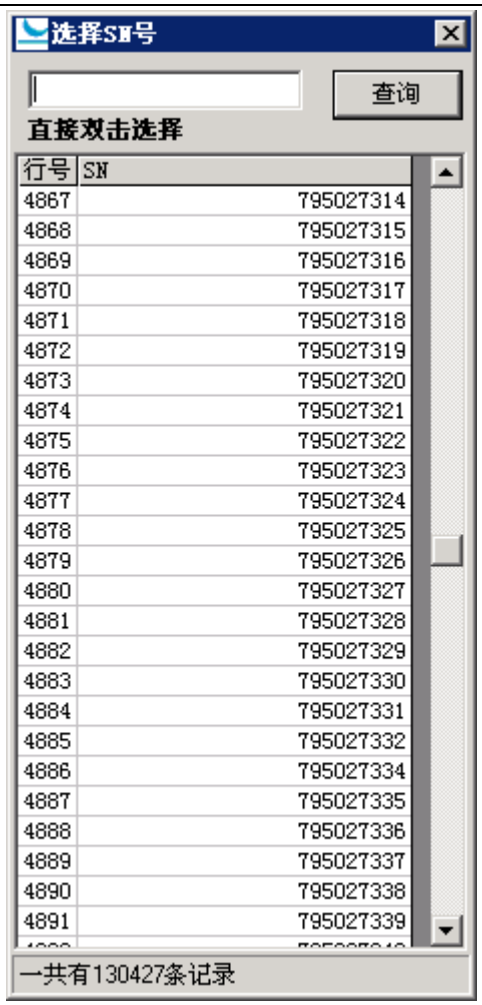
别外软件还支持别的导入格式,具体的格式请与海月通信联。

10. 查找用户，可以对已经开户的用户根据用户名，密码卡的 SN 号，用户组等信息进行查找。通过“管理”→“查询”菜单操作或者直接点击工具栏的“查询”。

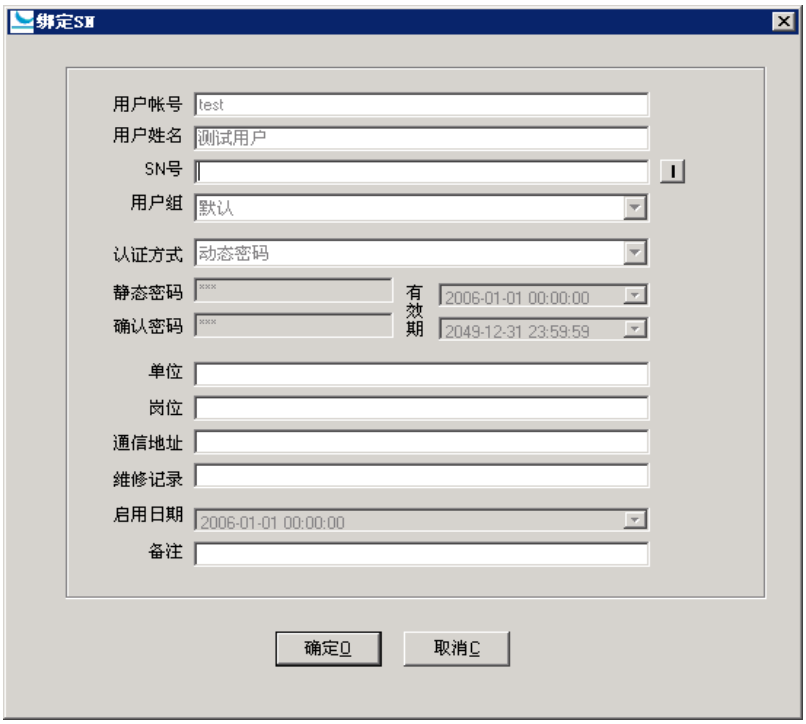
11. 新增加用户，新增加用户时使用，通过“管理”→“新增用户”或者直接点击工具栏“新增”，在弹出的窗口中输入用户帐号和 SN 号。然后点击“确定”按钮保存。如下图所示：



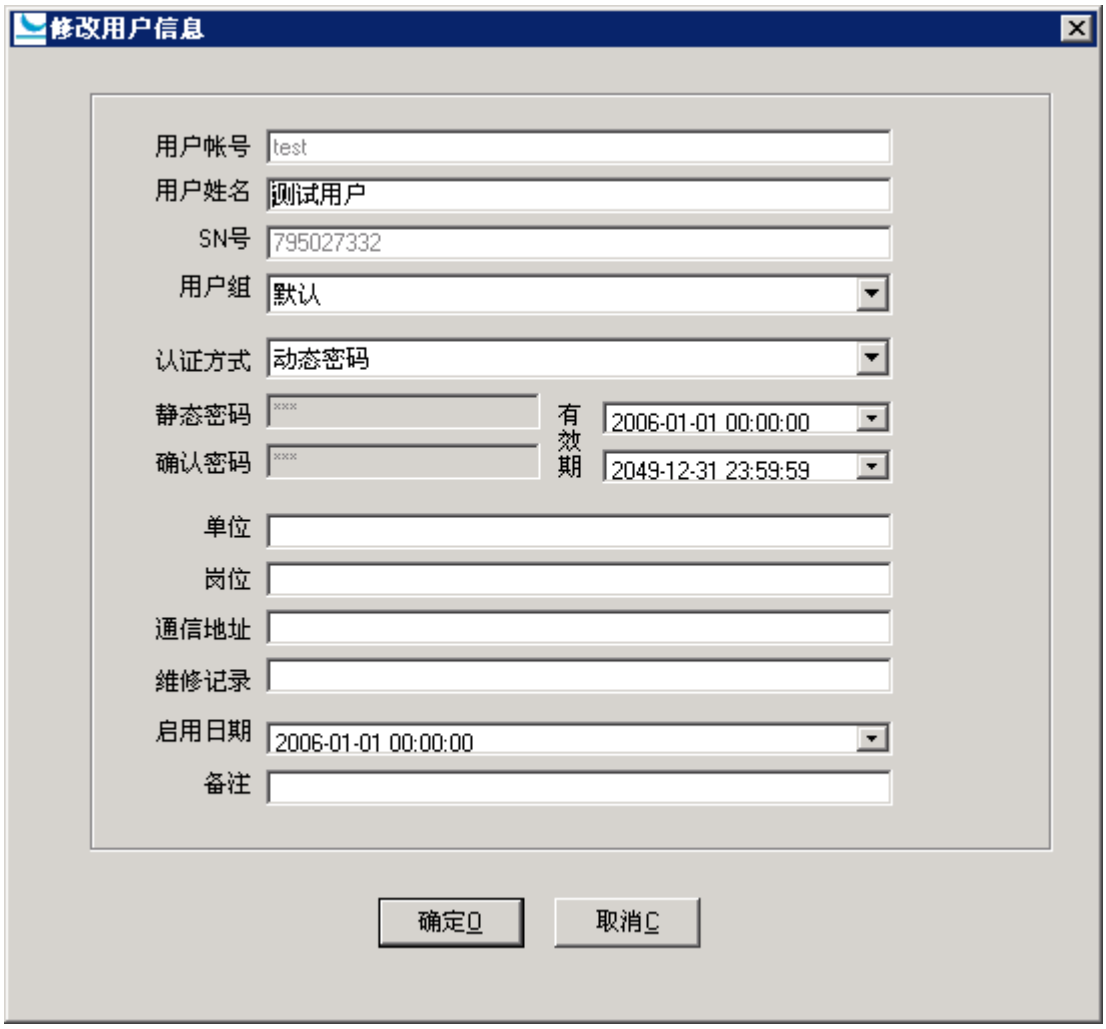
说明：用户的认证方式有三种，动态密码、静态+动态密码、静态密码方式，SN 号可以通过点击旁边的按钮在弹出的窗口中进行选择，在弹出的窗口选中要选择的 SN 号，然后双击即可。如下图所示：



12. 绑定 SN，通过“管理”→“绑定 SN”或者直接点击工具栏“绑定”，在弹出的窗口中，输入 SN 号或者选择 SN 号，如下图所示：



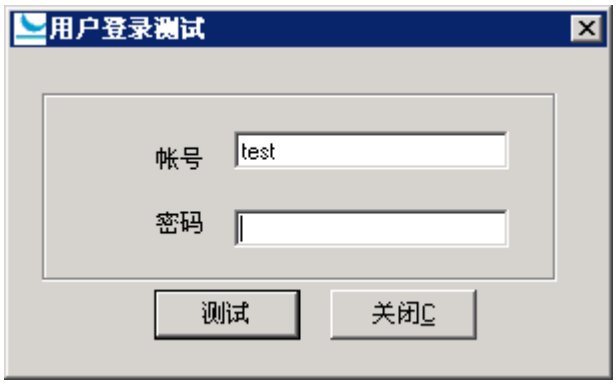
13. 解除绑定 ，通过“管理”→“取消绑定”或者直接点击工具栏“解除”，在弹出的窗口中点击“确定”按钮
14. 停用处理，通过“管理”→“停用用户”或者直接点击工具栏“停用”，在弹出的窗口中点击“确定”按钮。
15. 恢复，通过“管理”→“恢复用户”或者直接点击工具栏“恢复”，在弹出的窗口中点击“确定”按钮。
16. 修改用户信息，主要是修改用户的信息，通过“管理”→“修改用户”或者直接点击工具栏“修改”，在弹出的窗口修改所需要的信息，然后点击“确定”按钮。如下图所示：



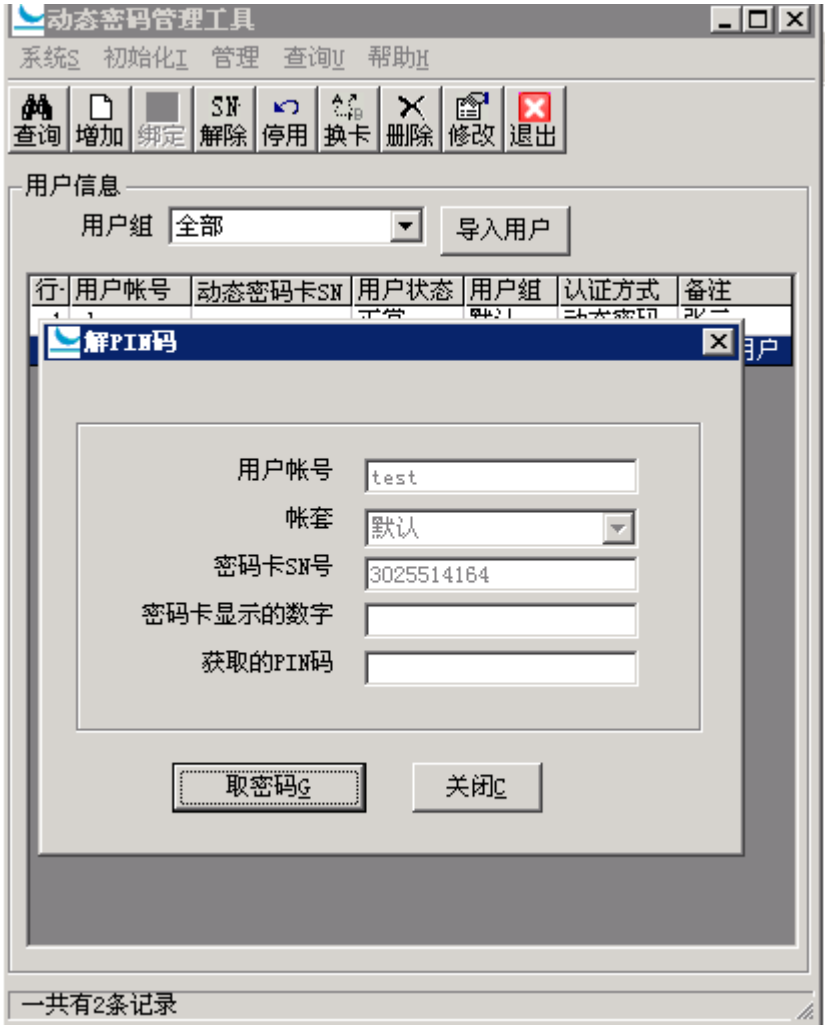
17. 换卡，当用户更换密码卡时使用，通过“管理”→“用户换卡”或者直接点击工具栏“换卡，在弹出的窗口输入新的密码卡的 SN 号，然后点击“确定”按钮，保存数据。如下图所示：

18. 删除用户，通过“管理”→“删除用户”或者直接点击工具栏“删除”，在弹出的窗口中点击“确定”按钮。

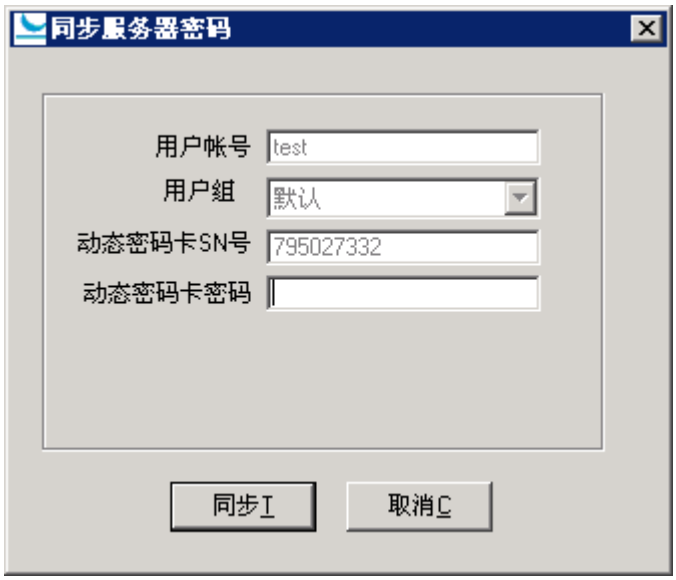
19. 登录用户登录，增加用户后，可能通过此功能来测试用户登录是否正常，如果用户是“静态+动态密码”认证方式，先输入个人的静态密码，再输入动态密码。如下图所示，



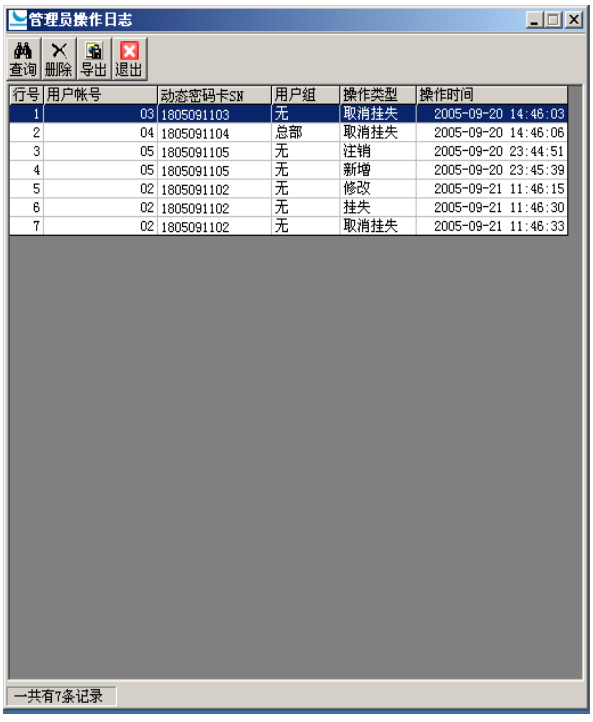
20. 解 PIN 码，通过“工具”→“解 PIN 码”进行操作（这个操作只针对 SecureCard）。在出现的窗口中，输入密码卡的显示的 10 位数字(说明：密码卡被锁定时，连接按两下 ON 键，在密码卡上显示的 10 位数字，第一次按下的显示是密码卡的 SN 号)，点击“取密码”，然后用生成的 6 位密码来解除密码卡的锁定。如下图所示：



21. 同步服务器密码，当动态密码产品的时候与服务器时间出现偏差，这时需要同步服务器密码，同步以后。用户的密码卡生成的密码可以继续使用。通过“管理”→“同步密码”进行操作，在出现的窗口中，输入用户密码卡当前的密码，然后点击确定。如下图所示：



22. 管理员操作日志，要对系统的管理员操作日志进行管理，可以通过“查询”→“管理员操作日志”菜单进行操作，操作日志记录有对用户新增、绑定 SN、取消绑定、修改，停用、取消停用、删除的操作记录，操作日志功能可以查询到这些日志。管理员可以对这些日志进行查询、导出和删除。如下图所示：

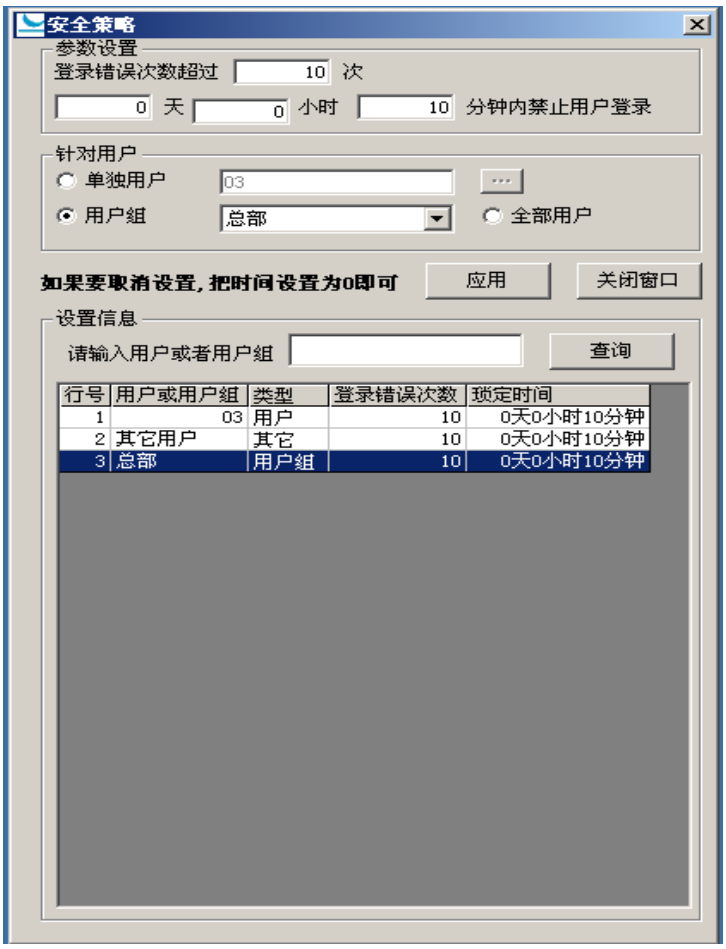


23. 用户登录日志分析，主要用于分析用户通过“密码安全系统”登录系统的数据，通过分析，可以统计出用户登录次数、登录成功次数，登录错误次数的信息，以及对于应该安全策略的用户取消不能登录系统的限制。通过“查询”→“用户登录日志分析”进行操作，如下图所示：

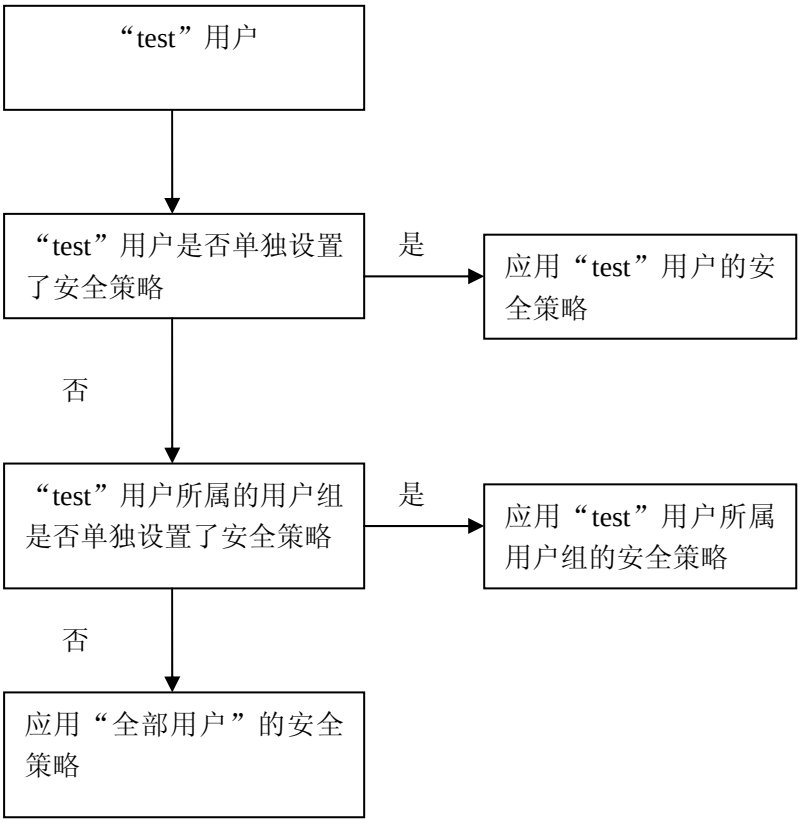
对于已经被锁定的用户，系统管理员可以取消锁定，方法：先选择被锁定的用户，然后点击“取消锁定”即可。

如果想查看用户的登录的详细日志，选择要查看的用户，然后点击“详细日志”按钮或者直接双击要列表上面的用户进行查看。

24. 密码卡使用情况，可以查询密码卡的总数、已使用数、未使用数。通过“查询”→“密码卡使用情况”来查看。
25. 安全策略。安全策略是设置用户登录系统尝试次数达到规定次数时，系统中止用户与系统之间的会话。防止用户受到恶意攻击。通过“管理”→“安全策略”进行操作。如下图所示：



说明：设置安全策略时，可以针对单独的用户、用户组、或者全部的用户进行设置，优先组别最高的是“单独用户”，然后是“用户组”，用户或者用户所属的用户组没有设置安全策略时，用户所使用的安全策略是“全部用户”的安全策略。例如有一用户“test”，“test”用户所属的用户组为“总部”，假如“test”用户单独设置了安全策略，那么“test”用户的安全策略为“test”用户单独设置的策略，如果“test”用户没有单独设置安全策略，那么 test 用户应用的策略为“总部”用户组的策略。如下图所示


“test”用户
“test”用户是否单独设置了安全策略
是
应用“test”用户的安全策略
否
“test”用户所属的用户组是否单独设置了安全策略
是
应用“test”用户所属用户组的安全策略
否
应用“全部用户”的安全策略