纹宁指纹安全系统网络版

（v2.0）

使用说明书

WINUIM
纹宁信息

深圳市纹宁信息技术有限公司

Shenzhen WINUIM Information Technology Co., Ltd.

目 录

1 前言 2

2 指纹安全系统客户端 2

2.1 软件安装 2
2.2 首次使用 3
2.3 指纹登录计算机 8
2.4 用户管理 9
2.4.1 创建用户 11
2.4.2 删除用户 13
2.4.3 用户设置 14
2.4.4 密码设置 15
2.4.5 指纹管理 16
2.4.6 管理云帐户 17
2.4.7 同步云帐户 18
2.5 日志管理 19
2.5.1 查看本地用户日志 20
2.5.1 查看本地登录日志 21
2.5.3 查看网络用户日志 22
2.5.4 查看网络电脑保护日志 23
2.6 AD 域管理 23
2.6.1 参数设置 24
2.6.2 账户同步 25
2.6.3 绑定管理 26
2.7 电脑保护 29
2.7.1 参数设置 29
2.7.2 绑定管理 31
2.7.3 高级选项 36
2.8 远程桌面 37
2.8.1 管理设置 37
2.8.2 建立远程桌面连接 38
2.9 软件卸载 40
2.10 常见错误代码列表 41

3 联系我们 42

1 前言

纹宁指纹安全系统是由深圳市纹宁信息技术有限公司自主研发的一款基于计算机与网络的指纹身份认证登录计算机系统的安全管理软件，软件主要功能包括通过指纹认证安全登录计算机操作系统桌面、通过指纹认证安全登录 AD 域桌面、通过指纹认证安全登录远程服务器桌面、通过指纹认证安全登录 VPN、通过指纹认证安全访问 Linux SSH、通过指纹认证对计算机文件加解密、通过指纹认证远程授权、通过指纹认证保护应用程序等，功能强大、通用性强、操作简单、容易上手。特别适合于政府、军队、军工单位、大中型企业、事业单位等客户使用。

2 指纹安全系统客户端

2.1 软件安装

确保 FPWSS-Setup-纹宁指纹安全系统(客户端-电脑登录).exe 与 config.ini、FPDev.lic 在同级目录，点击软件安装图标 ，弹出安装首页，选择安装语言：



图 1：选择安装语言界面

点击确定按钮，进入安装向导界面，如下图：



图 2：安装向导界面

安装成功后需要重启计算机才能正常使用纹宁指纹安全系统软件。

【注意】安装纹宁指纹安全系统后，系统默认启用交互式登录界面方式——需要按 Ctrl+ALT+DEL 才能进入登录界面，此种方式有利于降低用户受到企图截获密码的攻击和确保用户输入密码时通过信任的路径进行通信。

2.2 首次使用

纹宁指纹安全系统网络版安装完成后，需要重启计算机进入首次使用向导界面：

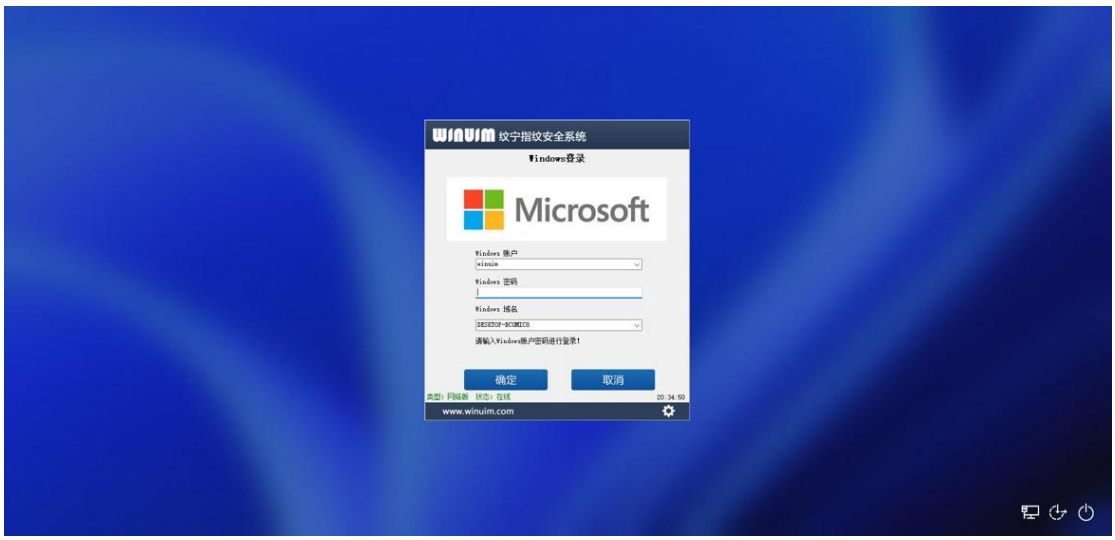

图 3：用户首次登录计算机界面

用户需要输入 Windows 帐户和密码，选择对应 Windows 域或计算机名，点击“确定”按钮登录系统。登录操作系统后，桌面和 Windows 开始菜单会增加如下图标：



图 4：桌面快捷方式图标

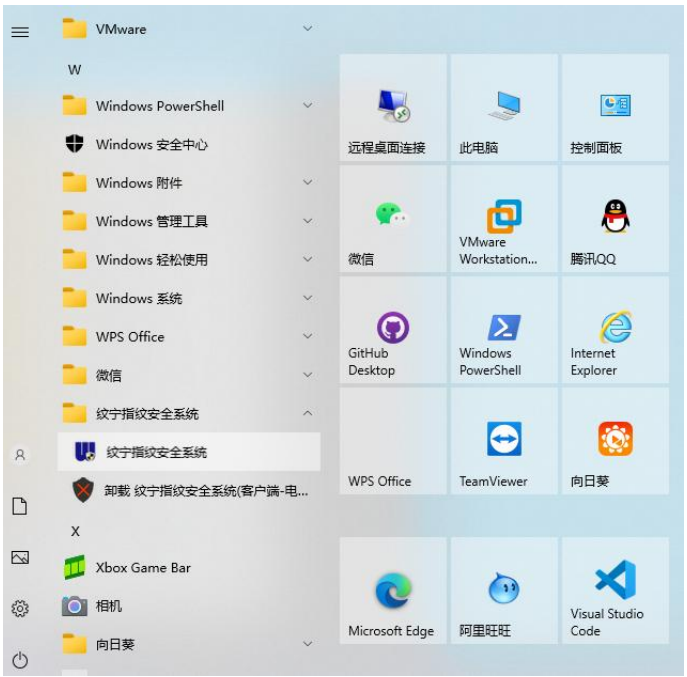

图 5：开始菜单图标

程序安装完成后会自动运行，软件运行在桌面右下角通知区域图标栏处 。



图 6：任务栏程序运行图标

右键程序图标，列出程序管理菜单：



图 7：程序菜单

选择用户管理菜单，将弹出新用户注册界面：







图 8：新用户注册

点击确定按钮，新用户注册成功。



图 9：注册用户成功

注意：

1、系统首次使用时注册成功的用户为指纹安全系统的超级管理员角色用户；

2、超级管理员角色具备系统管理的最高权限；

3、超级管理员角色用户在指纹安全系统有且只有一个；

4、administrator 为指纹系统内置用户，用户名不可选用；

系统已注册超级管理员帐户，将弹出用户身份认证界面，如下图：



图 10：管理员身份认证界面

2.3 指纹登录计算机

计算机在启动、锁定、注销、切换用户、屏幕保护状态下将进入指纹登录界面，如下图：



图 11-1：Windows 指纹登录操作系统界面

用户输入用户名并选择输入指纹、密码或指纹+密码等认证方式进行身份认证，认证成功后即可正常进入桌面。

对于 AD 域控安全策略要求“用户下次登录时须更改密码”的用户，用户在完成身份验证后弹出如下界面：

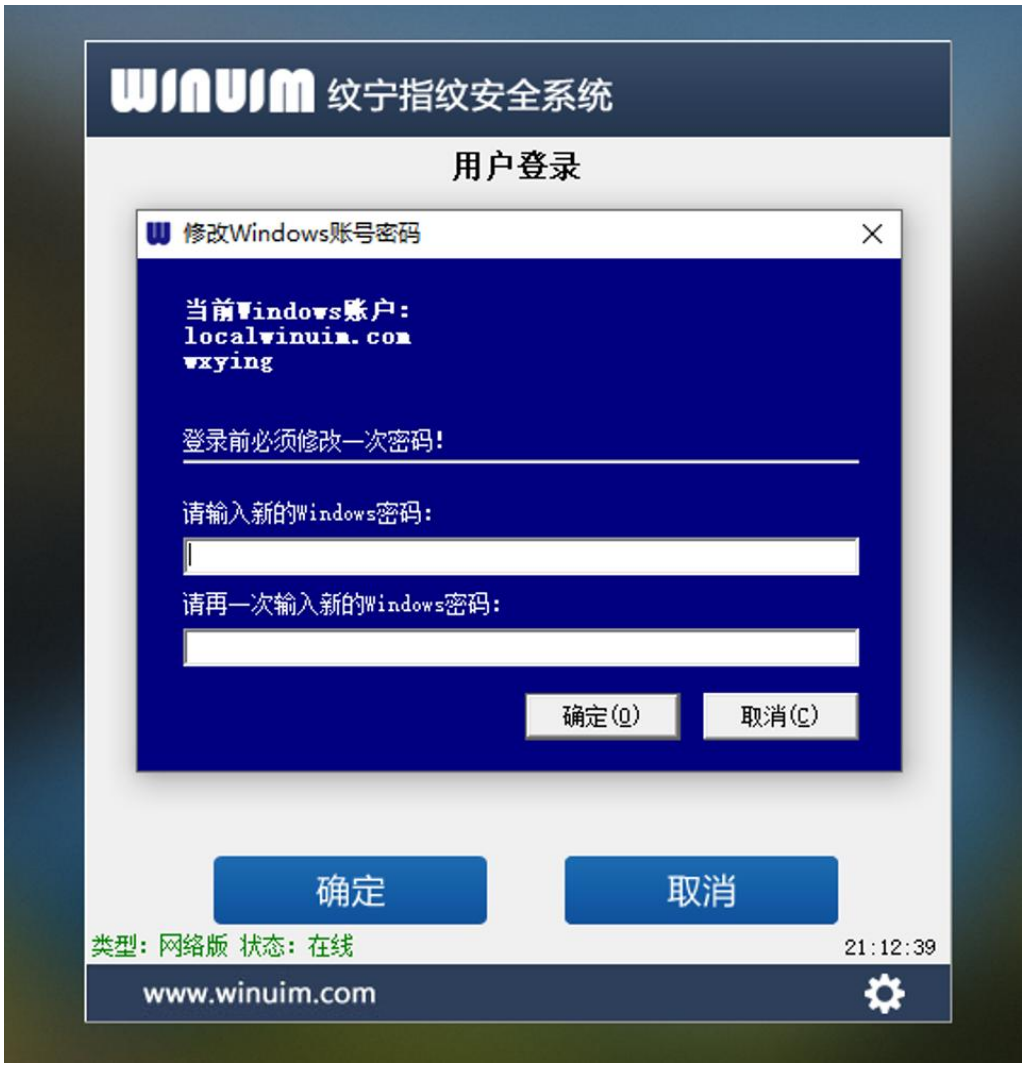

图 11-2：修改 Windows 账号密码界面

用户按照 AD 域控安全策略要求设置好新密码后才能进入桌面。

2.4 用户管理

用户可在桌面右下角通知区域图标栏中右键图标，列出程序管理菜单，如下图：

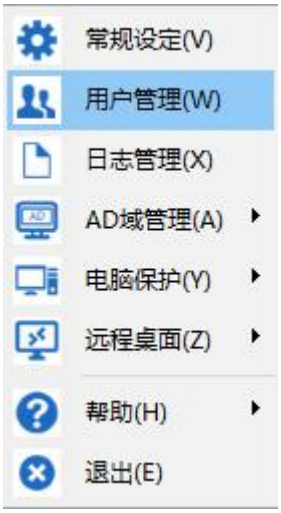

图 12：程序管理菜单

选择用户管理菜单，将弹出身份认证界面，如下图：



图 13：身份验证界面

身份认证通过后可进入用户管理界面，如下图：

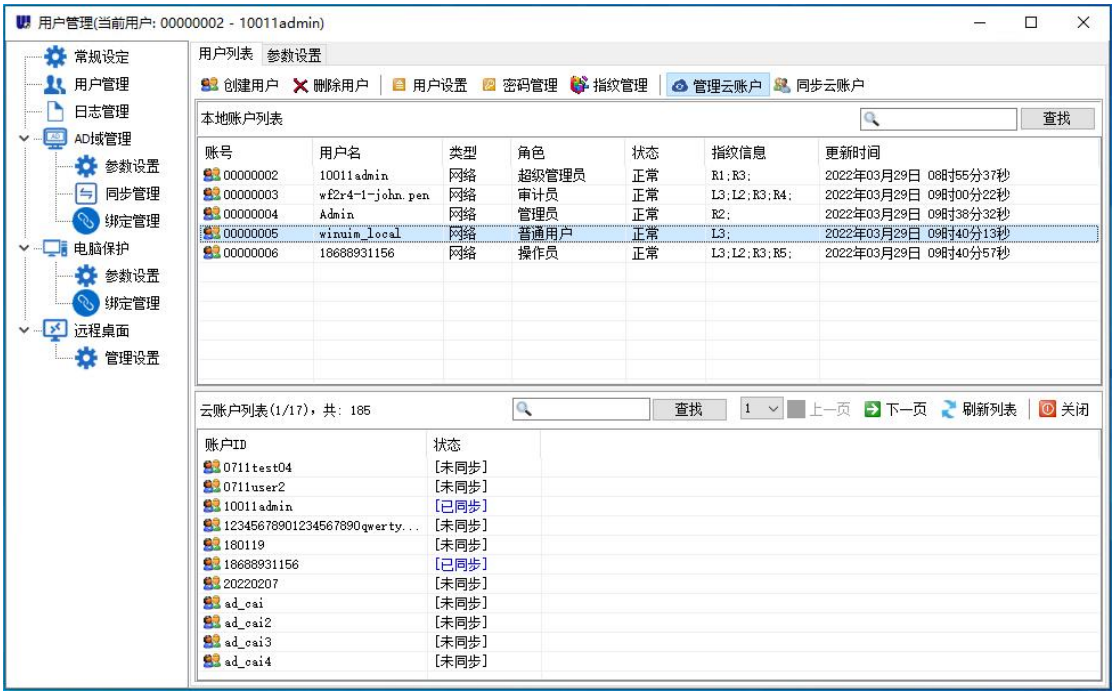

图 14：用户管理界面

系统分为超级管理员、管理员、审计员、操作员、普通用户等角色；

系统默认分配首次注册的用户为超级管理员，超级管理员角色唯一；

超级管理员具备常规设定、用户管理、角色分配、AD 域设置、电脑保护设置等权限；

管理员具备常规设定、用户管理、AD 域设置、电脑保护设置等权限；

审计员仅具备日志管理权限；

操作员仅具备软件卸载时身份认证授权管理权限；

普通用户仅具有本用户同步云帐户权限。

2.4.1 创建用户

输入用户名、密码，录入至少一枚指纹即可完成用户创建，系统会自动分配用户唯一 ID 号；创建用户是在管理员授权下且与服务器网络连接正常的环境下完成的，如需对创建的用户进行密码修改、指纹修改、绑定 Windows 账号等操作，需要切换到相应用户的用户管理及电脑保护设置模块下完成相应操作。

注意：

1、用户名不区分大小写，可以由 3-32 位小写字母、数字、下划线（_）、中杠（-）、点（.）特殊字符组成；

2、密码区分大小写，可以由 6-16 位大小写字母、数字、特殊字符组成；

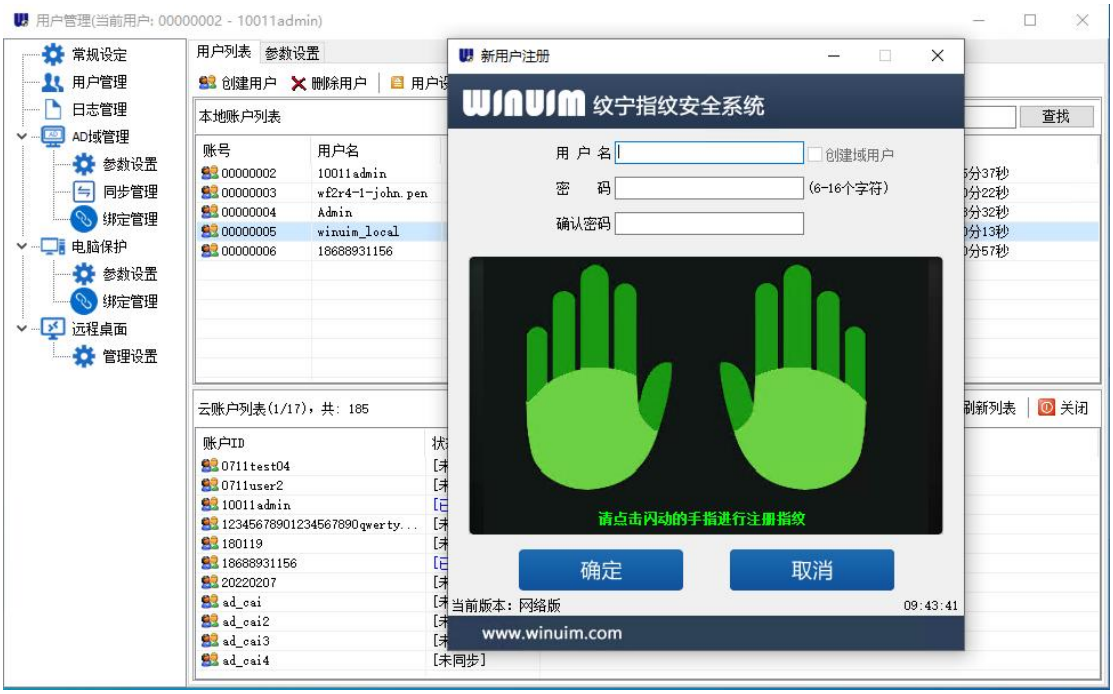

图 15：创建用户界面



图 16：创建用户-输入密码及注册指纹界面

点击确定按钮，系统将注册的用户信息提交到服务器进行注册，如下图：



图 17：创建用户-申请云帐号界面

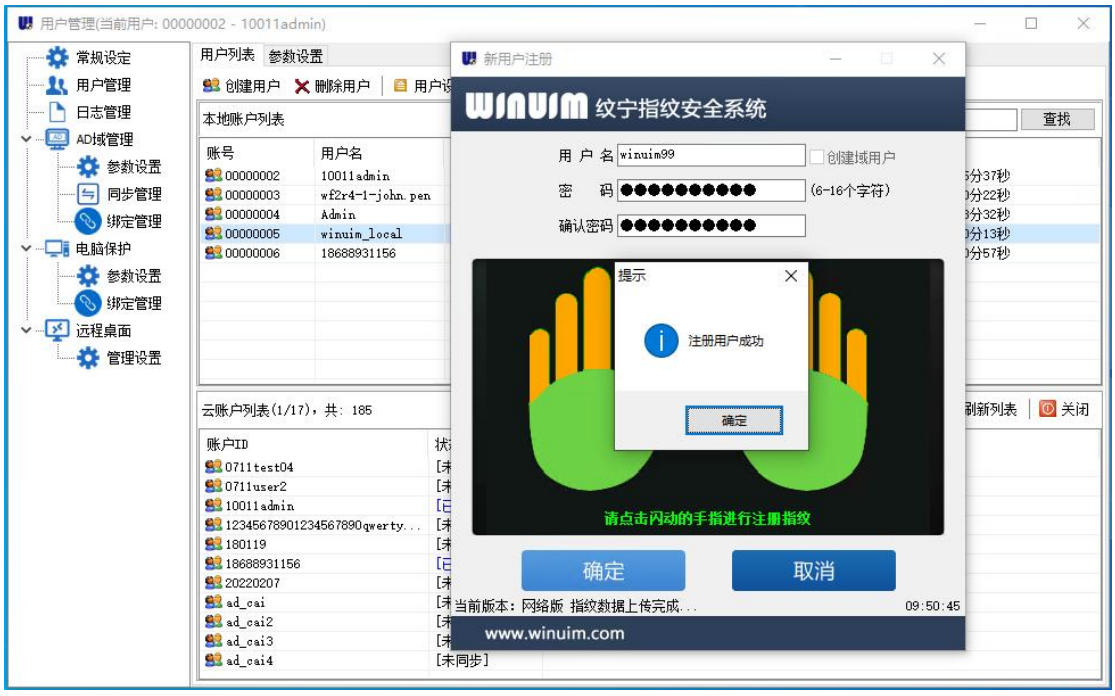

图 18：创建用户成功界面

2.4.2 删除用户

选择需要删除的用户，点击删除用户按钮即可完成用户删除，如下图：

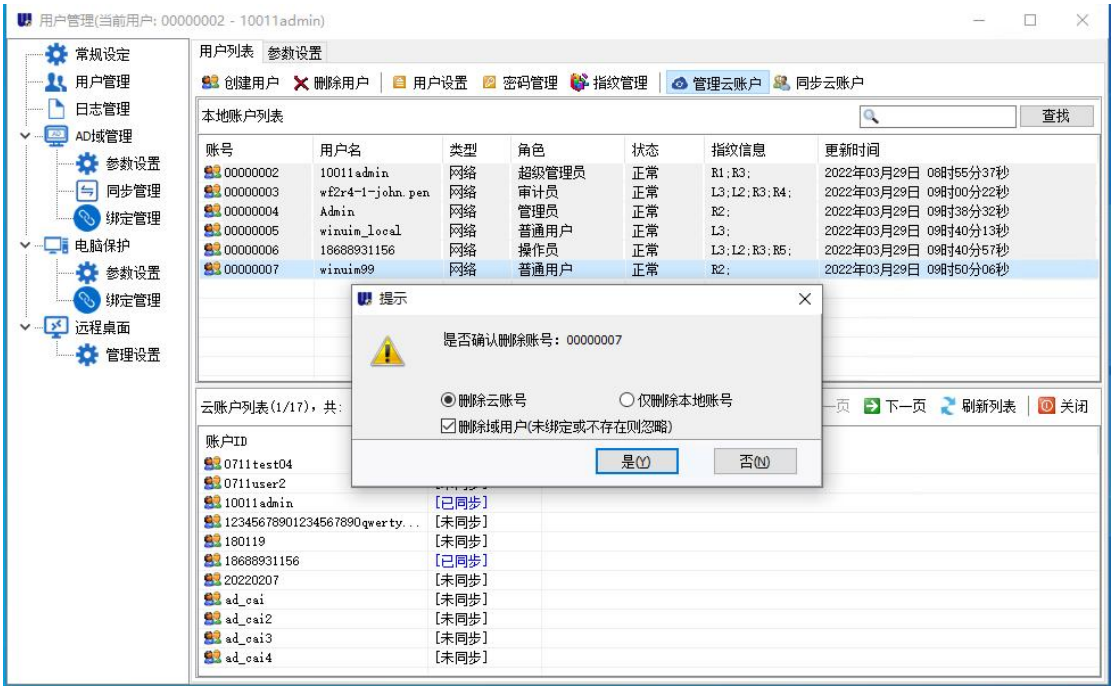

图 19：删除用户界面

删除用户操作可选择删除云账户、删除本地账户和删除域账户，选择删除云账号将删除该用户在服务器端的用户信息，包括用户名、密码、指纹、角色、状态、绑定信息等，不过与该用户有关的登录日志将不会被删除；选择删除本地账号则仅仅是删除该用户在客户端的用户信息，服务器端的信息不会删除；如域控服务器部署纹宁指纹安全系统 AD_Services 服务，在删除有绑定域账号的云账号时勾选删除域用户选项，系统会将该云账号绑定的域账号从域控服务器删除。

2.4.3 用户设置

选择当前用户，并点击“用户设置”图标，可以对用户进行用户名修改和认证方式的设置，具体如下图：

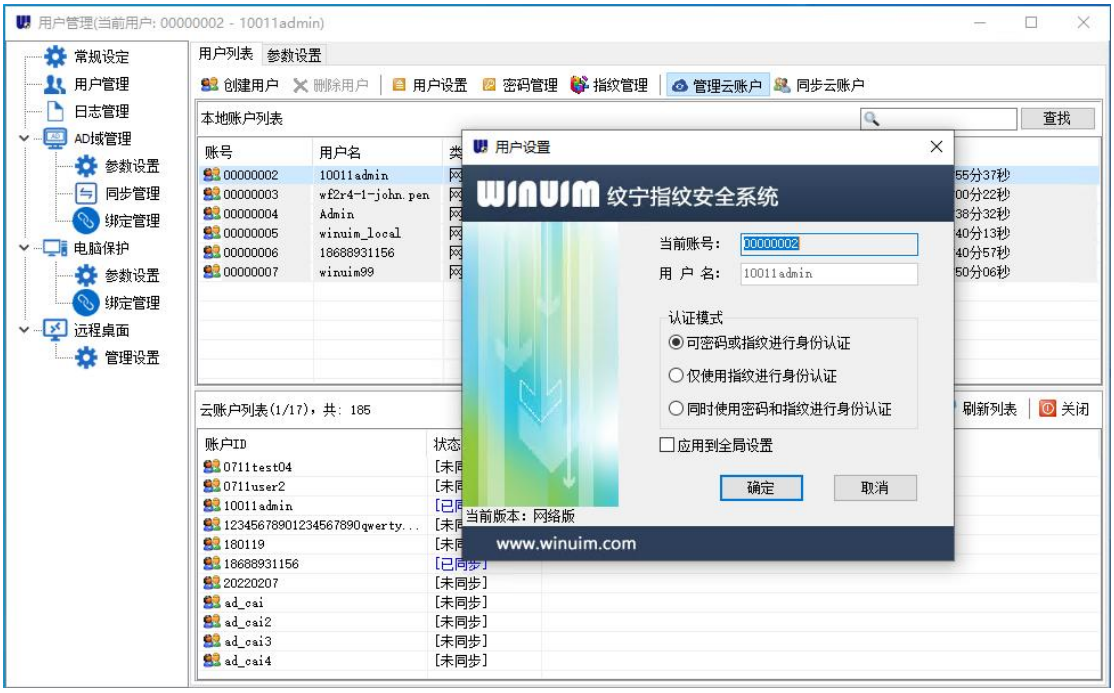

图 20：用户设置界面

可选的身份认证模式有以下三种：

认证模式	认证安全级别
可密码或指纹进行身份认证	一级
仅使用指纹进行身份认证	二级
同时使用密码和指纹进行身份认证	三级

若对超级管理员进行用户设置，具备“应用到全局设置”选项，可针对全局用户认证模式进行统一设置；若全局设置为一级，可对个人用户单独设置二级或三级的认证模式；若全局设置为二级，可对个人用户单独设置三级的认证模式；若全局设置为三级，则无法再对个人用户设置低级别的认证模式；

2.4.4 密码设置

选择当前用户，并点击“密码设置”图标，可以对用户进行密码设置，具体如下图：



图 21：密码设置界面

密码设置包括修改密码和重置密码：修改密码需要验证旧密码成功才能完成密码的修改；重置密码则不需要输入旧密码即可完成密码的更新，一旦新密码更新成功将覆盖原有旧密码。

2.4.5 指纹管理

选择当前用户，并点击“指纹管理”图标，可以对用户进行指纹设置，包括指纹新增、指纹修改、指纹删除等，鼠标选取对应手指即可对该手指进行操作，具体如下图：



图 22：指纹管理界面

2.4.6 管理云帐户

点击“管理云帐户”图标，可以列出服务器端的用户，列出的用户均未同步到本计算机，显示角色和更新时间均为“未同步”，具体如下图：

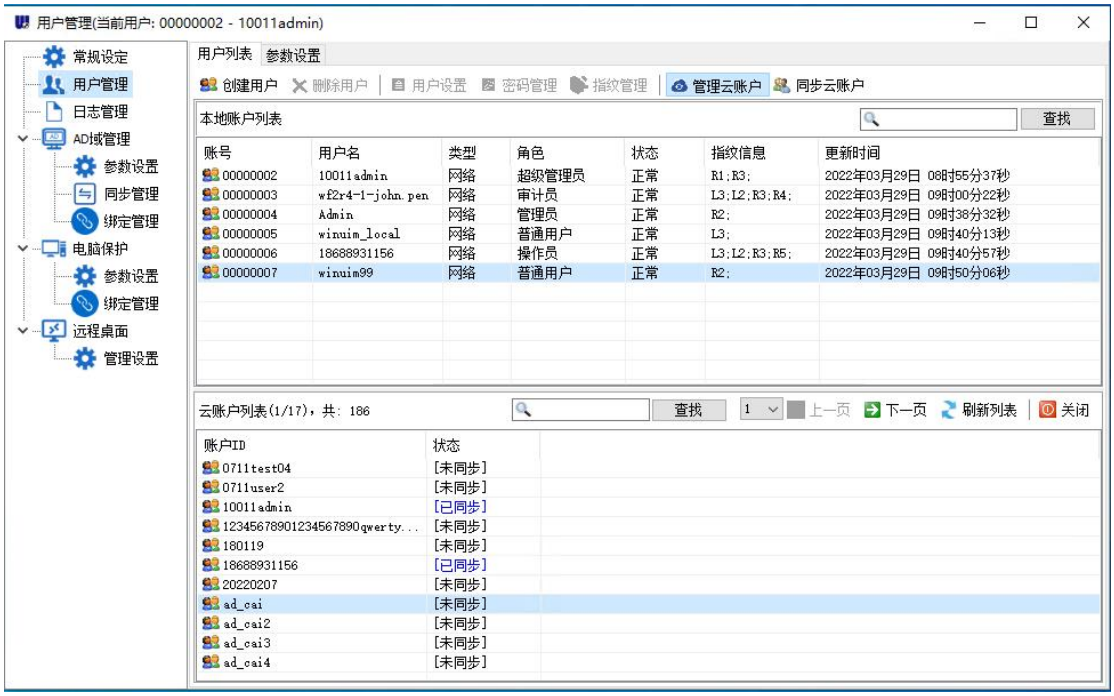

图 23：管理云帐户界面

2.4.7 同步云帐户

同步云帐户有 2 种方式实现：

1、点击“列出云帐户”图标，可以列出服务器端的用户，选择一条列出的云账户右键，选择“同步云帐户”菜单进行云账户同步。具体如下图：

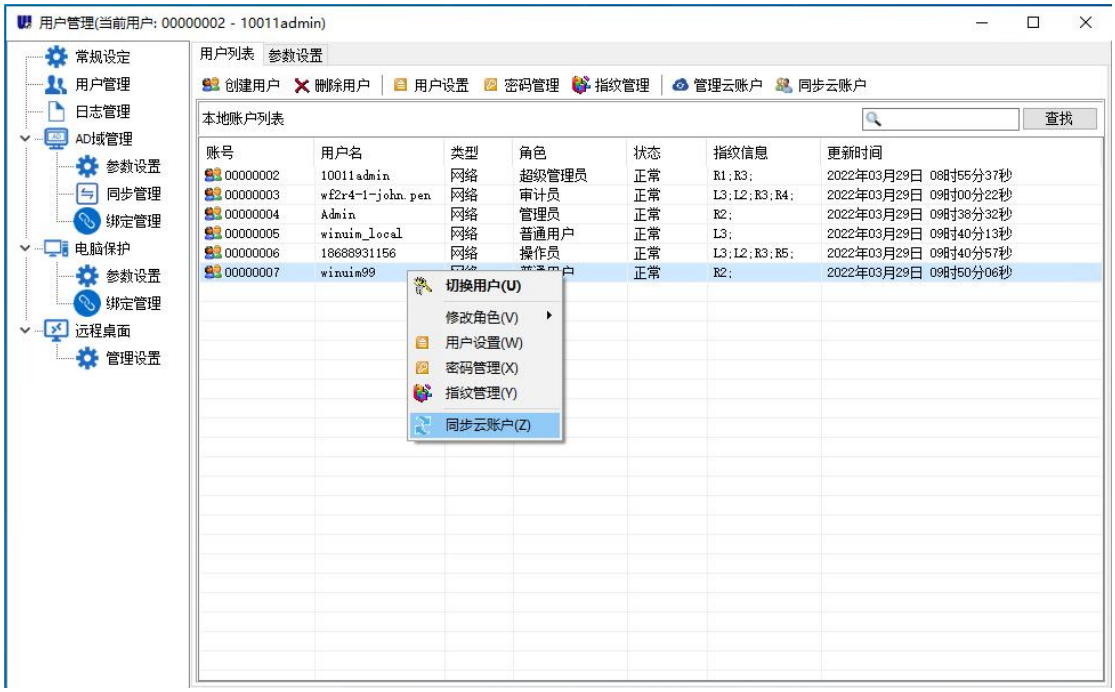

图 24：同步云帐户界面

2、点击“同步云帐户”图标，弹出“同步云帐户”窗体，可以选择同步当前用户列表中的所有帐户或同步指定帐户。具体如下图：

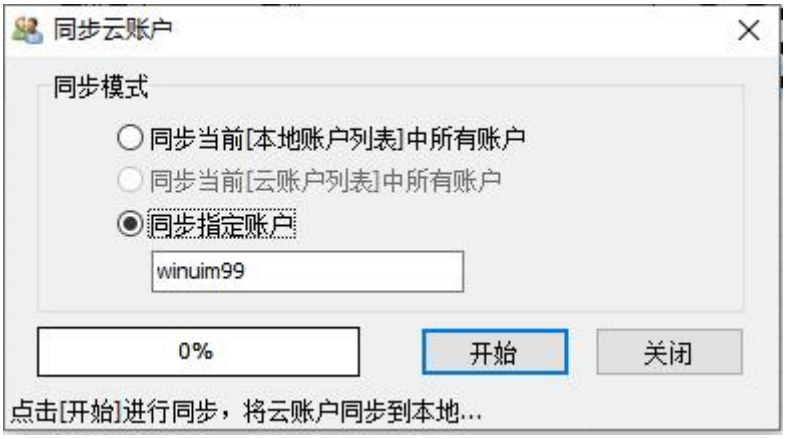

图 25：同步云帐户界面

点击“开始”按钮，执行同步云帐户任务，任务完成后将提示如下：

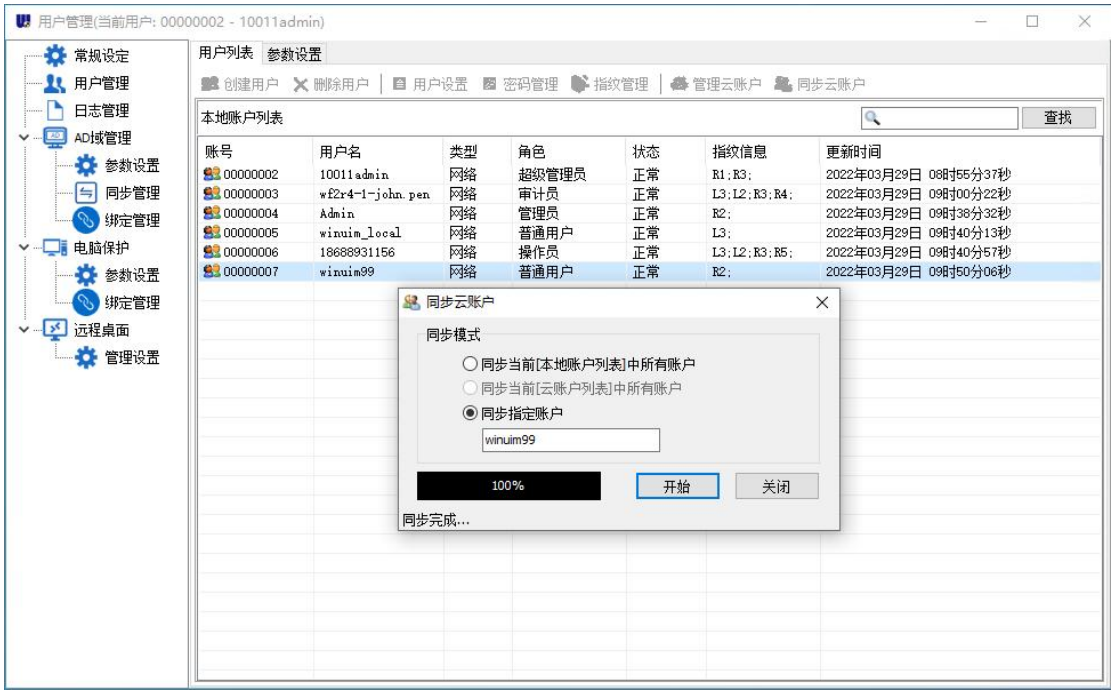

图 26：同步云帐户结束界面

同步成功的用户将会自动分配本地帐号（数字编号）、显示正常的角色信息、指位信息、更新时间。

关于指位信息的文字描述：

L——左手（已同步指纹信息到本地）；

R——右手（已同步指纹信息到本地）；

l——左手（未同步指纹信息到本地）；

r——右手（未同步指纹信息到本地）；

1-5 分别代表——拇指、食指、中指、环指、小指；

关于指位信息的色彩标识：

指纹窗体出现的手指颜色分别代表：

黄色——服务器已注册且在本地已保存的指纹；

蓝色——服务器已注册且在本地未保存的指纹；

绿色——未注册的指纹；

橙色——正在注册或待注册的指纹；

2.5 日志管理

日志包括本地日志和网络日志，均由用户日志和登录日志组成。用户日志是记录管理员

对用户管理的所有操作日志记录；登录日志是记录用户登录、解锁计算机桌面的所有操作。

系统中仅审计员用户具备管理日志管理权限，具备设置日志、清除日志、查看日志的本地日志管理功能和查看网络日志和导出网络日志的网络日志管理功能。

审计员用户可在桌面右下角通知区域图标栏中右键图标，列出程序管理菜单，如下图：



图 27：程序管理菜单

选择日志管理菜单，弹出身份认证界面，完成身份认证后进入日志管理界面，如下图：

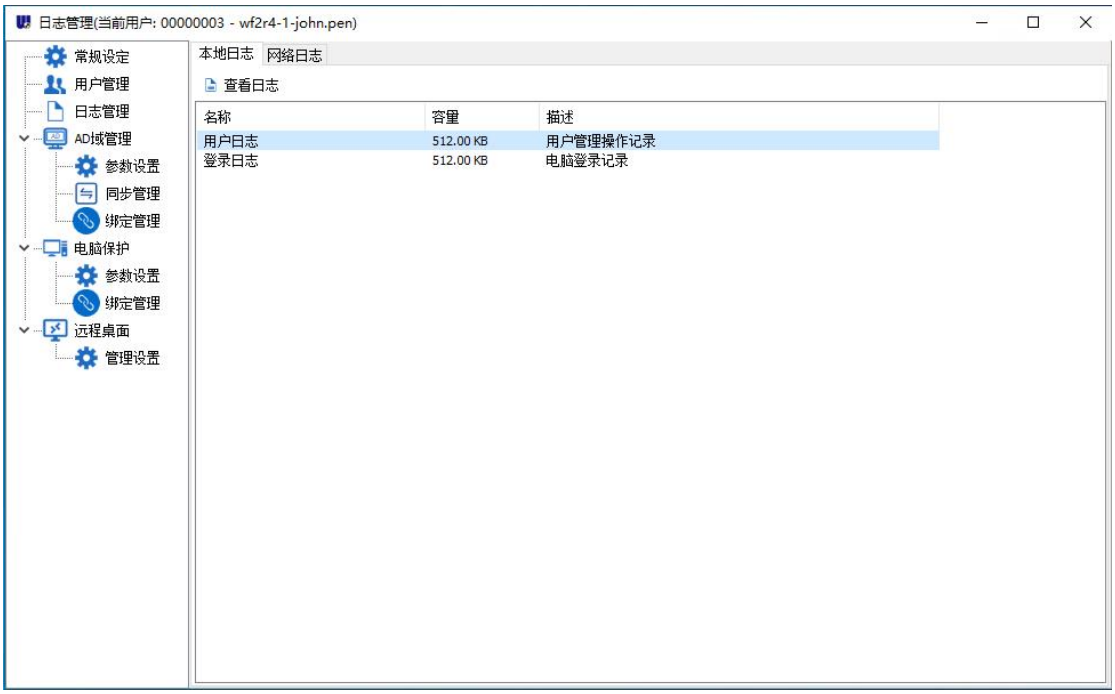

图 28：日志管理界面

2.5.1 查看本地用户日志

选择本地日志菜单，选中用户日志行，点击查看日志图标，可以对本地日志的用户日志进行查看，如下图：

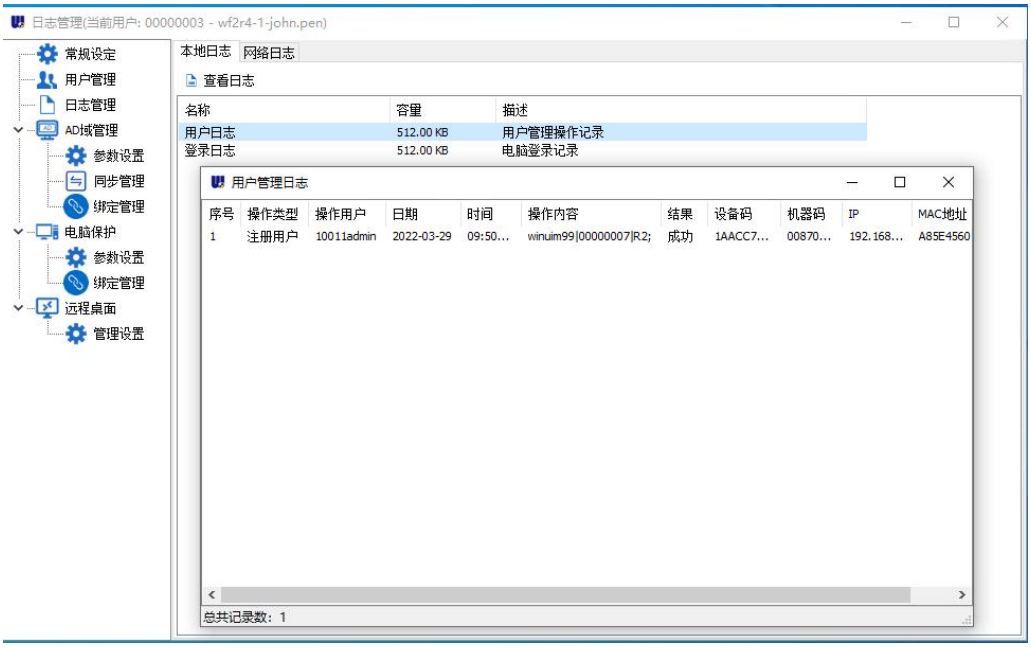

图 29：查看本地用户日志界面

2.5.1 查看本地登录日志

选择本地日志菜单，选中登录日志行，点击查看日志图标，可以对本地日志的登录日志进行查看，如下图：

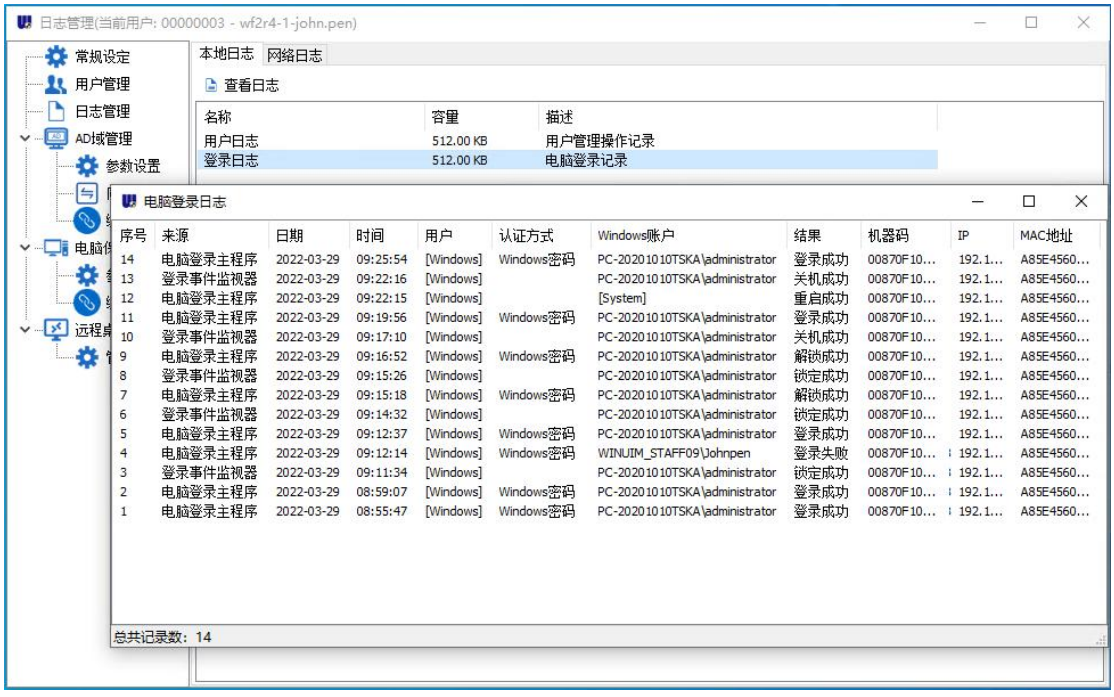

图 30：查看本地用户日志界面

2.5.3 查看网络用户日志

点击查看网络日志菜单，选择用户管理日志下拉菜单可以对系统全局用户管理日志根据起止日期进行查询，符合日期条件的用户管理日志将被列表，如下图：

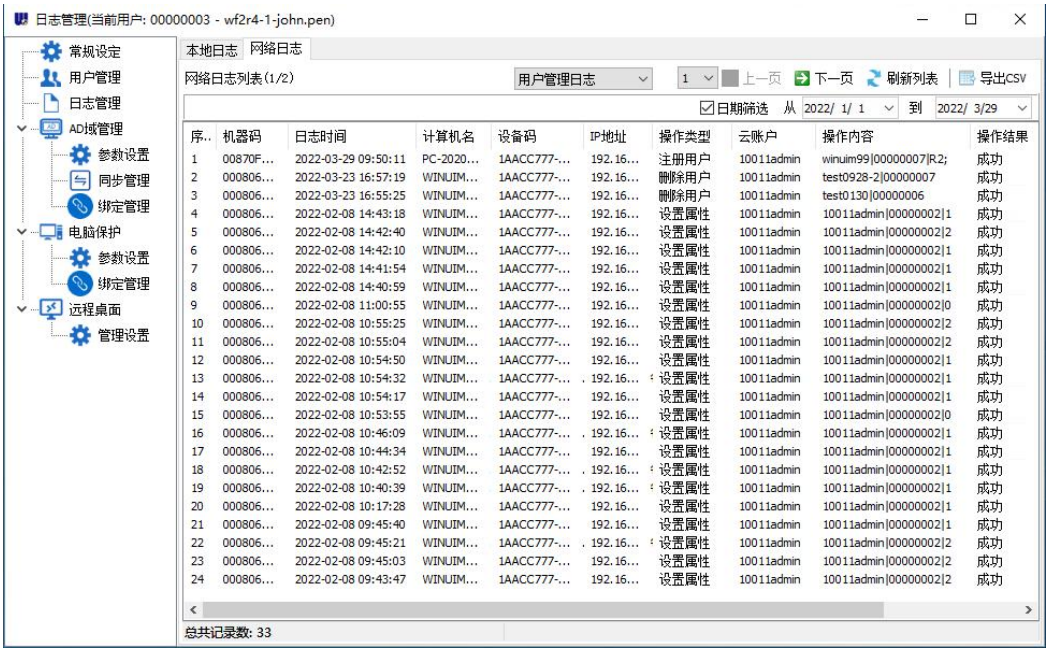

图 31：查看网络用户日志界面

操作内容由若干个字段组成，字段之间用“|”隔开，这些字段是：

用户名|用户 id|操作内容

1、用户名：被云账户操作的用户对象；

2、用户 id：用户对象所在电脑的用户 id；

3、操作内容：随操作类型而定，具体对应如下表：

操作类型	**操作内容**
注册用户	记录当次注册的指位信息
指纹管理	记录当次指纹变更后的指位信息
设置属性	记录当次用户属性代号： 0 表示指纹或密码 1 表示仅指纹 2 表示指纹和密码
设置角色	记录当次用户角色代号： 4 表示管理员 5 表示普通用户

	6 表示审计员 7 表示操作员

2.5.4 查看网络电脑保护日志

点击查看网络日志菜单，选择电脑保护日志下拉菜单可以对系统全局电脑保护日志根据起止日期进行查询，符合日期条件的电脑保护日志将被列表，如下图：

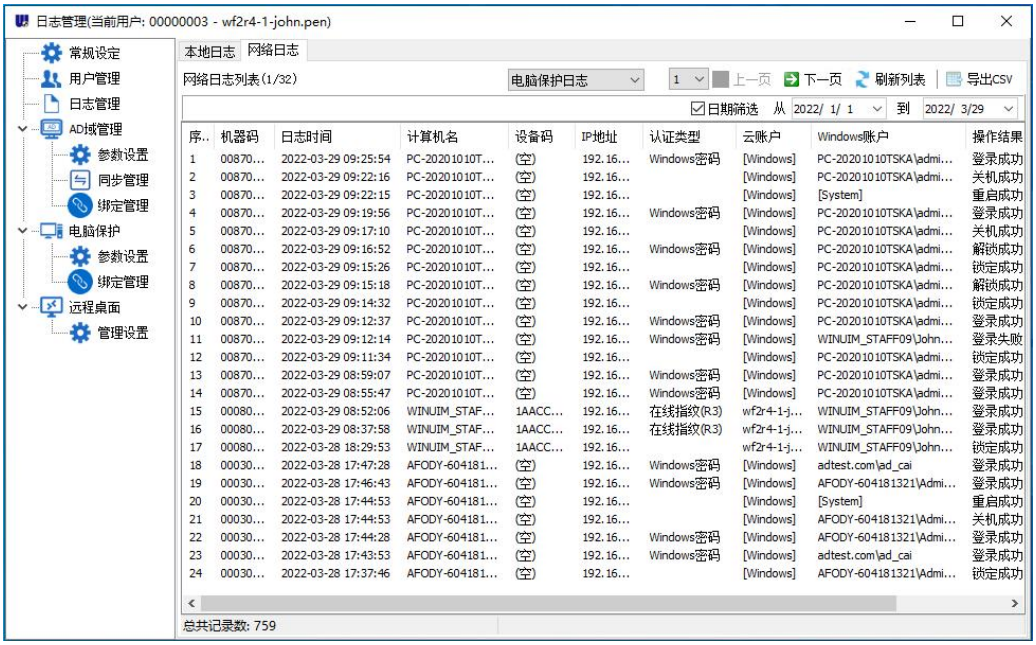

图 32：查看网络电脑保护日志界面

2.6 AD 域管理

用户可在桌面右下角通知区域图标栏中右键图标，列出程序管理菜单，如下图：



图 33：程序管理菜单

2.6.1 参数设置

选择 AD 域管理-参数设置菜单，弹出身份认证界面，完成身份认证后进入 AD 域管理参数设置界面，如下图：



图 34：AD 域管理参数设置界面

AD 域服务器：系统将自动列表已部署纹宁指纹安全系统 AD_Services 服务的 AD 域服务器信息，如有多台服务器部署则列表多条 AD 域服务器记录；

自动同步域账户：勾选该项表示系统会在 AD 域控服务器创建 AD 域账号的同时自动创建同名指纹账户到指纹安全系统；不勾选该项则不会同步域账号到指纹安全系统。

启用密码同步：勾选该项表示启用对 AD 域账号的密码进行同步更新策略；不勾选改项

则不会启用对 AD 域账号的密码进行修改。

默认：在启用密码同步策略时，选择默认项表示让 AD 域账号的密码与指纹账户密码保持一致；

自动：在启用密码同步策略时，选择自动项表示让 AD 域账号的密码每次都更新为随机密码。

认证修改策略：在选择自动项时，选择“先认证账户，后修改密码”项表示先进行身份认证且成功后修改域账号密码；选择“先修改密码，后认证账户”项表示先修改域账号的密码后进行身份认证。

应用场景：勾选启用一次一密的场景，勾选的项次表示在勾选的应用场景下将执行一次一密的密码同步策略。

网络共享：添加网络共享地址后将自动连接域账户的网络共享地址；管理员可以添加和删除网络共享目录地址。

密码有效期（天）：勾选该项表示启用 AD 域账号的密码有效期，并可设置对应的天数，设置的天数需要小于域控服务器的密码策略

2.6.2 账户同步

选择 AD 域管理-账户同步菜单，弹出身份认证界面，完成身份认证后进入 AD 域管理账户同步界面，如下图：

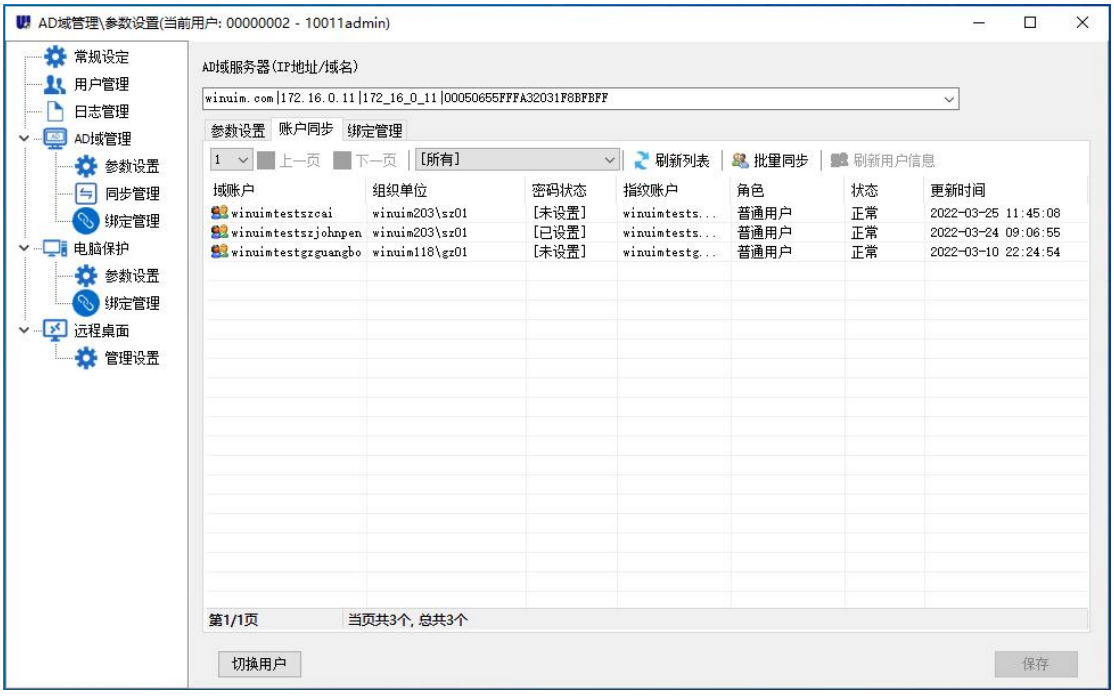

图 35：AD 域帐户同步管理界面

点击“刷新列表”菜单按钮，系统将列出选择的 AD 域服务器上的所有域用户；点击“批

量同步”菜单按钮，系统将根据同步策略对域账号进行批量同步，如图：

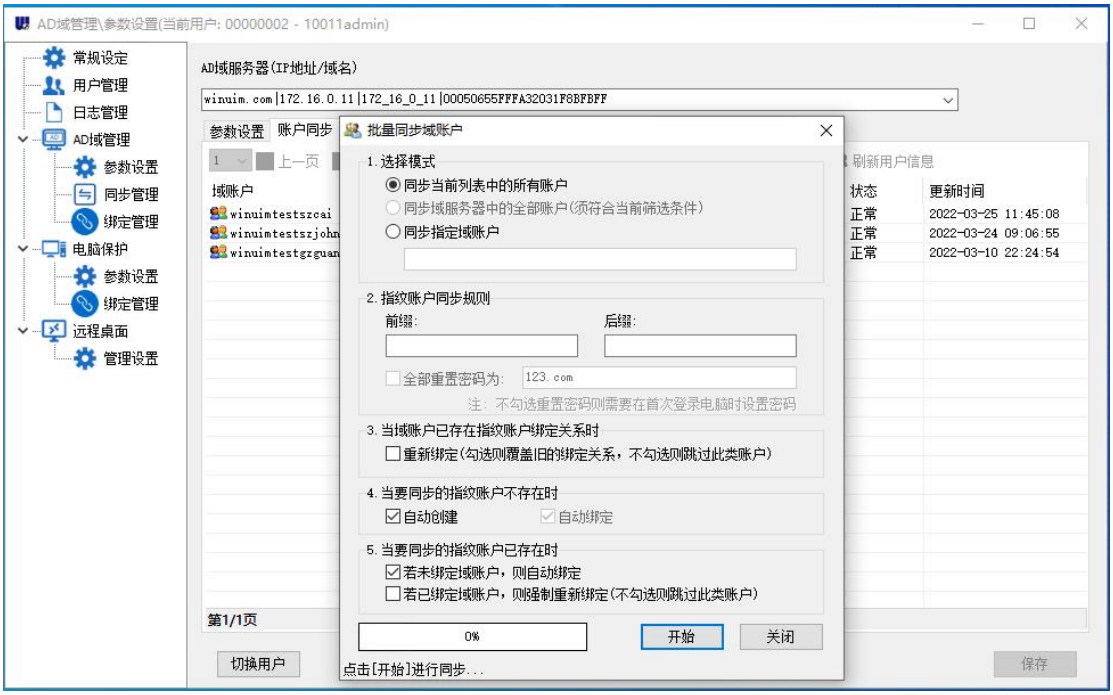

图 36：AD 域帐户批量同步界面

选择模式：同步用户范围可以选择当前列表中的所有用户或指定域账户；

指纹账户同步规则：创建同步指纹账户的账户名规则，可以批量在域账户名前置或后置相应的字符生成指纹账户名；

当域账户已存在指纹账户绑定关系时：勾选重新绑定则在批量同步时自动重新绑定指纹账户，旧的绑定关系将被新的绑定覆盖；不勾选则保持原有绑定关系；

当要同步的指纹账户不存在时：勾选自动创建将自动创建指纹账户，且自动完成绑定；

当要同步的指纹账户已存在时：勾选“若未绑定域账户，则自动绑定”则自动绑定未绑定的域账户，不勾选则不会自动绑定域账户；勾选“若已绑定域账户，则强制重新绑定”则自动重新绑定域账户；不勾选则忽略此类指纹账户的绑定；

点击开始按钮即按设置的同步规则进行批量同步域账户操作。

2.6.3 绑定管理

选择 AD 域管理-绑定管理菜单，弹出身份认证界面，完成身份认证后进入 AD 域管理域账户绑定管理列表界面，如下图：

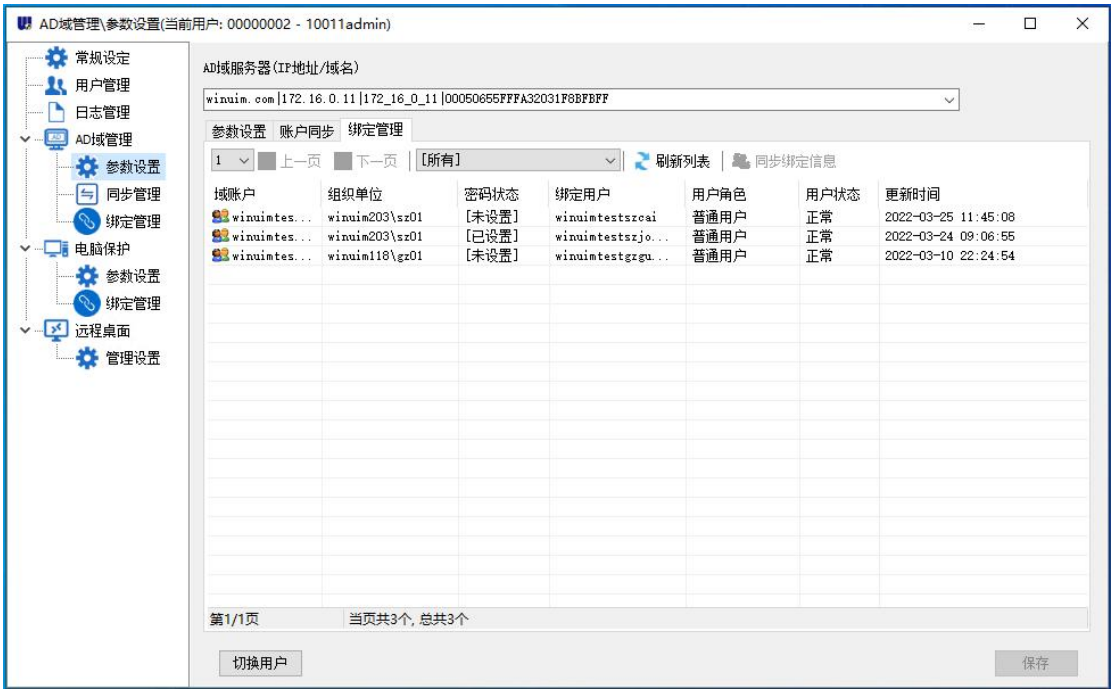

图 37：AD 域帐户绑定管理界面

选中域账户点击右键可以进行设置绑定、解除绑定、设置密码、同步绑定信息等操作，对未绑定指纹用户的域账号可进行设置绑定操作，如图：

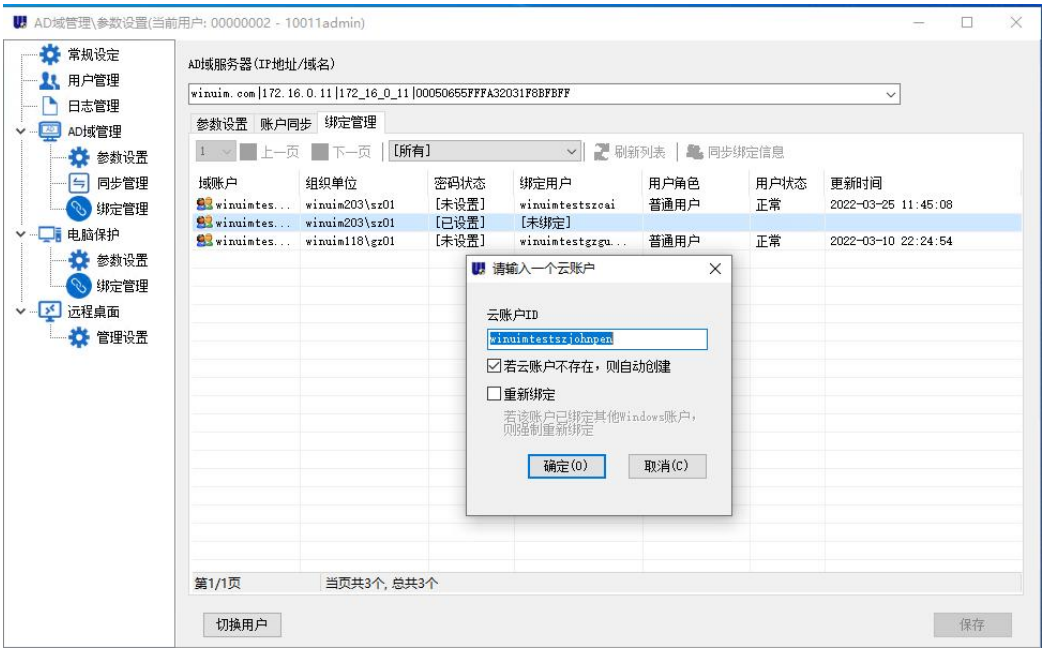

图 38：AD 域帐户设置绑定指纹账户界面

对已绑定指纹用户的域账号可进行解除绑定操作，如图：

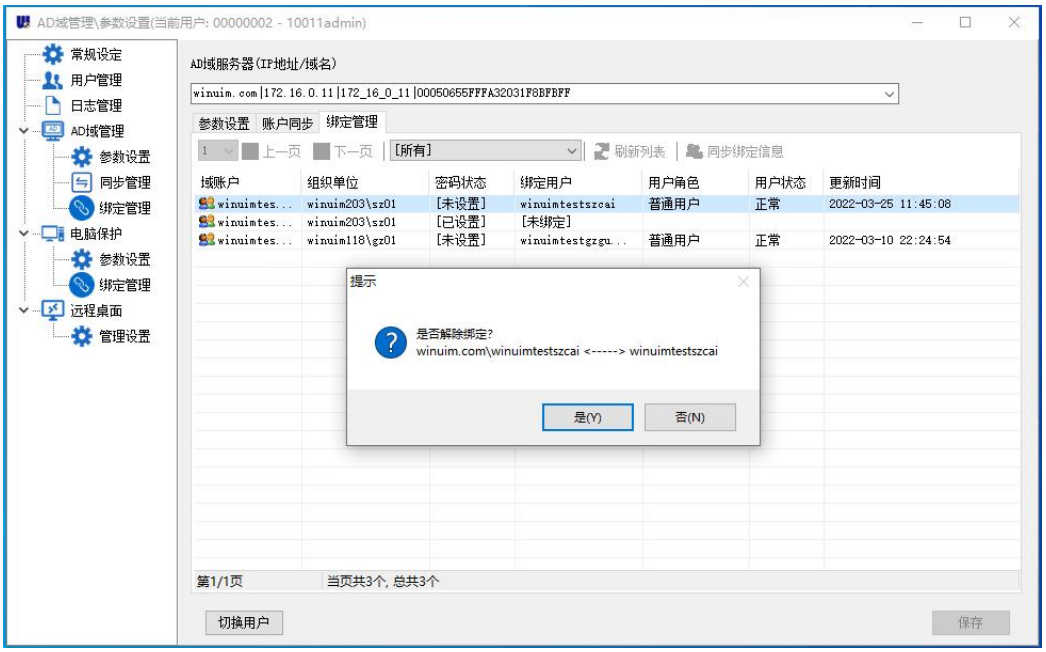

图 39：AD 域帐户解除绑定指纹账户界面

对域账号和指纹账号设置密码操作，如图：

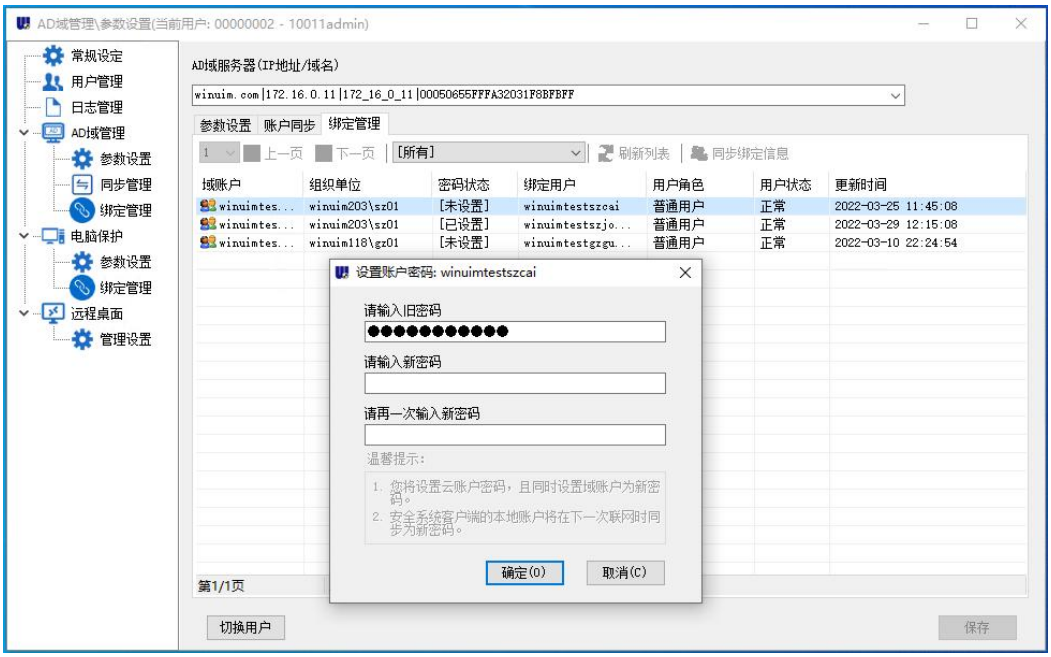

图 40：AD 域帐户设定密码界面

注意：AD 域管理版块属于指纹安全系统选配功能，该功能的实现需要在域控服务器安装纹宁指纹安全系统服务端（AD 域）软件，该软件将在域控服务器端部署双向同步域账户数据服务。

2.7 电脑保护

用户可在桌面右下角通知区域图标栏中右键图标，列出程序管理菜单，如下图：



图 41：程序管理菜单

2.7.1 参数设置

电脑保护包括参数设置和绑定管理，具体设置界面如下图：

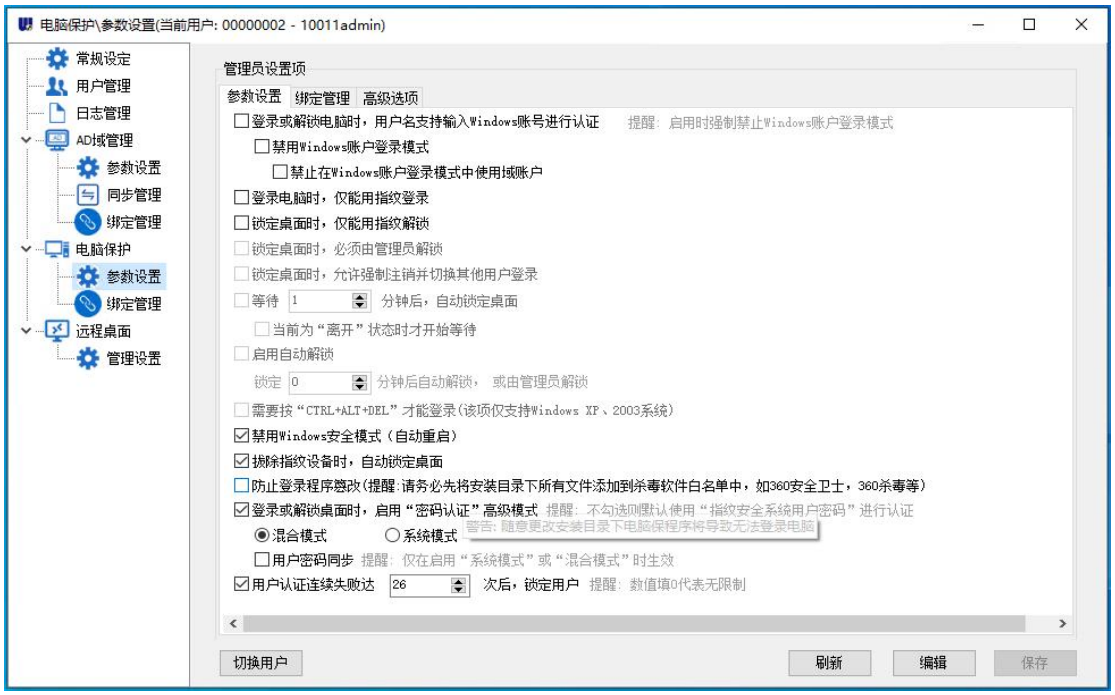

图 42：电脑保护管理系统设置界面

超级管理员角色点击编辑按钮方可对参数进行设置，设置项及对应功能说明列表如下：

设置项	描述
登录或解锁电脑时，用户名支持输入 Windows 账号进行认证	勾选该项将对指纹登录界面的用户名允许输入 Windows 账户名。*【注意】勾选该项会自动关联勾选禁用 Windows 账户登录模式选项，也会自动关联取消勾选禁止在 Windows 账户登录模式中使用域账户*
禁用 Windows 账户登录模式	勾选该项将对 Windows 账户登录模式进行禁用，用户登录 Windows 桌面时只能通过指纹安全系统的账号、密码、指纹的认证方式进行 Windows 桌面登录。
禁止在 Windows 账户登录模式中使用域账户	勾选该项将对 Windows 账户登录模式的域账号用户登录进行禁用；用户通过本地 Windows 账号、密码的认证方式进行 Windows 桌面登录。*【注意】域控策略限制了本地账户登录的客户请谨慎勾选该项设置*
登录电脑时，仅能用指纹解锁	勾选该项将限制用户只能通过指纹认证的方式登录桌面：开机登录状态、注销状态、切换用户状态、重启状态。
锁定桌面时，仅能用指纹解锁	勾选该项将限制用户只能通过指纹认证的方式解锁桌面： 锁定状态、睡眠状态、休眠状态。
锁定桌面时，必须由管理员解锁	勾选该项将限制用户只能通过管理员身份认证方可登录桌面。(该功能在高级版提供)
锁定桌面时，允许强制注销并切换其他用户登录	勾选该项将允许用户在锁定桌面状态时切换用户登录 Windows 桌面。（该功能在高级版提供）
等待 N 分钟后，自动锁定桌面	勾选该项将限制用户在 N 分钟后自动锁定 Windows 桌面。（该功能在高级版提供）
启用自动解锁	勾选该项将限制用户在 N 分钟后方可解除 Windows 桌面锁定。（该功能在高级版提供）
需要按“Ctrl+ALT+DEL”才能登录	在 WindowsXP、Win2003 系统下，勾选该选项，将需要按“Ctrl+ALT+DEL”键方可进入指纹认证界面。

禁用 Windows 安全模式（自动重启）	勾选该项将限制用户通过安全模式进入操作系统桌面，安全模式、网络安全模式、带命令提示符的安全模式均被禁用
拔除指纹设备时，自动锁定桌面	勾选该项将实现用户拔除指纹设备时，自动锁定计算机桌面。
防止登录程序篡改	勾选该项将禁止用户篡改系统文件绕过指纹安全系统客户端界面。*【注意】随意更改或删除安装目录下电脑程序的行为将导致无法登录操作系统*
登录或解锁桌面时，启用“密码认证”高级模式	勾选该项将启用密码认证高级模式
密码认证--混合模式	选择该项将允许用户在指纹安全系统指纹登录/指纹解锁界面输入指纹账号的密码或与该指纹账号绑定的 Windows 账户密码
密码认证--系统模式	选择该项将允许用户在指纹安全系统指纹登录/指纹解锁界面输入与指纹账号绑定的 Windows 账户密码
密码认证--用户密码同步	勾选该项将启用 Windows 账户密码同步：用户在指纹安全系统指纹登录/指纹解锁界面输入 Windows 账户密码验证成功后，系统将用户指纹账户的密码自动同步为该用户的 Windows 账户密码。
用户认证连续失败达 N 次后，锁定用户	勾选该项将限制用户在 N 次身份认证失败后自动锁定该用户状态，锁定状态的用户需要管理员角色用户解除锁定方可正常使用。

2.7.2 绑定管理

管理员将对用户进行 Windows 帐户绑定管理，具体设置界面如下图：

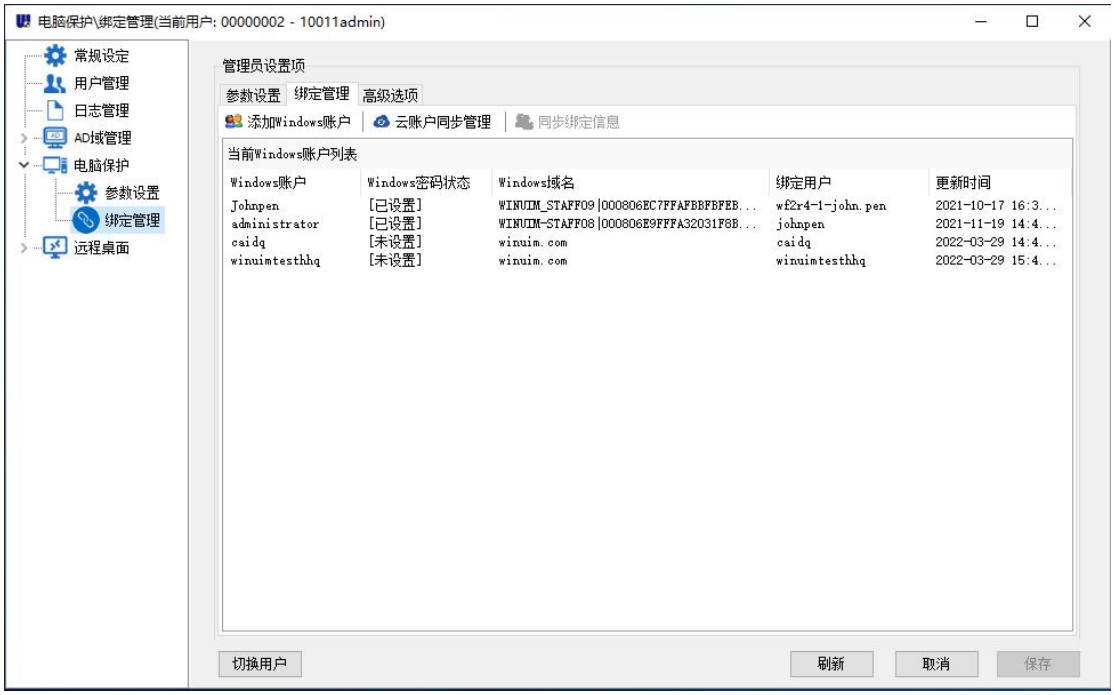

图 43：电脑保护管理绑定管理界面

新创建的用户或从 AD 域控服务器同步的用户需要进行 Windows 帐户绑定方可实现计算机指纹安全保护，Windows 账户与安全系统创建的用户须一对一绑定，否则将出现绑定 Windows 账户失败，具体如下图：

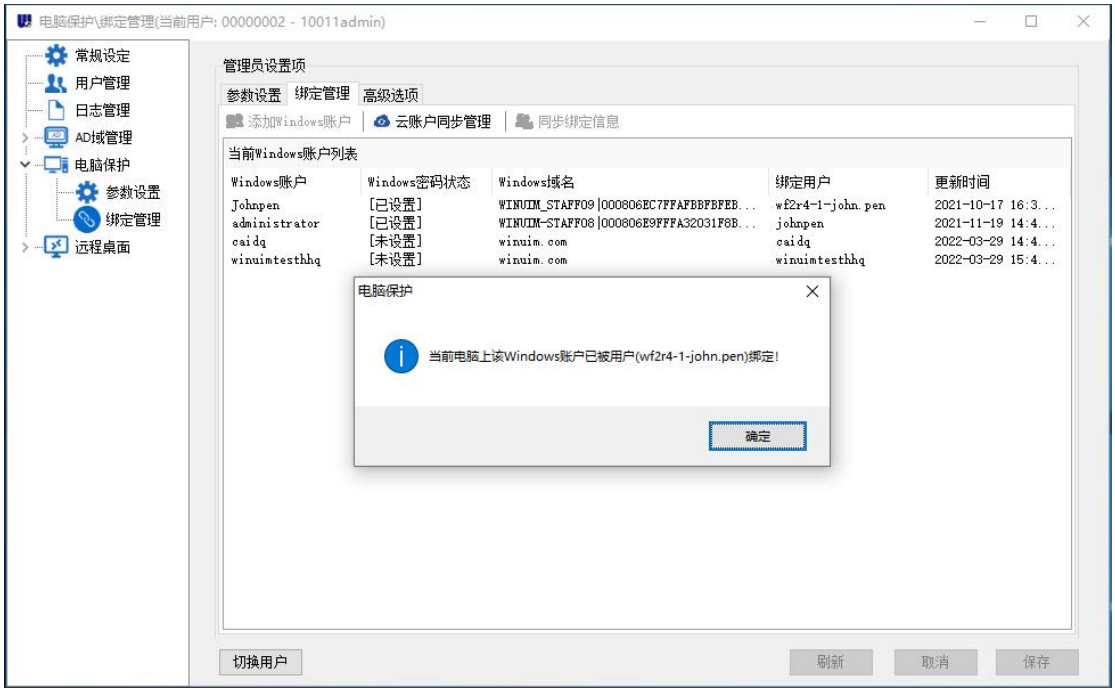

图 44：帐户重复绑定界面

绑定 Windows 账户可选择固定账户和可变账户：固定账户为通常的 Windows 本地账户或 Windows AD 域账户；可变账户为指纹安全系统特别设计的特殊的 Windows 虚拟账户，可变账户全局唯一，一旦它绑定了某一个指纹账户，则该指纹账户可以在任意一个设置

了可变账户的客户端登录其指定的 Windows 本地账户。

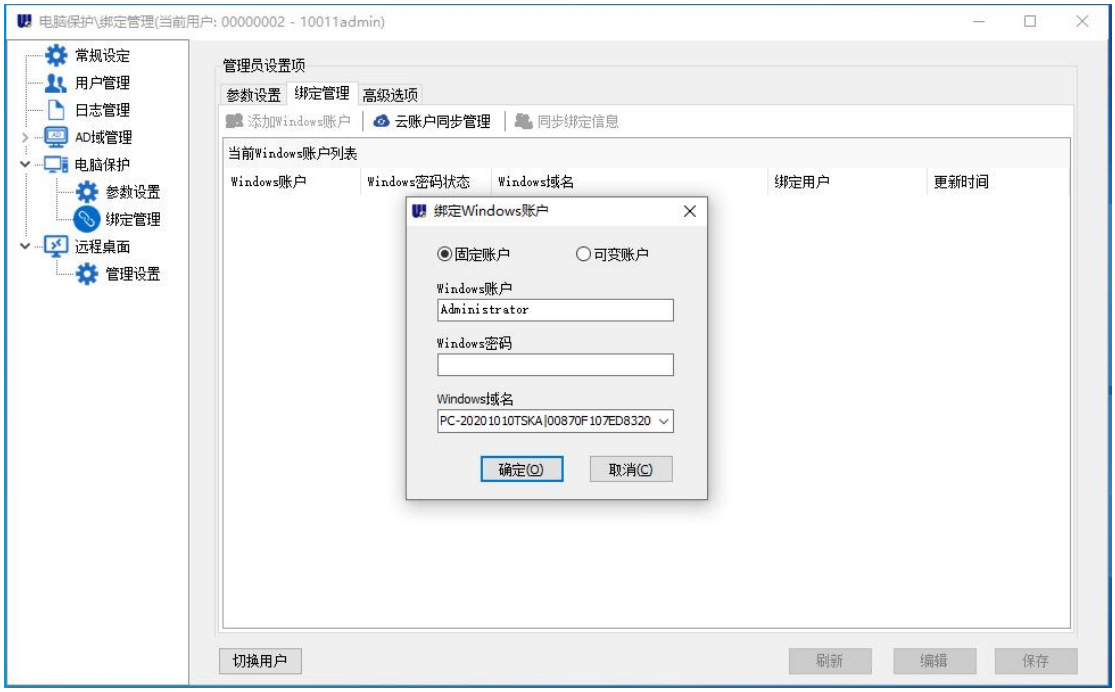

图 45：绑定 Windows 固定帐户界面

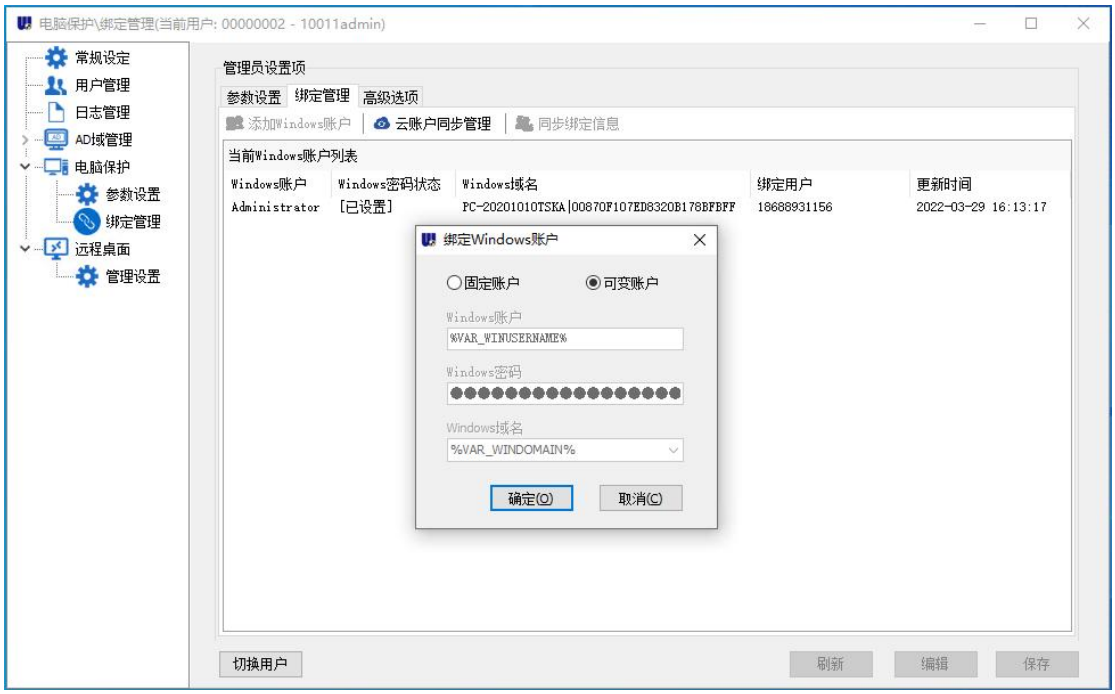

图 46：绑定 Windows 可变帐户界面

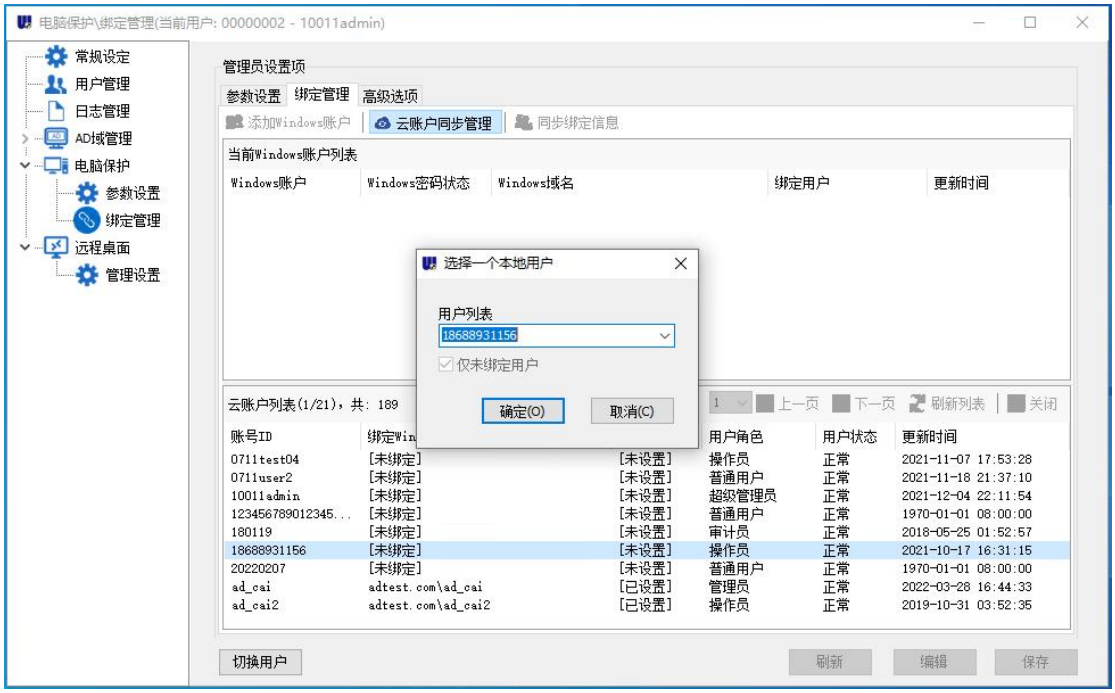

图 47：绑定指纹用户列表界面

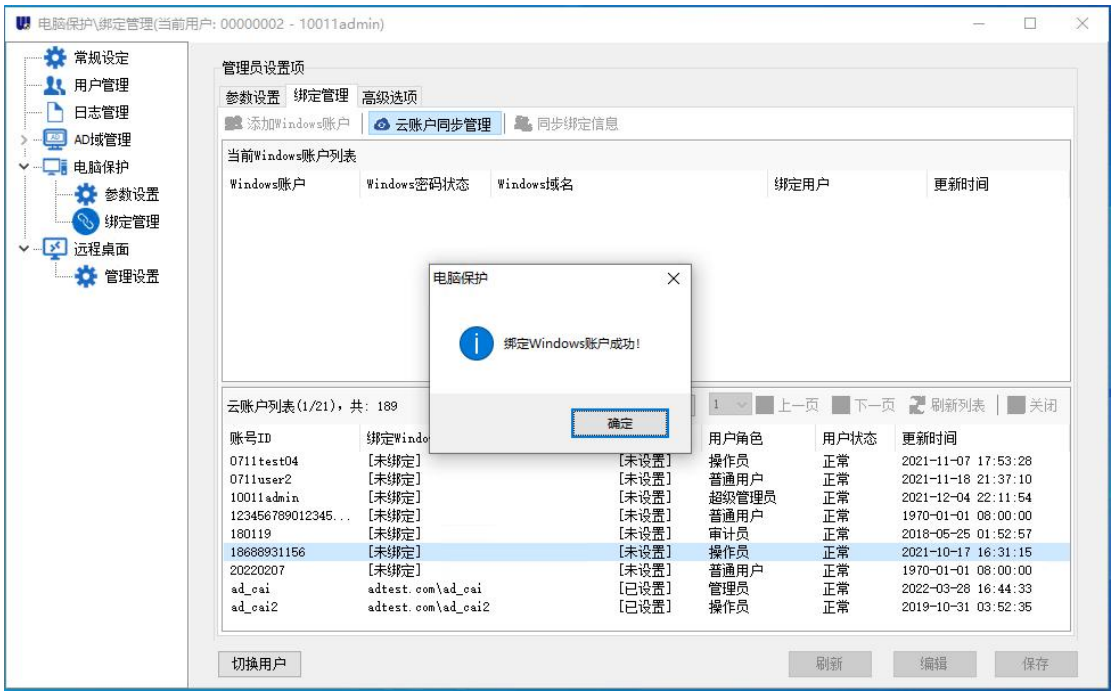

图 48：绑定 Windows 帐户成功界面

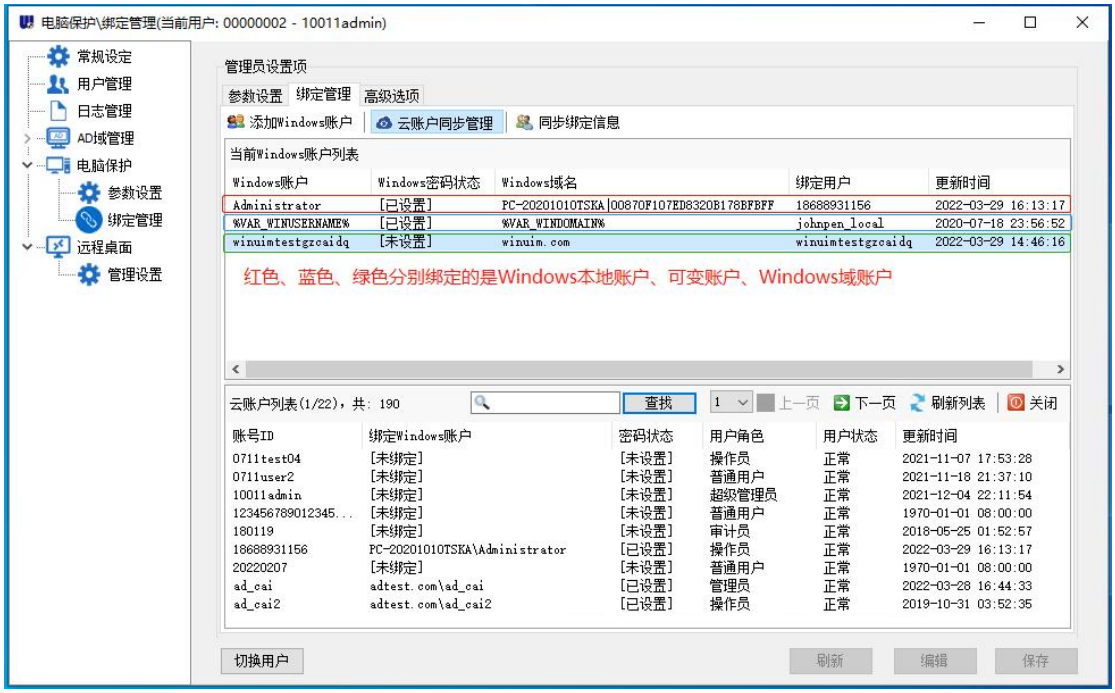

图 49：已绑定的 Windows 账户列表界面

绑定过的 Windows 帐户密码发生变更将导致 Windows 登录或解锁失败，需要用户输入最后一次设置的 Windows 帐号密码或域密码进行身份认证，具体如下图：



图 50：重新确认 Windows 账户身份界面

禁用 Windows 账户登录模式的情况下，首次安装指纹安全系统客户端软件的计算机或 Windows 所有账户均未绑定指纹账户的计算机首次登录用户可通过 Windows 账户模式登录桌面，具体如下图：

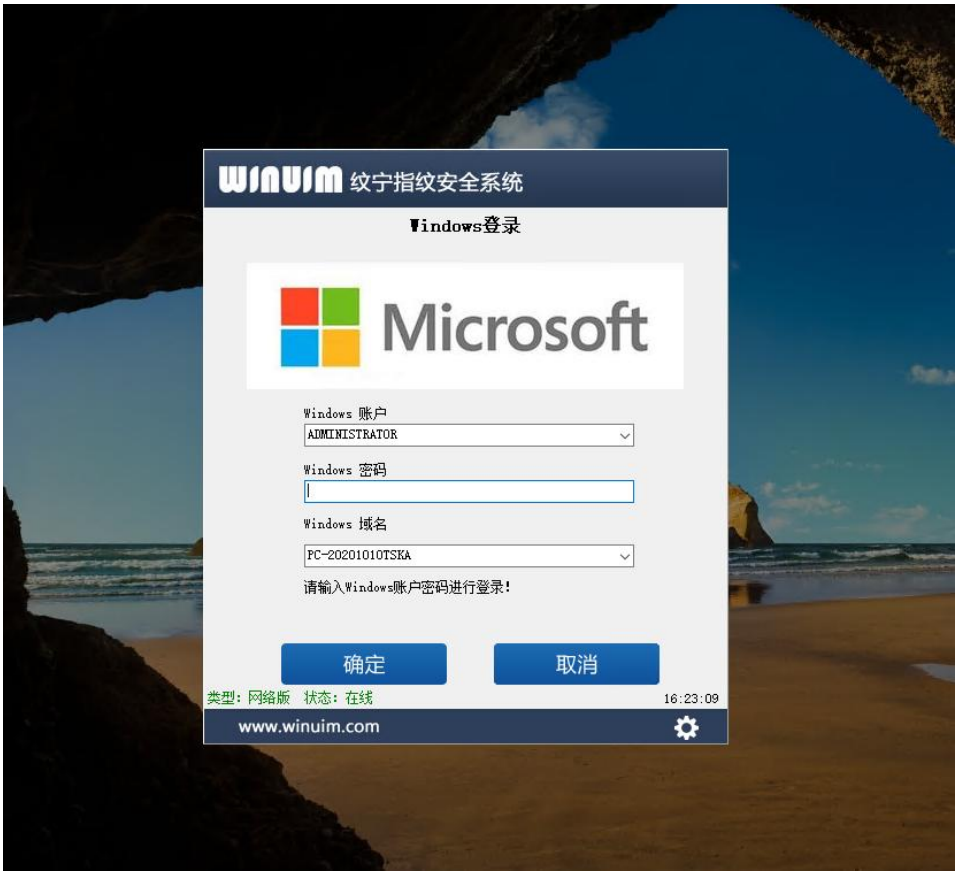

图 51：Windows 账户模式登录界面

2.7.3 高级选项

管理员可对用户进行绑定管理的高级选项设置，具体设置界面如下图：

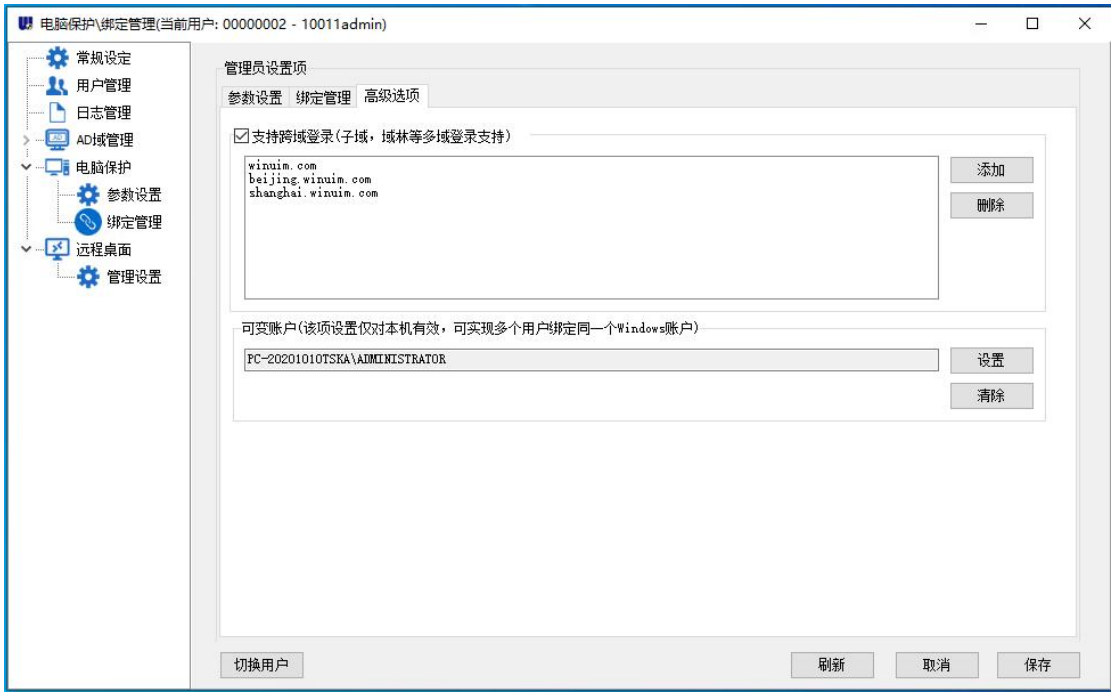

图 52：绑定管理高级选项

如网络环境有子域或林域等多域环境需要支持跨域登录，则需要勾选“支持跨域登录”勾选框，并添加相关的子域域名或林域域名。

针对域控管理员可能需要管理多台计算机的本地账户，可变账户的绑定可以解决一个指纹账户绑定可变账户，从而实现一个指纹账号通过身份认证进入多个计算机的本地账号桌面管理。**注意：可变账户绑定仅对本机设定的本地账户生效。**

2.8 远程桌面

远程桌面管理是专门针对多用户共用超级管理员账号访问计算机远程桌面的安全管理方案，管理员可以对需要管理的服务器列入管理列表，授权访问服务器的指纹用户，实现对访问者访问远程桌面的管控。

2.8.1 管理设置

管理员在远程桌面服务器端添加服务器信息，具体设置界面如下图：

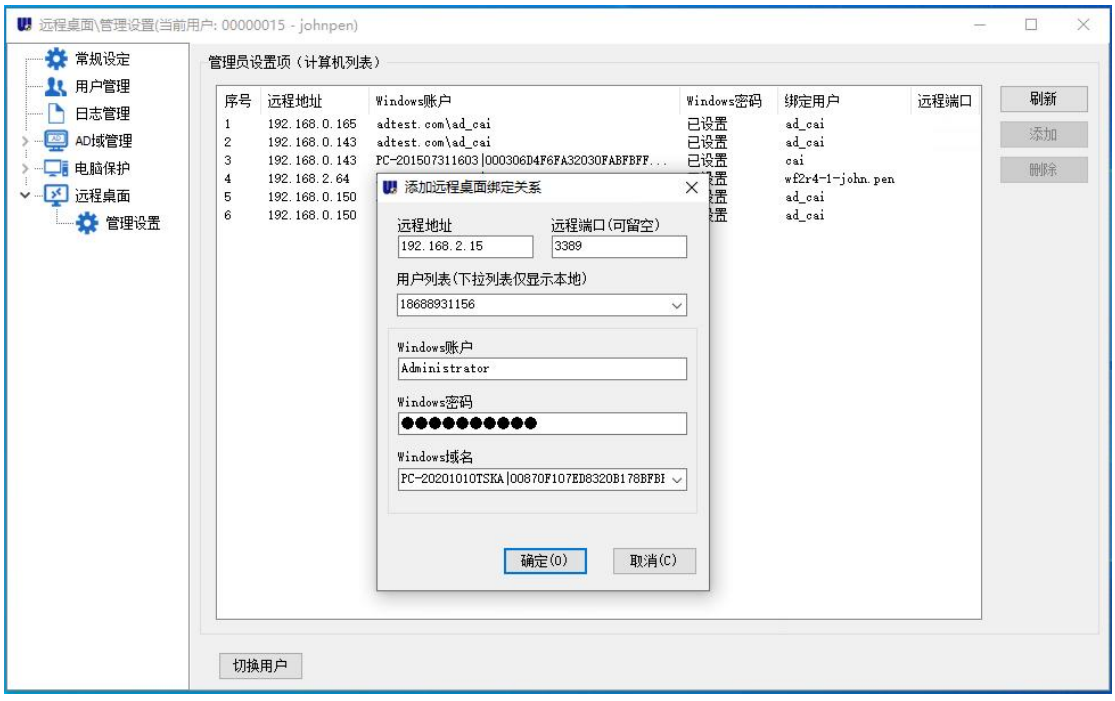

图 53：添加远程桌面界面

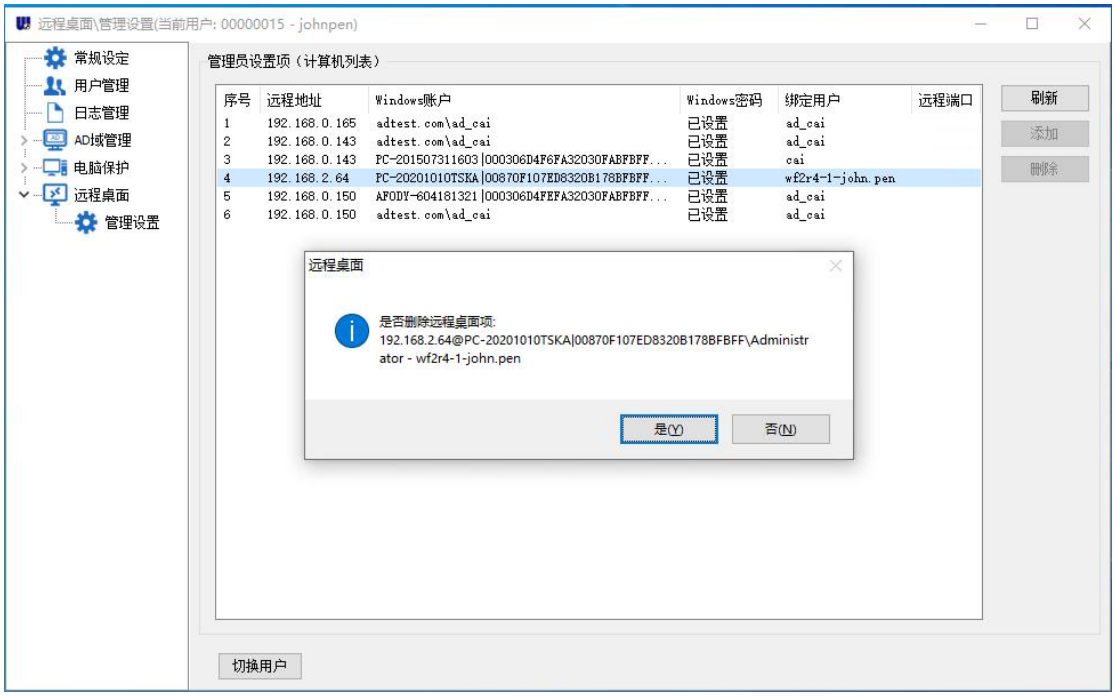

图 54：删除远程桌面界面

2.8.2 建立远程桌面连接

用户可在桌面右下角通知区域图标栏中右键图标，列出程序管理菜单，点击新建连接，如下图：



图 55：程序管理菜单

系统将加载远程计算机列表，选择需要远程桌面连接的计算机，点击连接按钮，如下图：



图 56：远程计算机列表

系统将弹出身份认证界面，完成身份认证后进入远程计算机桌面，如下图：



图 57：远程计算机列表

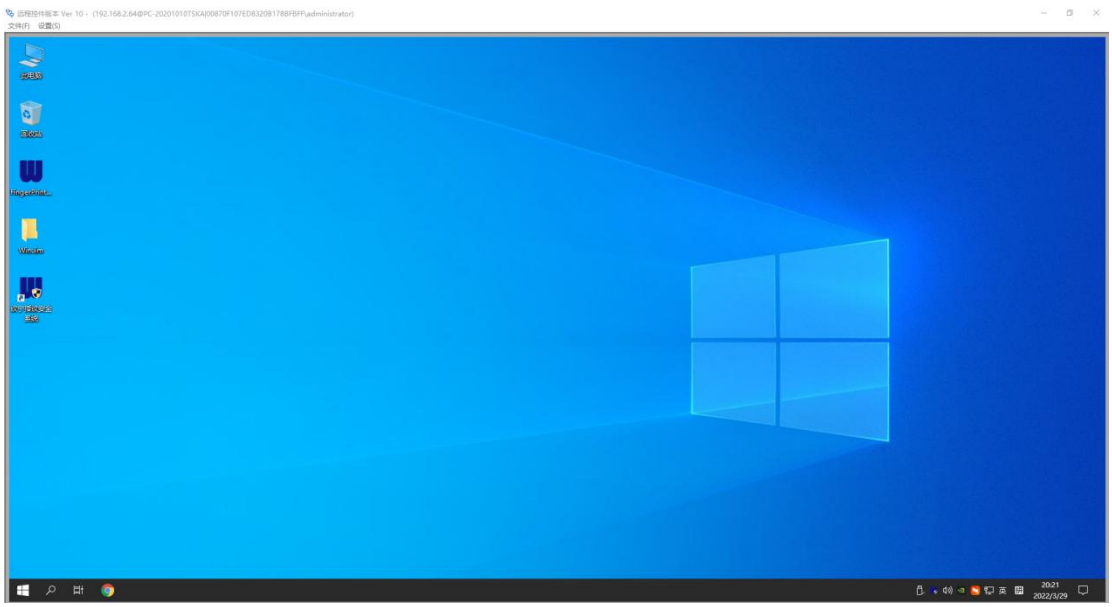

图 58：远程计算机桌面界面

2.9 软件卸载

软件卸载可通过控制面板的“程序与功能“卸载。

注意：纹宁指纹安全系统客户端软件卸载一定需要通过操作员角色身份认证通过方可正常卸载，非正常方式的卸载可能导致系统无法使用。

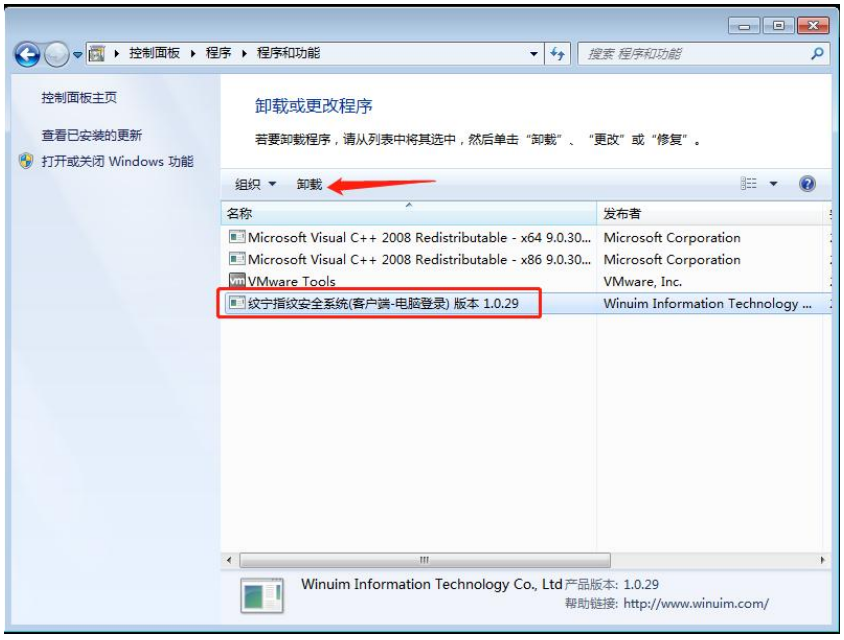

图 59：客户端软件卸载方式

点击卸载菜单或卸载按钮，进入卸载向导界面，验证完操作员身份后方可正常卸载软件，如下图：

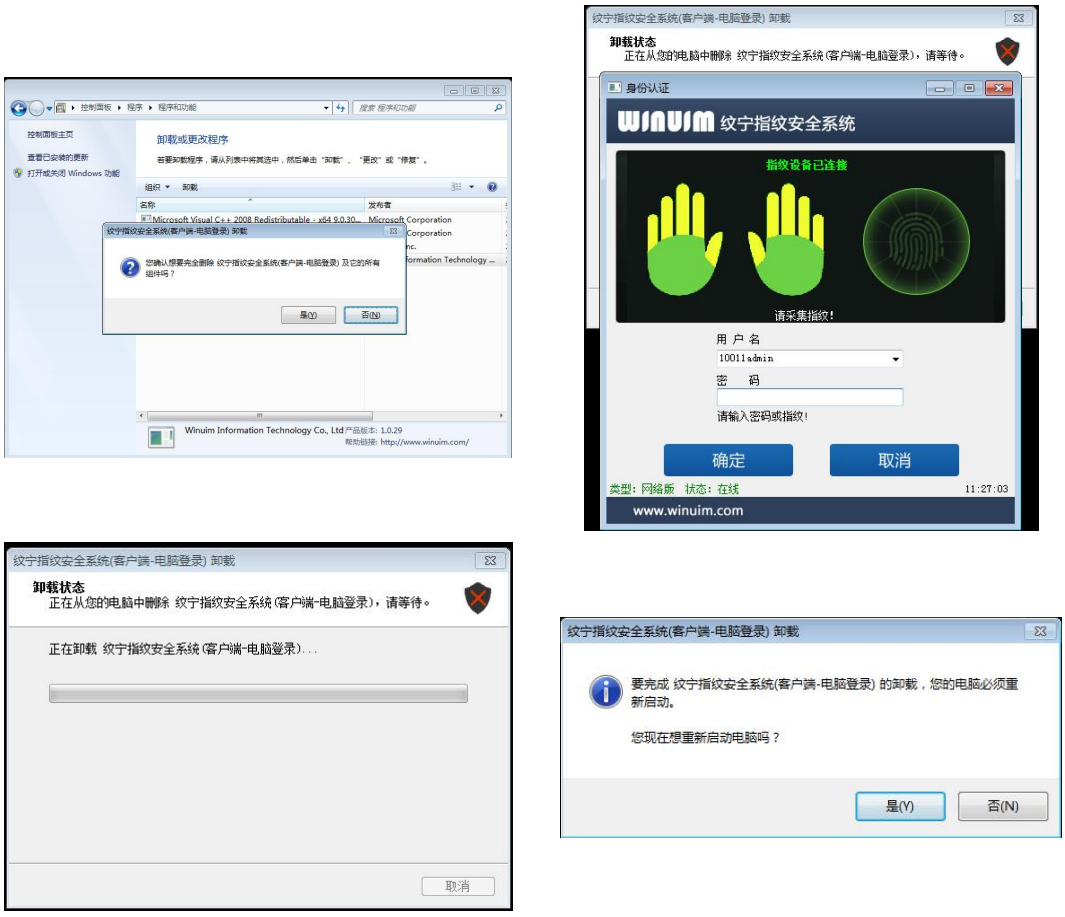

图 60：卸载向导界面

2.10 常见错误代码列表

管理员可以对身份认证界面状态提示信息及错误码进行对照查询，一般的错误码信息如下：

状态码	状态信息	状态描述
0	OK	操作成功
1	Fail	操作失败，原因未知
2	UsernameRepeat	用户名重复
3	FingerRepeat	指纹重复
4	UserNotExists	用户名不存在
5	FingerNotExists	指纹不存在

6	VerifyFailure	一比一失败
7	IdentifyFailure	一比 N 失败
8	ServiceStop	服务正在维护
9	AppNotExists	App 不存在
10	AppPwdError	App 密码错误
11	LicenseError	引擎授权错误
12	UsernameEmpty	用户名为空
13	TokenExpire	Token 时间过期
14	Unauthorized	操作未经过授权
21	UsernameFormatError	用户名格式错误(用户名可由 3-32 位数字、字母、下划线、中杠、点自由组合)
22	FingerDataError	指纹数据格式错误
23	SignError	http 签名错误
24	AppExpire	App 授权过期
25	LicenseTimeExpire	引擎授权时间过期
26	LicenseUserCountLimit	引擎授权用户数不足
27	LicenseServerMacAddrError	引擎授权服务器 Mac 地址错误
28	TimeStampExpire	操作时间戳过期
29	PermissionDenied	操作不允许

3 联系我们

深圳市纹宁信息技术有限公司

地址：深圳市宝安区新安街道宝民一路 223 号福城时代广场一单元 3211

电话：0755-27920930

网站：www.winuim.com

邮箱：services@winuim.com