

林阳域计算机扫描与管理系统 9

使 用 手 册

非常感谢您使用我们的产品，如果您有什么疑问或需要请随时联系我们。

目录

一、软件简介	4
二、软件运行环境.....	4
三、软件的获取	5
四、域计算机开启远程管理的方法	6
五、软件的主要功能及使用方法操作简介.....	11
5.1、扫描计算机的配置信息	11
5.1.1、通过 IP 地址段进行扫描.....	11
5.1.2、通过对 txt 文件内容进行扫描.....	12
5.1.3、通过常用主机列表进行扫描.....	13
5.1.4、通过单机连接管理进行扫描.....	14
5.1.5、设置定时扫描计划.....	15
5.2、计算机信息查看及管理	15
5.2.1、通过单机连接管理.....	16
5.2.2、通过常用主机列表.....	17
5.2.3、通过扫描的计算机配置信息.....	17
5.2.4、多用户登录计算机时切换不同的用户.....	18
5.3、连接身份验证类型	19
5.4、扫描检测选项的设置	21
5.5、常用主机列表参数设置	22
5.6、执行前 PING 操作.....	24
5.7、查看连接错误的记录	25
5.8、添加计算机到常用主机列表中	27
5.8.1、通过扫描的计算机配置信息结果进行添加	27
5.8.2、通过计算机信息查看及管理进行添加.....	29
5.8.3、通过 EXCEL 批量导入主机	30
5.9、批量执行相关操作命令	32
5.10、保存计算机配置信息到数据库	34
5.10.1、通过扫描的计算机配置信息.....	34
5.10.2、通过计算机信息查看及管理.....	35
5.10.3、保存计算机配置信息的基本信息参数设置.....	37
5.11、查看及管理数据库中保存的计算机配置信息.....	38
5.12、AD 域对象的操作	40
5.12.1、查看域信息及帐户密码策略信息.....	41
5.12.2、查看及管理域用户信息.....	41
5.12.3、查看域组信息.....	43
5.12.4、查看及管理域计算机信息.....	44
5.12.5、批量管理域计算机的本地管理员.....	45
5.13、查看指定路径下文件夹及子文件夹的权限	46
5.14、查看已成功连接的历史记录	47
六、常见问题	48

6.1、请分别尝试用计算机名或 IP 地址进行计算机信息查看及管理.....	48
6.2、通过强制开启计算机可被远程管理	53
6.3、通过执行解决 RPC 服务器不可用等问题应用程序	55
6.4、通过关闭 WINDOWS 防火墙.....	56
七、购买注册	57
八、软件技术支持.....	59

由于产品不断更新，本公司不承诺实际产品与该数据一致，同时也不承担由于实际技术参数与本数据不符而导致的任何争议。

一、软件简介

“林阳域计算机扫描与管理系统”是我工作室经过多年的自主开发和设计的，它包含大量 IT 常用的功能，无需在被连接的计算机上安装服务端程序，专门用于批量扫描或远程管理域计算机。

您只需要在任意一台加入域并用域管理员用户（Domain Admins 组成员）登录或当前登录的域帐户属于被连接计算机的本地管理员（Administrators 组成员）的计算机上运行此软件，无需部署服务端程序，通过简单的操作即可实现批量扫描或远程管理整个域中所有计算机的软件信息、硬件信息、系统维护、系统优化、事件日志、运行状态、使用记录等用户最关心的问题。

软件还包含一个强大的 AD 对象浏览器，如域用户、域组、域计算机对象的属性批量查看或管理，另外还提供了计算机资产管理系统、查看共享文件目录的权限列表、批量执行相关操作命令、强制开启计算机可被远程管理等多种功能，有效的集中帮助用户快速发现和解决问题，是企业域管理员/系统管理员/IT HelpDesk 等 IT 人员信赖且不可或缺之日常管理工具。

产品优势：

1. 无需在客户端电脑上安装服务端程序。
2. 一个管理端可跨网段批量扫描或远程管理域中所有计算机的软硬件等信息。
3. 批量扫描或远程管理时，被连接客户端无需确认、静默执行无任务提示信息。
4. 包含大量 IT 常用的功能和 AD 域用户、域组、域计算机对象的批量查看或管理。
5. 常用主机列表的管理。
6. 简单易用的图形化操作界面。

二、软件运行环境

应用平台：Windows XP/2003/Vista/7/8/10/11/2008/2012/2016/2018/2019/2022 32 位或 64 位操作系统

CPU：双核 CPU 主频 2 GHz 或以上

内存：1GB 或更高

显示：支持 1360*768 或更高分辨率的显示器

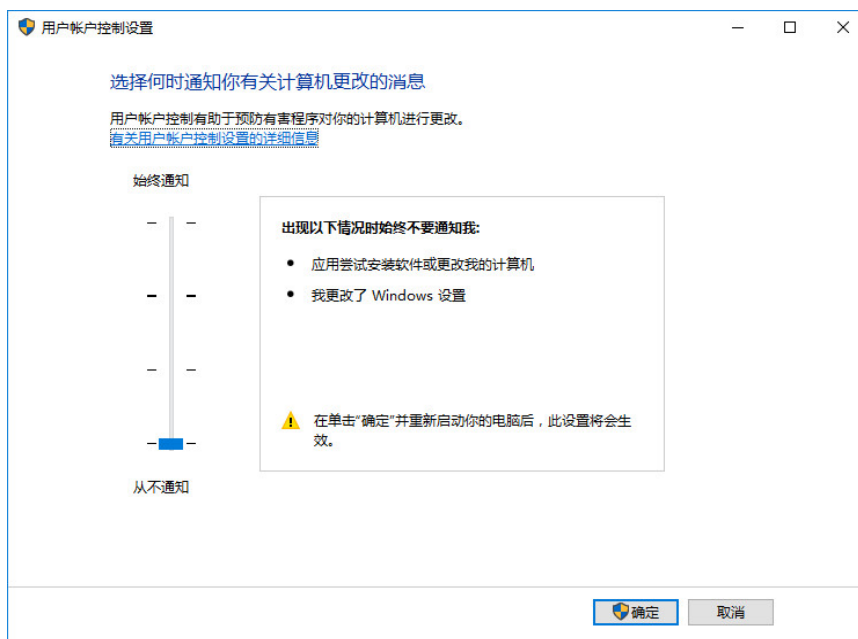
Office：MS Office 2013 或以上版本

建议运行环境：

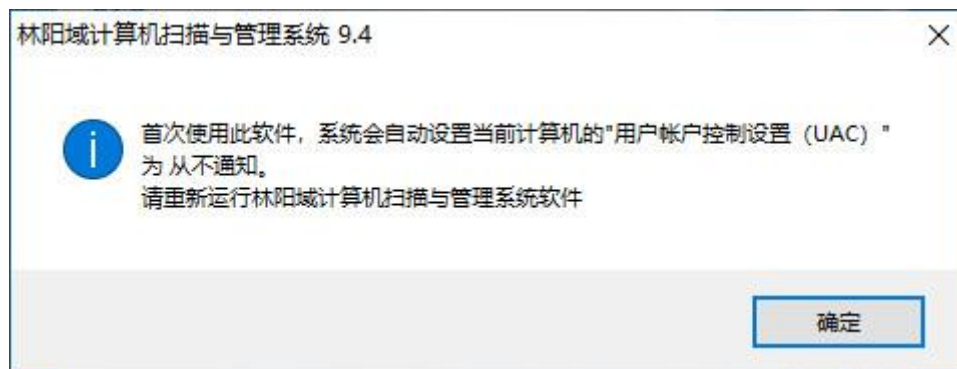
- 1、当前登录计算机的域帐户属于 Domain Admins 组的成员或属于被连接计算机的本地 Administrators 组的

成员。

- 2、建议在 Windows 10 64 位或以上版本的操作系统上安装并运行软件。
- 3、软件运行前请先设置 UAC 为从不通知并重新启动计算机（说明：如果没有手动关闭 UAC 为从不通知，则软件第一次运行时会自动设置 UAC 为从不通知，已设置为 UAC 为从不通知或操作系统为 Windows XP、2003 可跳过此步骤。），如下图所示：



如未设置 UAC 为从不通知，则第一次打开软件会弹出如下提示：



- 4、安装了 Microsoft Office 2013 或以上软件版本，导出操作需用到 Excel。
- 5、建议勾选使用当前登录凭据进行连接验证。

三、软件的获取

请访问林阳软件工作室的官方网站，网址：<http://www.linyangrj.com> 下载最新的版本，软件有新版本发布后，都可以免费升级到最新版本。

四、域计算机开启远程管理的方法

为了确保林阳软件可以正常远程扫描或远程管理域计算机，请检查确认域计算机的以下项：

1、计算机已加入域，到域控制器的网络已连接。命令：`ping`

2、确保与域控制器的时间差不能大于 5 分钟。命令：`net time /domain`

3、您拥有域管理员权限（Domain Admins 组成员）或远程计算机的本地管理员（Administrators 组成员）的帐户和密码，密码不能为空，帐户未过期或停用。

4、在 Windows 防火墙有设置允许“远程管理”例外（Windows 防火墙如有关闭此步骤可以略过），具体设置命令如下：

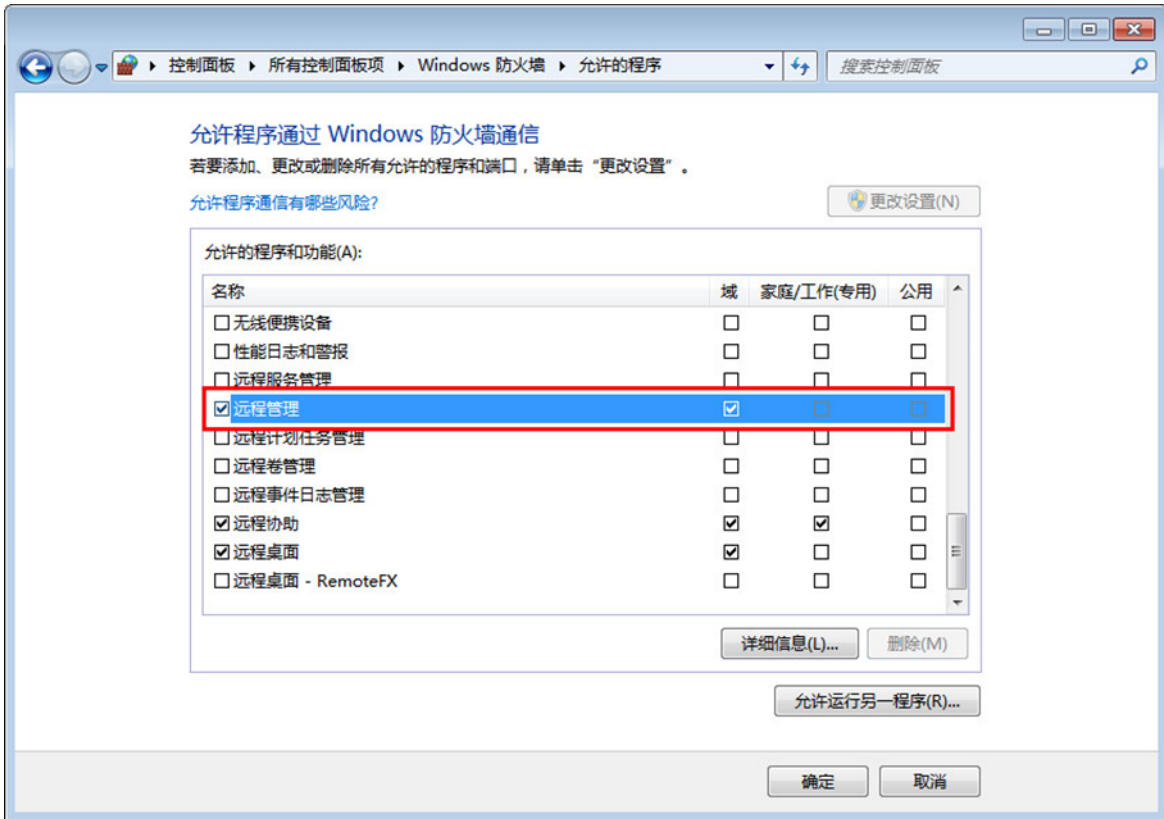
方法一（适用于 Windows XP/2003）：

```
netsh firewall set service RemoteAdmin enable      '允许远程管理
netsh firewall set service FileAndPrint enable     '允许文件和打印机共享
```

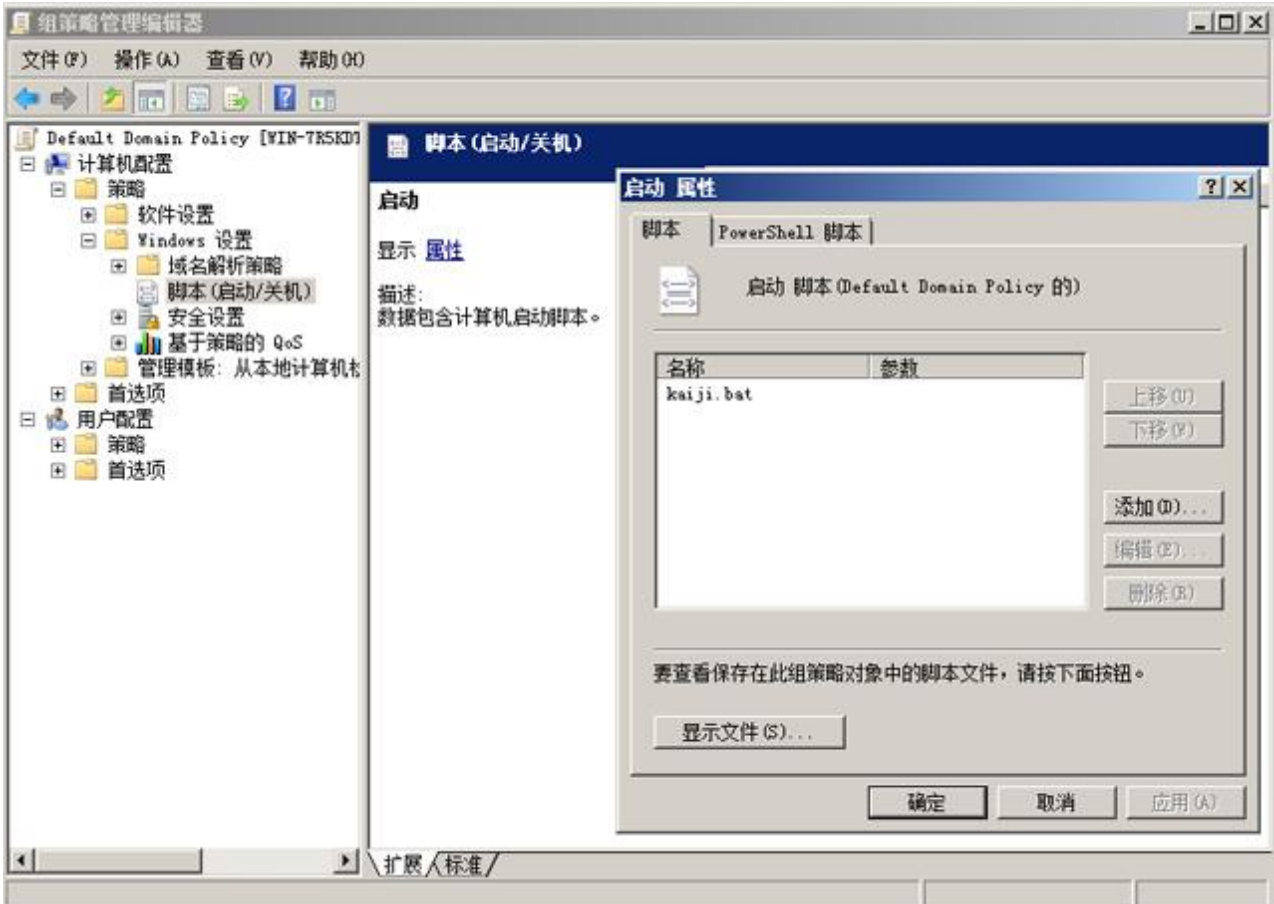
方法二（适用于 Windows Vista 及以上系统，请以管理员身份在 CMD 中执行。）：

```
netsh firewall set service RemoteAdmin enable      '允许远程管理
netsh firewall set icmpsetting 8                  '开启允许 Ping 操作（Windows XP 下不用）
netsh firewall add portopening TCP 135 DCOM_TCP135
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

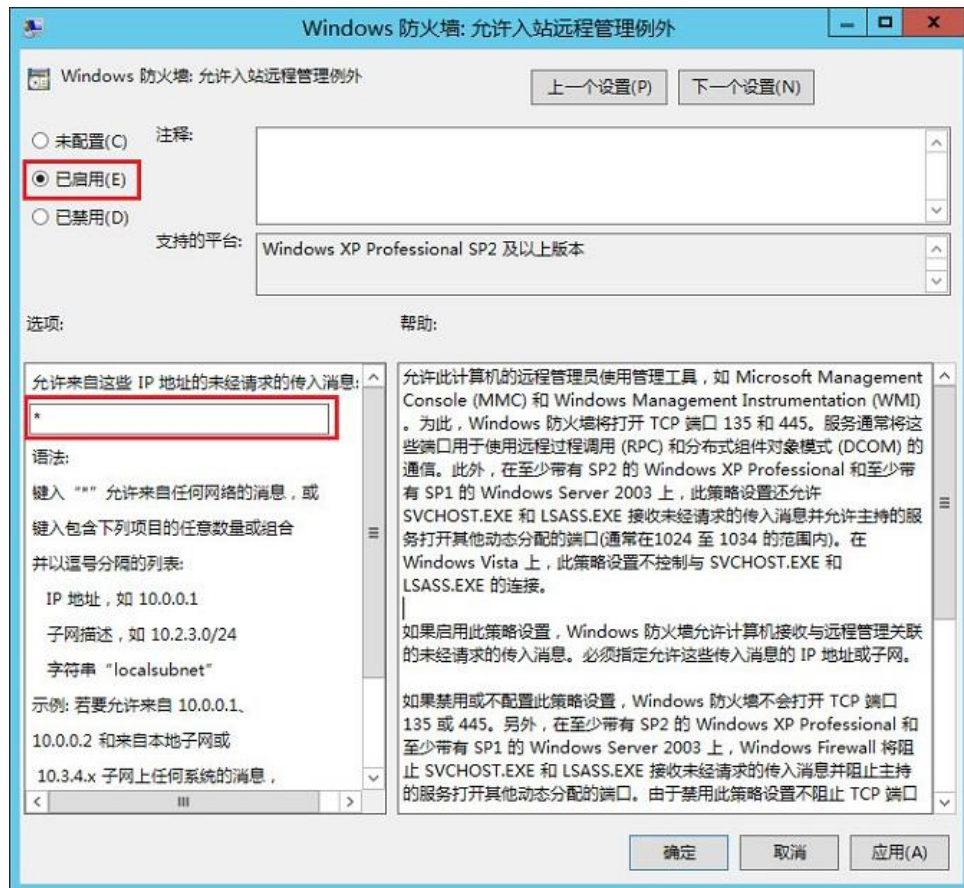
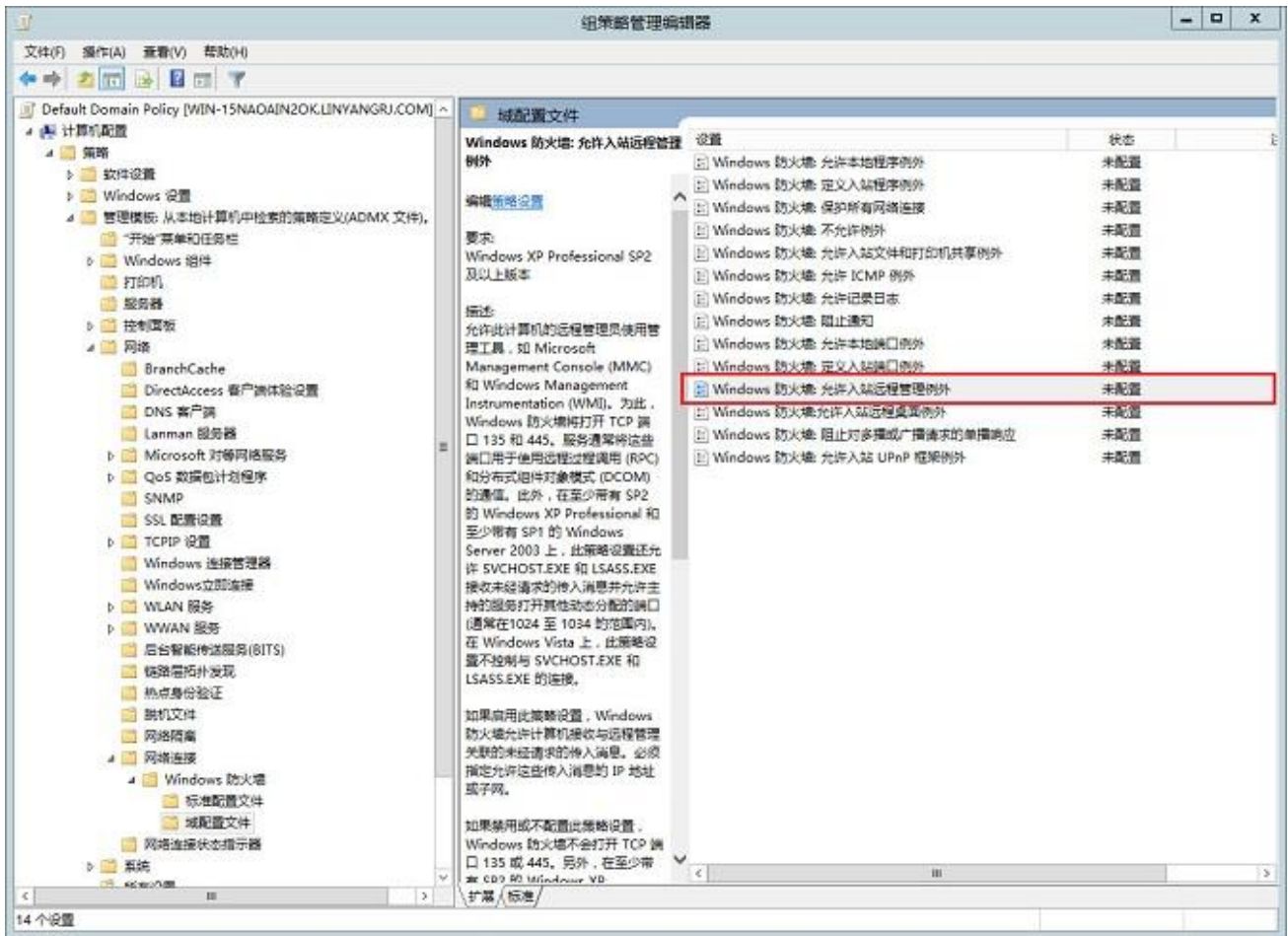
说明：netsh firewall set service RemoteAdmin enable 命令其实就是在 Windows 防火墙中例外“远程管理”，如下图所示：



小提示：你也可以将以上命令保存为.bat 或.cmd 文件，再通过域策略设置开机启动脚本（说明：这个脚本域计算机只需执行一次就可以了。），这样就可以批量开启域计算机的远程管理功能了，如下图所示：



另外也可以通过域策略设置允许远程管理，如下图所示：



5、确认注册表项值

路径	名称	类型	数值
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	EnableDCOM	REG_SZ	Y
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	LegacyAuthenticationLevel	REG_DWORD	2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa	forceguest	REG_DWORD	0

未加入域的计算机（Windows Vista 及以上版本操作系统）

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system

LocalAccountTokenFilterPolicy REG_DWORD 1

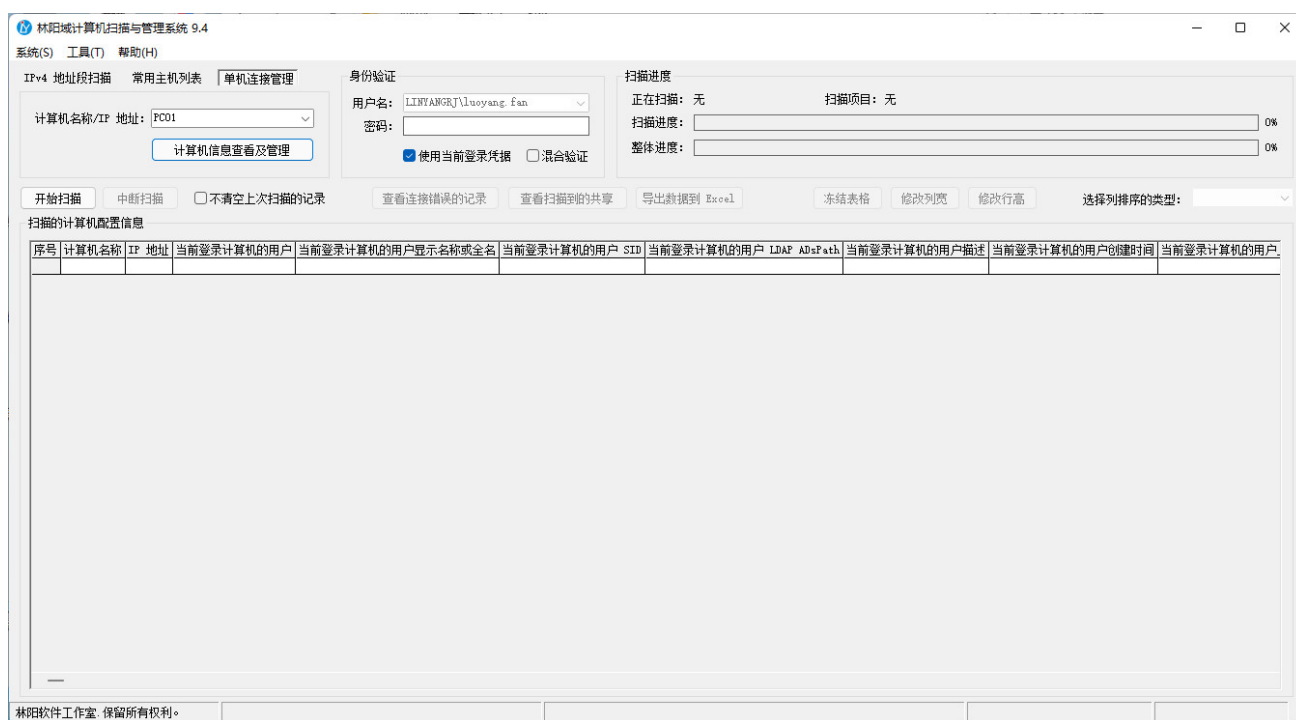
如果你觉得第 4~5 步骤操作很麻烦，那就在每一台域计算机上执行我们的一键修复软件，如下图所示：



6、直接关闭 Windows 防火墙，前提是你已安装了防毒软件。

五、软件的主要功能及使用方法操作简介

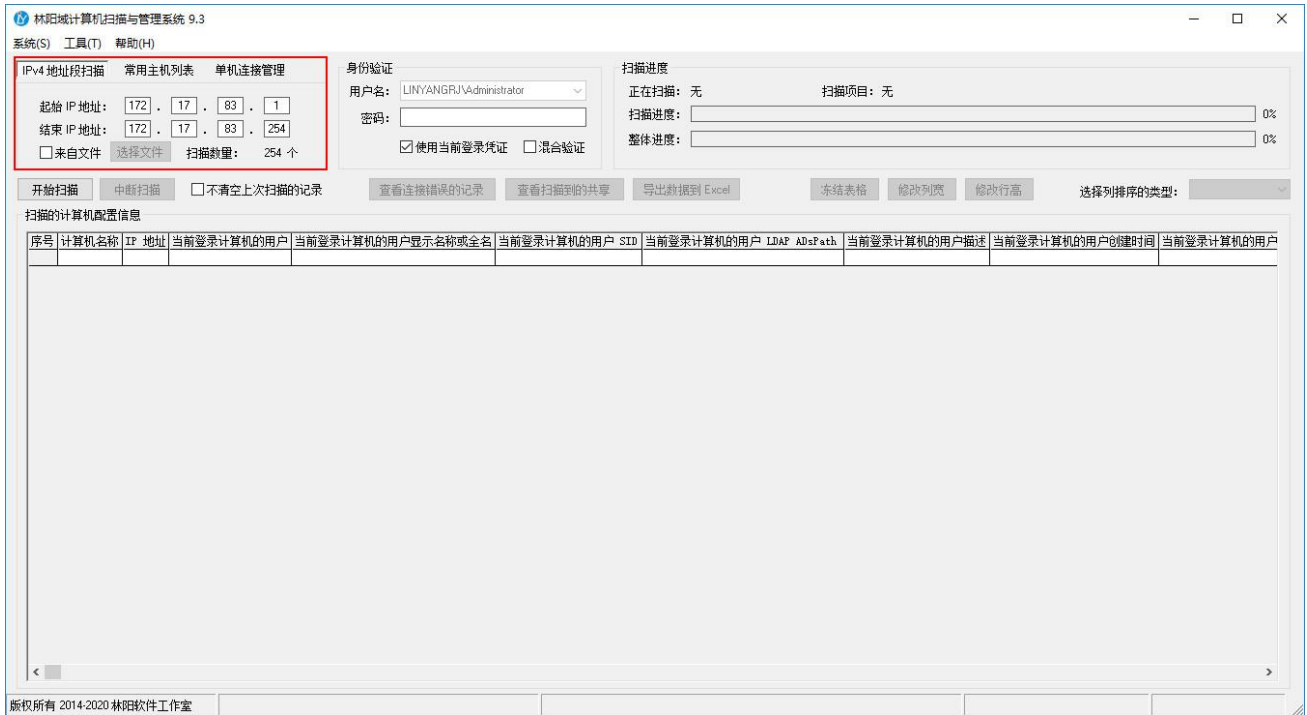
软件打开启动的界面如下图所示：



5.1、扫描计算机的配置信息

5.1.1、通过 IP 地址段进行扫描

1、打开软件，单击“IPv4 地址段扫描”选项卡，手动输入要扫描的指定 IP 地址范围，再单击“开始扫描”按钮即可，如下图所示：

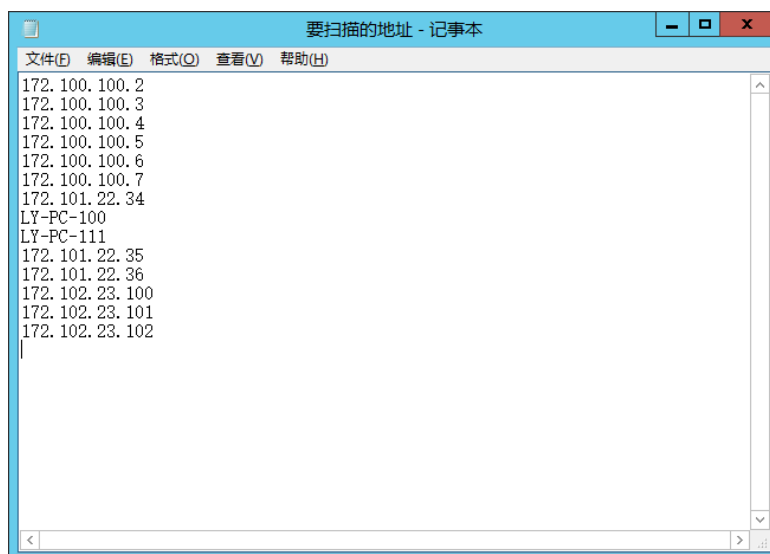


5.1.2、通过对 txt 文件内容进行扫描

1、如果网络规划的 VLAN 比较多，但每个 VLAN 网段已在使用的 IP 地址又不多，通过输入指定网段进行扫描，需频繁地输入不同的 IP 地址段，现有一个简便的操作方法，大家可以通过 DHCP 服务器把已租用的 IP 地址或计算机名称导出来，如下图所示：

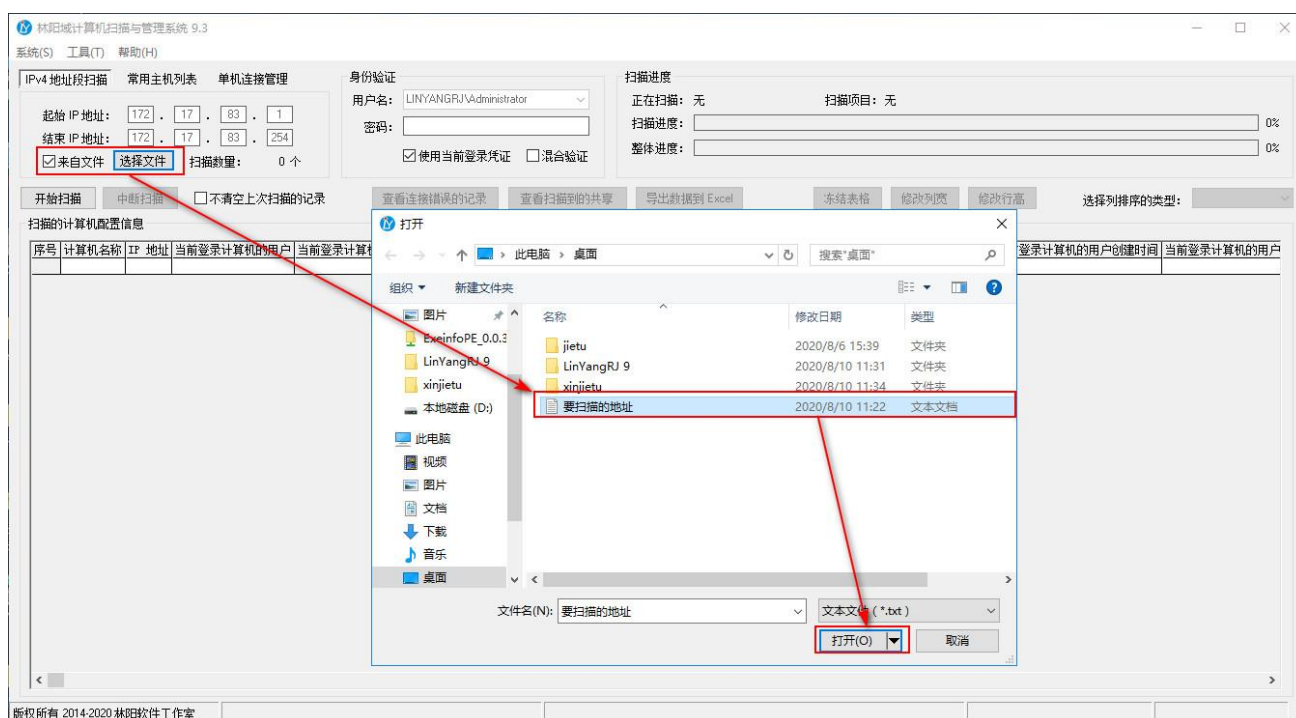


2、再把导出出来的内容整理后保存为.txt 文件，一个 IP 地址或一个计算机名为一行，此文件内容可以包含 IP 地址和计算机名称，如下图所示：



提示：当然你也可以直接将加入域的计算机名称导出来，可以通过点击“系统-查看及管理域计算机信息”导出域计算机名称，保存为txt文件，还是一个计算机名为一行。

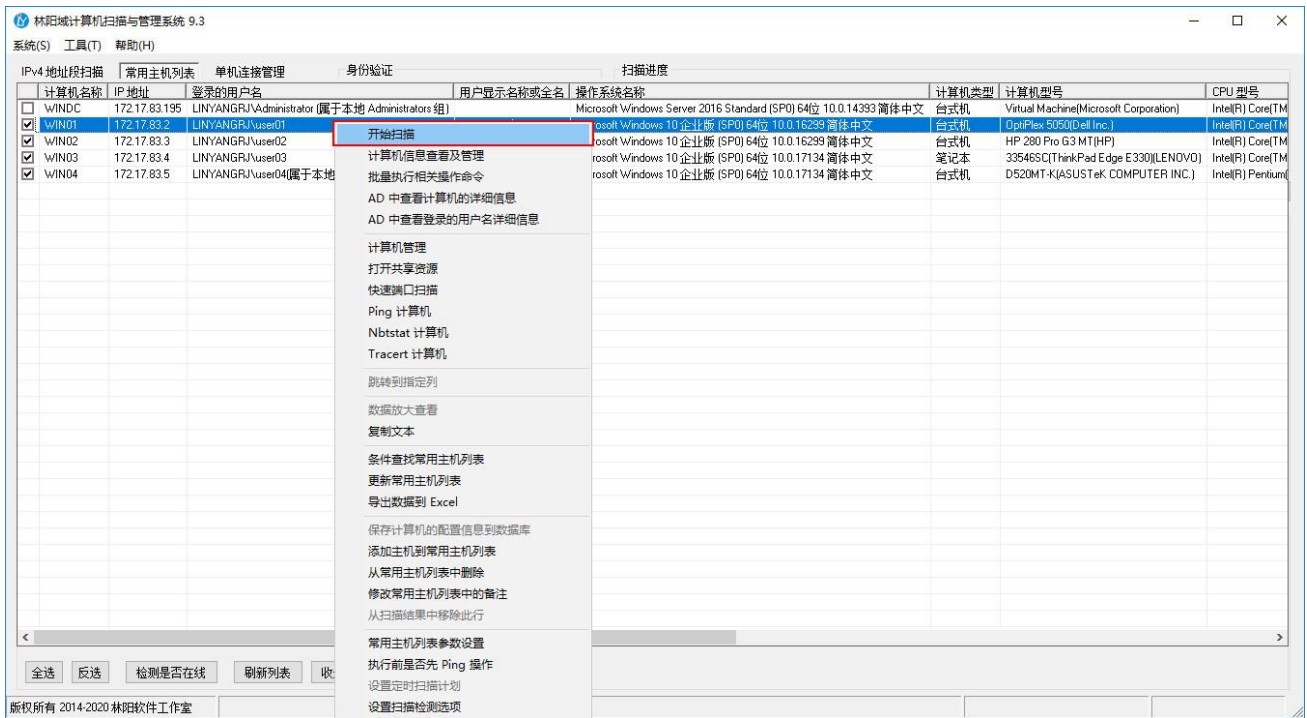
3、打开软件，单击“IPv4 地址段扫描”选项卡，先勾选“来自文件”复选框，再单击“选择文件”按钮，选择自己要扫描的txt文件并单击“打开”按钮，软件自动检测txt文件的行数，也就是要扫描的数量，再单击“开始扫描”按钮即可，如下图所示：



5.1.3、通过常用主机列表进行扫描

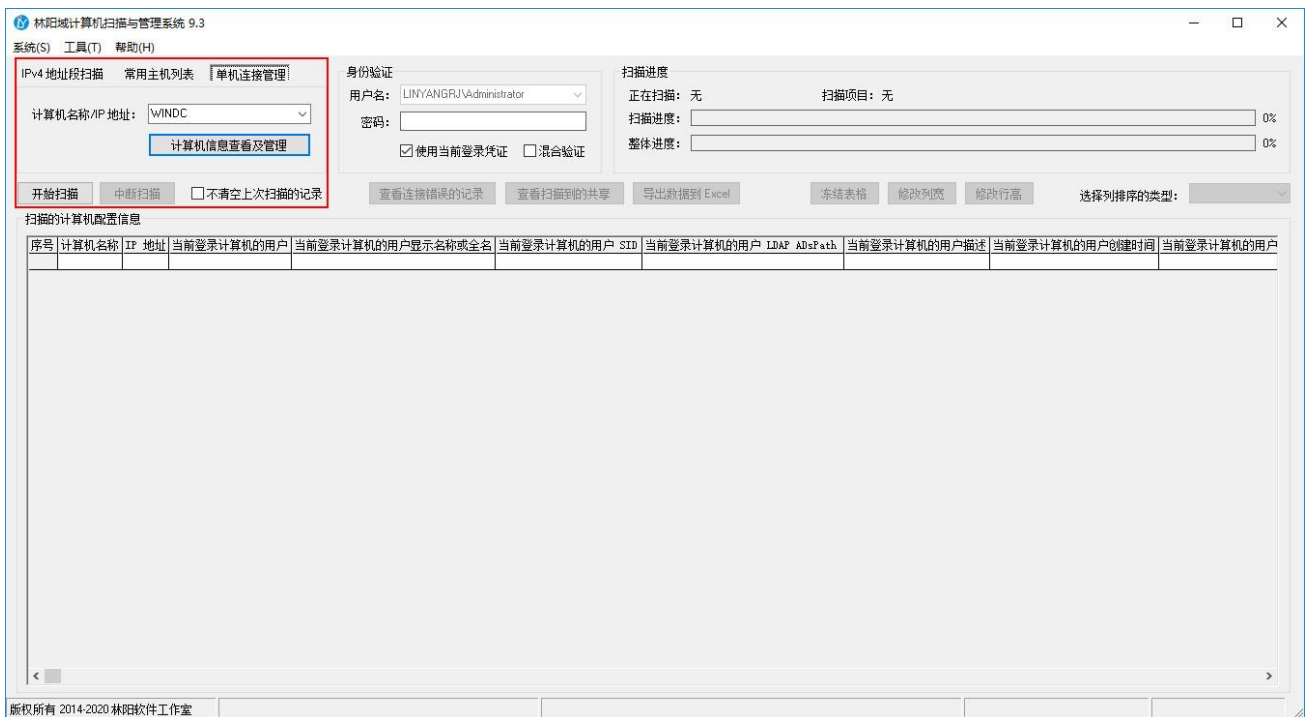
打开软件，单击“常用主机列表”选项卡，先勾选你要扫描的计算机列表，再单击右键“开始扫描”

菜单即可，如下图所示：



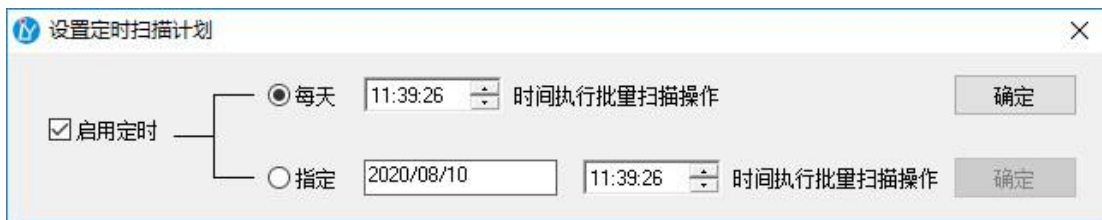
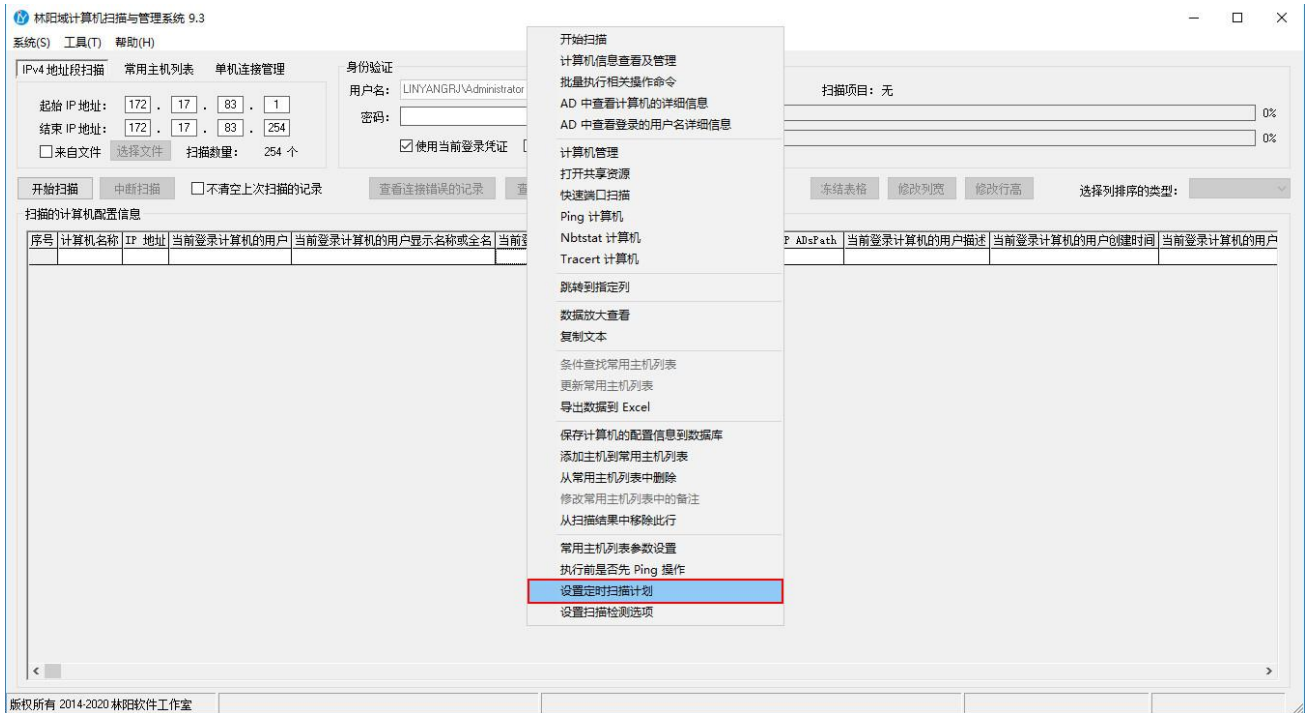
5.1.4、通过单机连接管理进行扫描

打开软件，单击“单机连接管理”选项卡，输入你要扫描的计算机名称/IP 地址，再单击“开始扫描”按钮即可，如下图所示：



5.1.5、设置定时扫描计划

如你需要每天定时对计算机进行扫描，打开软件，在“扫描的计算机配置信息”列表上单击右键“设置定时扫描计划”菜单，如下图所示：



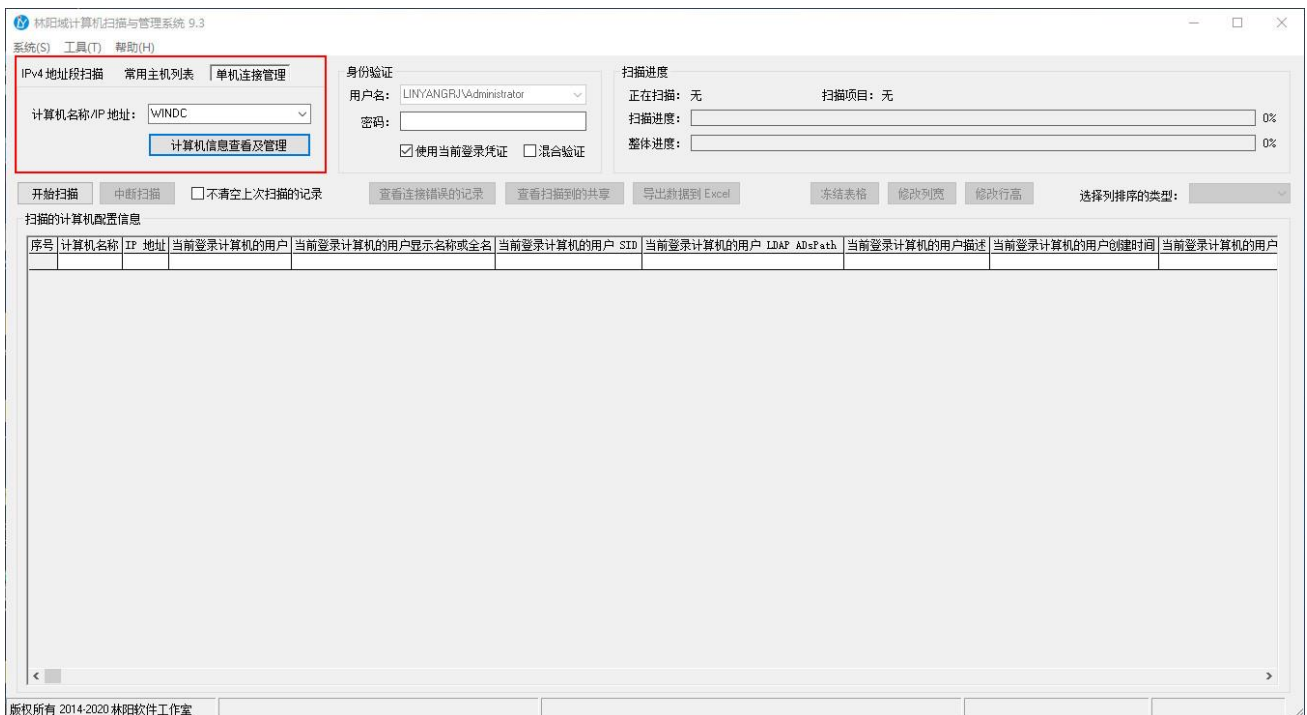
5.2、计算机信息查看及管理

主要用于对指定的单个计算机信息的查看及管理操作，这里包含大量 IT 常用的功能，如：计算机名/域更改、Windows 远程桌面连接、计算机管理、TCP/IP 设置、截取屏幕、远程 CMD、关机操作、发送消息、USB 存储设备管理、用户登录管理、清理系统垃圾、进程管理、服务管理、共享管理、用户和组管理等功能，这里不一一介绍，主要的界面如下图所示：



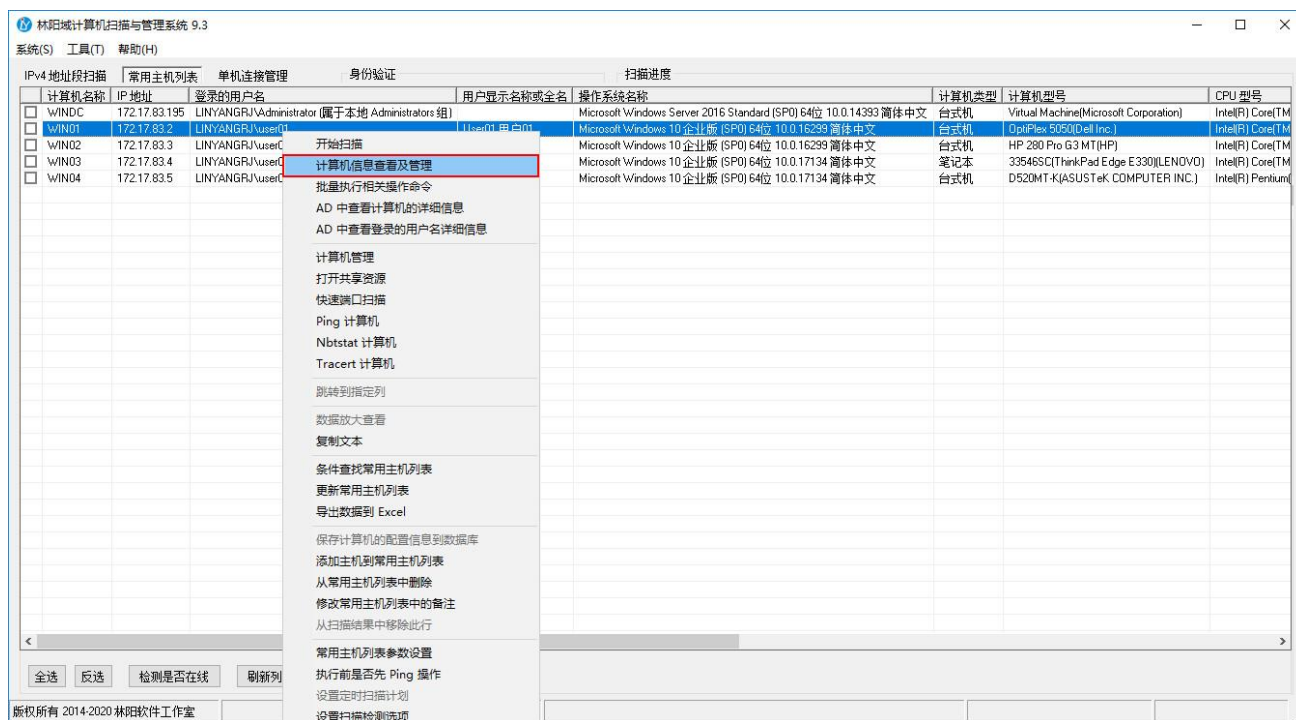
5.2.1、通过单机连接管理

打开软件，单击“单机连接管理”选项卡，输入你要管理的计算机名称/IP 地址，再单击“计算机信息查看及管理”按钮，如下图所示：



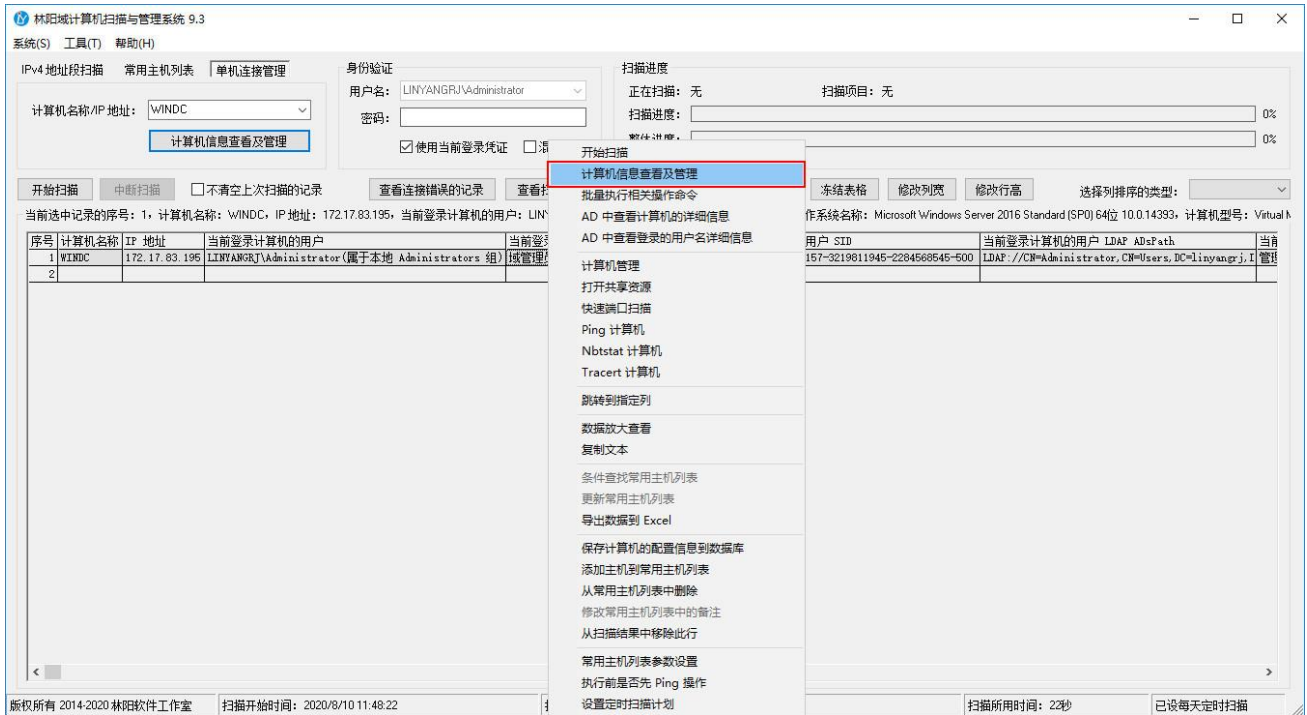
5.2.2、通过常用主机列表

打开软件，单击“常用主机列表”选项卡，选择你要管理的计算机列表，再单击右键“计算机信息查看及管理”菜单，如下图所示：



5.2.3、通过扫描的计算机配置信息

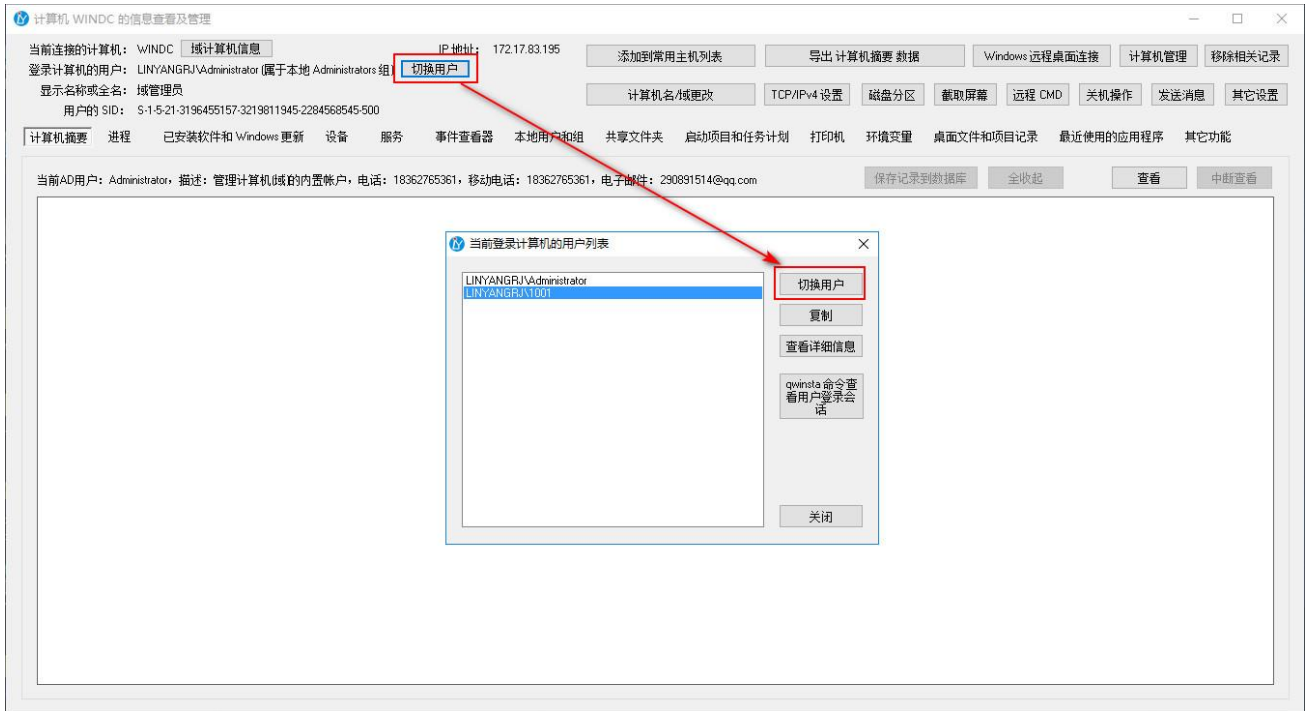
打开软件，在“扫描的计算机配置信息”列表上选择你要连接的计算机，再单击右键“计算机信息查看及管理”菜单，如下图所示：



说明：软件的其它功能界面也有“计算机信息查看及管理”的按钮，方便大家快速对指定的计算机进行操作，这里不再详细介绍了。

5.2.4、多用户登录计算机时切换不同的用户

1、当多个用户登录同一台计算机时，我们可以分别切换到指定用户对其进行相关的操作，在计算机信息查看及管理界面单击“切换用户”按钮，在弹出窗口中选择你要切换的指定用户，再单击“切换用户”按钮，如下图所示：



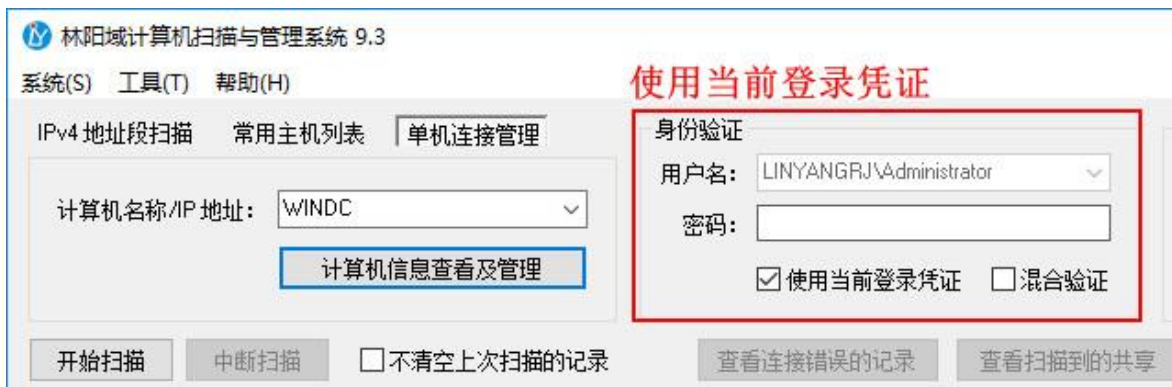
5.3、连接身份验证类型

软件的身份验证连接类型支持 5 种方式，默认勾选的是“使用当前登录凭证”，我们也建议大家使用当前登录凭证，这样执行批量扫描或远程管理等操作时执行速度也比较快一些，但你也可以使用指定的用户名和密码进行远程连接，大家可根据自己的实际情况，自由进行选择。

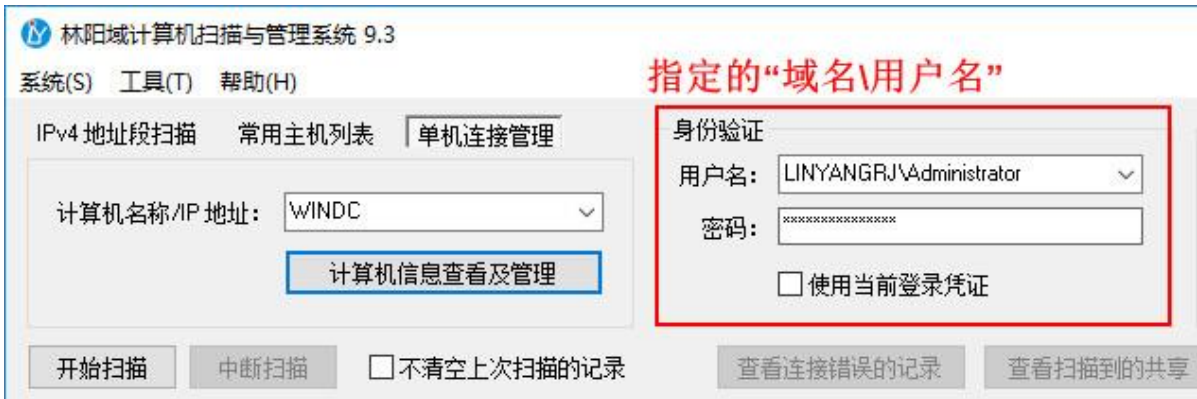
另软件也支持混合验证，混合验证的原理是当使用当前登录凭证连接操作失败后，自动切换使用指定的用户名和密码进行连接验证，所以当用户勾选了混合验证，也需要大家输入指定的用户名和密码（验证类型 3）。

说明：只有在域帐户下运行此软件时，才可以使用混合验证功能。

验证类型 1：使用当前登录凭证，如下图所示：



验证类型 2：使用指定的“域名\用户名”登录凭证，如下图所示：



验证类型 3：使用指定的“\本地用户名”登录凭证（说明：其中“.”代表的是计算机名称，这样不用担心因为每一台计算机名称不一样，要来回的输入不同的计算机名称。），如下图所示：



验证类型 4：使用指定的“计算机名称\本地用户名”登录凭证，如下图所示：



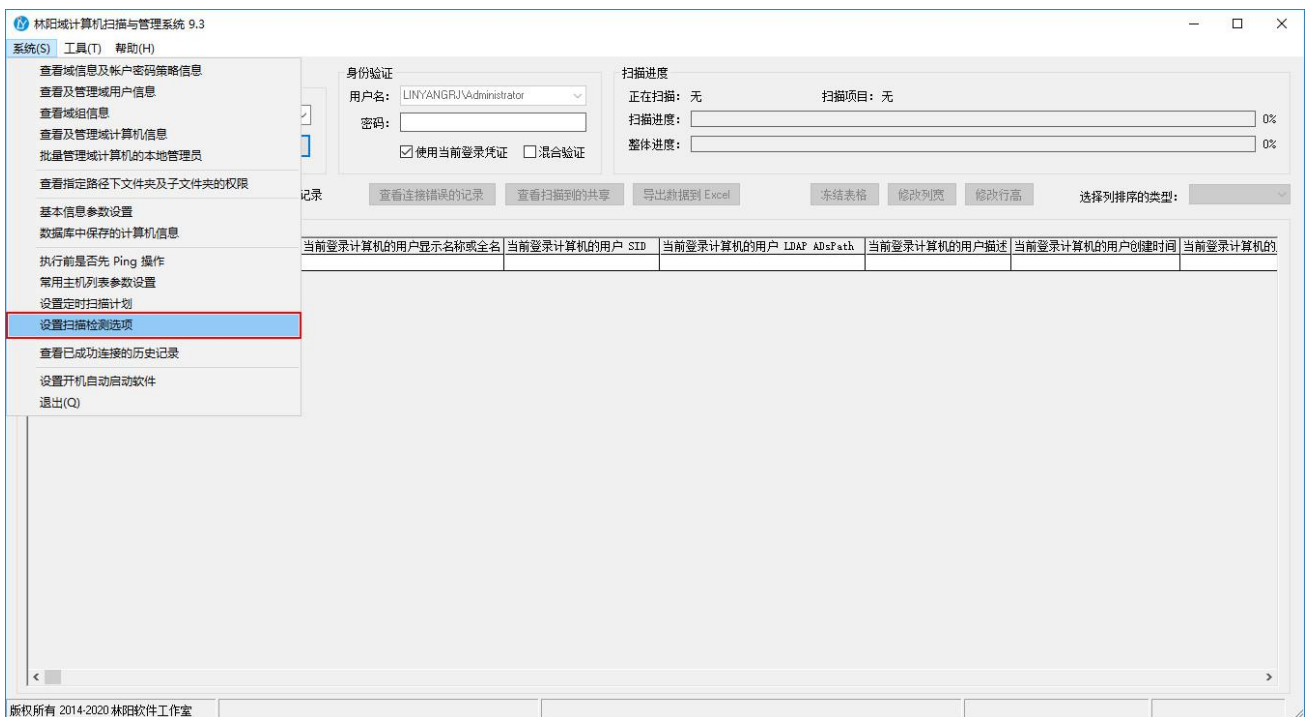
验证类型 5：使用混合验证，需要同时勾选“使用当前登录凭证”和“混合验证”，并输入指定的用户名和密码（验证类型 3），如下图所示：

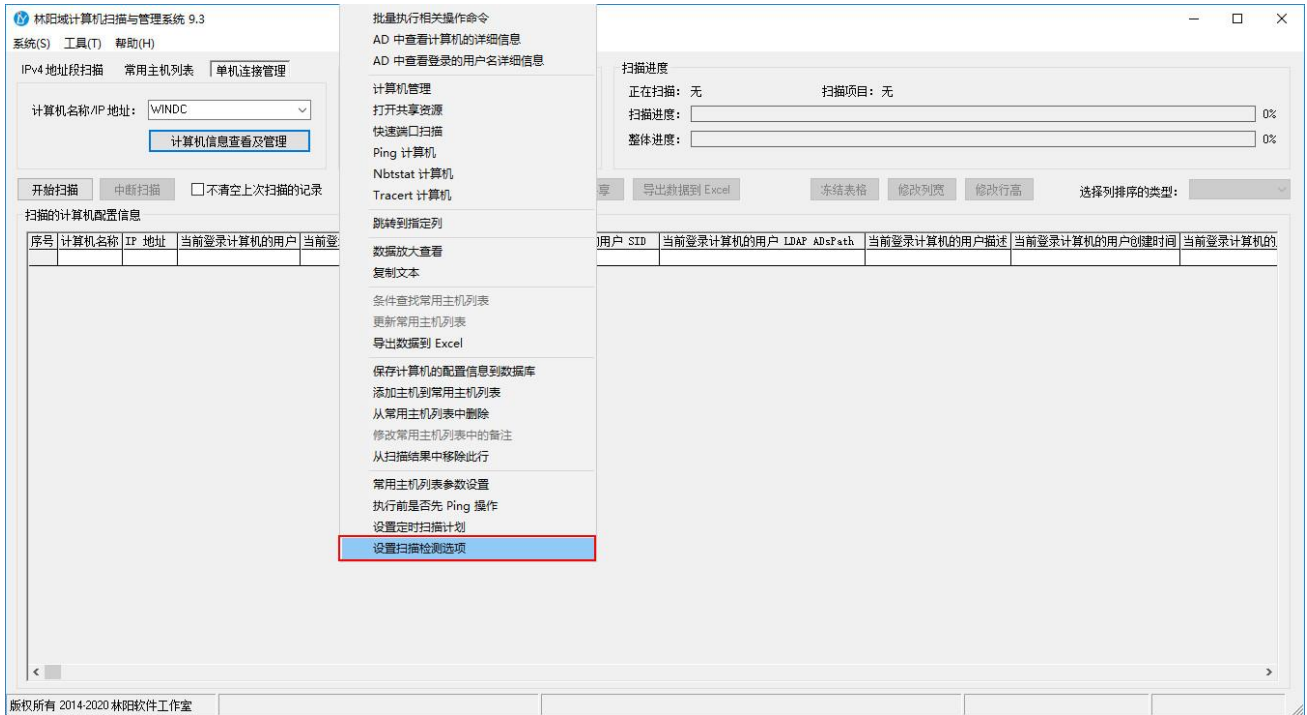


5.4、扫描检测选项的设置

软件设置有默认扫描项，但部分项的扫描速度慢没有被勾选，大家可以根据自己实际需要设置扫描一些指定的项，扫描项越少，扫描速度越快，反之扫描项越多，扫描速度就相对慢了。

打开软件，单击“系统—设置扫描检测选项”菜单，或在“扫描的计算机配置信息”下方单击右键“设置扫描检测选项”菜单可进行相关设置，如下图所示：





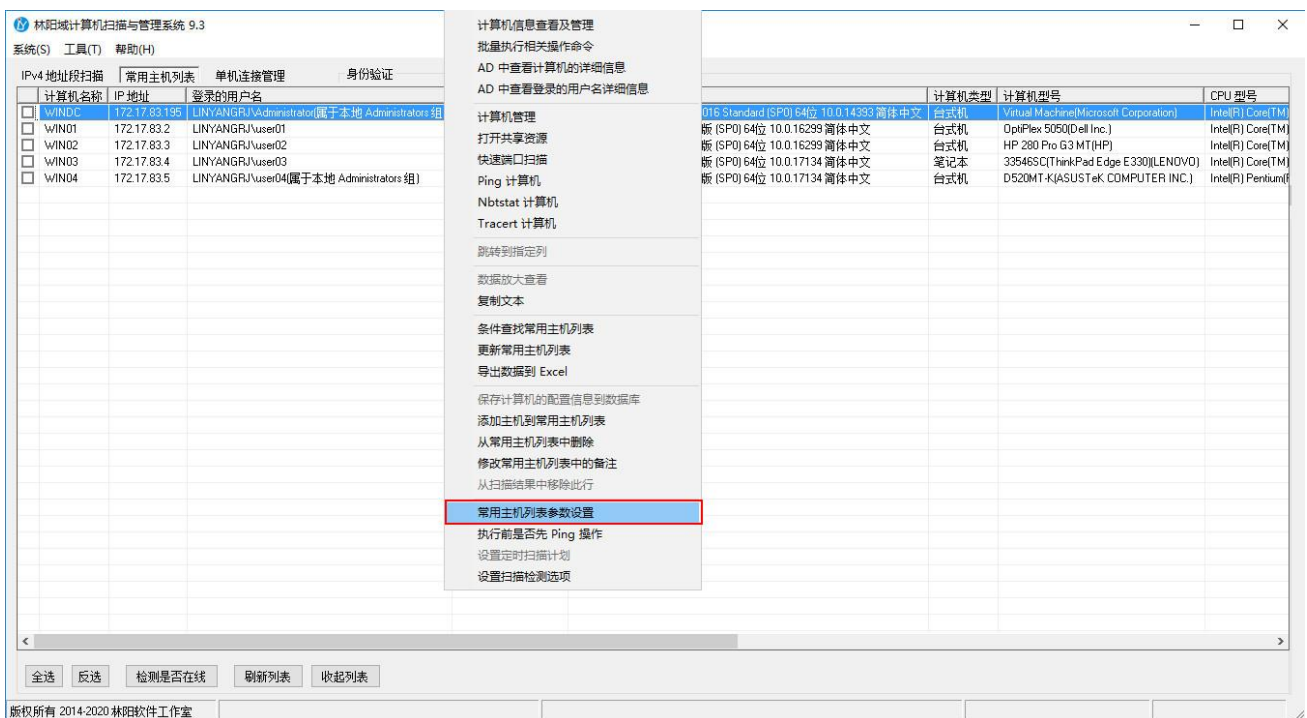
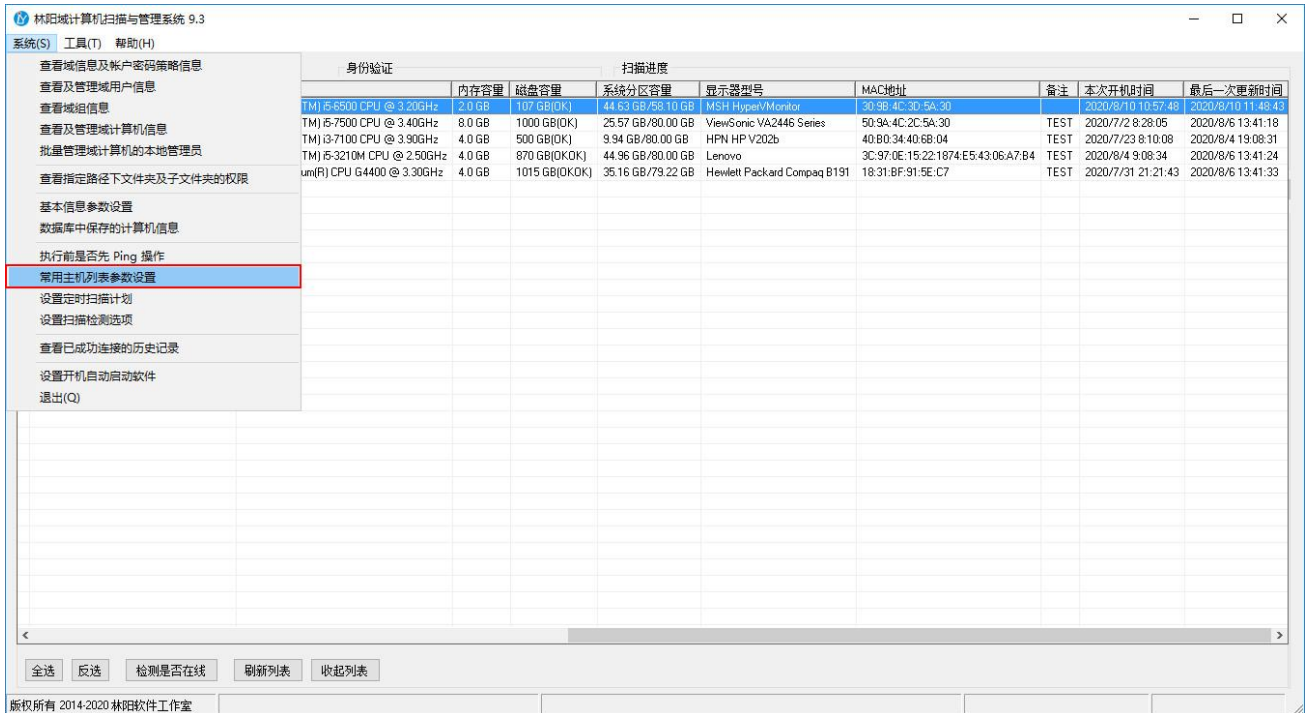
设置完毕之后，只需单击“确定”按钮即可，如下图所示：



使用软件默认勾选的扫描项进行扫描时，一台计算机的扫描时间平均是 1 分钟左右。

5.5、常用主机列表参数设置

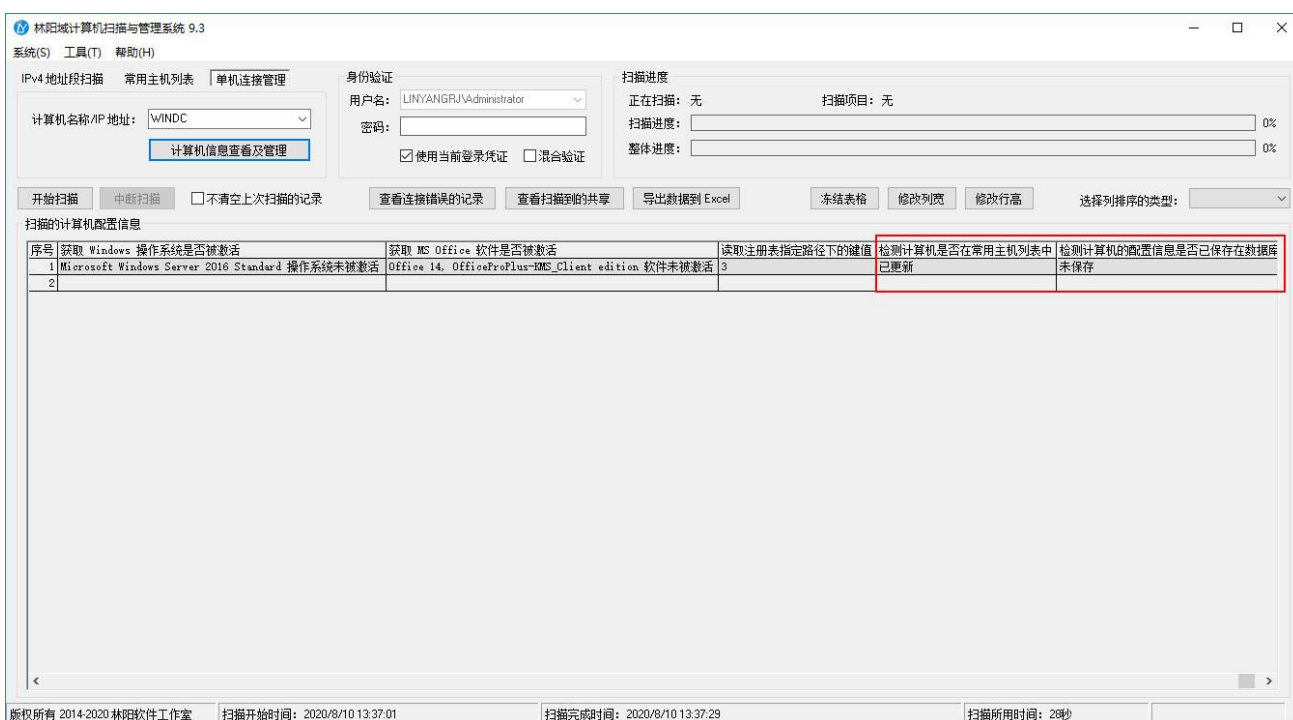
打开软件，单击“系统—常用主机列表参数设置”菜单，或在“扫描的计算机配置信息”下方单击右键“常用主机列表参数设置”菜单，如下图所示：



它主要用于设置连接时先以计算机名连接失败后，是否再尝试用对应的 IP 地址进行连接，以及扫描时自动检测计算机是否在“常用主机列表”或“计算机的配置信息是否已保存在数据库中”，如下图所示：



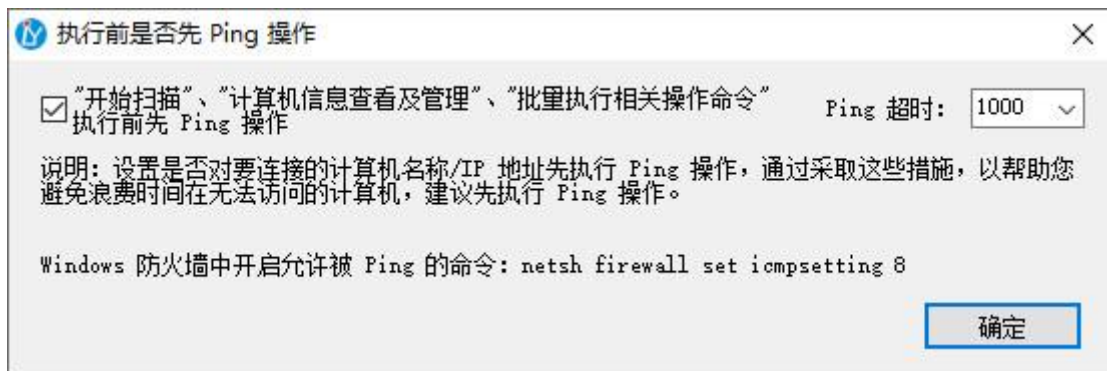
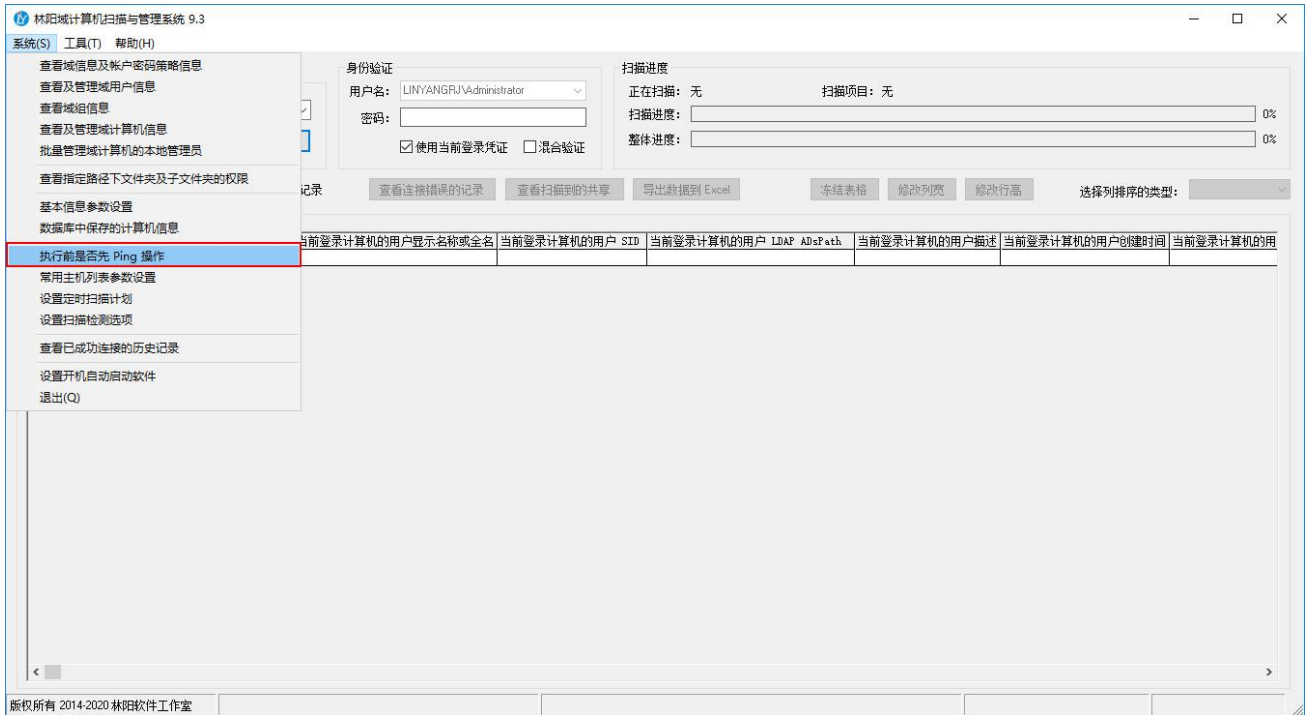
说明：当用户多次执行扫描时，如何确认哪些计算机之前有扫描过了，哪些没有被扫描过，大家可以把扫描过的计算机添加到常用主机列表和保存计算机配置信息到数据库中，在扫描完成后，最后二列会显示计算机是否在常用主机列表和计算机的配置信息是否已保存在数据库中的结果。



5.6、执行前 Ping 操作

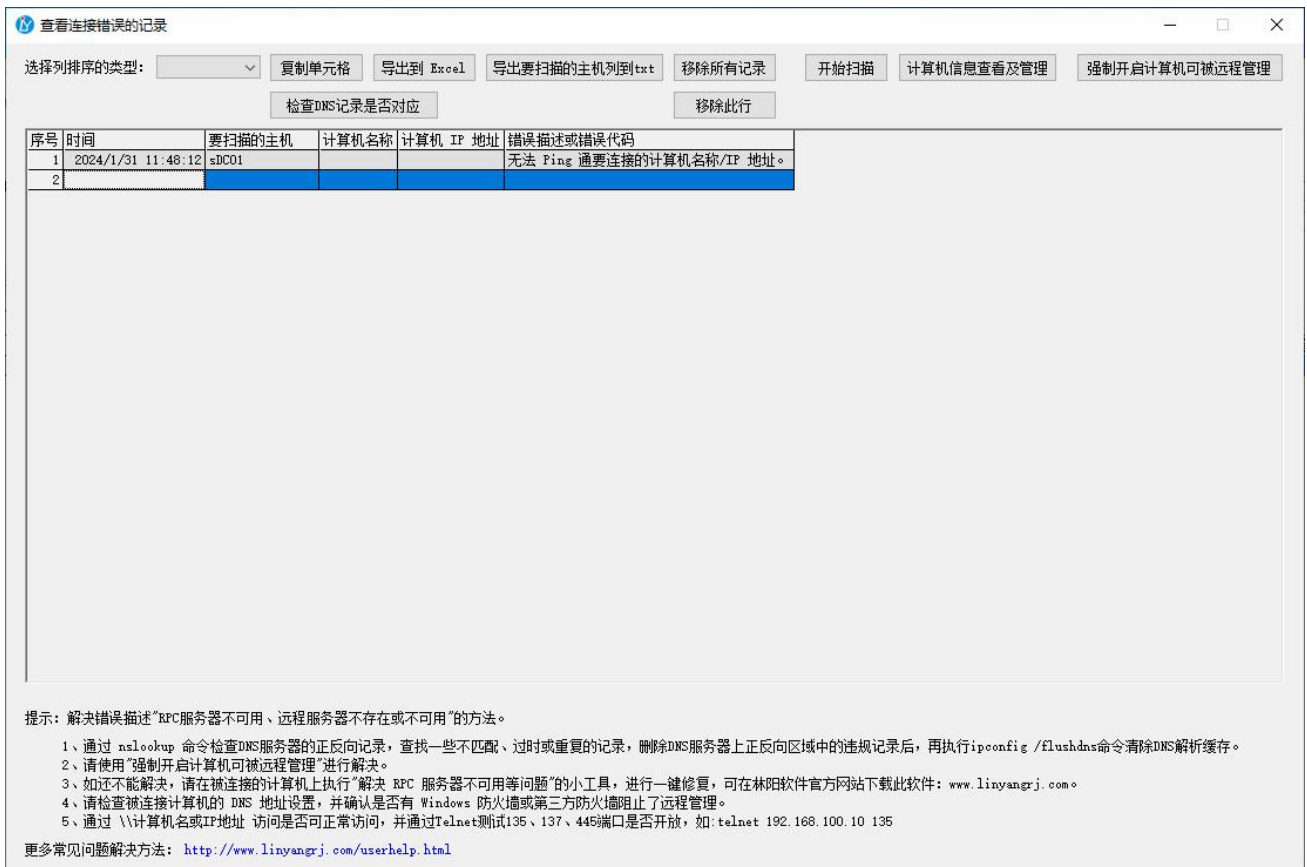
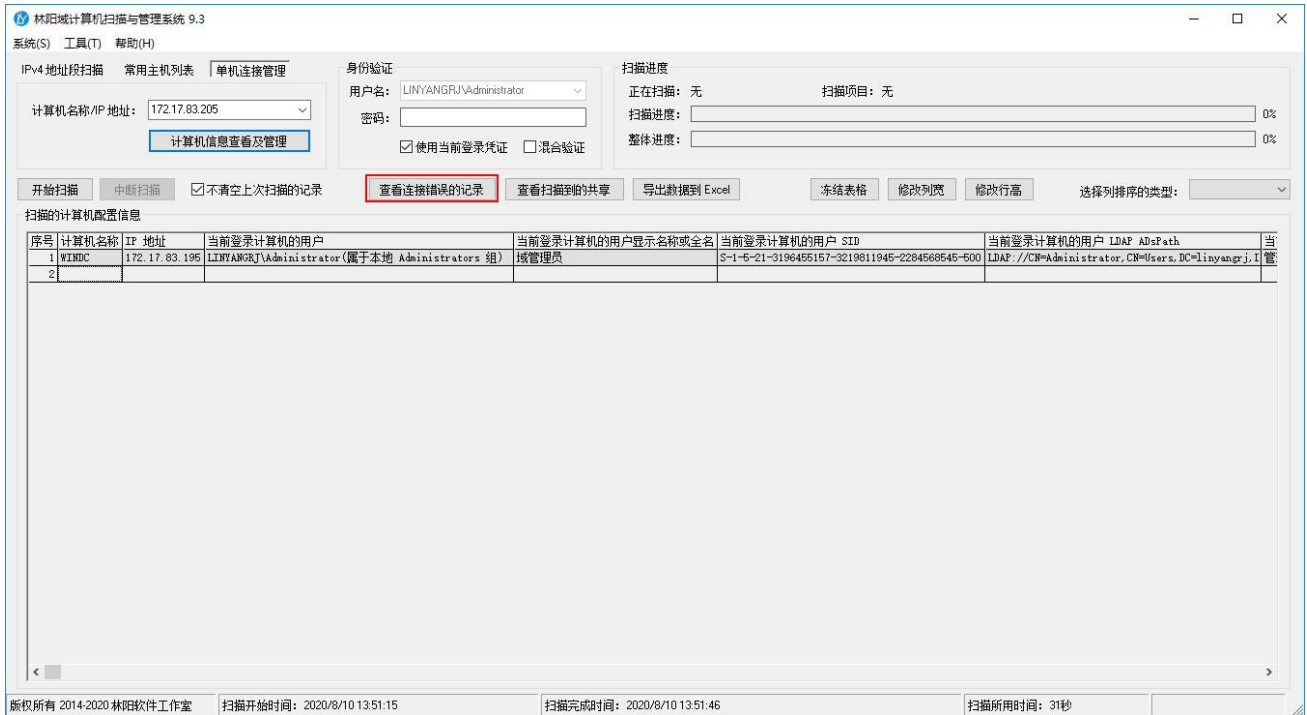
软件默认是对所连接的计算机名称/IP 地址先执行 Ping 操作，Ping 通后再执行连接操作，有些计算机由于启用了禁止 Ping 操作，所以我们无法进行连接，我们可以在连接前先关闭执行前 Ping 操作，再执行连接操作。

打开软件，单击“系统—执行前是否先 Ping 操作”菜单，或在扫描的计算机配置信息下方单击右键“执行前是否先 Ping 操作”菜单进行设置，如下图所示：



5.7、查看连接错误的记录

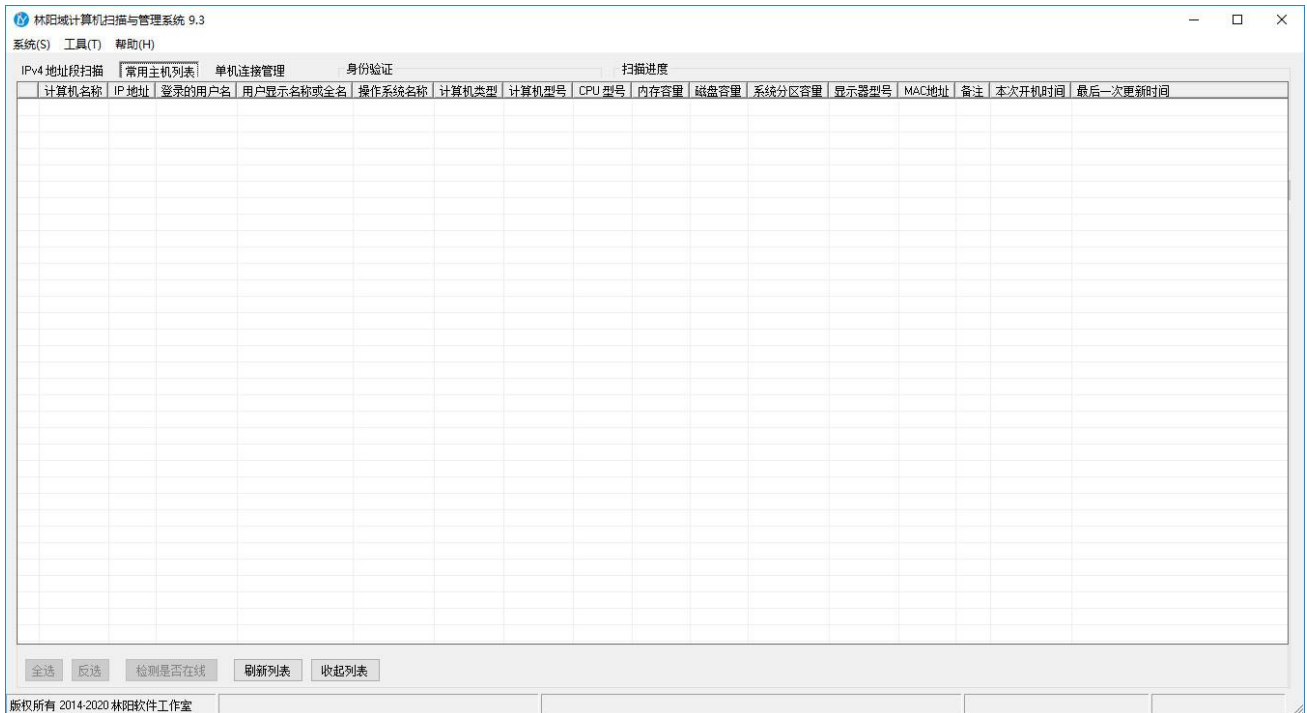
在扫描结束后，大家经常反映说好多计算机无法进行扫描，这时我们可以单击“查看连接错误的记录”按钮，就可以查看扫描过程中不能连接的计算机信息及错误原因，如下图所示：



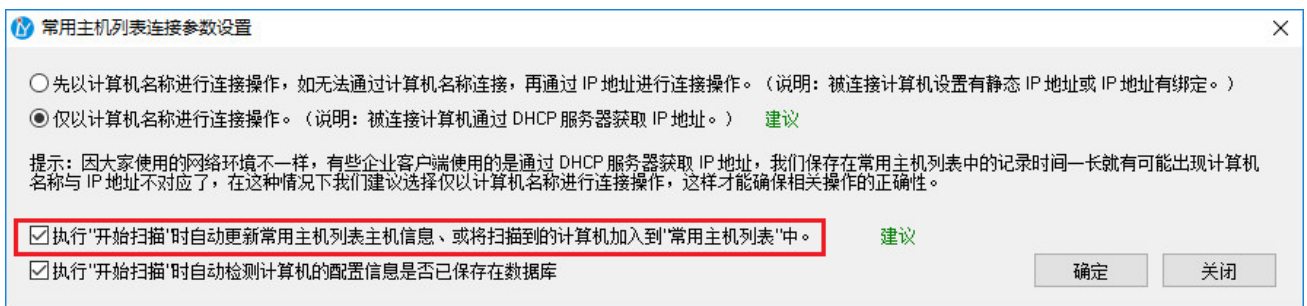
在这里我们也可以先对无法连接的计算机执行“强制开启计算机可被远程管理”或“通过快速连接管理”这个 2 项分别进行尝试，看看可不可以进行连接。

5.8、添加计算机到常用主机列表中

方便日常我们对常用的一些计算机进行扫描或远程管理及一些基本信息的查看。

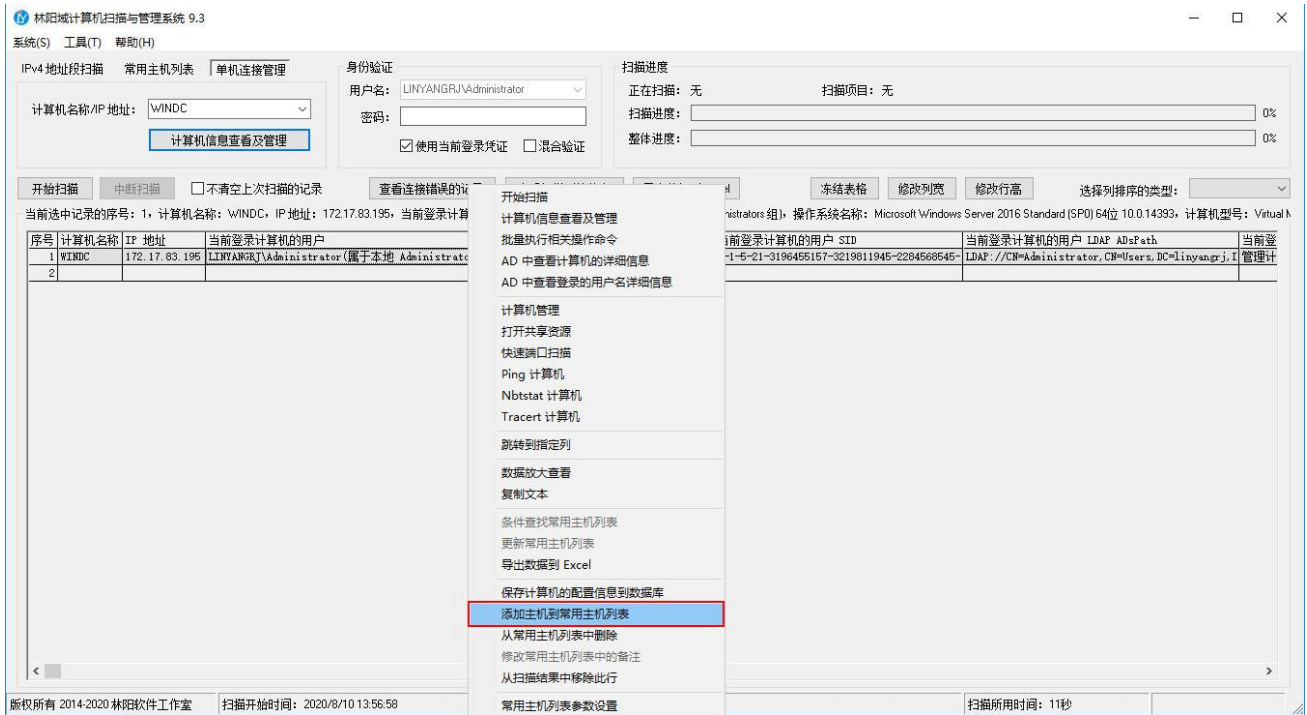


软件默认是在“常用主机列表连接参数设置”界面中有勾选在执行开始扫描时自动更新常用主机列表主机信息、或将扫描到的计算机加入到常用主机列表中，这样扫描时会自动添加及更新常用主机列表，如下图所示：



5.8.1、通过扫描的计算机配置信息结果进行添加

1、在“扫描的计算机配置信息”列表上选中指定行单击右键“添加主机到常用主机列表”菜单，如下图所示：



2、单击“确定”按钮即可，如下图所示：

添加到常用主机列表

计算机名称: DC01 IP 地址: 192.168.25.100

登录的用户名: LINYANG\Administrator (属于本地 Administrators 组)

用户显示名称或全名:

操作系统名称: Microsoft Windows Server 2022 Datacenter (SP0) 64位 10.0.20348 简

计算机类型: 虚拟机

计算机型号: VMware20,1 (VMware, Inc.)

CPU型号: Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz

内存容量: 2.0 GB

磁盘容量: 107 GB (OK)

系统分区容量: C:, 43.95 GB/57.88 GB

显示器型号:

MAC地址: 00:0C:29:AF:BF:94

本次开机时间: 2024/1/31 11:29:46

登录过此计算机的用户: LINYANG\Administrator

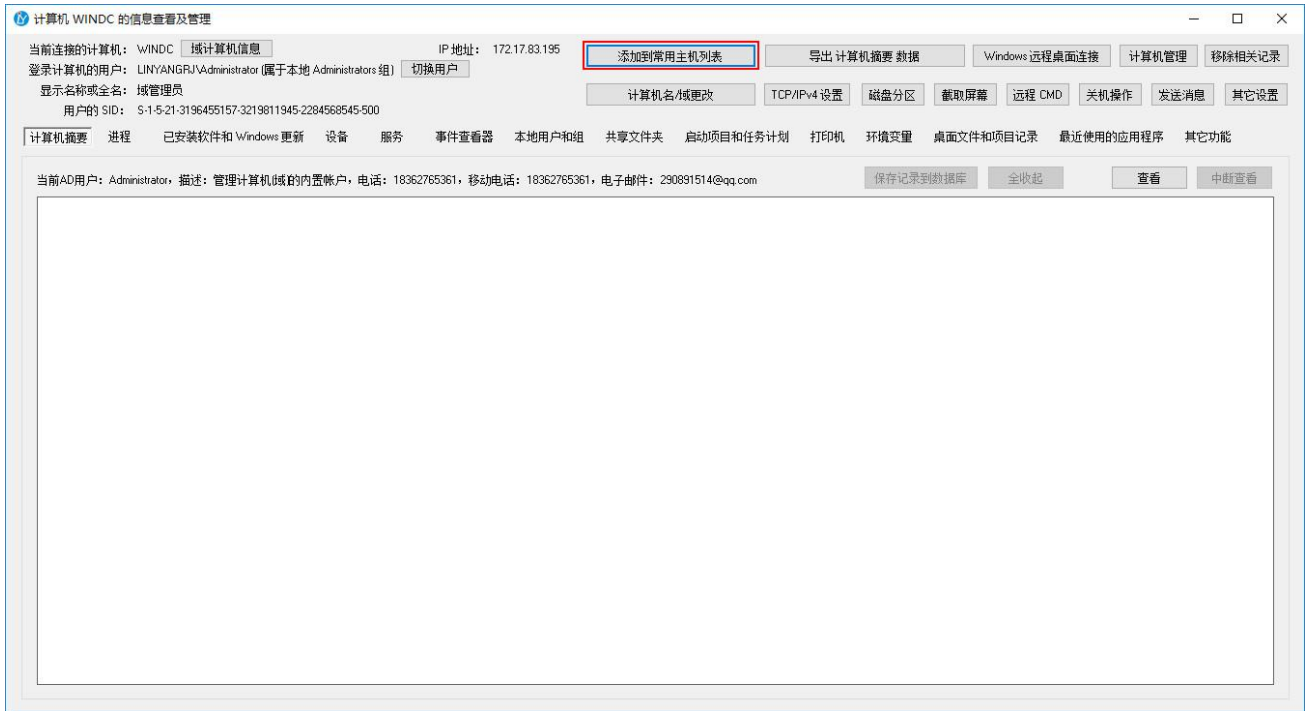
备注: -

从 Excel 导入 确定 关闭

说明：如有多条记录需添加，我们可以单击“上一个”或“下一个”按钮，软件会自动显示出对对应行相关信息，再直接单击“确定”按钮即可。

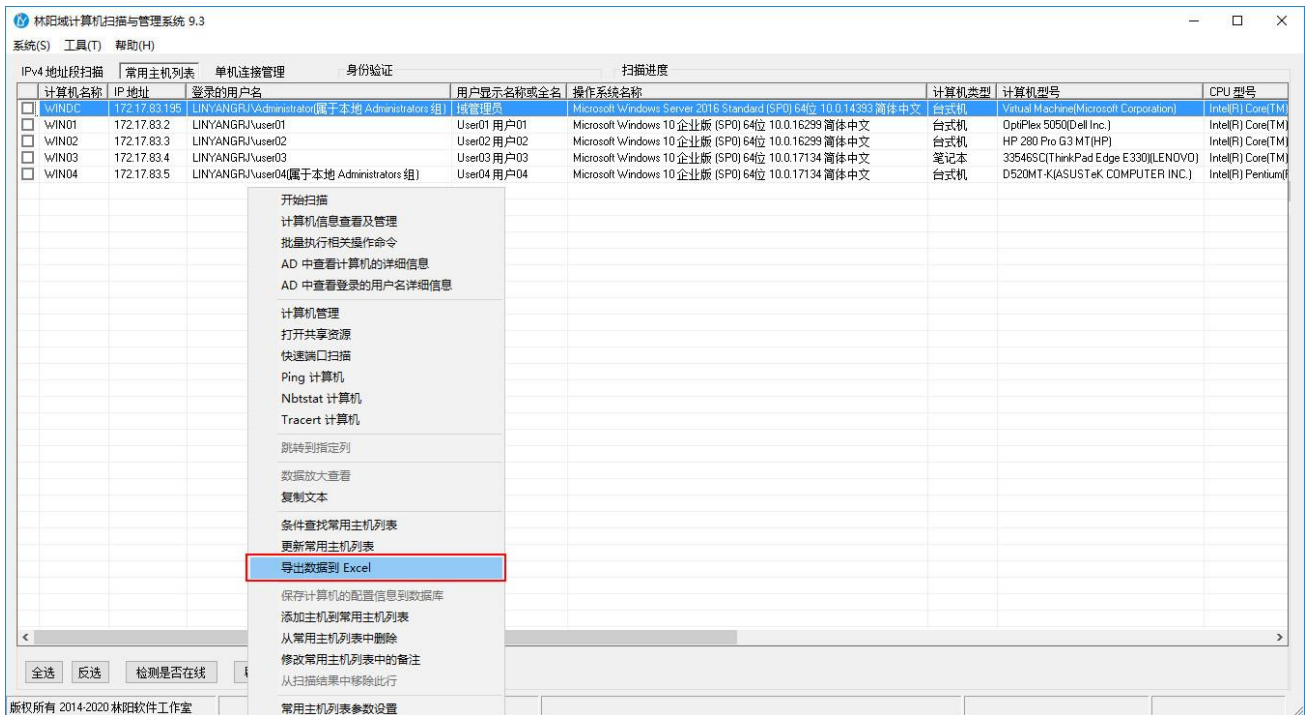
5.8.2、通过计算机信息查看及管理进行添加

在计算机信息查看及管理窗体上单击“添加到常用主机扫描列表”按钮，如下图所示：



5.8.3、通过 EXCEL 批量导入主机

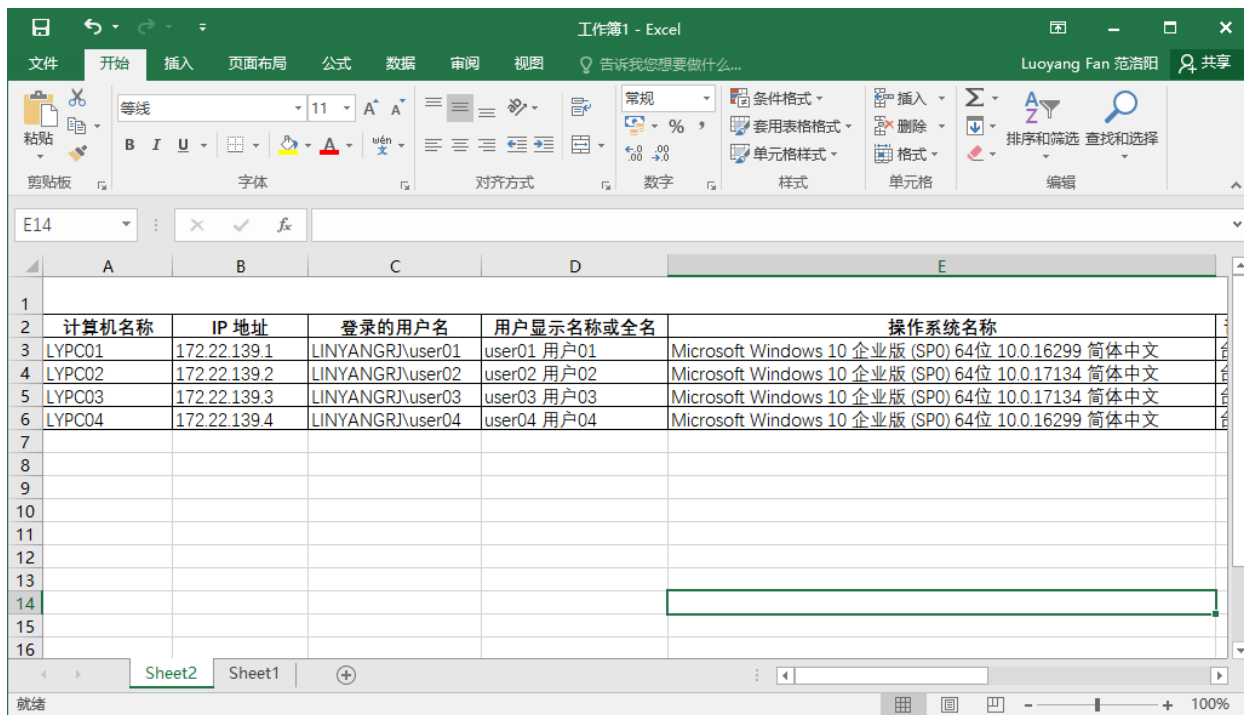
1、打开软件，单击“常用主机扫描”选项卡，在常用主机扫描列表上先单击右键“导出数据到 Excel”菜单，如下图所示：



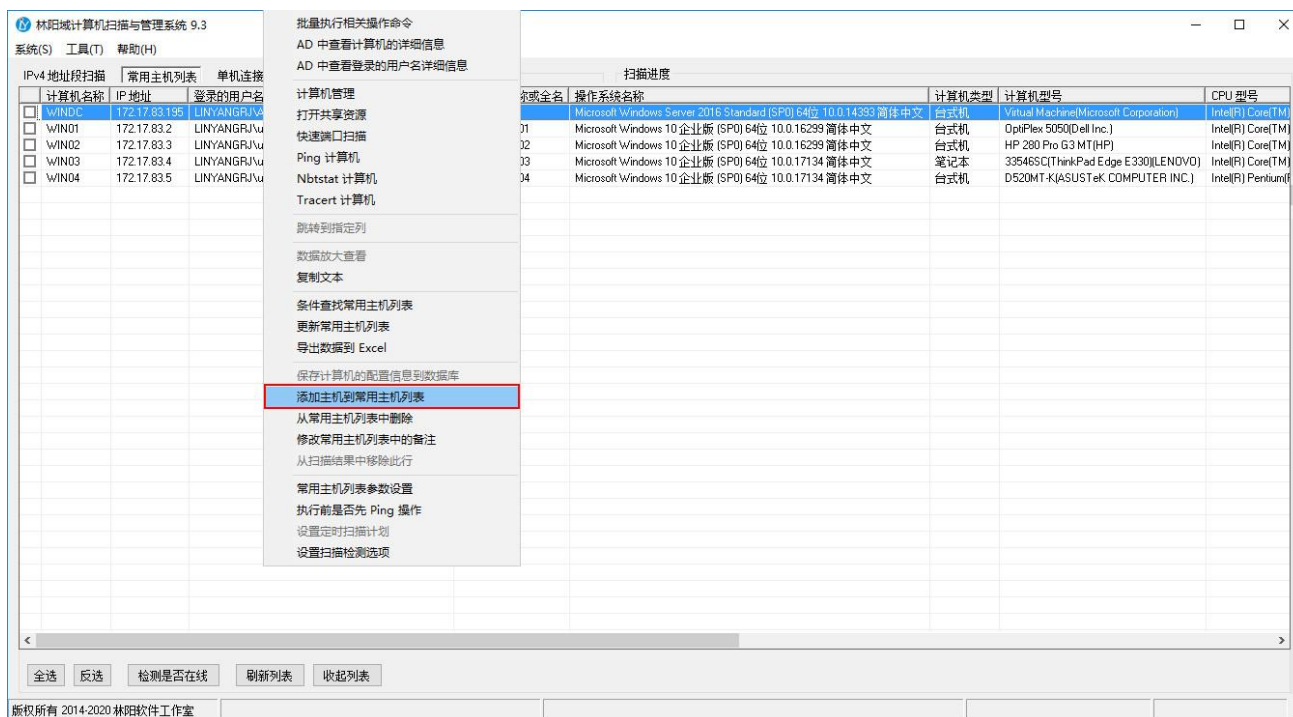
说明：为什么是先要导出呢，主要是为了先导出指定的 Excel 格式，这样方便我们在这个格式中添加自

已导入的数据即可。

2、完成导出操作后，大家根据导出的 Excel 格式把要添加的新数据按现有的格式输入完成，再保存 Excel 文件，如下图所示：



3、在“常用主机列表”上再单击右键“添加主机到常用主机扫描列表”菜单，如下图所示：

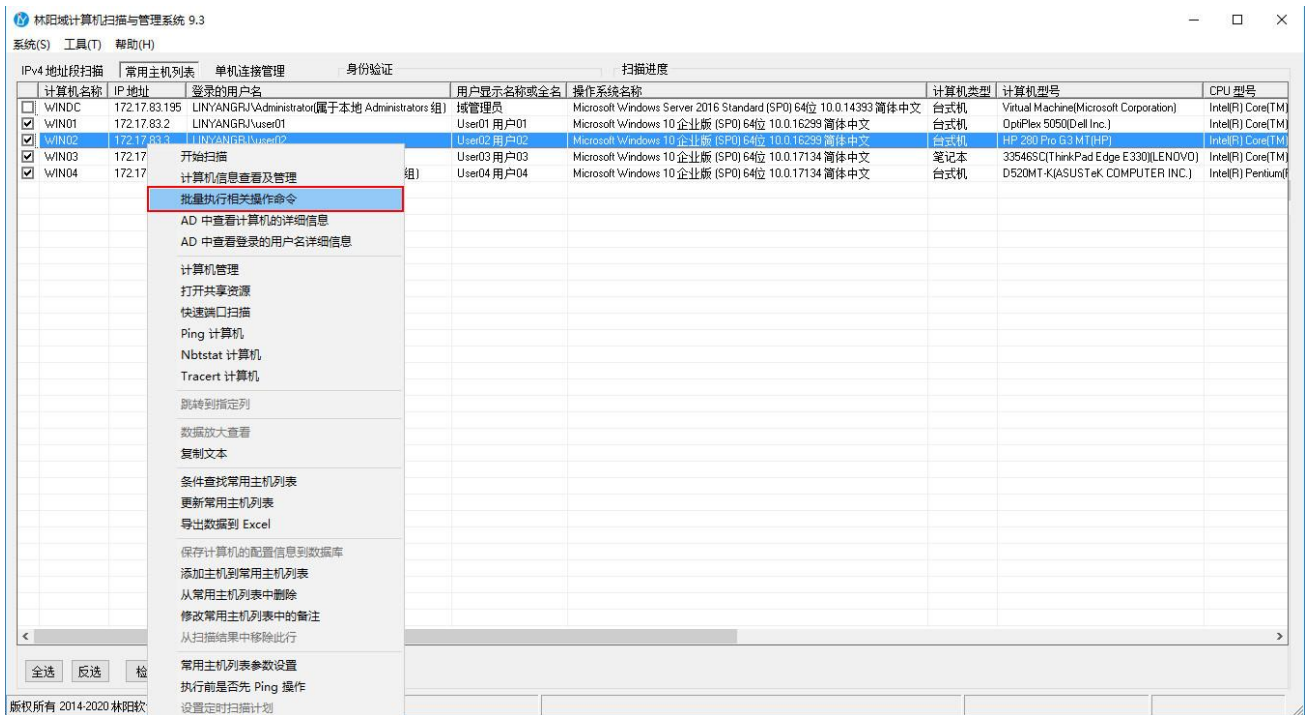


4、选择我们要导入的 Excel 文件即可完成导入操作。

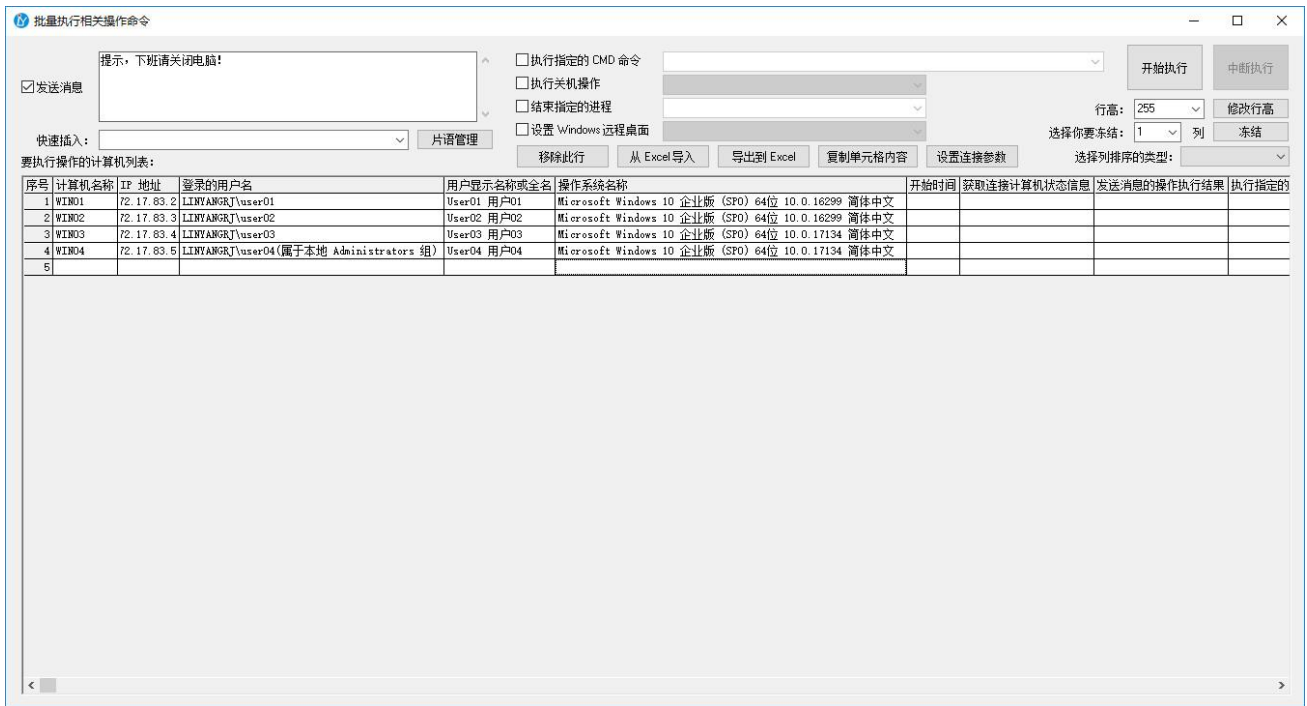
5.9、批量执行相关操作命令

批量在指定的一些计算机上同时执行一个或多个命令。

1、打开软件，单击“常用主机列表”选项卡，先勾选你要执行批量操作的计算机列表，再单击右键“批量执行相关操作命令”菜单，如下图所示：

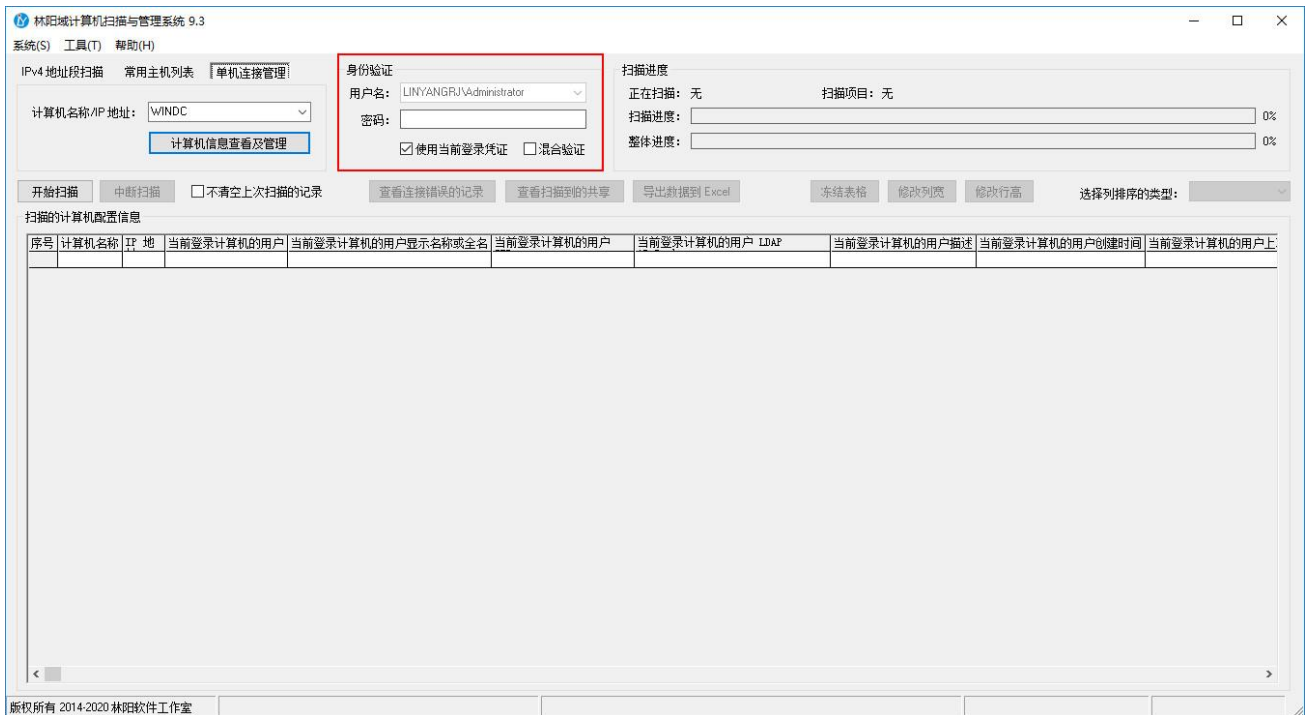


2、在批量执行相关操作命令的窗体上方勾选你要执行的操作，可以勾选多个选项，勾选设置完成后单击“开始执行”按钮即可，如下图所示：



说明：大家也可以在“扫描的计算机配置信息”上分别选中指定的计算机记录，再多次单击右键“批量执行相关操作命令”菜单，添加这些计算机列表到批量执行相关操作命令的“要执行操作的计算机列表”中。

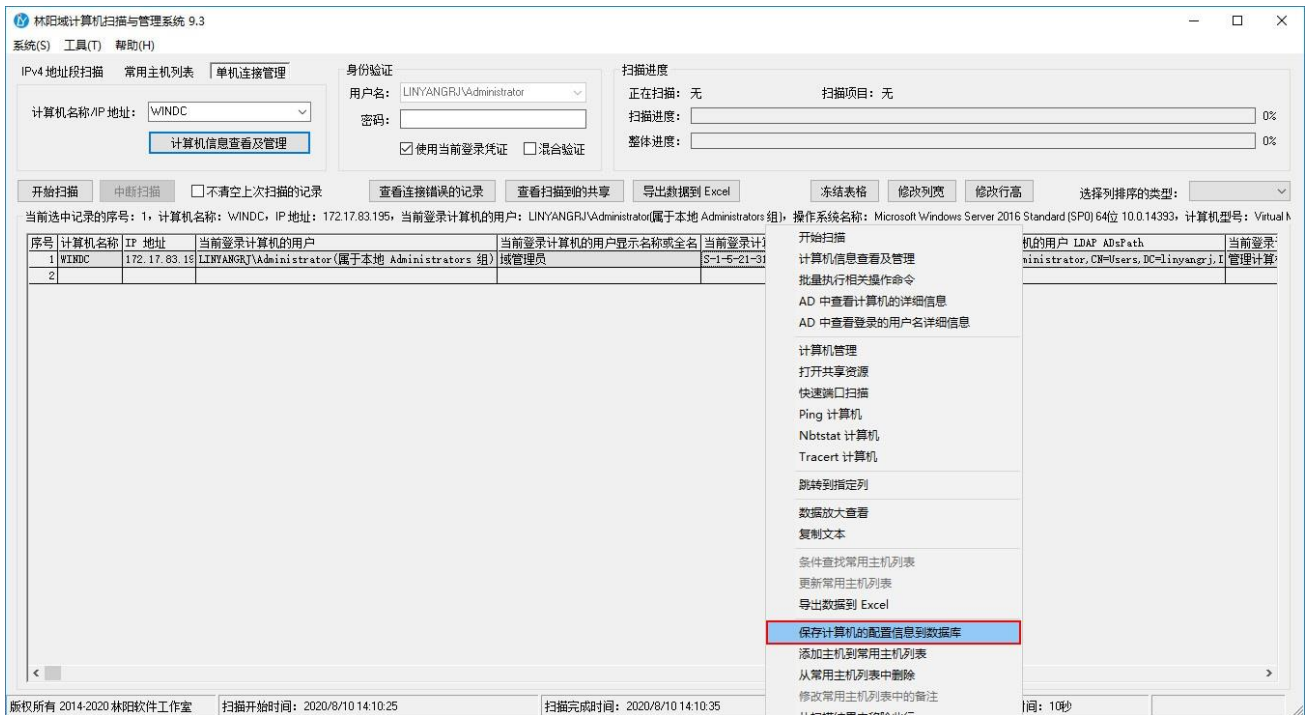
说明：批量执行相关操作的命令的身份验证也是来自主窗体上的身份验证设置，如下图所示：



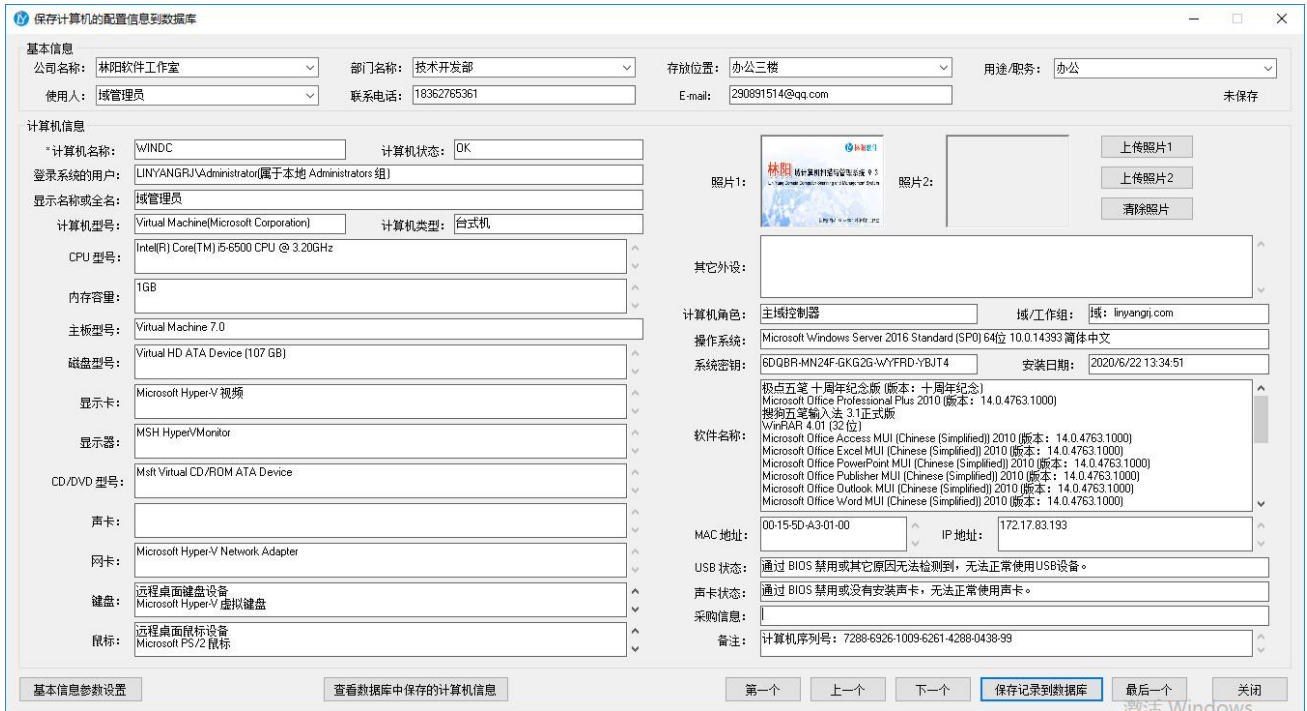
5.10、保存计算机配置信息到数据库

5.10.1、通过扫描的计算机配置信息

1、在“扫描的计算机配置信息”列表中选中指定的行，双击左键或单击右键“保存计算机的配置信息到数据库”菜单，如下图所示：



2、我们只需输入基本信息，如公司名称、部门名称、存放位置等，其它信息基本都是自己带出来的，除了计算机名称不能更改（前面带*符号），其它信息均可进行修改，如下图所示：



3、确认无误后，单击“保存记录到数据库”按钮，这样就完成了保存操作，如下图所示：

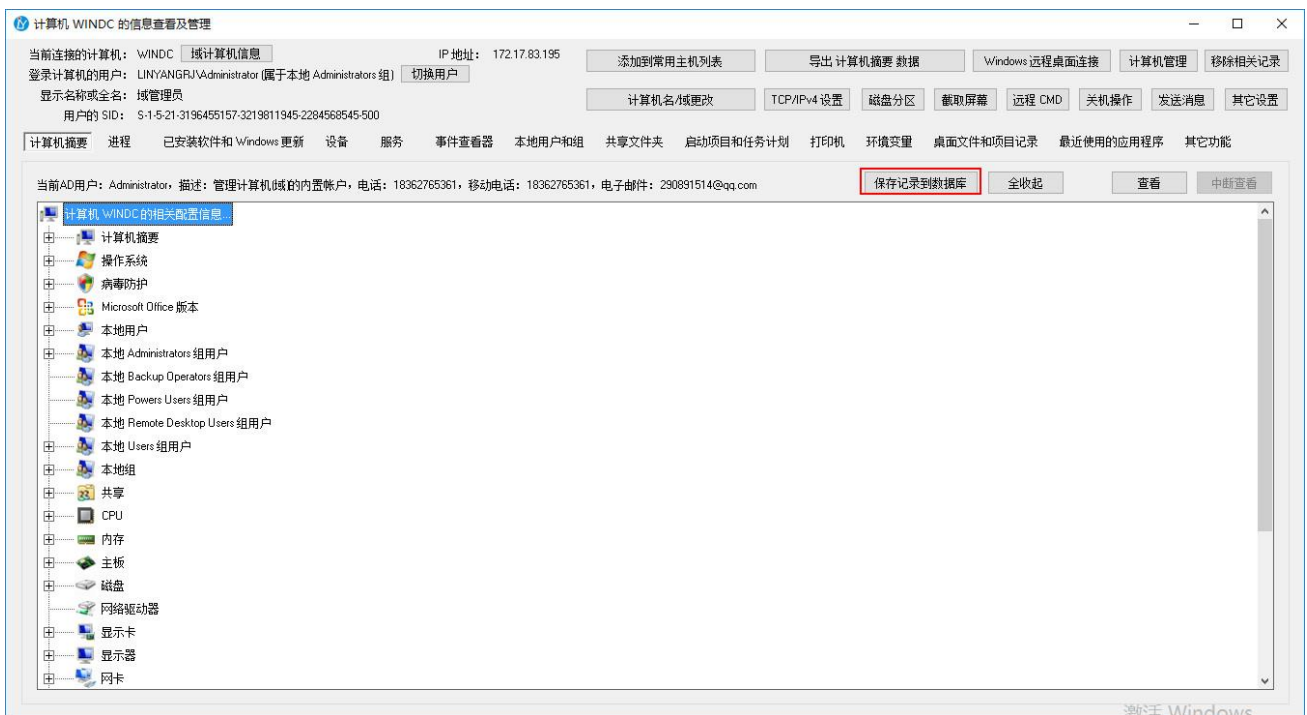


5.10.2、通过计算机信息查看及管理

1、在计算机信息查看及管理窗体上选择“计算机摘要”选项卡，先单击“查看”按钮，如下图所示：



2、等检测结束后再单击“保存记录到数据库”按钮，如下图所示：



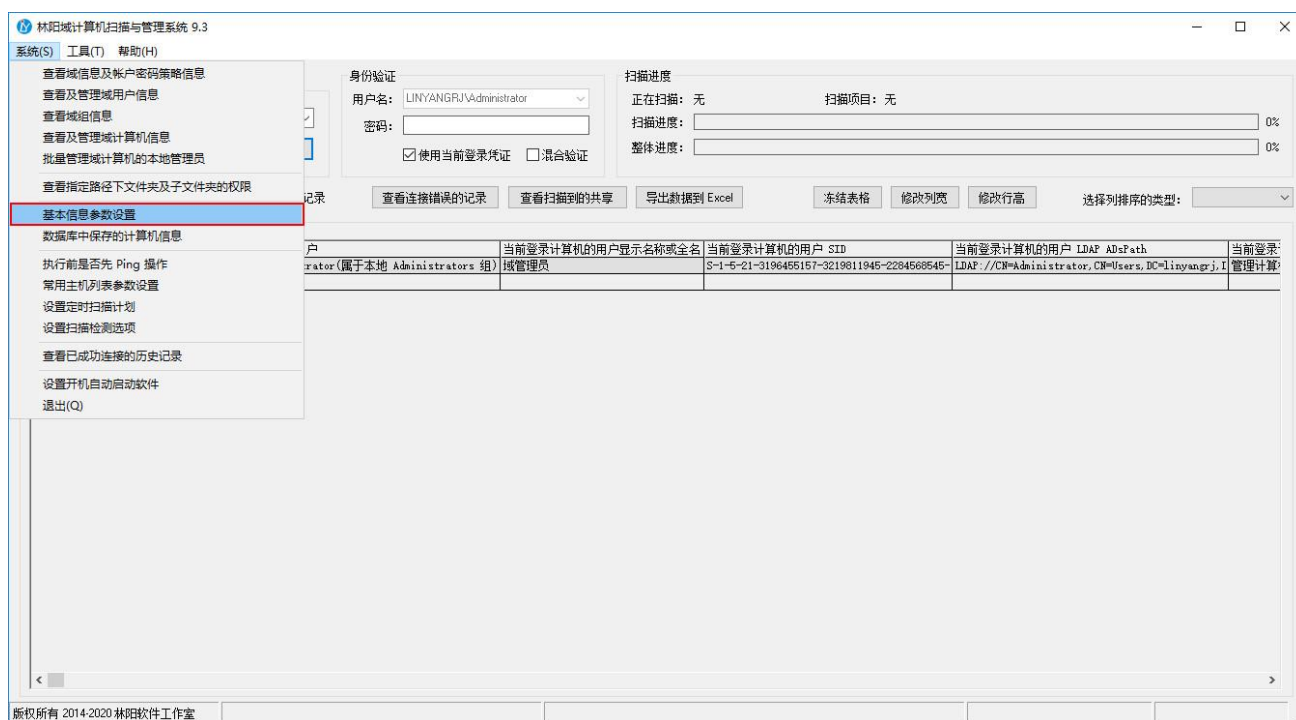
3、只需输入基本信息，如公司名称、部门名称、存放位置等，其它信息是自动带出来的，除了计算机名称不能更改，其它信息均可进行修改，确认无误后，单击“保存记录到数据库”按钮即可完成保存操作。

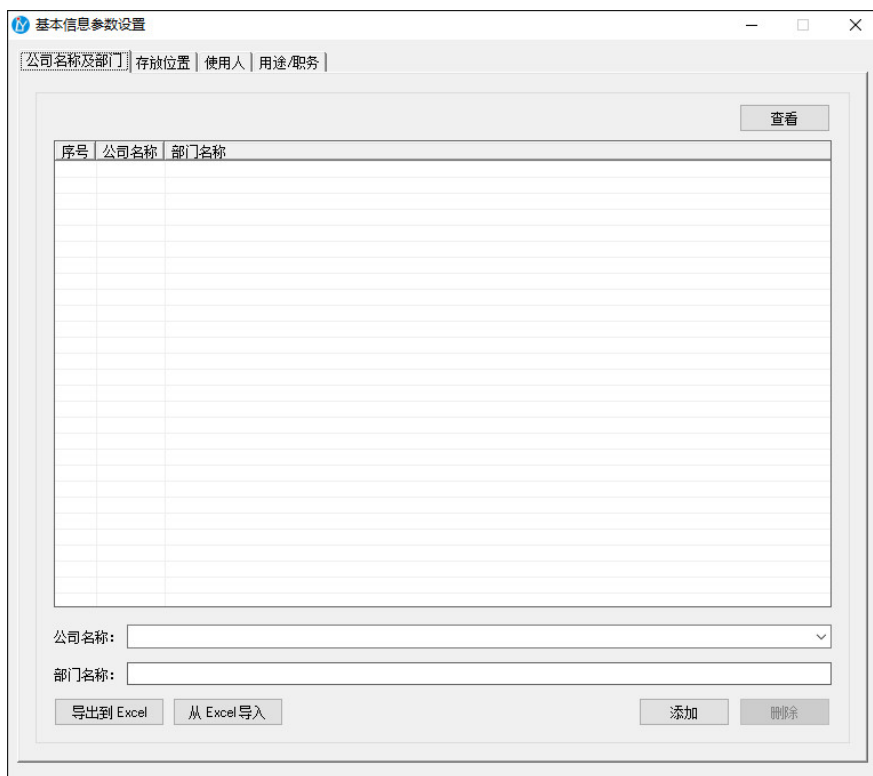
5.10.3、保存计算机配置信息的基本信息参数设置

在保存计算机配置信息到数据库后，基本信息的相关数据如公司名称及部门、存放位置、使用人、用途/职位信息也会保存到“基本信息参数设置”中对应的列表中。

用户也可以提前将这个基本信息添加到数据库中，方便以后在保存计算机配置信息到数据库时基本信息时就可以直接从下拉框中进行选择。

打开软件，单击“系统—基本信息参数设置”菜单，如下图所示：

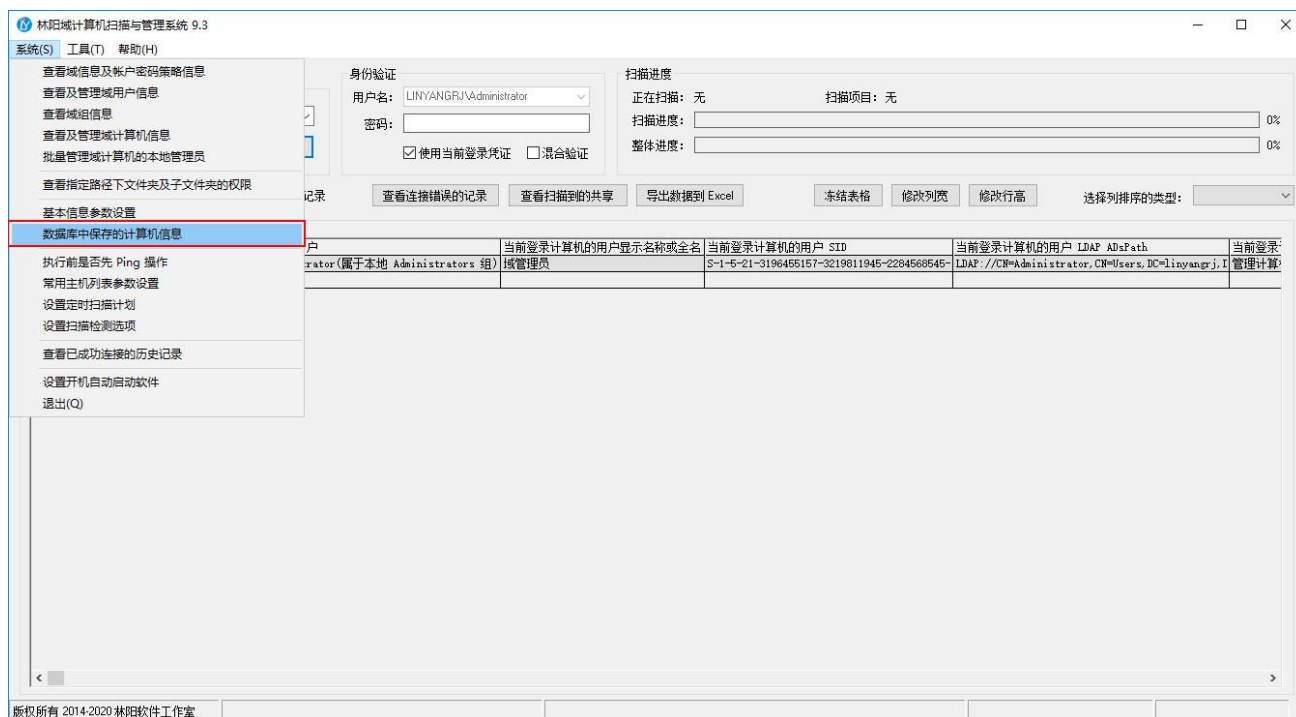




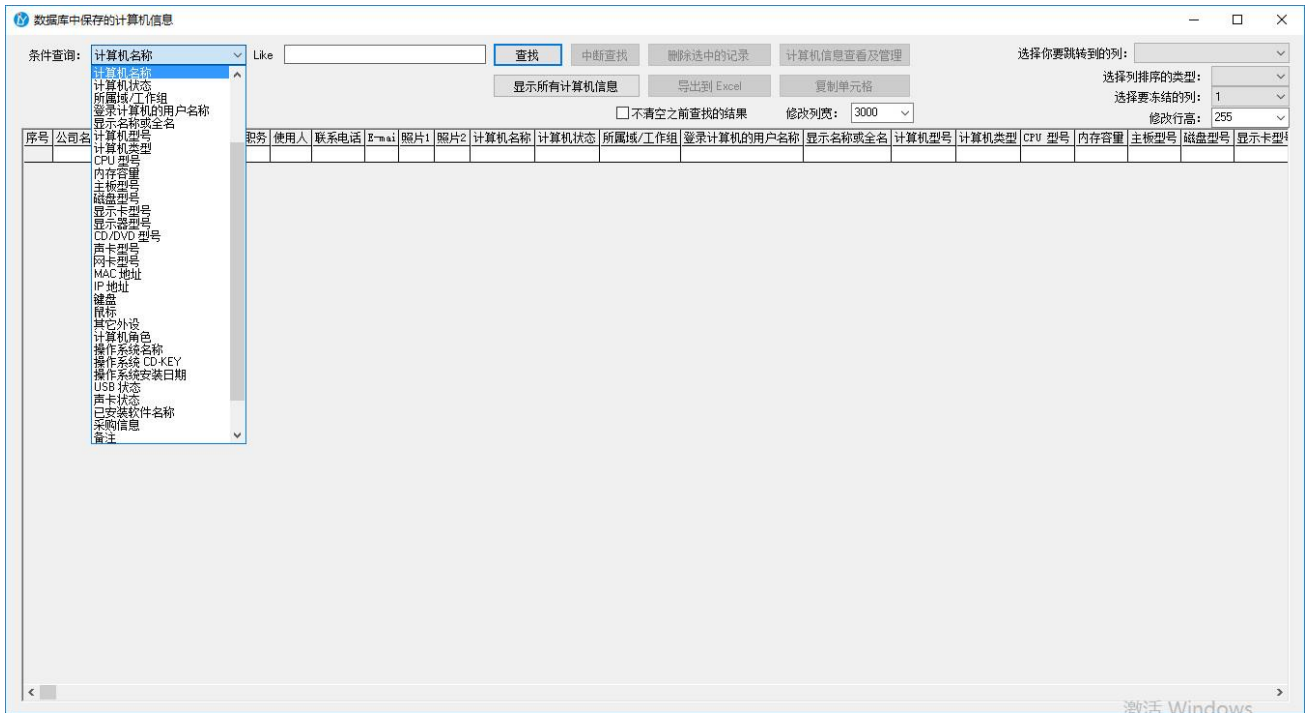
说明：基本信息参数设置里的数据删除或修改操作不会影响到数据库中已保存的计算机配置信息的相关数据。

5.11、查看及管理数据库中保存的计算机配置信息

1、打开软件，单击菜单“系统—数据库中保存的计算机信息”，如下图所示：

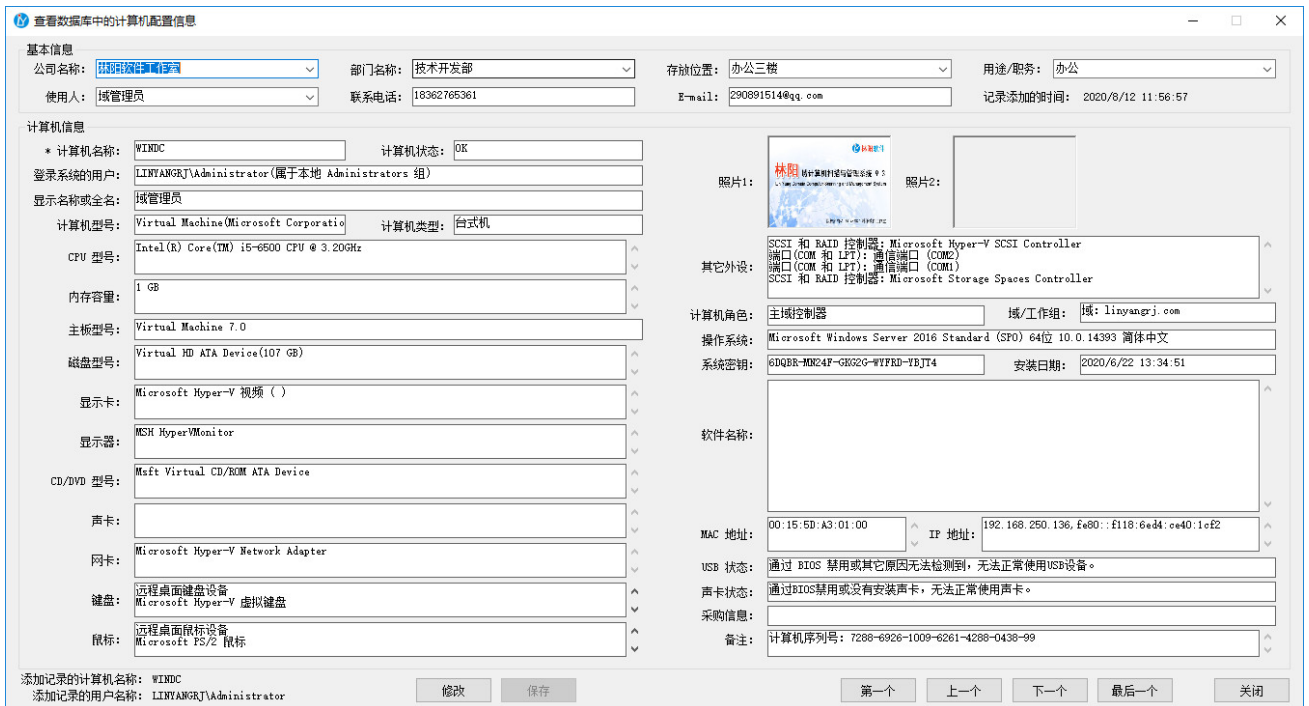


2、你可以根据输入的条件对指定的计算机进行查找，也可以直接单击“查找”按钮显示数据库中所有的记录，如下图所示：



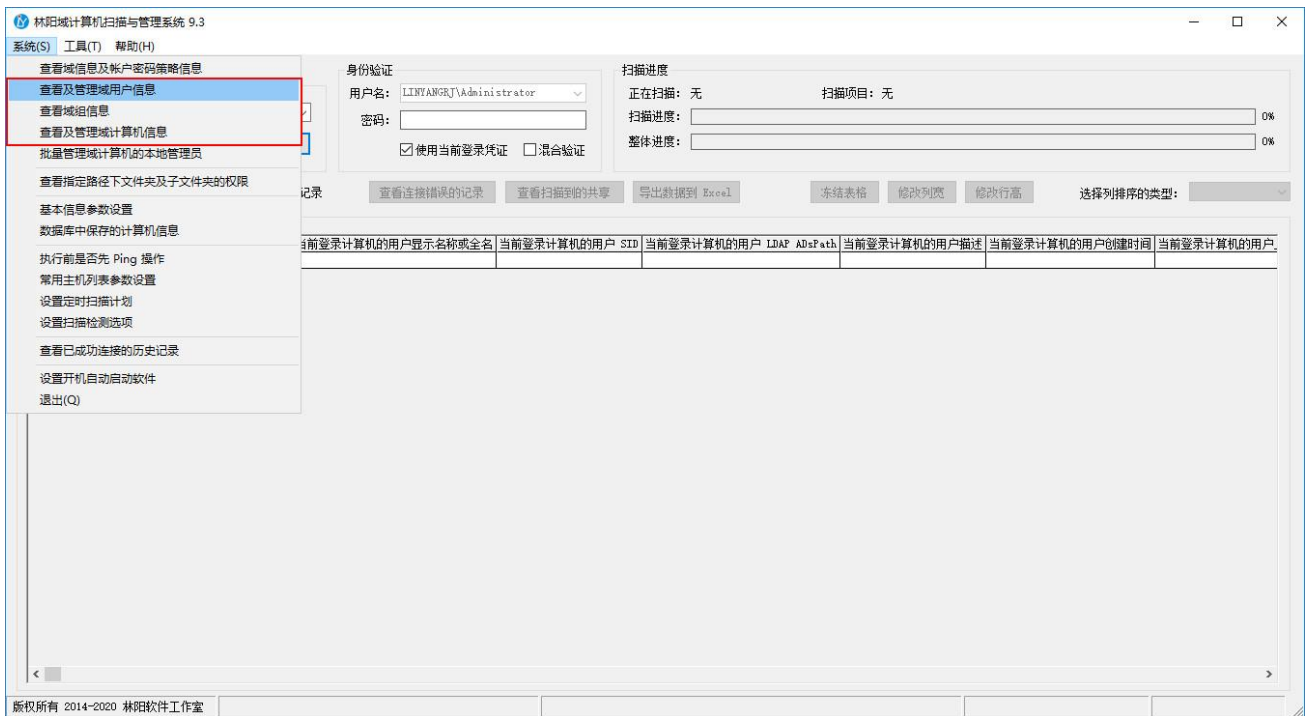
说明：列表中照片 1、照片 2 列显示的内容是乱码，这个属于正常情况，因为图片是以二进制流的方式存放在数据库的对应字段中，如显示内容为空那就是没有照片。

3、当我们需要查看或修改指定计算机信息时，双击指定的计算机列表，就可查看或修改指定计算机的相关信息。



5.12、AD 域对象的操作

主要是对域用户、域组、域计算机对象的属性批量查看或管理操作，大家可以单击下图红色方框中的菜单进行相关操作，如下图所示：



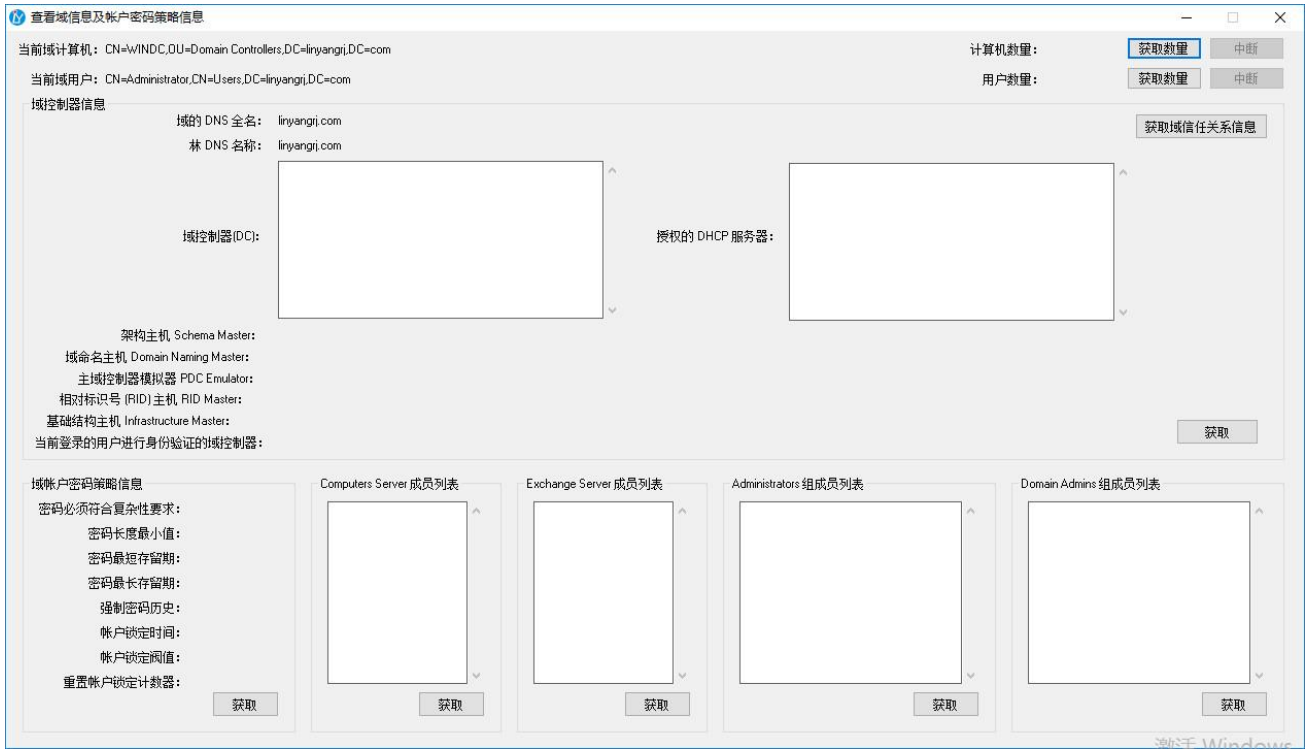
说明：有“选择文件”的操作，它是来自.txt 格式的文件，文件内容大家请按以下格式输入内容，一条记录占一行，如下图所示：



可以按指定 OU 进行查询，如果不知道指定 OU 怎么写，先查找一条记录，点击这个记录，就会自动显示当前选中对象所在的 OU，当然也可以在这个 OU 的基础上进行修改。

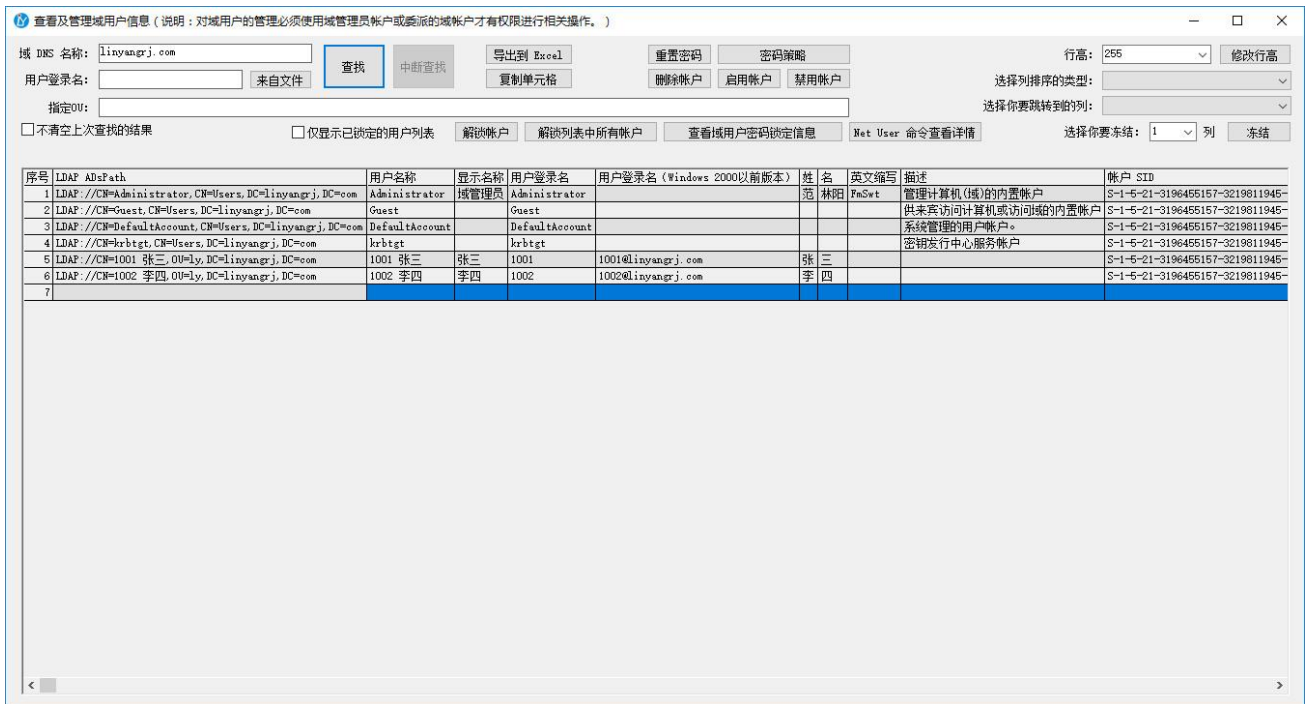
5.12.1、查看域信息及帐户密码策略信息

打开软件，单击“系统—查看域信息及帐户密码策略信息”菜单，单击“获取”按钮即可，如下图所示：

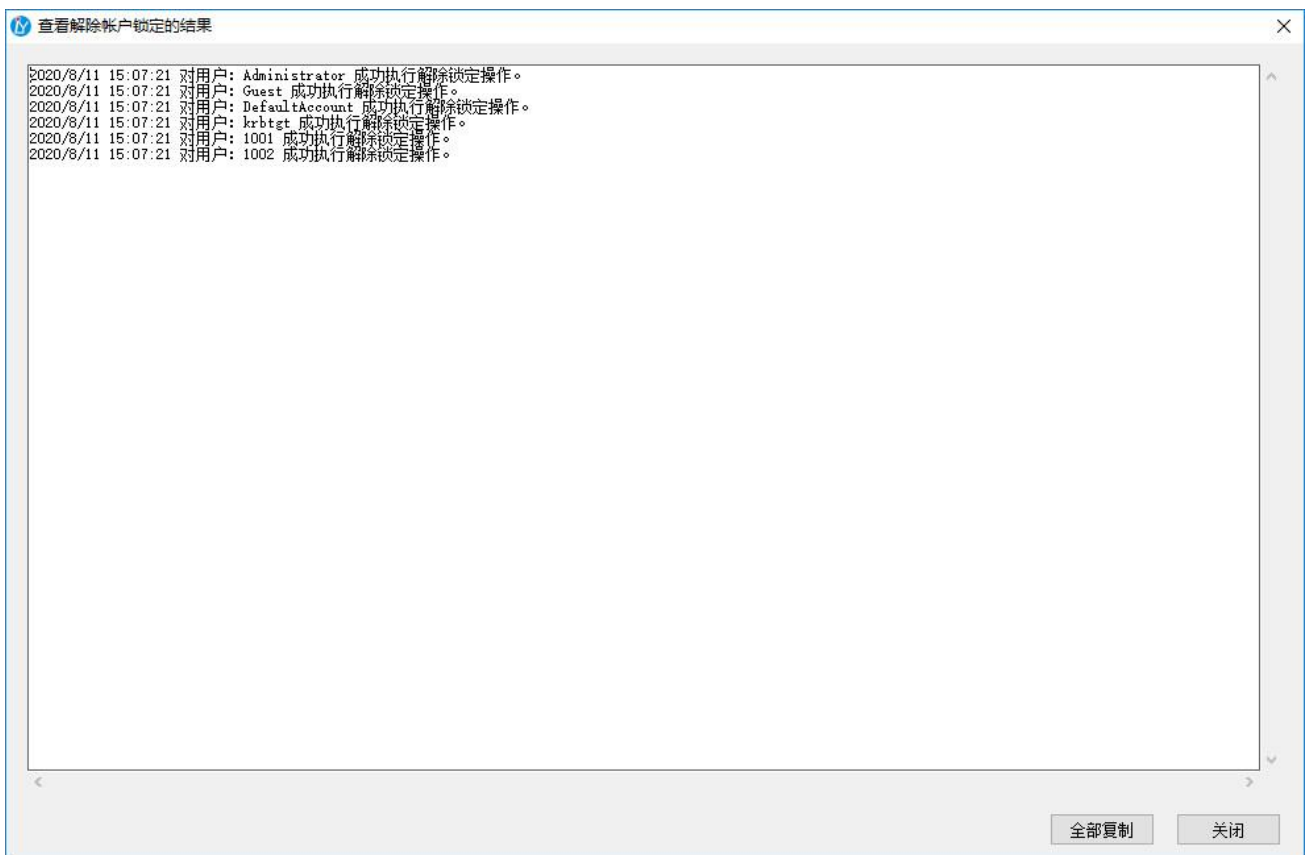


5.12.2、查看及管理域用户信息

你可以根据条件输入指定用户名、指定 OU 进行查找，也可以直接单击“查找”按钮显示域中所有域用户的信息，如下图所示：

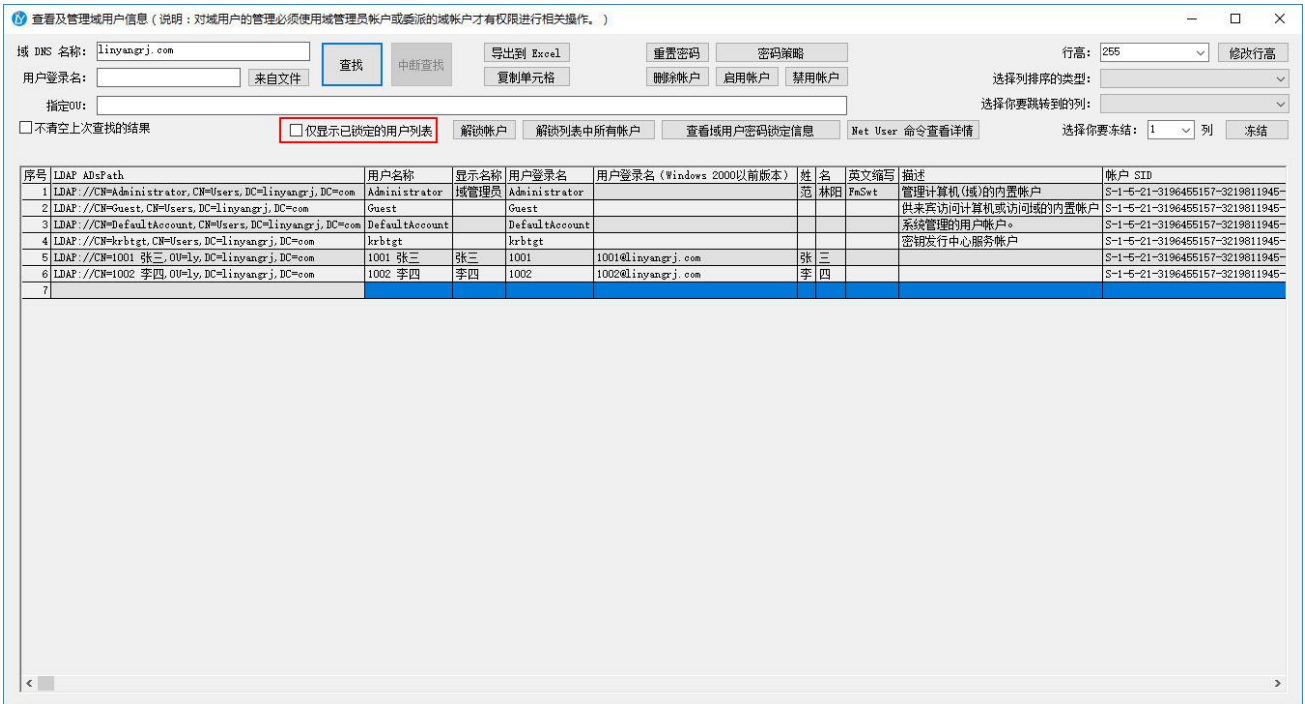


说明：解锁列表中所有帐户主要用于当设置了帐户锁定阈值不为 0 时，有部分域帐户因电脑病毒或密码输入错误等原因造成帐户的锁定无法登录，这时我们可以通过此操作对列表中的域用户进行批量解锁操作，解除锁定的结果如下图所示：



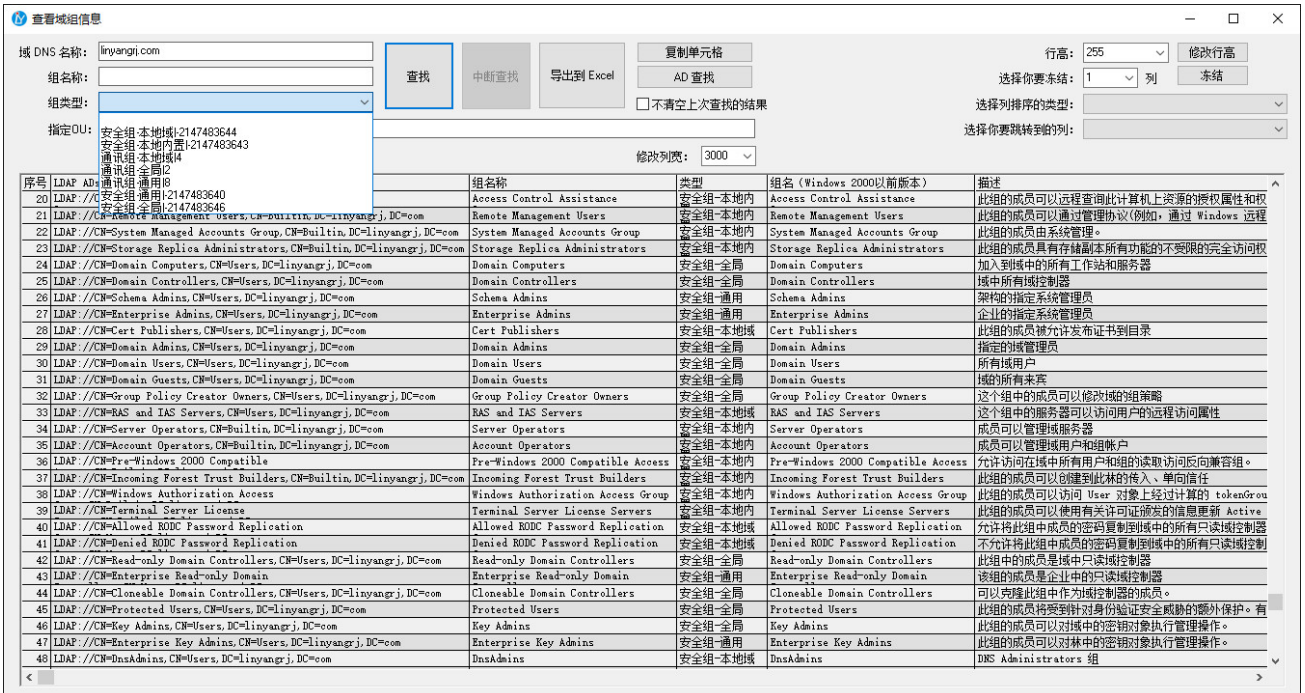
说明：即使用户的域帐户没有被锁定，执行了解锁操作也不会有任何影响的。

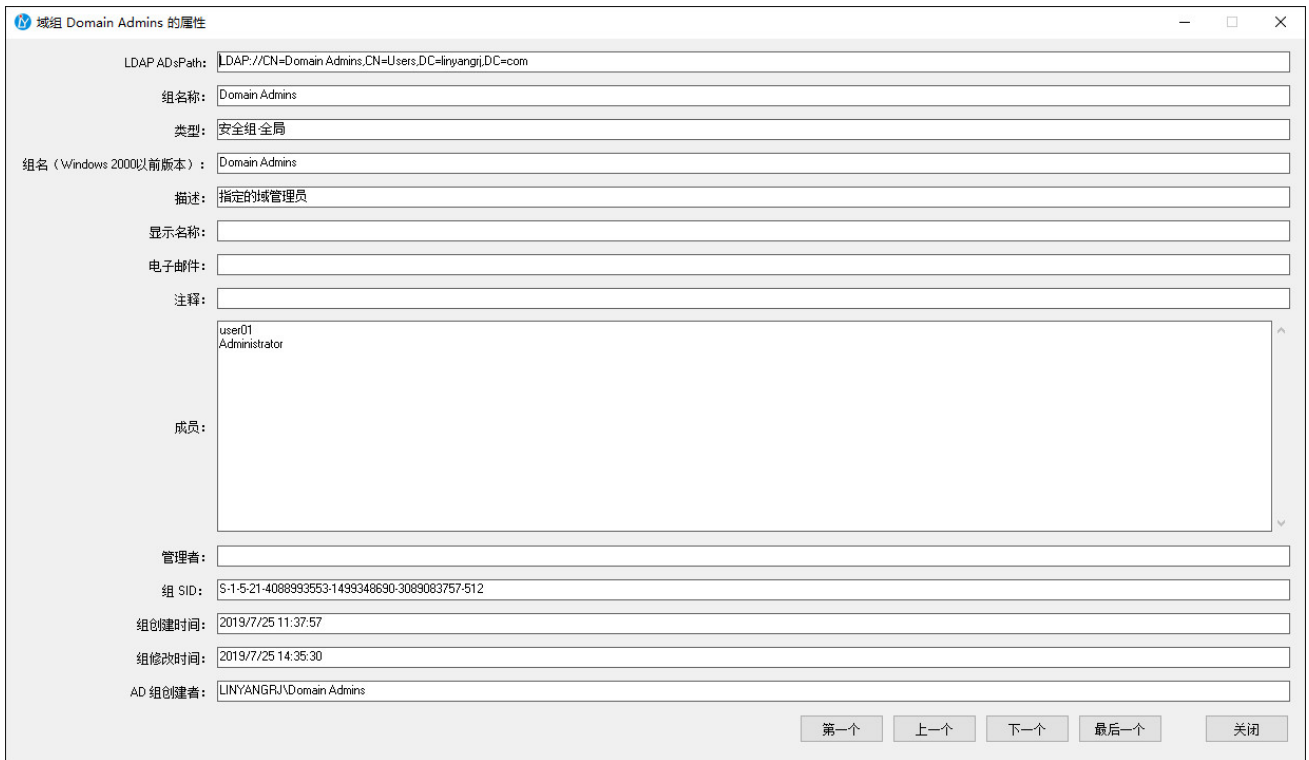
当然也可以先勾选“仅显示已锁定的用户列表”，再执行解锁列表中所有帐户。



5.12.3、查看域组信息

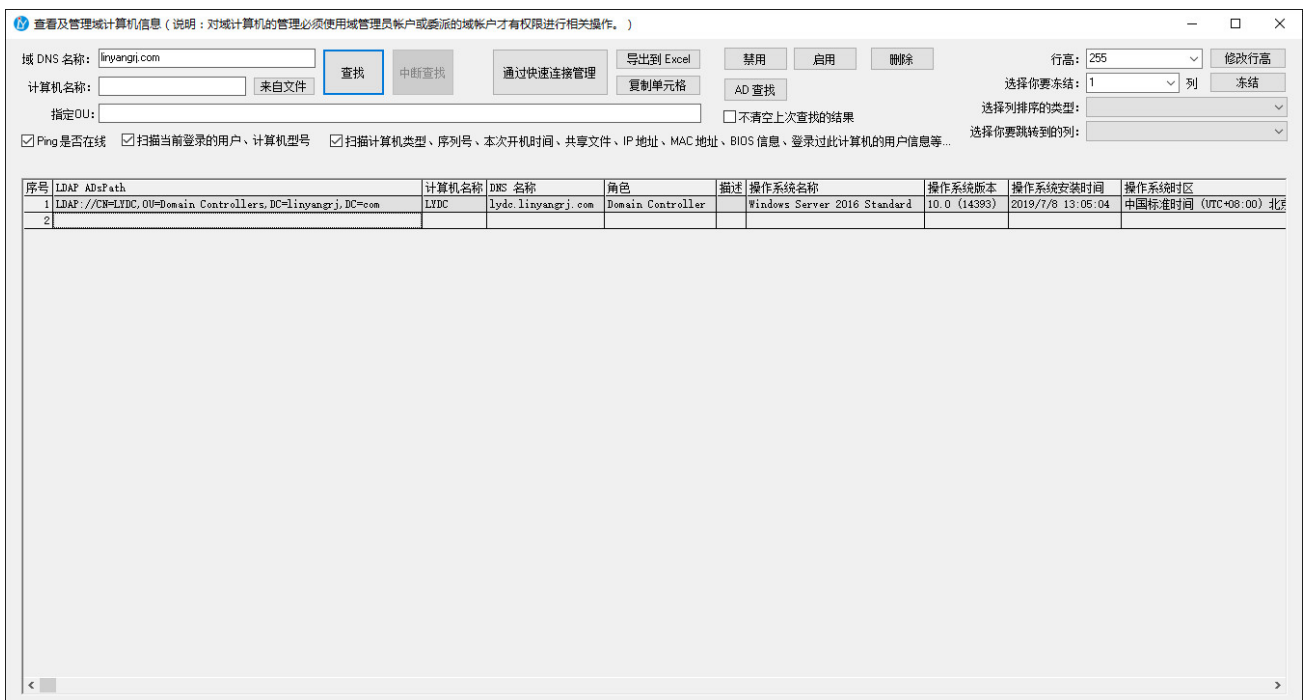
你可以根据条件输入指定组名称、组类型或指定 OU 进行查找，也可以直接单击“查找”按钮显示域中所有组的信息，如下图所示：





5.12.4、查看及管理域计算机信息

你可以根据条件输入指定计算机名称、指定 OU 进行查找，也可以直接单击“查找”按钮显示域中所有计算机的信息，如下图所示：





5.12.5、批量管理域计算机的本地管理员

1、先准备好批量管理的域计算机列表，我们可以根据条件输入指定的计算机名或 OU 地址在域计算机中进行查找，也可以直接单击“查找”按钮显示域内所有计算机的信息，这里直接点击“导入数据来自常用主机扫描列表”，如下图所示：



2、我们在执行批量操作时，需要双击左键先勾选你要执行的计算机列表，再根据自己的需求勾选及设

置要执行的操作，一次可以勾选多个选项，确认无误后，再单击“执行”按钮即可，如下图所示：



5.13、查看指定路径下文件夹及子文件夹的权限

主要用于查看共享文件服务器上的共享文件的权限，建议在文件服务器上运行此软件，如在非文件服务器上运行须先把共享文件在本地计算机映射为网络驱动器，再对网络驱动器进行操作。

打开软件，单击“系统—查看指定路径下文件夹及子文件夹的权限”菜单，输入要查找的指定文件夹路径如“D:\share file”，再单击“查看”按钮，如下图所示：

查看指定路径下文件夹及子文件夹的权限 (说明: 用于查找计算机上的共享文件夹权限, 其它计算机上的共享文件可以先在本地映射为网络驱动器。)

指定的文件夹路径: D:\share file 浏览文件 查看 导出到 Excel 查看指定路径下文件夹或文件 行高: 255 修改行高

目录深度: 1 层 获取文件大小 获取域组成员/显示名称 移除此行 复制文本 选择排序的类型:

序号	文件夹路径	创建日期	最后一次修改日期	大小	压缩	加密	隐藏	组或用户	域组成员/显示名称	组或用户的权限	组或用户的 SID	所有者	分类
1	D:\share file	2023/11/27 15:47:22	2023/11/27 16:24:34		False	False	False	CREATOR OWNER		允许完全控制	S-1-3-0	Administrators	
2	D:\share file	2023/11/27 15:47:22	2023/11/27 16:24:34		False	False	False	NT AUTHORITY\SYSTEM		允许完全控制	S-1-5-18	Administrators	
3	D:\share file	2023/11/27 15:47:22	2023/11/27 16:24:34		False	False	False	LIYANG\linyngj	Lin Yang 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1103	Administrators	
4	D:\share file	2023/11/27 15:47:22	2023/11/27 16:24:34		False	False	False	LIYANG\linyngj01	LinYang-01 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1108	Administrators	
5	D:\share file	2023/11/27 15:47:22	2023/11/27 16:24:34		False	False	False	LIYANG\LinYang_All	LinYang-03 林阳软件	读取	S-1-5-21-2649014967-615678022-511609766-1112	Administrators	
6	D:\share file	2023/11/27 15:47:22	2023/11/27 16:24:34		False	False	False	BUILTIN\Administrators		允许完全控制	S-1-5-32-544	Administrators	
7	D:\share file	2023/11/27 15:47:22	2023/11/27 16:24:34		False	False	False	LIYANG\linyngj03	LinYang-03 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1110	Administrators	
8	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	BUILTIN\Administrators		允许完全控制	S-1-5-32-544	Administrators	
9	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	CREATOR OWNER		允许完全控制	S-1-3-0	Administrators	
10	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	NT AUTHORITY\SYSTEM		允许完全控制	S-1-5-18	Administrators	
11	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	LIYANG\linyngj	Lin Yang 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1103	Administrators	
12	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	LIYANG\linyngj01	LinYang-01 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1108	Administrators	
13	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	LIYANG\LinYang_All	LinYang-03 林阳软件	读取	S-1-5-21-2649014967-615678022-511609766-1112	Administrators	
14	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	BUILTIN\Administrators		允许完全控制	S-1-5-32-544	Administrators	
15	D:\share file\abc	2023/11/27 15:51:30	2023/11/27 16:26:14		False	False	False	LIYANG\linyngj03	LinYang-03 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1110	Administrators	
16	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	LIYANG\linyngj03	LinYang-03 林阳软件	允许完全控制	S-1-5-21-2649014967-615678022-511609766-1110	linyngj03	
17	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	CREATOR OWNER	LinYang-03 林阳软件	允许完全控制	S-1-3-0	linyngj03	
18	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	NT AUTHORITY\SYSTEM	LinYang-03 林阳软件	允许完全控制	S-1-5-18	linyngj03	
19	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	LIYANG\linyngj	Lin Yang 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1103	linyngj03	
20	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	LIYANG\linyngj01	LinYang-01 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1108	linyngj03	
21	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	LIYANG\LinYang_All	LinYang-03 林阳软件	读取	S-1-5-21-2649014967-615678022-511609766-1112	linyngj03	
22	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	BUILTIN\Administrators		允许完全控制	S-1-5-32-544	linyngj03	
23	D:\share file\lwo	2023/11/27 16:21:59	2023/11/27 16:26:52		False	False	False	LIYANG\linyngj03	LinYang-03 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1110	linyngj03	
24	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	BUILTIN\Administrators		允许完全控制	S-1-5-32-544	Administrators	
25	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	CREATOR OWNER		允许完全控制	S-1-3-0	Administrators	
26	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	NT AUTHORITY\SYSTEM		允许完全控制	S-1-5-18	Administrators	
27	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	LIYANG\linyngj	Lin Yang 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1103	Administrators	
28	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	LIYANG\linyngj01	LinYang-01 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1108	Administrators	
29	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	LIYANG\LinYang_All	LinYang-03 林阳软件	读取	S-1-5-21-2649014967-615678022-511609766-1112	Administrators	
30	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	BUILTIN\Administrators		允许完全控制	S-1-5-32-544	Administrators	
31	D:\share file\软件	2023/11/27 16:24:20	2023/11/27 16:24:34		False	False	False	LIYANG\linyngj03	LinYang-03 林阳软件	读取/修改	S-1-5-21-2649014967-615678022-511609766-1110	Administrators	

说明: 大家可以通过对组或用户名列进行排序, 这样就可以直观查看哪些用户拥有哪些文件的权限。

5.14、查看已成功连接的历史记录

打开软件, 单击“系统—查看已成功连接的历史记录”菜单, 如下图所示:

林阳域计算机扫描与管理系统 9.3

系统(S) 工具(T) 帮助(H)

- 查看域信息及帐户密码策略信息
- 查看及管理域用户信息
- 查看域组信息
- 查看及管理域计算机信息
- 批量管理域计算机的本地管理员
- 查看指定路径下文件夹及子文件夹的权限
- 基本信息参数设置
- 数据库中保存的计算机信息
- 执行前是否先 Ping 操作
- 常用主机列表参数设置
- 设置定时扫描计划
- 设置扫描检测选项
- 查看已成功连接的历史记录**
- 设置开机自动启动软件
- 退出(Q)

身份验证: 用户名: LINYANGRJ\Administrator 密码: 使用当前登录凭证 混合验证

扫描进度: 正在扫描: 无 扫描项目: 无
扫描进度: 0%
整体进度: 0%

记录: 选择排序的类型:

用户	当前登录计算机的用户显示名称或全名	当前登录计算机的用户 SID	当前登录计算机的用户 LDAP Adspath	当前登录计算机的用户管理计划
Administrator (属于本地 Administrators 组)	域管理员	S-1-5-21-319645517-3219811945-2284568645-	LDAP://CN=Administrator,CN=Users,DC=linyngj,I	

版权所有 2014-2020 林阳软件工作室

大家可以根据条件输入指定的计算机名称/IP 地址进行查找, 也可以直接单击“查找”按钮显示所有已成功连接的历史记录, 如下图所示:

序号	日期	时间	被连接的计算机	连接类型	身份验证	执行连接的用户	执行连接的计算机	备注
1	2020/8/10	14:14:35	WINDC	计算机信息查看及管理	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
2	2020/8/10	14:10:25	WINDC	开始扫描	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
3	2020/8/10	13:40:31	WINDC	开始扫描	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
4	2020/8/10	13:37:02	WINDC	开始扫描	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
5	2020/8/10	11:55:41	WINDC	计算机信息查看及管理	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
6	2020/8/10	11:48:22	WINDC	开始扫描	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
7	2020/8/10	11:43:09	WINDC	计算机信息查看及管理	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
8	2020/8/10	11:42:26	WINDC	计算机信息查看及管理	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
9	2020/8/10	11:41:09	WINDC	计算机信息查看及管理	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
10	2020/8/10	11:25:01	WINDC	计算机信息查看及管理	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC
11	2020/8/10	11:10:51	WINDC	开始扫描	LINYANGRJ\Administrator(使用当前登录凭证)	LINYANGRJ\Administrator	WINDC	WINDC

说明：建议当历史记录数据量比较大时，删除历史记录可以提高软件的运行速度。

六、常见问题

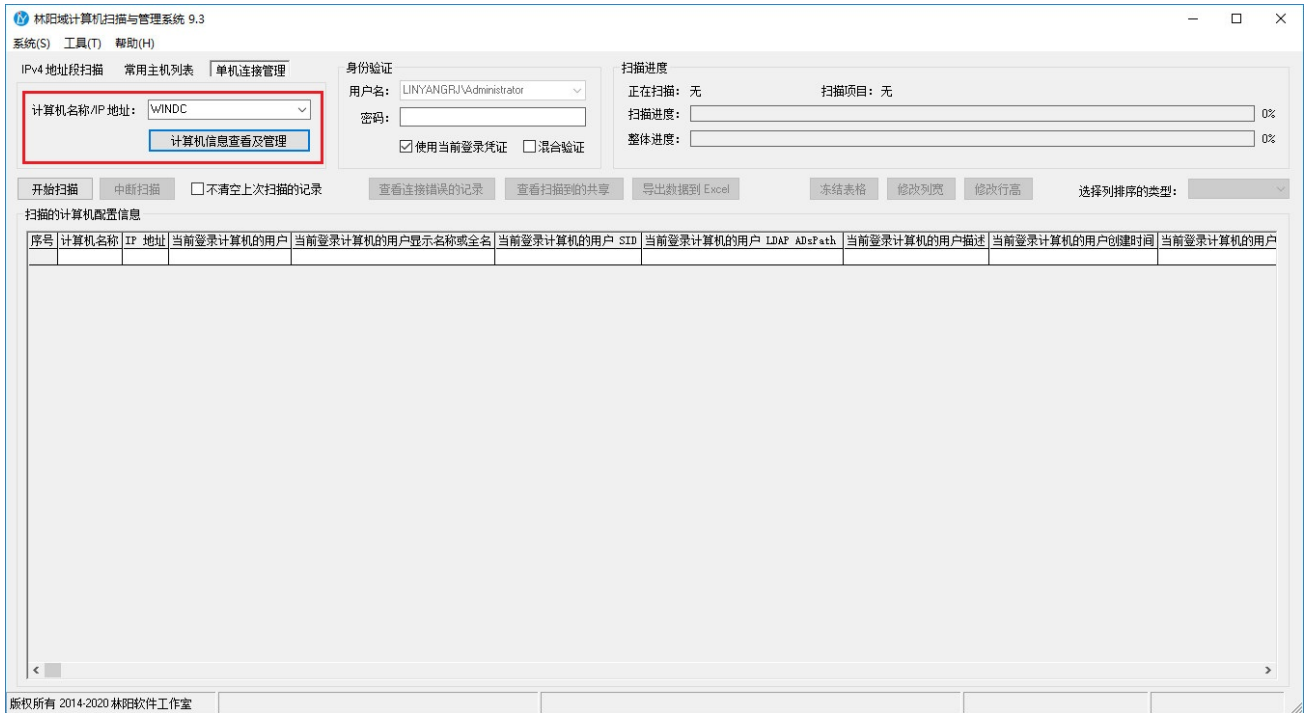
在扫描或远程管理域计算机时提示 462、-2147023174 错误代码“远程服务器不存在或不可用”或“RPC 服务器不可用”等错误，请先参照 P6 “四、域计算机开启远程管理的方法”进行检查处理，如检查完成还提示“远程服务器不存在或不可用”，请参照我们官方网站的说明进行排除：

<http://www.linyangrj.com/yuanchengbukuyong.html>

另你也可以按以下方法进行处理。

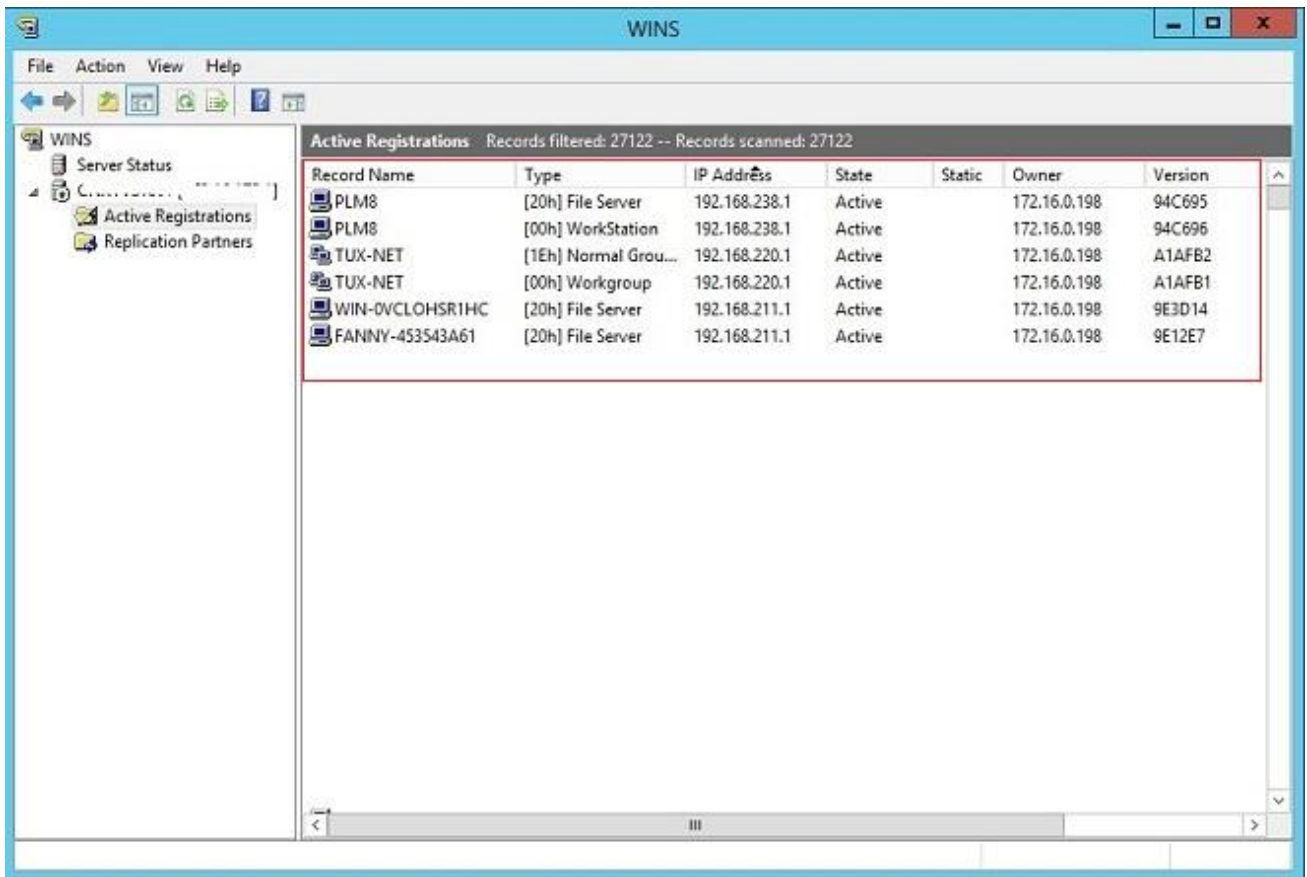
6.1、请分别尝试用计算机名或 IP 地址进行计算机信息查看及管理

请分别输入计算机名或 IP 地址进行尝试连接，如下图所示：



说明：

- 1、在 CMD 命令提示符中尝试 “ ping computer.domain.local ”（计算机的完全限定名称），如 ping pc01.linyangrj.com，再尝试 “ ping -a IPAddress ”，验证这些是否正确。
- 2、确保在客户端计算机、扫描的计算机和就近的域控制器上正确设置了本地时间，这 3 者的时差不能大于 5 分钟。
- 3、确保使用的用户名和密码正确，且指定的用户或当前登录凭证的用户都有管理员权限，用户的密码不能为空，帐户未过期。
- 4、如检测出来的计算机名称都一致或无法连接时，请检查 Wins、DNS 服务器的记录，确认记录名称和 IP 地址是否一一对应，如有错误的记录，请手动在 Wins 或 DNS 服务器上进行删除，如下图所示：



DNS 的检查请检测正向区域和反向区域。

DNS 管理器

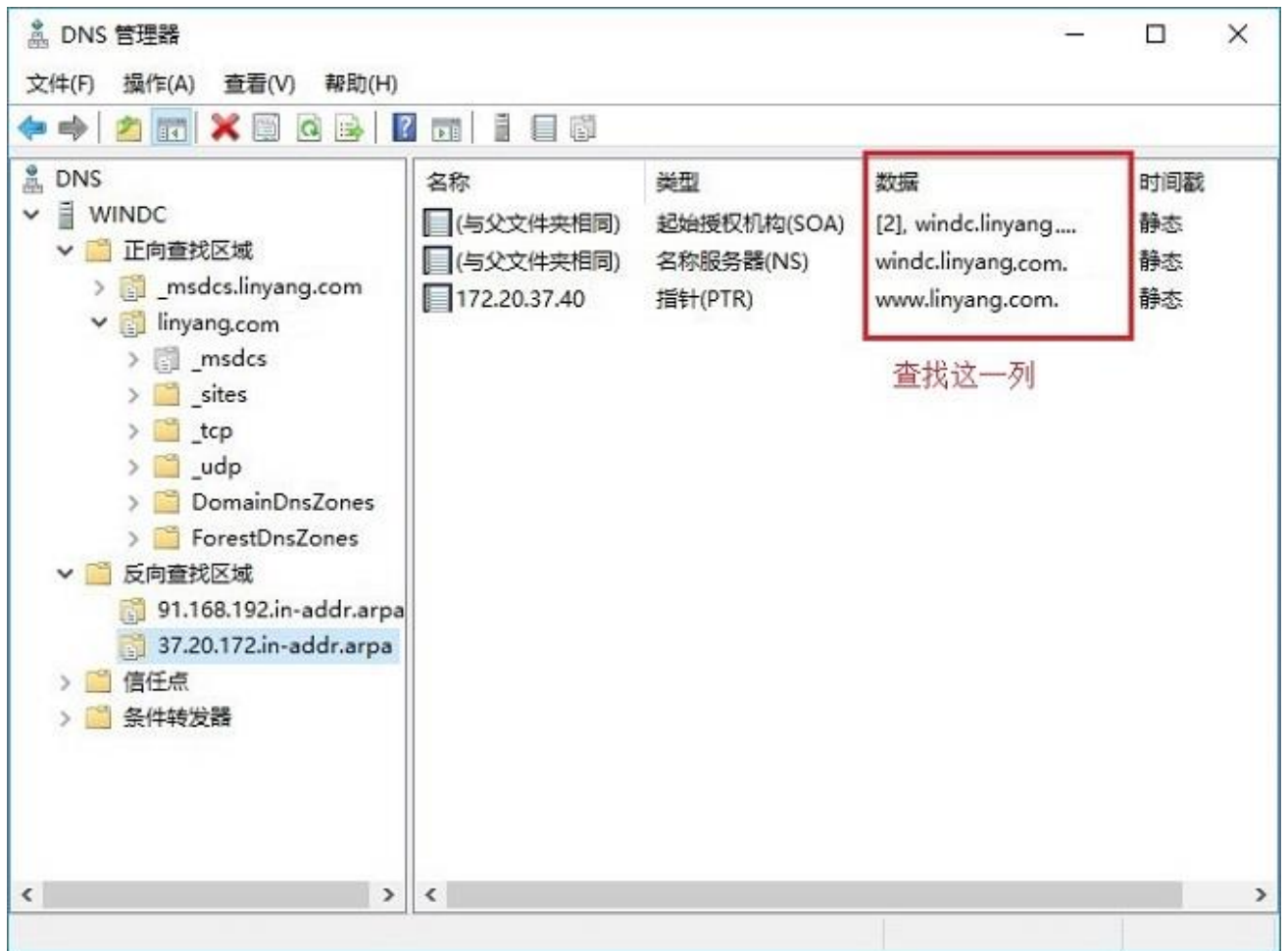
文件(F) 操作(A) 查看(V) 帮助(H)

DNS

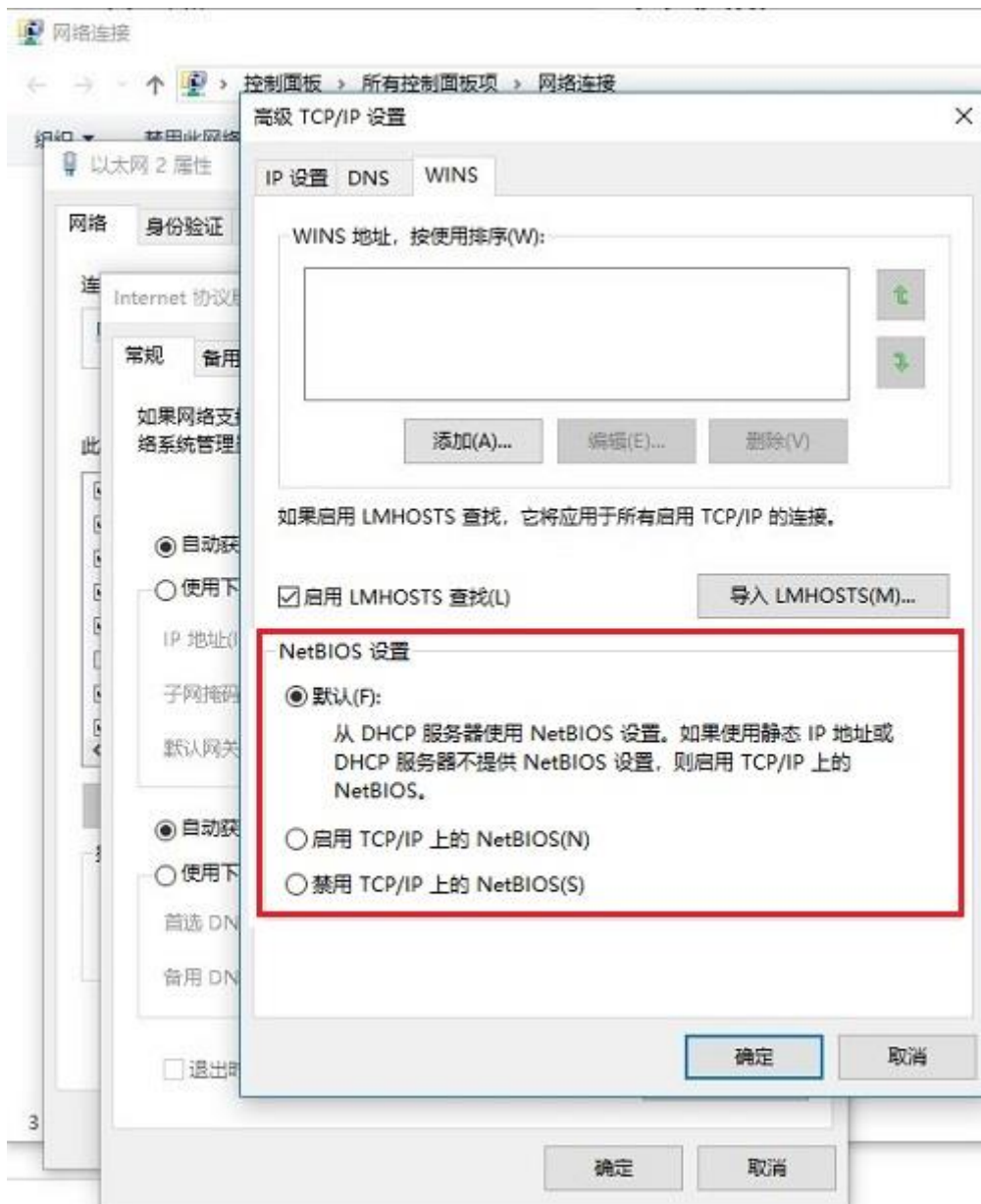
- WINDC
 - 正向查找区域
 - _msdcs.linyang.com
 - linyang.com
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - 反向查找区域
 - 91.168.192.in-addr.arpa
 - 37.20.172.in-addr.arpa
 - 信任点
 - 条件转发器

名称	类型	数据	时间戳
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(与父文件夹相同)	起始授权机构(SOA)	[126], windc.linyang...	静态
(与父文件夹相同)	名称服务器(NS)	windc.linyang.com.	静态
(与父文件夹相同)	主机(A)	192.168.91.128	2020/8/28 14
win01	主机(A)	192.168.91.129	2020/8/18 10
windc	主机(A)	192.168.91.128	静态
www	主机(A)	172.20.37.40	

查找这一列



另请再确认远程计算机的“本地连接-Internet 协议版本 4 (TCP/IPv4)”属性中的 NetBIOS 设置，如下图所示：

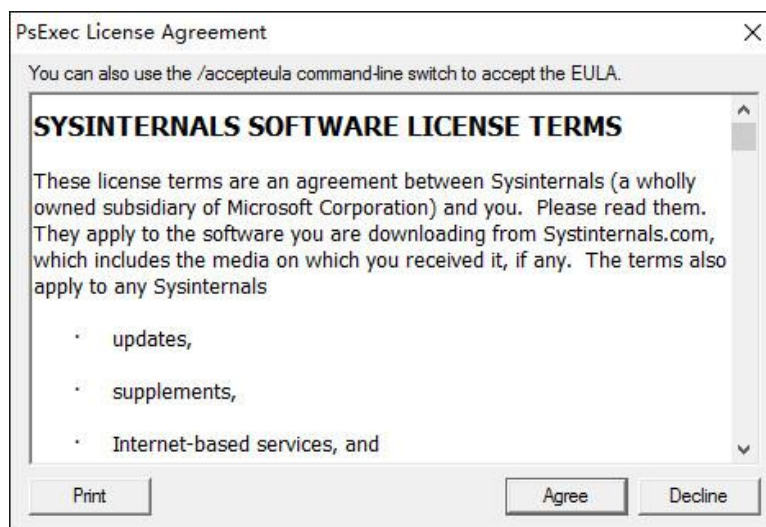


6.2、通过强制开启计算机可被远程管理

- 1、打开软件，单击“工具—强制开启计算机可被远程管理”菜单，打开如下图所示：



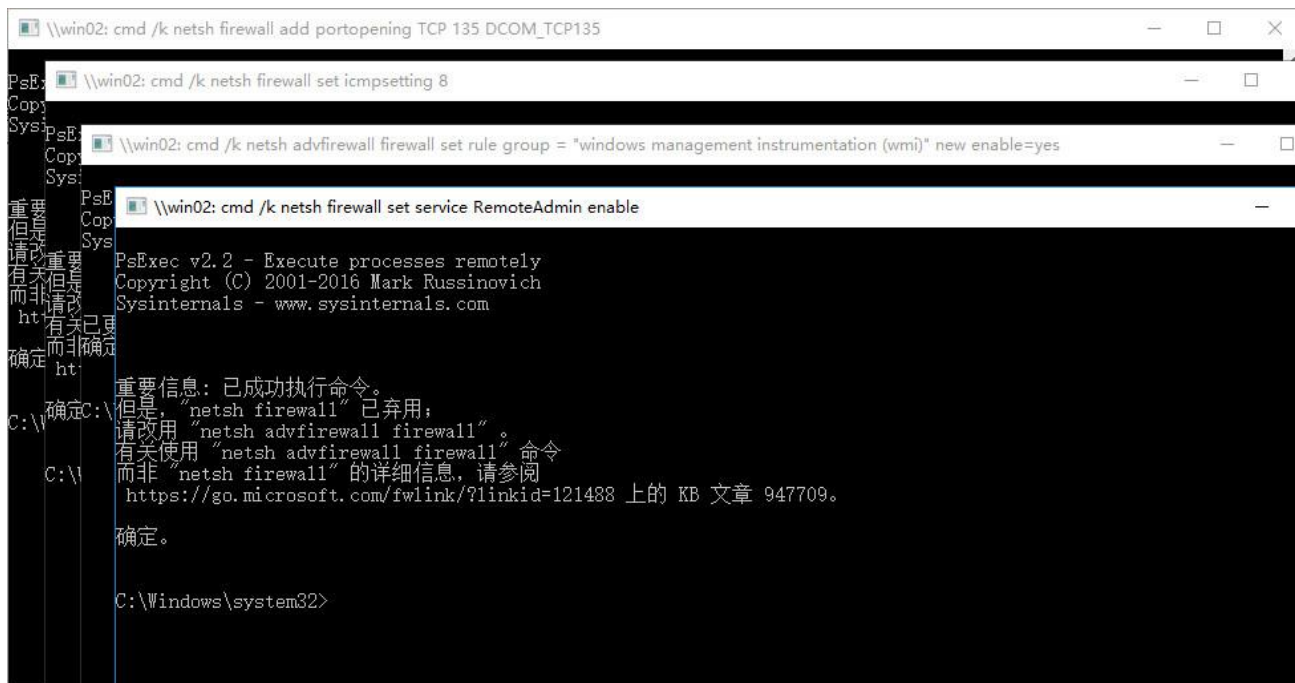
2、输入计算机名称/IP 地址，使用当前登录凭证或输入指定的有管理权限的用户名和密码，单击“强制开启”按钮，第一次使用林阳软件的此功能时，会提示“PsExec License Agreement”的许可协议，单击“Agree”按钮，如下图所示：



说明：这里使用的是 Psexec.exe，它是微软的一个系统辅助工具，它不需要在被连接的计算机上安

装客户端也不需要做任何设置，第一次使用时需要同意许可协议才可以。

3、软件会自动弹出如下图所示的命令提示符，说明已成功强制开启计算机可被远程管理，如弹出的命令提示符窗口自动关闭，则说明无法执行强制开启计算机可被远程管理的操作。



说明：如果以上操作执行都提示成功了，但还是无法远程连接，请扫描远程计算机的 135、137 和 445 端口是开放，如下图所示：

6.3、通过执行解决 RPC 服务器不可用等问题应用程序

1、请在被连接的计算机上执行“ScanRpcOpen.exe”应用程序，如下图所示：

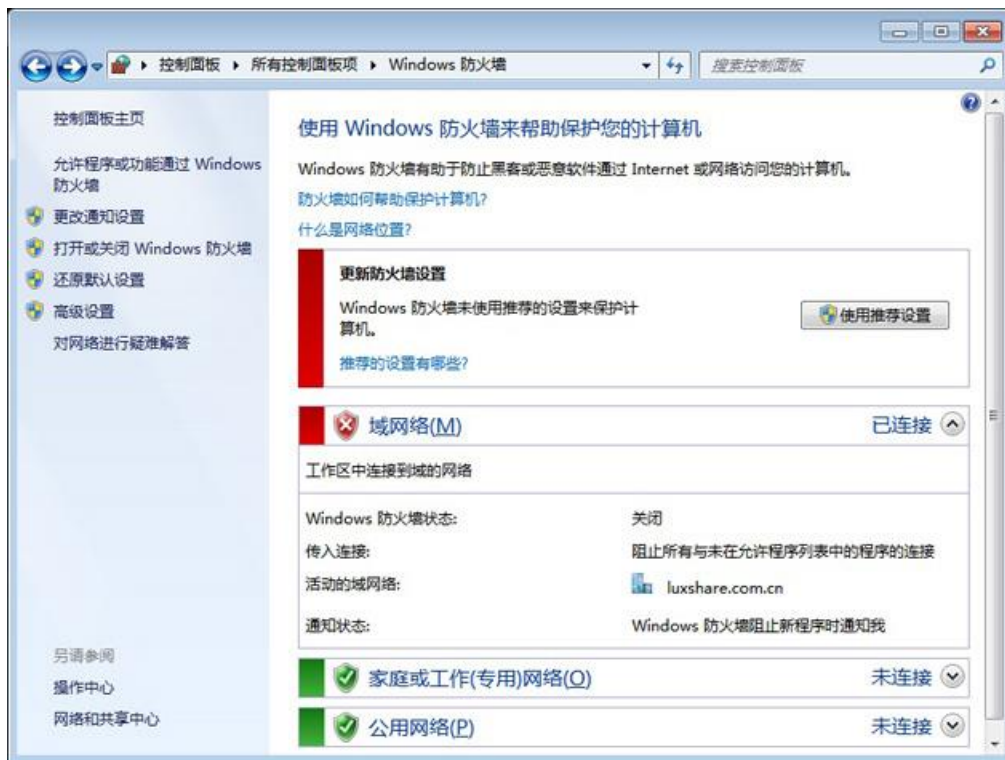


2、单击“一键修复”按钮即可，如下图所示：



6.4、通过关闭 Windows 防火墙

关闭 Windows 防火墙或其它杀毒软件的防火墙即可，如下图所示：



小提示：前提是域计算机有安装杀毒软件，否则我们不推荐直接关闭 Windows 防火墙。

七、购买注册

我们设计开发的软件为共享软件，您可以自由下载和免费试用，为了方便测试和试用，还提供了 30 次的全功能试用版以及免费的 E-mail、QQ、微信、电话技术支持。如果您觉得不错，建议您购买注册，注册用户不仅可以获得我们更全面更优质的技术支持服务，而且还能享受软件的终身免费升级服务，更重要的是：您的注册还将鼓励我们不断改进和完善软件。

软件都是一次性购买，永久使用，永久免费升级，无后期费用和隐含费用。

在软件试用和购买注册过程中有不明白的地方可以随时与我们联系，电话：18362765361。

购买注册流程：

- 1、请先安装试用我们的软件。
- 2、联系我们确定要购买的产品名称、数量、费用和支付方式等。
- 3、请将确定的报价，通过支付宝、微信或银行转账方式，支付软件的注册费用至我们的账户。
- 4、付款后请即时通过电话或 QQ 或微信等方式联系我们，并将软件的注册申请码（注册申请码的查看方法：打开软件，点击“帮助-软件注册”菜单，就可以看到软件的注册申请码）提供给我们。
- 5、我们确认收到你的付款和注册申请码后，并在 8 小时之内将您软件的注册认证码发送给您，让您获

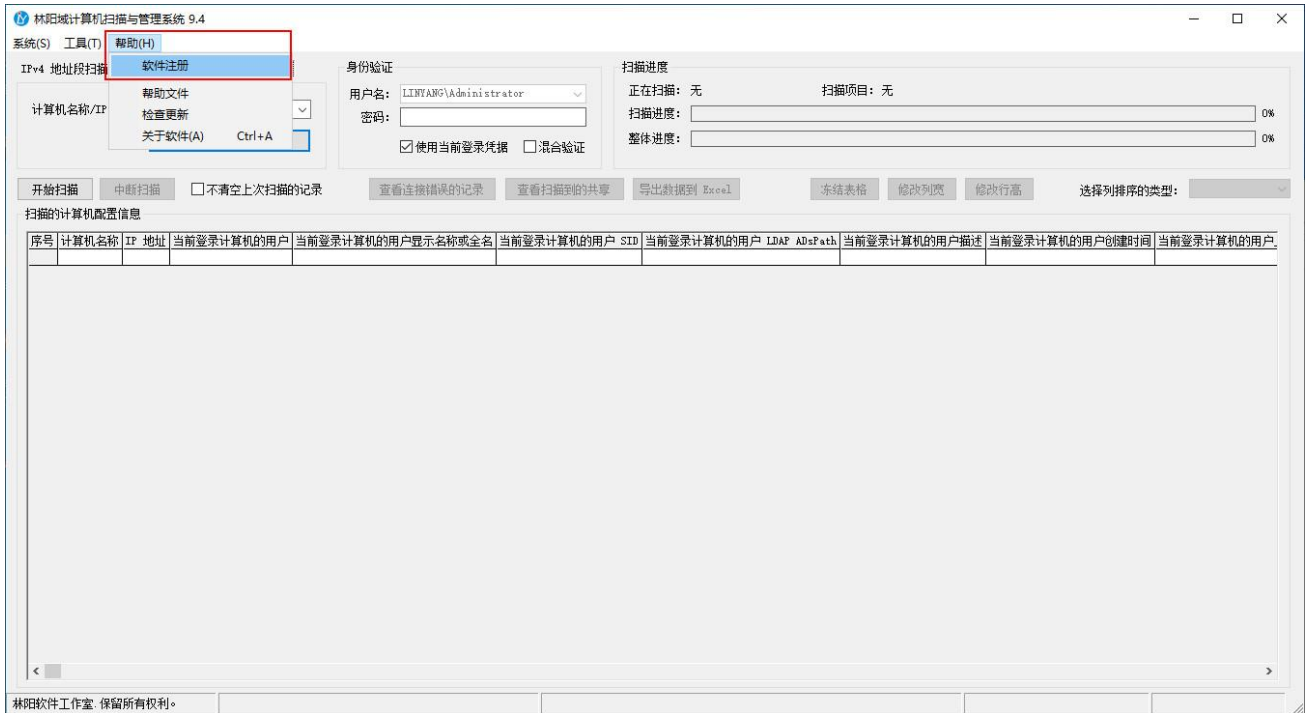
取得该软件的使用授权。

提示：如需要开具发票或签合同，请通过“天空云商城”下单购买，它是本站委托的代理商，天空云商城是国内知名的共享软件注册平台，提供了非常完备和安全的支付方法，有足够的信誉保证。

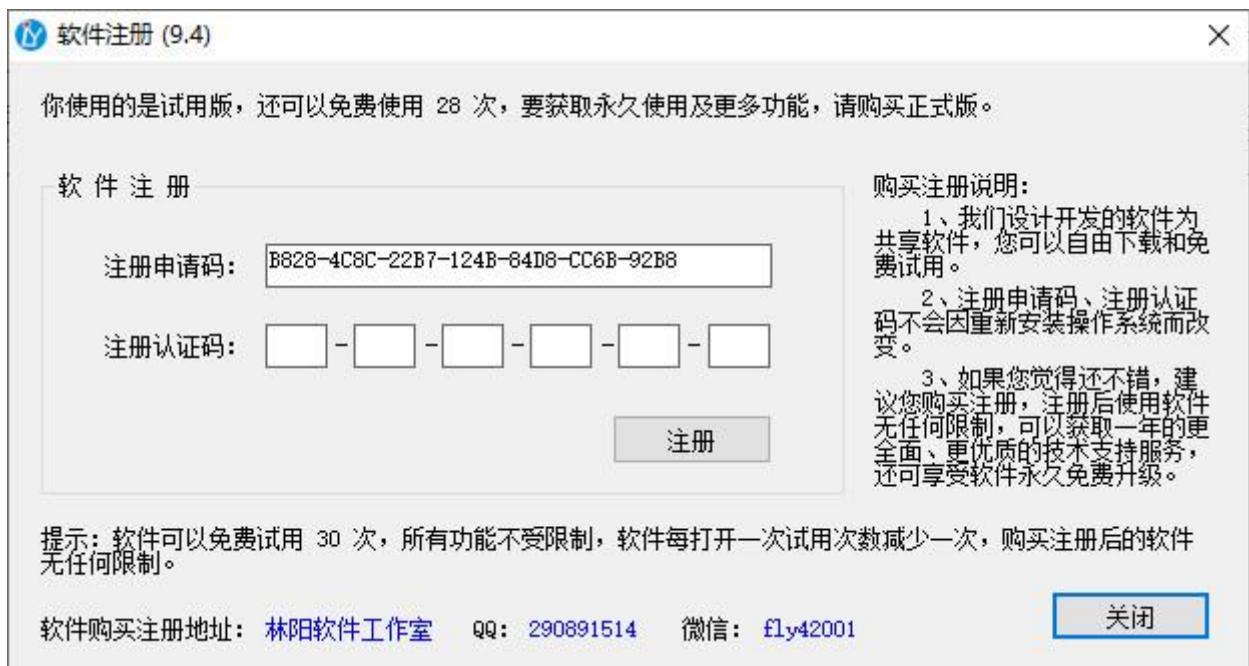
“天空云商城”在线购买注册地址：<http://www.regsky.com/index.php?c=goods&a=info&zcid=3667>

软件注册方法：

1、打开软件，单击“帮助-软件注册”菜单，如下图所示：



2、输入你收到的注册认证码，点击“注册”按钮即可，如下图所示：



注册认证码说明：

软件的注册认证码是与计算机的硬件进行了绑定，更换 Windows 操作系统或重新安装 Windows 操作系统，原有购买过的注册认证码还可以继续使用。

购买注册过的用户如计算机的主要硬件进行了更换或更换新的计算机时，使用之前购买过的注册认证码无法注册我们林阳软件时，这时请您或公司提供说明原因的文件，我们确认你购买过我们的产品，将免费给您或公司再提供一个新的注册认证码。

八、软件技术支持

请访问林阳软件的官方网站 <http://www.linyangrj.com> 检查是否有最新版本的软件或查看常见问题的解决方法。

林阳软件的升级是终身免费的，只要我们发布了新版本，你就可以免费升级至最新版本。

软件购买日起一年内技术支持也是免费的，大家可以发送邮件到：290891514@qq.com

QQ: 290891514

微信: fly42001

为了提供及时准确的服务，您在报告错误时请提供以下信息：

- 1、您使用的软件名称及版本。
- 2、你使用的操作系统版本及登录电脑域帐户的权限级别。
- 3、请提供完整的错误信息，最好包含截图。
- 4、您的联系方式。

更多常见问题请访问我们的官方网站 <http://www.linyangrj.com>

林阳软件工作室

二〇二四年一月三十一日