NETSYS AC
产品使用手册

深圳市网域科技有限公司

二零零九年五月

目 录

第 一 章 简介

现代企业越来越离不开电脑和网络，但是电脑和网络的管理成为一大问题，员工经常用电脑来聊天，做私事、打游戏、下载、访问网站，这样不仅影响工作，而且对公司文化建设产生不好的影响。另外，公司电脑多了以后，经常都是到资产检查的时候才发现电脑的内存、硬盘、CPU 更换、丢失。

伴随网络的快速发展，互联网成为企业发展不可缺少的工具，然而，目前多数企业的网络管理方式，已经不能满足企业管理和发展的需要，不能解决企业网络安全，文档信息保护，高效利用网络带宽，管理员工上网，管理员工的工作情况等现实问题。为了解决这些问题，很多企业需要多种解决方案，同时伴随大量的信息化投资建设。这对于中小企业是个比较大的经济负担，并且，网管人员需要掌握多种软件的使用，增大了应用的难度，同时也增加了系统后续维护的困难。

NETSYS 硬件设备，是一款功能强大的网络管理工具，它一方面控制管理组织的上网行为、有效进行宽带管理，另一方面能对局域网计算机进行全面的管理，具备监视、控制与管理功能。NETSYS 是企业网络的安全助手，通过其企业级的 VPN 防火墙模块保护内部网络，通过其文档安全模块实现文档资料安全，通过网络磁盘来安全方便的管理企业的公共文件。总而言之，NETSYS 包括了企业防火墙路由器、VPN 互联、上网行为管理、桌面行为管理、文档安全管理、远程视频监控录像以及网络磁盘功能，它为企业提供一站式的网络管理解决方案，通过高科技、实用、易用，以及高性价比来满足客户的需求，为客户创造商业价值。
企业网络化的弊端

图 1.1 企业网络风险图

互联网在为企业创造效益的同时，也起到了一定的负面效果。

公司员工在上班时间用计算机是在工作吗，还是在玩游戏、聊天、上网、看电影？既浪

费时间影响工作效率，又影响公司网络安全。在互联网为企业带来便利和效率的同时，企业也正在受到意想不到的损失。 随意访问网站、下载安装软件等操作是造成公司局域网内病毒、木马泛滥的根源。网络中存在病毒，造成资源浪费，让系统变慢，不堪重负，甚至各种后门程序会盗走贵重信息资料。企业设备多了，资产管理就造成麻烦，资产管理人员很难过目每台电脑。如果内存、CPU、硬盘被人偷换了，如果不彻底检查，难以发现资产信息是否准确。如果公司有子公司或分支机构，那公司网络的整体管理就更加麻烦。

1.1 NETSYS AC 解决方案

图 1.2 NETSYS AC 功能实现图

基于现状，网域科技 NETSYS AC 产品的出现能帮助企业管好网络，用好网络，同时解决在网络环境下的企业管理问题和安全问题。提高工作效率，提示企业竞争力，创造效益和价值，NETSYS AC 为企业创造的价值。

1.2 产品功能

NETSYS AC 的六大主流功能：

- VPN/防火墙——保证企业的上网，解决企业分支之间的互联问题；
- 上网行为管理——控制上网相关行为，避免员工在网络上浪费时间，专注工作；
- 桌面行为管理——规范和监管员工在电脑桌面上的行为，提高员工工作效率；管理电脑硬件资产，规范电脑的软件使用；
- 文档安全管理——保护公司文档安全，阻止资料泄密；
- 网络磁盘——企业的文件服务器，支持在内部和外部的访问，完善的权限管理。

1.3 多功能和高性能的结合

NETSYS AC 高度集成将各个模块结合起来是需要一个很好的核心纽带，NETSYS AC 的核心纽带就是实名制的管理模式。

NETSYS AC 的所有功能都采用模块化设计，模块的功能可以选择和配置。NETSYS AC 网络采取实名管理模式，突破传统的 IP 方式的管理，直观、简单、高效。同时，通过简单的配置，就可以明确被管理对象的权限、信息、日志等。

NETSYS AC 在硬件上采用了高性能的配置，具有很好的处理能力，在存储上也配备了大容量的硬盘。并且 NETSYS AC 的软件设计出色，良好的模块化设计，高优化的算法处理，这些因素都保证了产品的高处理能力和稳定运行情况。

第 二 章 网络部署架构

NETSYS AC 作为一个网络硬件设备，首先考虑的是设备应该如何部署在网络中。这需要了解两方面的问题：NETSYS AC 支持的什么样的部署模式；客户自身的网络限制，如何选择适合公司网络部署方式。

2.1 NETSYS AC 部署模式

NETSYS AC 支持 3 种部署形式：网关模式、网桥模式、旁路模式。

2.1.1 网关模式

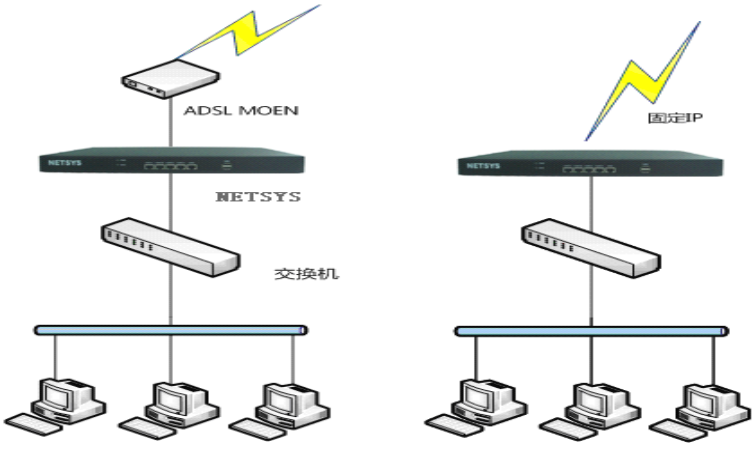


图 2.1.1 网关模式

网关模式是把 NETSYS AC 作为一个路由设备使用，一般是把 NETSYS AC 硬件设备放在内网网关出口的位置，代理局域网上网；或者把 NETSYS AC 放在路由器后面，再代理局域网上网。

NETSYS AC 工作在网关模式时，局域网内电脑的网关 IP 都是指向 NETSYS AC 的 LAN 口 IP，数据由 NETSYS AC 做 NAT 转发出去。

在企业条件允许的情况下，我们建议选择路由模式。

- 网关模式配置举例，针对 ADSL 拨号用户的(如下图):

该设置主要让 NETSYS AC 代理上网，进行拨号，我们只需要设置用户名、密码。

2.1.2 网桥模式

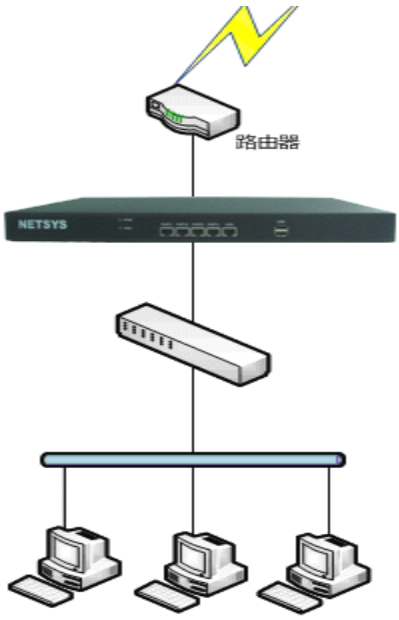


图 2.1.2 网桥模式

网桥模式是把 NETSYS AC 视为一条带过滤功能的网线使用，一般在不方便更改原有网络拓扑结构的情况下启用。把 NETSYS AC 接在原有的网关及内网用户之间，在原网关及内网用户不需做任何配置改变的情况下，对 NETSYS AC 进行配置即可。对原网关及内网用户而言，不知 NETSYS AC 的存在，即所谓对网关及内网用户透明。网桥模式的主要特点是：

网桥模式是可以穿透数据链路层的数据，对用户做到完全透明。

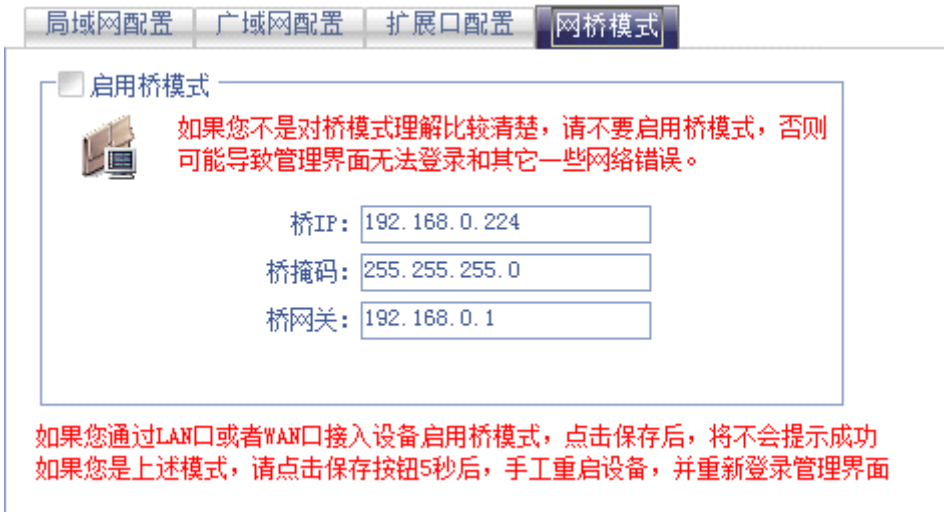
在网桥模式启用时，不能使用 NAT 功能。

NETSYS AC 工作在网桥模式时，必须保证所有数据透传 NETSYS AC，不能存在内网用户绕行而到达网关的物理线路。

NETSYS AC 工作在网桥模式时，局域网内电脑的网关地址无需更改。

- 网桥模式配置举例(如下图):

  启用网桥模式，添加桥 IP、掩码、网关地址。



2.1.3 旁路模式

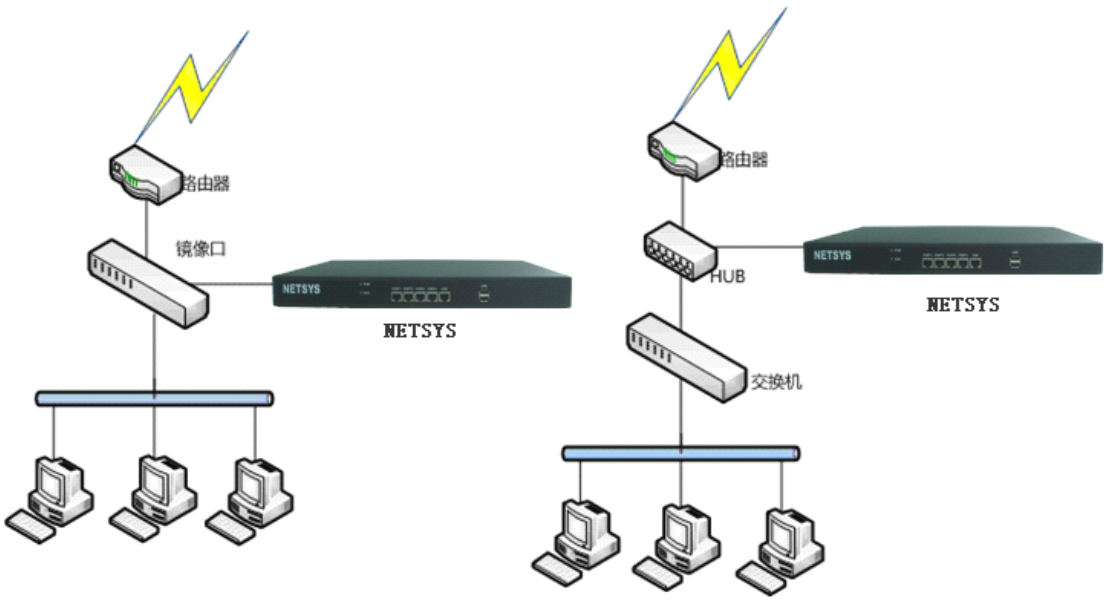


图 2.1.3 旁路模式

旁路模式实现监控和管理的同时，可以不必更改公司的网络架构，可以避免设备中断对网络用户访问造成的风险。用户把 NETSYS AC 接在交换机的镜像口或者接在 HUB 上，对网络进行旁路式的监听和控制。

用户必须使用具有端口镜像的交换机或者 HUB。如果交换机没有镜像端口，可以在交换机前加接 HUB 实现。

- 旁路模式配置举例(如下图):

当 NETSYS AC 作用于旁路模式下，我们只需要给设备配置一个内网地址，使 NETSYS AC 与内网所有电脑互通。

2.1.4 模式对比

为了适应不同的网络形态需求，客户根据自己的网络结构，选择适合自己企业网络模式来部署。下表是三种模式的优缺点对比：

接入模式	优势	劣势
网关模式	设备的 WAN 口一般具备公网 IP 地址，NETSYS AC 的管理软件，不需要端口映射，就可以实现远程的网络管理，用户在可以上网的任何地方进行管理，查看日志信息等。并且可以充分的利用 NETSYS AC 的 VPN 等功能。完成公司、分公司的互联，建立自己的虚拟专网，共享企业资源。也可以方便的使用，NETSYS AC 的远程视频监控和 VOIP 功能。	可能需要修改现有网络配置，也可能要替换掉现有的路由上网设备或者防火墙设备，因为这部分功能和 NETSYS AC 设备的功能重叠。
网桥模式	不需要改变用户网络配置，方便连接和使用，设备配置部署快速。保护现有设备投资，高档路由设备和 NETSYS AC 设备协同工作，同时提升网络处理性能和网络管理能力。	设备不具备公网 IP 地址，外部管理需要端口映射。不支持 VPN 功能。对于没有高档路由设备的用户，这种模式不能发挥 NETSYS AC 的网络处理和防火墙方面的优势，限制了设备价值。
旁路模式	网络数据包不通过这个设备，对网络环境没有产生任何影响。	网络数据包不通过这个设备，所以还需在交换机的端口上启用端口镜像（交换机支持端口镜像），如果没有端口镜像功能，就要接一个 HUB，如果不启用端口镜像或接入 HUB，NETSYS AC 功能会有所丧失。

表 2.1.4

2.2 网络结构典型实例

企业的网络结构是多样化的，我们列举 3 个最为常见的结构，用户可以根据实例部署自己的网络。对于在部署过程中遇到的问题，可以通过我司 0755-83285850 电话做技术咨询。

2.2.1 典型二层网络

这是一个非常典型的二层网络架构的拓扑图，ADSL 的拨号接入，路由器为网关，该网络架构能够满足基本目前绝大多数企业（如下图 1）。

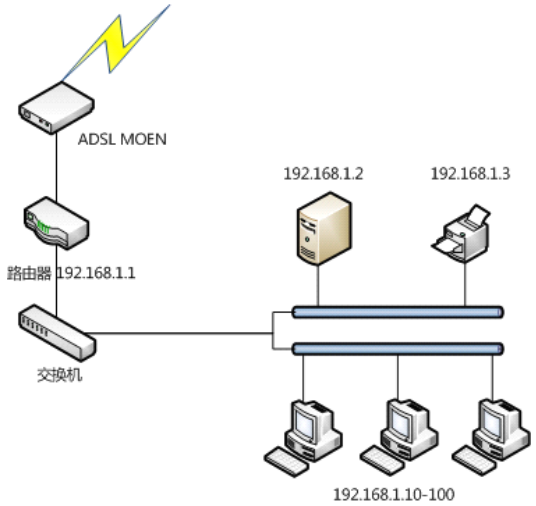


图 1

NETSYS AC 的接入实际上顶替了路由器，在功能上也实现了一个网关的作用，内网的所有设备网关都指向 NETSYS AC，通过 NETSYS AC 拨号设置代理上网，也可以启用 DHCP 服务，让内网设备自动获取 IP 等（如下图 2）。

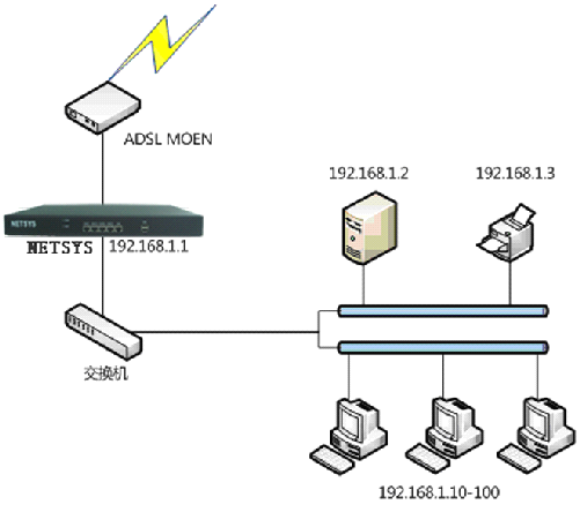


图 2

2.2.2 典型三层网络

固定 IP 接入，内网电脑超过 200 台（如下图 1）。

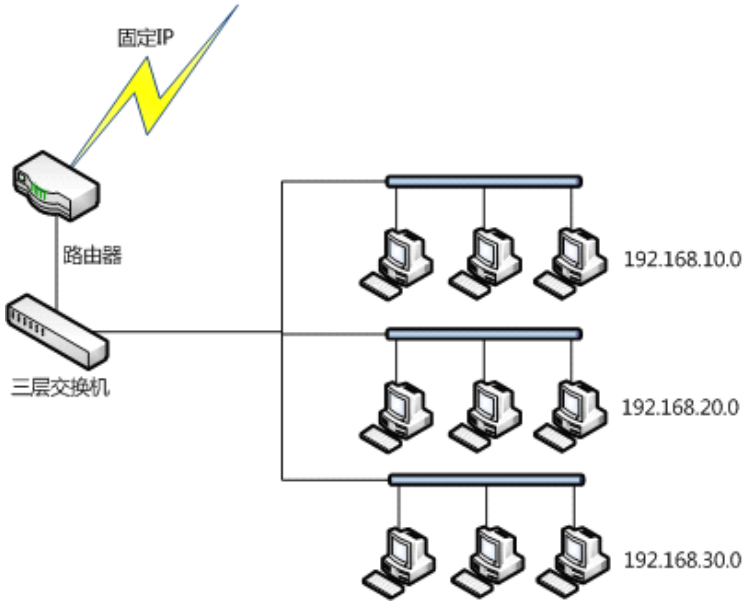


图 1

不改变原网络结构，在路由器和三层交换机之前接入 NETSYS AC，使用网桥模式或旁路模式（如下图 2）。

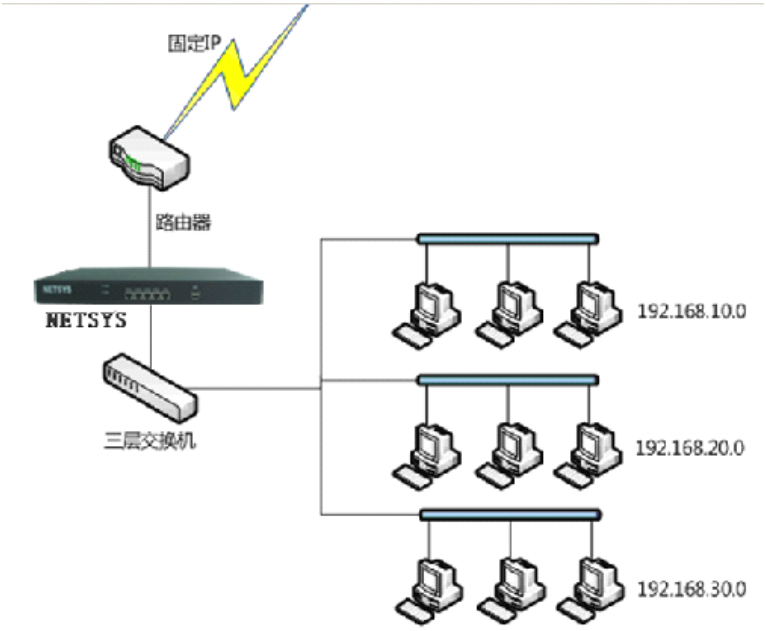


图 2

2.2.3 双线路接入网络

单一的 ADSL 不能保证带宽需求，同时，公司需要将不同的部门网络隔离，分成两个

网络来上网（如下图 1）。

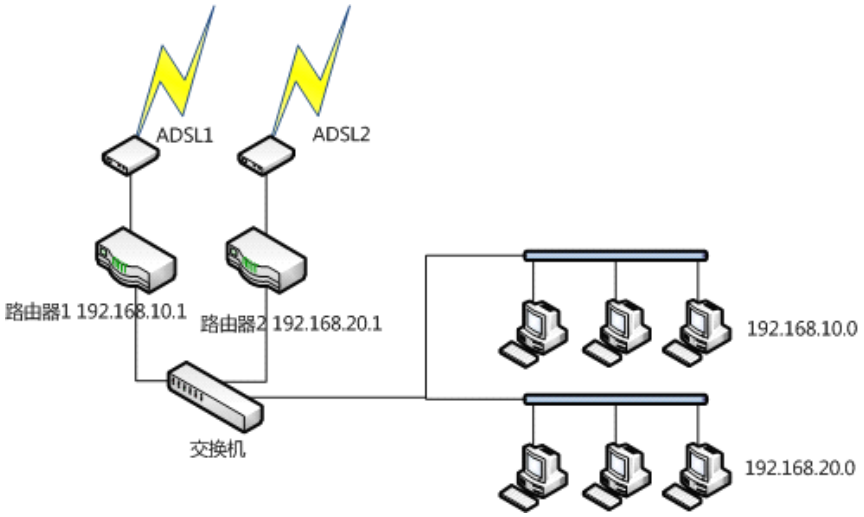


图 1

这种网络结构有两个作用，既可以保证部门之间的隔离，有可以保证某些部门的关键业务不受到整个网络流量的影响。通常用户选用 NETSYS AC 设备，需要对这两个网络都管理的，NETSYS AC 的连接方法（如下图 2）。

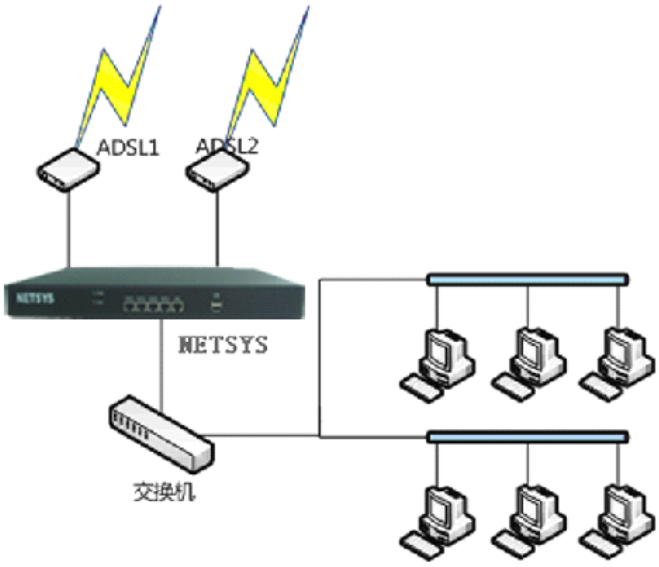
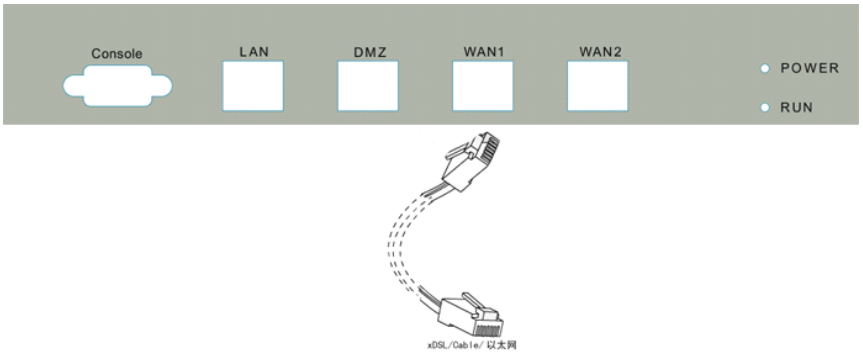


图 2

在这种环境下，NETSYS AC 通过配置双线路、防火墙来控制，2 个网段之间的互通。NETSYS AC 对两个网段用户统一做管理。这种模式下，NETSYS AC 设备作路由器使用，通过 NETSYS AC 的路由规则来确定转发线路。

第 三 章 设备安装

本章节主要介绍 NETSYS AC 系列产品的构成和硬件安装。硬件安装正确之后，才能进行配置调试。



接口	地址
LAN 口	192.168.1.1
WAN 口	192.168.0.200
DMZ（扩展）口	10.0.0.200

图 3 接口示意图

LAN 口，内部局域网口，一般与公司网络的交换机连接；WAN 口，网关的外部出口，一般与公司网络的路由器或 ADSL MODEM 连接；DMZ 口，即扩展口，当企业使用双线路上网时，需要启动该接口。

NETSYS AC 物理接口不适合自适应，所以上行连接路由器时，需要使用交叉网线。下行连接交换机时，使用直连线。

3.1 检查连通情况

首先将 NETSYS AC 硬件连接好电源，加电启动。再将您的计算机接到 NETSYS AC 的任意接口。如果是直接连接使用交叉网线，通过交换机间接连接使用直通网线。如：接到设备的 LAN 口（默认 IP 为 192.168.1.1 子网掩码为 255.255.255.0）接下来把您的计算机 IP 地址和所接入 NETSYS AC 的接口 IP 设置在同一个网段。如：把本机 IP 设置为 192.168.1.xxx，子网掩码要相同。此时可以通过 ping 检查是否正常启动。

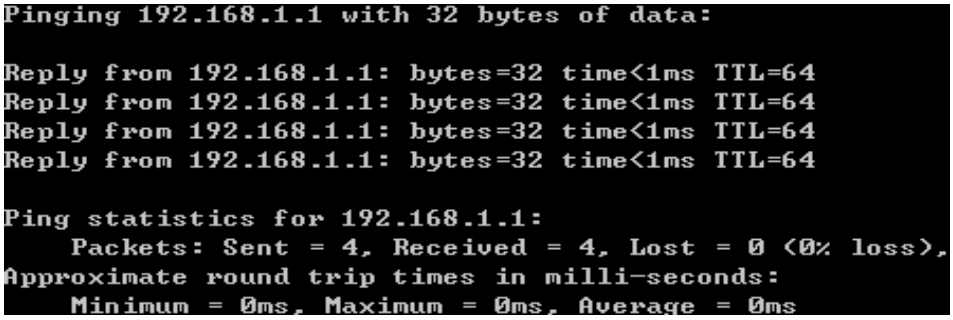
按[开始]→[运行]，在命令框中输入 CMD，然后按回车键，在出现的界面里输入：ping 192.168.1.1 。如果屏幕显示为图[1]表示“NETSYS AC”已启动，并且已经和您的计算机联通；如果屏幕显示为图[2]表示“NETSYS AC”没有正常启动或没联通。您可以按照下列顺序检查:

1） 硬件连接是否正确

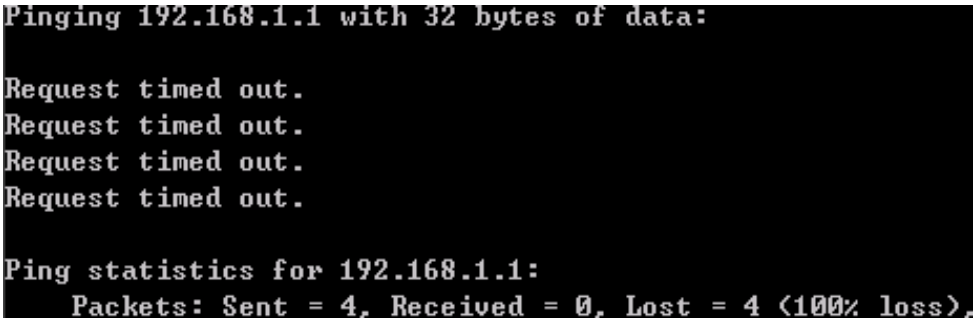
“NETSYS AC”面板上 LAN 接入端口的指示灯和您计算机上的网卡指示灯必须亮。

2） 您的计算机的 TCP/IP 设置是否正确

如果“NETSYS AC”的 IP 地址为 192.168.1.1，那么您的计算机 IP 地址必须为 192.168.1.x (x 范围是 2 至 254)。



图[1]



图[2]

3.2 初始登陆账号

登陆 NETSYS AC 时，系统已设置 4 个初始化用户，可以为默认用户更改密码、权限和类型；也可以手动添加管理用户，只需填写相关信息和选择用户权限、认证方式和用户类型即可生成。

用户全名	用户登陆 ID	认证方式	读写权限	用户类型
超级用户	root	密码方式	读写权限	超级用户
老板	boss	密码方式	读写权限	行政管理员
系统管理员	system	密码方式	读写权限	网络管理员
文档管理员	doc	密码方式	读写权限	文档管理员

表 3.2

注：1.默认账号密码都是 123456；

2.超级用户（root）是无法删除的。

3.3 系统登录界面

NETSYS AC 以直观的界面体现给用户，安装本公司提供的光盘“NETSYS AC”，双击弹出登陆界面：

图 3.3 登陆界面

接入认证：登陆“NETSYS AC”设备接口的地址，支持 IP 地址和动态域名（动态域名目前只支持 3322.org 的动态域名）、用户名、密码。

终端设备选择：添加本地终端所需要登录的网管设备。

图 3.3.1 认证设备配置

3.4 系统界面说明

NETSYS AC 为管理者提供个性化的操作界面，易于操作。登陆到 NETSYS AC 系统界面后，可以看到以下配置模块：包括[设备管理]、[防火墙]、[网络互连]、[用户管理]、[上网行为]、[桌面行为]、[数据管理]、[报表中心]、[文档安全]、[视频监控]、[网络磁盘]等。

所有界面中如果有[保存]按钮，则配置完毕后，一定要点击按钮才能将配置保存进设备。

图 3.4 系统界面

【1】标题栏：NETSYS AC 系统当前的版本和支持的用户数。
【2】侧边栏：NETSYS AC 的侧边栏书签按钮。
【3】工具栏：NETSYS AC 主要功能按钮。
【4】信息显示区域：显示当前用户所选择功能配置操作界面。
【5】状态栏：显示当前设备运行的状态。

3.5 故障恢复

- **忘记设备登录地址**

1. 通过 DMZ 口接入设备，把您的计算机配置一个 10.0.0.x 的网段 IP 接入到设备的 DMZ 口（DMZ 口出厂地址为 10.0.0.200 一般是不会进行改动）登录到设备。查看[设备管理]→[网络设置]或[设备状态]就可知道设备的接口地址。
2. 通过“客户端维护工具”也可以查寻到设备地址，打开“客户端维护工具”点击设备维护，通过“获取设备地址”就可以得到。

- **忘记账号密码**

可以通过设备管理器进入“NETSYS AC”点击[数据管理]→[恢复出厂设置]账号和密码就能恢复出厂默认设置（注：对“NETSYS AC”所有设置都将恢复出厂默认设置）。

- **无法登录 NETSYS AC**

检查登录地址、域名接入认证信息是否正确，通过 ping 检查计算机和设备之间是否连通。

第 四 章 设备管理

我们通过设备管理界面对 NETSYS AC 进行配置，设备状态查询，设备功能控制和设备维护。

设备管理主要调试 NETSYS AC 的网络配置，包括网络接口、DHCP、DDNS、接口速率等。同时根据设备的接入方式，配置相应的接入模式，例如路由模式、网桥模式和旁路模式。其次，如果企业使用双线路接入公司网络，我们还可以满足双线路的设置，为两条线路设置负载均衡、分流策略、策略路由，分配企业外网线路总带宽使用比率，用户、业务数据流走向和指定运营商线路。除此之外还可以查看配置后的设备状态，线路是否上线、端口状态是否正常、功能和服务是否启用。

4.1 设备状态

[设备状态]是查看 NETSYS AC 设备的工作状态，通过查看[系统状态]、[内网口状态]、[外网口状态]、[扩展口状态]了解设备的工作情况。

系统状态：

此状态下，可以查看到设备当前时间、序列号、设备型号、软件版本、认证状态、防火墙状态、网桥模式、DDNS 状态。

认证状态只与 VPN 配置有关系，如果没有配置 VPN，该状态没有意义。

内网口状态：

外网口状态：

扩展口状态：

4.2 设备控制

设备控制是启用、停止上网行为、桌面行为、IP/MAC 绑定功能按钮，只有在功能被启用的状态下，上网行为、桌面行为、IP/MAC 绑定才能使用。

图 4.2 设备控制

认证失败处理策略，如果选择禁止上网，那么内网认证失败的用户就无法访问互联网，只有通过认证给予授权的用户才能访问。

由于在网桥模式不能做端口映射，避免外网用户无法访问企业内部的服务器；当启用禁止上网，内部特殊服务器通过验证后，我们将其 IP 地址添加到可访问列表中（如下图）。

“用户登陆时发现员工未配置模版弹出提示对话框”如果选择启用的话，那么就会提醒管理员未配置上网行为策略或桌面行为策略的用户在对话框中显示。

4.3 网络配置

网络接口参数和设备提供的网络服务配置。包括网络接口的配置，DHCP 服务，DDNS 域名服务，接口速率等。而且根据 NETSYS AC 的接入形式，配置相应的接入模式，例如路由模式、网桥模式和旁路模式。

4.3.1 网络接口配置

根据设备在网络中的接入形式我们来判断当前工作模式，一般我们在接口上只需要配置局域网、广域网、扩展口。具体配置方法如下：

1、 网关模式

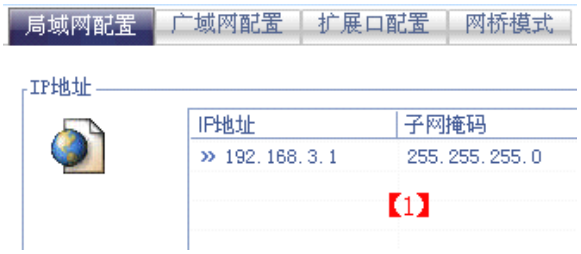


图 1

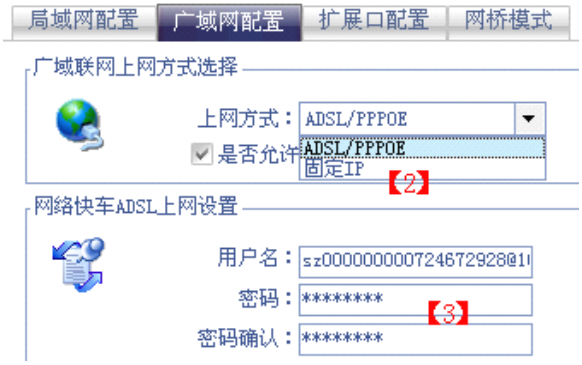


图 2

图 3

【1】 局域网配置，内网网关地址；
【2】 广域网配置，选择上网方式；
【3】 广域网配置，ADSL 的用户名和密码；
【4】 广域网配置，固定 IP 的网关；
【5】 广域网配置，固定 IP 地址。

2、 网桥模式

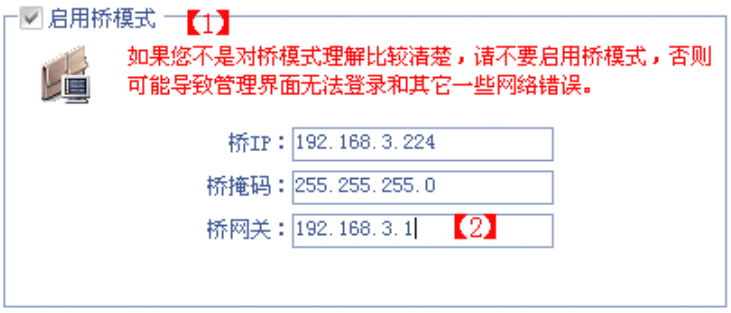


图 1

1. 启用桥模式；
2. 做网桥时的配置，上图的 NETSYS AC 管理地址为 192.168.3.224 网关(PC 上网网关)为 192.168.3.1。

4.3.2 DHCP 服务

DHCP 服务，即动态主机配置协议：计算机用来获得配置信息的协议。DHCP 允许给某一计算机自动分发 IP 地址而不需要管理者在服务器数据中配置有关该计算机信息。我们可以在 NETSYS AC 中开启 DHCP 服务，从而让计算机自动获取计算机信息和分配其动态 IP 地址。

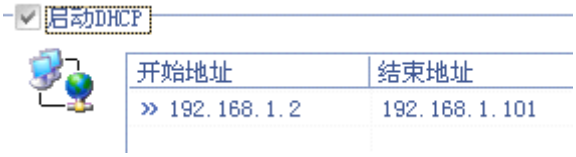


图 4.3.2 启用 DHCP

这里我们只需要手动添加动态分配的地址段，比如公司有 100 台电脑，即 192.168.1.2-192.168.1.102。

启用 DCHP 服务后，无法实现 IP/MAC 地址绑定。

网桥模式下不支持 DHCP 服务。

4.3.3 DDNS 服务

DDNS 是动态域名服务的缩写。DDNS 是将用户的动态 IP 地址映射到一个固定的域名

解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。

图 4.3.3 DDNS 服务

宽带运营商大多只提供动态的 IP 地址，DDNS 可以捕获用户每次变化的 IP 地址，然后将其与域名相对应，这样其他上网用户就可以通过域名来与用户交流了。

DDNS 可以帮你在自己的公司或家里构建虚拟主机。

4.3.4 接口速率

NETSYS AC 的物理接口 LAN、WAN、扩展口均可设置端口速率，分别有 10M/100M 全速、半速等选项；一般没有特定需求，都设置为自适应。

图 4.3.4 接口速率

4.3.5 设备维护

设备维护可以升级设备软件，重启设备硬件，修改客户端机器注册的设备地址，查看客户端版本号。

如果用户的设备当前软件版本需要升级，可以通过升级按钮。设备升级请在厂商技术人员支持下完成，否则可能会带来不可恢复的故障；

修改客户端注册地址作用是为了电脑安装客户端后快捷地寻找 NETSYS AC 设备。设置时间校准可以将 NETSYS AC 与您的 PC 同步，可以手动设置 NETSYS AC 的时间，也可以通过与网络时间服务器进行时间同步。

4.4 双线路说明

双线路实际上是物理性的带宽增加，即 2M+3M=5M。

双线路方案主要解决了 1.企业上网带宽的局限性，2.企业所在的地域通信的高延迟。

有些企业单一的线路带宽已经不能满足其需求，由于 10M 以上的光纤费用昂贵，此时我们的解决方法就是采用双线路，提高上网带宽。

在中国，南方的用户大多使用电信上网，北方大多使用网通上网，这样就造成使用不同供应商提供的线路之间访问延迟过高，延迟高通信就会慢。此时我们推荐企业在网络上使用双线路，采用电信/网通线路共存的方式来解决南北通信高延迟的问题。

4.4.1 负载均衡

该功能主要以手动托条的形式设置，作用是分配使用线路的带宽比率。

比如某公司选择双线路上网，一条是 3M 另一条 2M，分别将 3M 接入 WAN1，2M 接入 WAN2，那么公司的出口（互联网）带宽为 5M，此时我们可以设置流量比例，让 WAN1 的数据流占总线路带宽的 60%，而 WAN2 的数据流占总线路带宽的 40%。实际上这个比率是按照客户的用网需求自定义设置的。

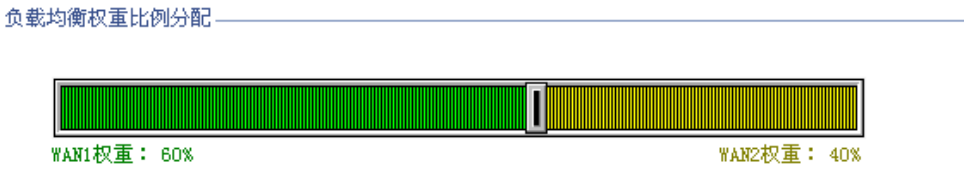


图 4.4.1 权重比例

4.4.2 分流策略

以路由定向指令数据到指定线路的方式，从而保证了带宽使用率。比如公司使用了双线路上网，需要安排某台电脑、某个网段、某个服务走指定的线路，那么我们在该线路上添加其电脑的 IP 地址、端口号和目的地址，从而将数据转发出去。

比如某公司选择双线路上网，其中公司安排财务部（网段为 3）走 WAN2 线路，保证部门的流量带宽。我们可以在分流策略中的 WAN2 路由信息中添加公司财务部这个网段，其他部门就会使用 WAN1，从而保证了部门的带宽。

WAN2分流策略路由信息：

序号	源地址	源地址掩码	目的地址	目的地址掩码
» 1	192.168.3.0	255.255.255.0	0.0.0.0	0.0.0.0

图 4.4.2 分流策略

4.4.3 策略路由

选择不同供应商线路，同时匹配线路的策略路由，使该线路会固定按照路由表内的地址访问互联网，从而达到低延迟，快速通信的效果。

这里我们只要确认接口线路的 ISP 供应商，同时在路由策略界面中选中使用该 ISP 策略路由，即可完成设置。

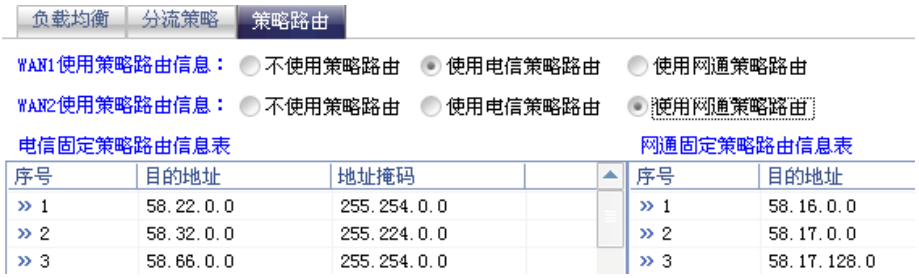


图 4.4.3 策略路由

5 防火墙

基于时间、地址、服务对象定义的策略相互间匹配生成的通用防火墙策略，有效地控制了企业员工全时间段的访问权限。

NETSYS AC 在路由模式下可以绑定网关的 IP/MAC 地址和内网所有计算机的 IP/MAC 地址，有效地预防 ARP 病毒攻击。

静态路由实现了 NETSYS AC 设备上行、下行设备的互联互通。端口映射达到外网访问内网服务的需求。

5.1 安全策略

在安全策略，由[MAC/IP 绑定]、[静态路由]、[源地址转换]、[端口映射]、[通用防火墙]、[高级设置]模块构成。

5.1.1 IP/MAC 地址绑定

什么时候会用到 MAC/IP 地址绑定功能：

1、 希望 IP 地址不会乱造成的地址冲突；

2、 当流动人员多，常常有新的人员加进网内，不希望不经授权而访问外网；

3、 小区网络以 MAC 为身份验证时；

4、 当设定访问规则时，需要严格的区分权限。

界面说明（如下图 5.1.1）：

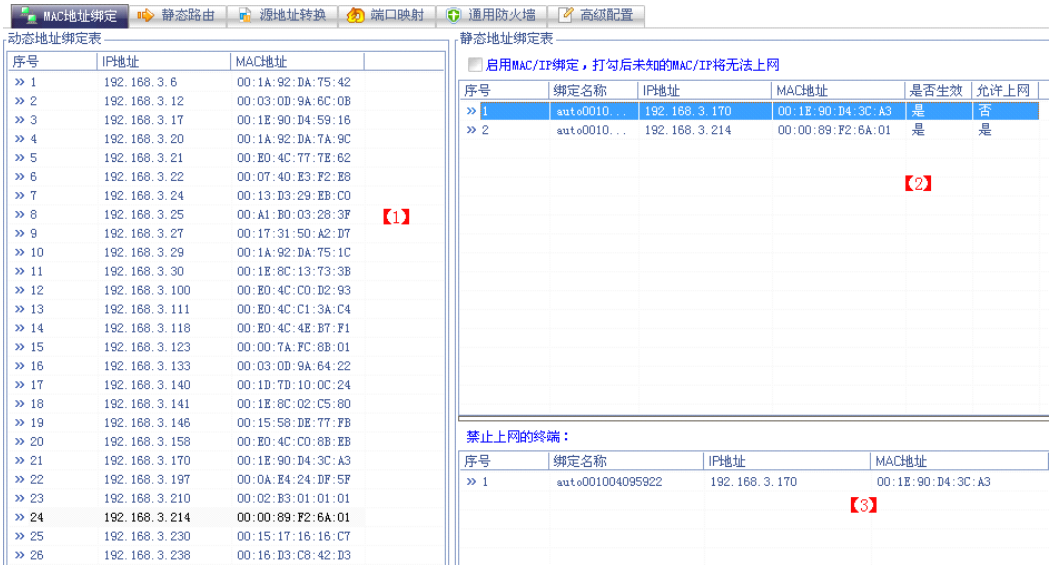


图 5.1.1 IP/MAC 地址绑定

【1】 表内显示的是 NETSYS AC 所获取到内网 IP 和 MAC 地址；

【2】 已绑定的地址，可以配置绑定名称、绑定规则、是否生效、是否允许接入 Internet;

【3】 已禁止用户接入 Internet，管理者能一目了然查询到哪些用户不允许上网。

MAC/IP 绑定在出厂设置下为禁用。

如果启用绑定功能，绑定表内无绑定 IP，绑定功能则没有启动。

5.1.2 静态路由

路由模式和网桥模式下，设置静态路由让不同网段数据传出外网。

例：有这样一个网络结构的公司，三层交换内有 3 个业务 Vlan（192.168.10~30），上行至 NETSYS AC，NETSYS AC 网关地址 192.168.40.1（如下图 5.1.2）。

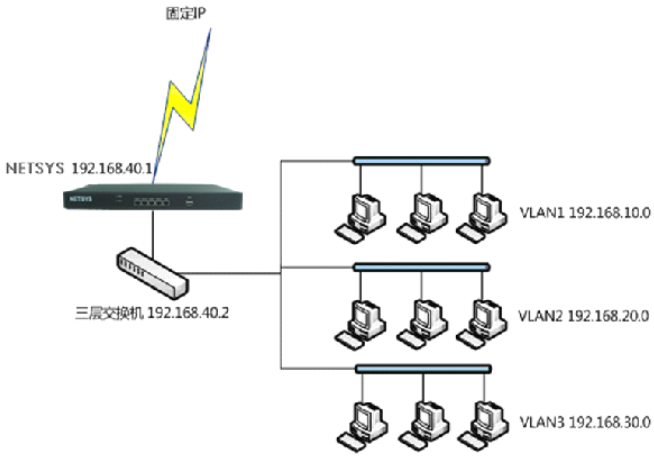


图 5.1.2 静态路由

在路由表中添加业务 Vlan：

序号	目的网络	子网掩码	网关	跳数	接口
» 1	192.168.10.0	255.255.255.0	192.168.40.1	1	LAN
» 2	192.168.20.0	255.255.255.0	192.168.40.1	1	LAN
» 3	192.168.30.0	255.255.255.0	192.168.40.1	1	LAN

5.1.3 源地址转换

源地址转换—对于多网关的网络，可以通过对源地址转换，使其找到正确的路由返回(如下图 5.1.3)。

图 5.1.3 源地址转换

5.1.4 端口映射

如果局域网内有服务器需要向 Internet 提供服务，那么就需要在网关上进行[端口映射设置]。NETSYS AC 也提供了这样的功能。设置界面如下（见图 5.1.4）：

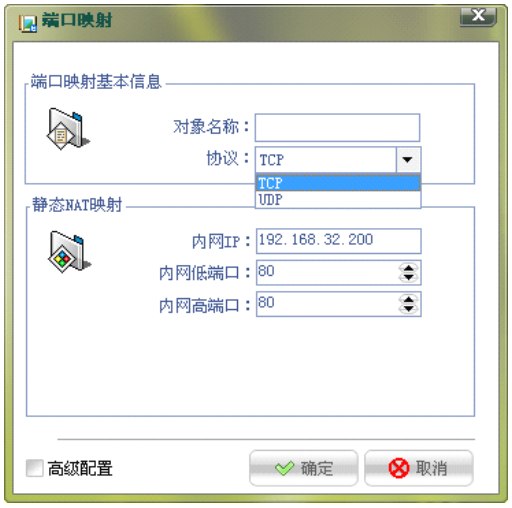


图 5.1.4 端口映射

例如，内网有一台 IP 为 192.168.32.200 的电脑要对外网提供 WEB 服务，所使用的端口为 80，那么我们的步骤为（见图 2）：

在[端口映射]中添加一条映射规则。[对象名称]可随便填写，便于标识。

<内网 IP 地址>：192.168.32.200，可选择<协议类型>为 TCP 或 UDP，[内网端口]为 80（0 代表所有端口）。

如果勾选<高级配置>，则可以进行更细化的设置。

图 5.1.4.1

<外网 IP 地址>设置为 WAN1 接口地址，<外网端口>为需要设定的服务端口。

一般对高级设置中的外网 IP，建议使用固定 IP 接入的才对使用，由于 ADSL 拨号的外网 IP 是动态获取的，不适合指定外网 IP。

5.1.5 通用防火墙

基于对象的防火墙是定义对象规则，利用封包的多样属性来进行过滤。对象类型有

三种：

时间对象——通过设置日期、时间段来定义对象；

地址对象——通过设置 IP 地址、IP 段或集合形式的地址组来定义对象；

服务对象——通过设置协议类型、源端口、目的端口号设定服务类型定义对象。

防火墙在以时间、地址、服务对象为准则，定义策略动作选择放行或阻止数据通过，从而达到访问控制。通过定义对象，可以灵活的定义出各种防火墙规则，来满足企业需求。

通用防火墙策略设置：选择已定义好的时间、地址、服务对象，选择策略动作，选用策略是否启动。

图 5.1.5 通用防火墙

5.1.6 高级配置

- **TCP 协议分片值**

此值设定 TCP/IP 协议传输数据报时的最大传输单元。MTU 值可以解决“部分网站打不开”、“上网速度慢”等问题，并且可以适当提升上网速度。但并不是数值越大越好，有可能会造成丢包，所以不是很明确该如何设置就已默认值（1350）。

- **连接数限制**

为了保护网络正常使用，建议配置每个中断的合法连接数，从而保证每个机器能够在异常状况下正常上网，如果配置为 0 标识不进行连接数限制。

设置方法：

1.可以全局设定所有 PC 的连接数（见图 1）：

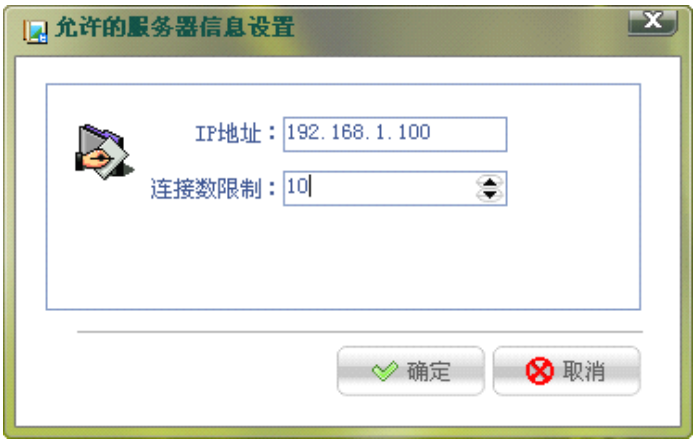


图 1

2.指定 IP 的连接数（见图 2）：

图 2

我们常用的操作系统 Windows，它的默认值为 10，微软这样做是为了防止蠕虫等病毒的传播。但限制了对点对点（P2P）协议数据传输的连接速度和下载速度。

5. 2 对象配置

对象主要是设定策略配置的条件准则。通过定义对象，满足对象条件的策略则受到访问和控制；一般对象和[通用防火墙]和[上网行为]等配合使用。

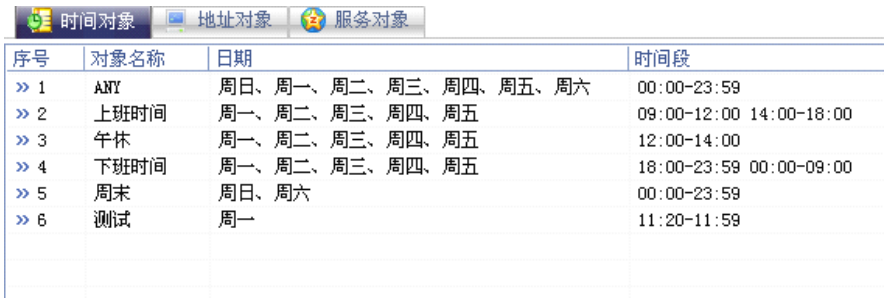
对象类型有三种：

时间对象——通过设置日期、时间段来定义对象；

地址对象——通过设置 IP 地址、IP 段或集合形式的地址组来定义对象；

服务对象——通过设置协议类型、源端口、目的端口号设定服务类型定义对象。

5.2.1 时间对象



序号	对象名称	日期	时间段
» 1	ANY	周日、周一、周二、周三、周四、周五、周六	00:00-23:59
» 2	上班时间	周一、周二、周三、周四、周五	09:00-12:00 14:00-18:00
» 3	午休	周一、周二、周三、周四、周五	12:00-14:00
» 4	下班时间	周一、周二、周三、周四、周五	18:00-23:59 00:00-09:00
» 5	周末	周日、周六	00:00-23:59
» 6	测试	周一	11:20-11:59

[时间对象]用于定义常用的时间段组合，然后在[通用防火墙]和[上网行为管理]等设置时，可以选择设置好的时间段定义，以设定这些规则生效或失效的时间。

点击添加按钮，出现对话框如下（如下图 5.2.1）：

图 5.2.1 时间对象

名称可以填写便于理解的文字，对应周期进行选择，然后添加时间段，点确定完成时间组的定义。

5.2.2 地址对象

[地址对象]是以 IP 地址为对象条件，可以选择设定添加好的地址对象、对象组定义，以设定这些对象生效或失效。

点击添加按钮，出现对话框（如下图 5.2.2）：

图 5.2.2 地址对象设置

对话框内可以填写对象的 IP 地址，这个对象可为一个地址，也可以是一个地址段（例如：192.168.5.0 255.255.255.0 或 192.168.5.120 255.255.255.255）。

也可以对让地址和地址段进行捆绑，以小组的形式作为对象。选择[地址对象组]，点击

添加按钮，出现对话框如下（如下图）：

选择对象目标，加入组，填写对象名称，确定即完成添加对象组设置。

5.2.3 服务对象

先在[服务对象]模块中定义各种防火墙，包括服务所使用的端口和协议，然后根据已定义了的服务来确定防火墙过滤规则或控制管理中根据已定义的服务来确定上网权限。

界面如下图：

序号	对象名称	协议信息	源低端口	源高端口	目的低端口	目的高端口
» 1	ANY	TCP	1	65535	1	65535
» 2	HTTP	TCP	1	65535	80	80
» 3	DNS	UDP	1	65535	53	53
» 4	HTTPS	TCP	1	65535	443	443
» 5	SMTP	TCP	1	65535	25	25
» 6	SMTP_SSL	TCP	1	65535	465	465
» 7	POP3	TCP	1	65535	110	110
» 8	POP3_SSL	TCP	1	65535	995	995
» 9	Telnet	TCP	1	65535	23	23
» 10	SSH	TCP	1	65535	22	22
» 11	远程桌面	TCP	1	65535	3389	3389
» 12	FTP	TCP	1	65535	21	21
» 13	TCP1863	TCP	1	65535	1863	1863
» 14	网管之星	TCP	1	65535	50253	50254
» 15	TAS设备管理器	TCP	1	65535	50100	50100
» 16	UDP_1701	UDP	1	65535	1701	1701
» 17	TCP_1720	TCP	1	65535	1720	1720
» 18	TCP_1723	TCP	1	65535	1723	1723
» 19	UDP_500	UDP	1	65535	500	500
» 20	UDP_4500	UDP	1	65535	4500	4500
» 21	fff	UDP	1	65535	1	65535

点击添加按钮，弹出新增服务对话框如下所示（如下图）：

图 5.2.3 服务对象设置

对象名称可填写便于理解的文字，选择服务用到的协议，支持 TCP、UDP。选好协议后，填写源端口号和目的端口号。

5.3 防火墙日志

NETSYS AC 日志包括[防火墙日志]、[应用层日志]和[连接跟踪表]，如下图：

图 5.3 NETSYS AC 网关日志

网络阻断日志含有“通用防火墙”、“未通过认证”、“超过连接数限制”、“入侵日志”四项日志。“通用防火墙”策略添加启用后，相关行为在日志里才会保留；同样安装客户端的电脑，才会在未通过认证界面显示信息；当启用连接数限制时，日志会保留超过连接数的终端信息。应用层日志也是对应用层所记录相符的选择进行过滤保留。

5.3.1 连接跟踪表

连接跟踪表主要作用面向管理者维护设备时，方便查看 NETSYS AC 设备与外网连接的终端的详尽信息。

5.4 快速配置

一般情况下上班时间只允许上网页和发邮件，下班后不限制；对于某个 IP，比如老板机器，则不限制。具体的配置，老板的 IP：192.168.1.88；

配置地址对象：

序号	对象名称	IP地址	掩码
» 1	ANY	0.0.0.0	0.0.0.0
» 2	老板	192.168.1.88	255.255.255.255

配置时间对象：

序号	对象名称	日期	时间段
» 1	ANY	周日、周一、周二、周三、周四、周五、周六	00:00-23:59
» 2	上班时间	周一、周二、周三、周四、周五	09:00-12:00 14:00-18:00
» 3	午休	周一、周二、周三、周四、周五	12:00-14:00
» 4	下班时间	周一、周二、周三、周四、周五	18:00-23:59 00:00-09:00
» 5	周末	周日、周六	00:00-23:59

配置服务对象：

序号	组对象名称	组对象成员
» 3	上网发邮件	HTTP, HTTPS, SMTP, SMTP_SSL, POP3, POP3_SSL

防火墙配置

序号	时间对象	源地址对象	目的地址对象	服务对象	策略动作	是否生效
» 1	ANY	老板	ANY	ANY	允许	是
» 2	上班时间	ANY	ANY	上网发邮件	允许	是
» 3	上班时间	ANY	ANY	ANY	拒绝	是
» 4	ANY	ANY	ANY	ANY	允许	是

1. 允许老板在任何时间都可以上网。

2. 允许其它员工上班时间只可以上网，收发邮件。

3. 禁止其它员工在上班时间做除上网，收发邮件外的动作。

其它时间不做限制。

6 VPN

VPN（虚拟专用网络）我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆之类的物理线路，主要应用环境如下：

1. 企业的各个分支机构的互联——各个分支地点直接通过设备到设备的互联，将企业不同地点的网络虚拟成一个局域网，这样实现异地互联，使一些应用软件能够跨 Internet 共享 。

2. 单个计算机到企业总部的互联（称为移动客户端）——单个用户的 PC 机，需要连接到总部，使用总部内部资源，或者满足某些应用软件的需要，必须把这个 PC 虚拟到企业网络内部。

对于设备到设备的 VPN 应用，NETSYS AC 提供 VPN 网络互联，用户可以方便的根据自己的网络情况，来实现 VPN 的建立和监控。

6. 1 功能配置说明

NETSYS AC 设备配置 VPN，分中心点设备和节点设备。型号匹配 AC100 以上设备支持 VPN 中心点和节点设置，AC50 和 AC70 只支持节点配置。中心点和节点在配置界面中也有所不同，型号 AC100 以上比 AC50、AC70 在界面中多隧道监视、分支节点、隧道配置、管理日志等配置模块。这些功能也只有当设备在 VPN 中作中心点时才需要使用。

下图为中心点和节点设备配置界面：

AC100 以上型号：

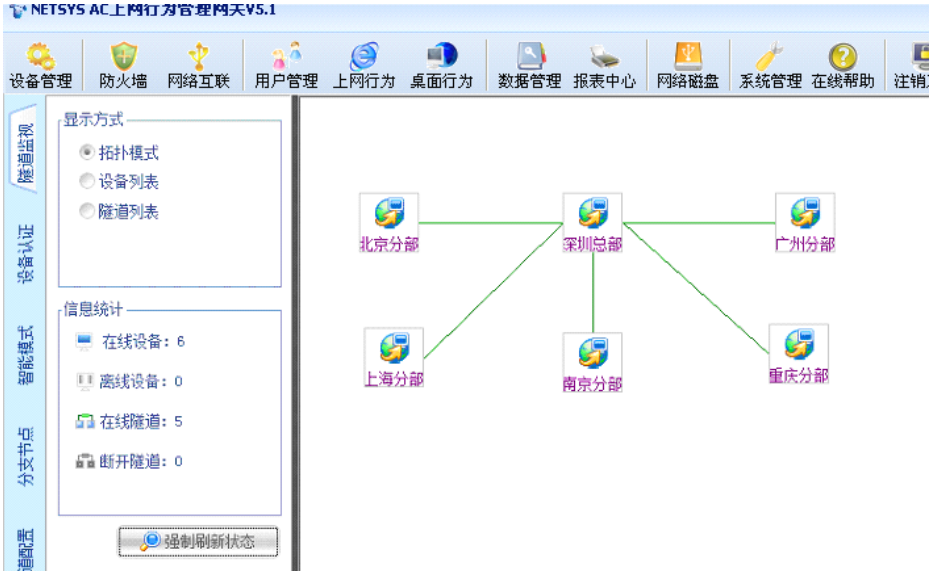


图 6.1 VPN 中心点界面

在界面中可以看到以下模块：[隧道监视]、[设备认证]、[智能模式]、[分支节点]、[隧道配置]、[日志管理]、[移动客户端]。

AC70 以下型号：

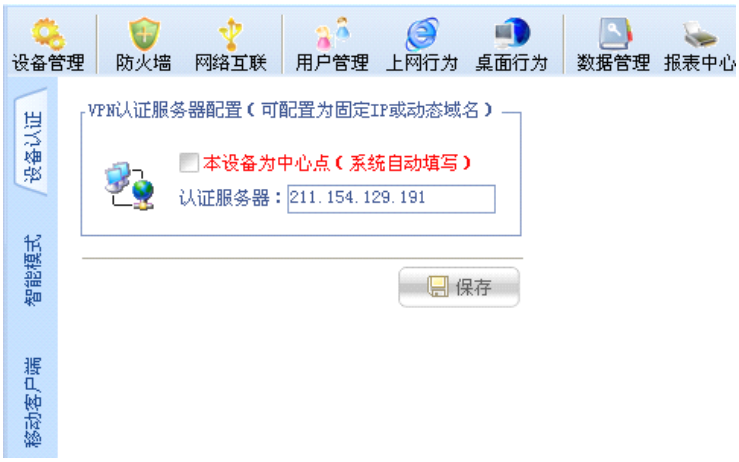


图 6.1.1 VPN 节点界面

所有配置界面中如果有[保存]按钮，则配置完毕后一定要点击按钮才能把配置保存至设备中。本章会涉及到“设备序列号”，<设备序列号>除了在设备背面的贴标可查询，也可以在“NETSYS AC 系统”[在线帮助]下[授权信息]内查询。

设备名称： test
设备序列号： 31100137
最大终端个数： 200
设备试用有效期至： 2011-04-29
设备型号： AC300

6.2 隧道监视

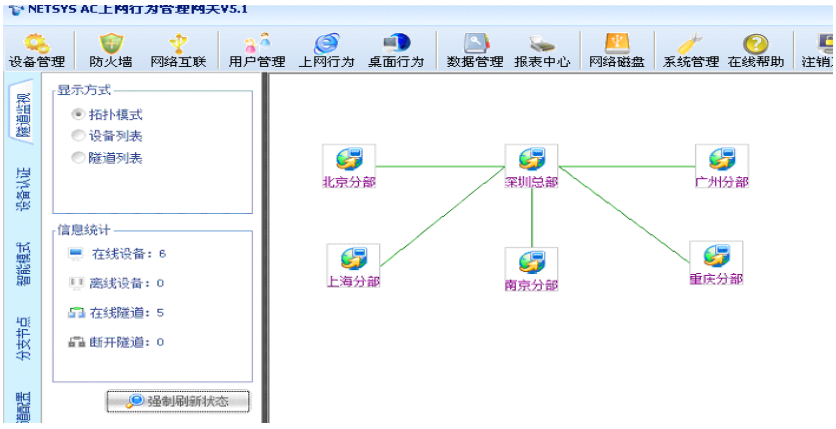


图 6.2 隧道监视

用于查看 VPN 隧道建立的状态。隧道监视状态显示方式包括：拓扑模式、设备列表、隧道列表。下面对显示方式做简要说明：

拓扑模式—— VPN 隧道成功建立后，以拓扑图的形式描述虚拟网的网络结构；

设备列表——虚拟网络内成功连接隧道的设备信息登陆在列表中；

隧道列表—— VPN 隧道建立后，设备之间的隧道信息都登陆在该列表中。

- **信息统计**

统计信息可以方便查看到虚拟网络内在线/离线设备，在线/断开隧道的总数量；通过按钮还可以即时地刷新状态信息。

界面下方显示设备和隧道连接/断开状态。

6.3 设备认证

VPN 建立时我们首先要设置 VPN 认证服务器。作用是让设备和设备之间通过密钥指令获取互相的认证信息。在设置中，一般以核心设备为中心点，只需勾选启用即可；分支机构的设备为节点，设置中心点的外网固定 IP 或者动态域名。

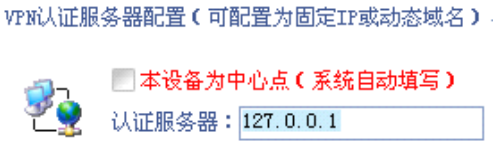


图 6.3 设备认证

6.4 智能模式

中心点需要共享子网段的资源给分支节点，并且网络存在多个网段的情况，那我们可以在智能模式下通过启用<启动子网共享支持>功能，然后添加需要共享的网段。

网段可以手动逐个添加，也可以通过已配置的所有网段从中选取需要共享的网段。

图 6.4 智能模式

6.5 分支节点

分支节点界面是建立 VPN 的节点设备添加设置的功能。

设置方法：在对话框中设置<设备序列号>即设备 ID、<设备名称>、<备注信息>。

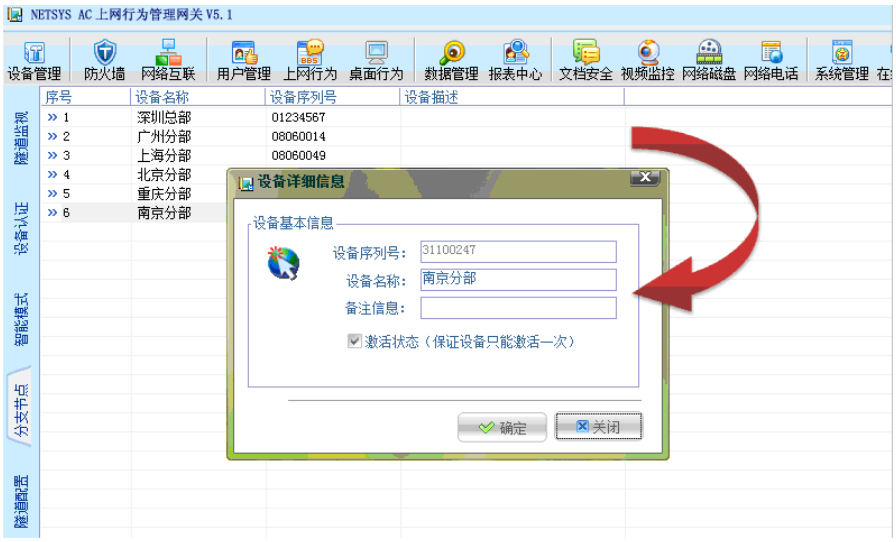


图 6.5 分支节点

6.6 隧道配置

NETSYS ACVPN 隧道建立是基于设备序列号相互间的认证。通过设置节点设备的序列号和标识以达到点对点之间建立。

界面的下方显示 VPN 隧道建立后的拓扑图。方便管理员查看和管理虚拟专网中各节点设备以及编辑网络拓扑图。

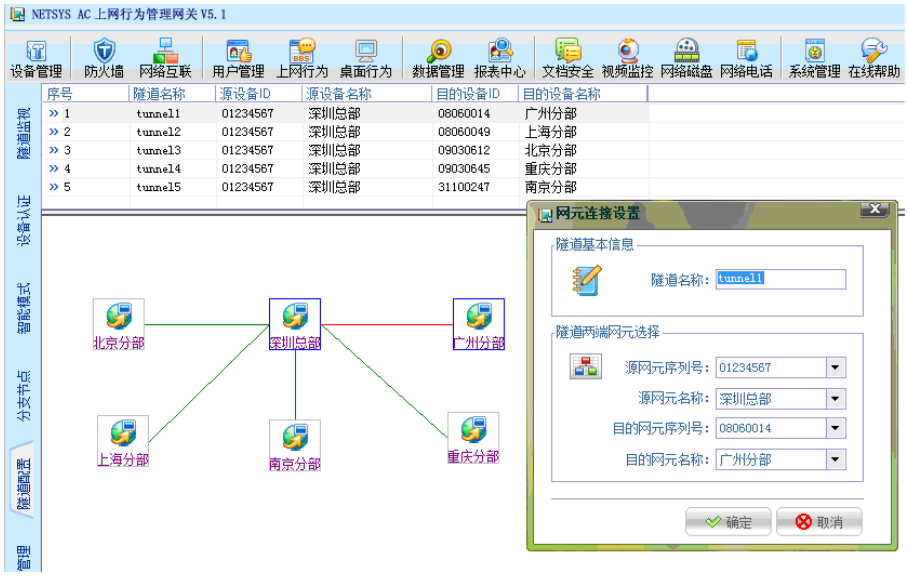


图 6.6 隧道配置

6.7 日志管理

用于查看设备的状态日志。

选择要查看的日期，会显示相应时间的日志记录。

序号	设备名称	设备序列号	变更时间	设备状态
1	重庆分部	09030645	2009-07-06 00:05:53	设备断线
2	重庆分部	09030645	2009-07-06 00:06:05	设备上线
3	重庆分部	09030645	2009-07-06 08:44:12	设备断线
4	重庆分部	09030645	2009-07-06 08:44:42	设备上线
5	深圳总部	01234567	2009-07-06 08:45:12	设备断线
6	深圳总部	01234567	2009-07-06 08:45:28	设备上线
7	上海分部	08060049	2009-07-06 09:21:29	设备上线
8	广州分部	08060014	2009-07-06 09:21:31	设备上线
9	北京分部	09030612	2009-07-06 09:21:32	设备上线
10	南京分部	31100247	2009-07-06 09:22:08	设备上线
11	南京分部	31100247	2009-07-06 09:23:09	设备断线
12	南京分部	31100247	2009-07-06 09:23:25	设备上线
13	南京分部	31100247	2009-07-06 09:24:25	设备断线
14	南京分部	31100247	2009-07-06 09:24:41	设备上线

图 6.7 日志管理

6.8 移动客户端

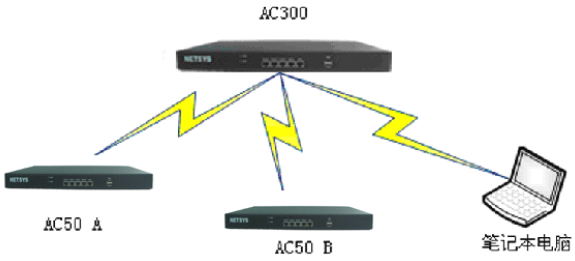


图 6.8 移动客户端

员工在外办公需要使用到公司内部资源时，需要使用 VPN 连接到公司内部，此时用户需要在电脑上启动<移动客户端>和公司专网进行连接。

6.8.1 接入监控

显示移动办公用户连接 VPN 的申请请求和信息。同样管理员也可以允许/禁止用户接入 VPN。

6.8.2 接入配置

1. [IP 地址池]是指由 NETSYS AC 指定设备内网中空闲的一段 IP 作为移动用户接入时的虚拟 IP。当移动用户介入后，分配一个虚拟 IP 给移动用户，移动用户对总部的任何操作都是以分配的 IP 作为源 IP、就完全和在总部局域网内一样。

2. 如果总部网络只有一个网段，移动客户端可以访问的网段默认就是这个网段，如果存在多个网段，则需要配置允许移动客户端可以访问的网段。

6.8.3 发布授权

管理员通过发布文件或者 UKey 给予移动用户使用权限。基本配置里只需要填写发布人的名称、备注、序列号和拨号地址或域名。高级配置是给发布人拨号时添加策略，1.是否“禁用拨号终端进入互联网”、2. 是否“拨号终端绑定 MAC”。

<禁用拨号终端进入互联网>是禁止移动用户的 PC 访问 Internet；

<拨号终端绑定 MAC>是绑定移动用户的 PC 的 MAC 地址。

6.9 VPN 配置实例

- **VPN 中心点配置**

1. 首先在[分支节点]界面下添加需要做 VPN 的设备；

图 1

2. 启用认证服务器，让设备为 VPN 中心点；

图 2

3. 在[隧道配置]里单击右键，单击[申请拓扑编辑]，框选所有设备右键，选择自动建立拓扑结构（网状、星状）。

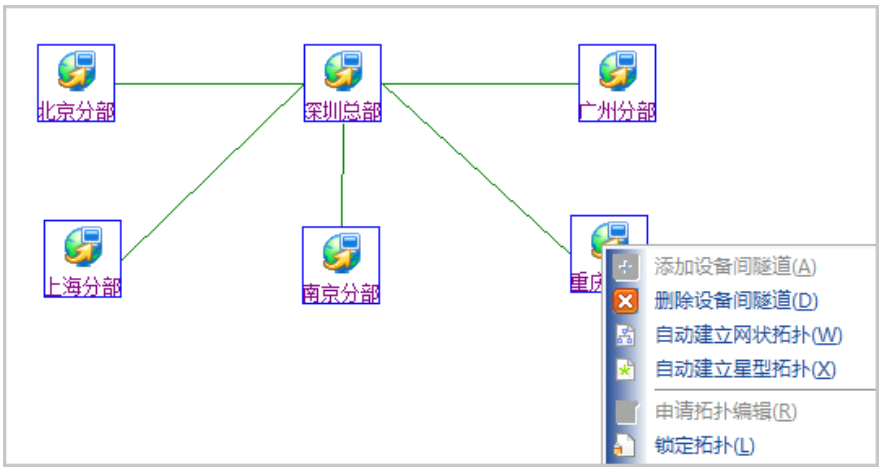


图 3

4. 点击添加把要创建的设备分别选上，如总部，分部, 添加隧道名称 tunnel1（注意：隧道名称需要是英文、数字的）。

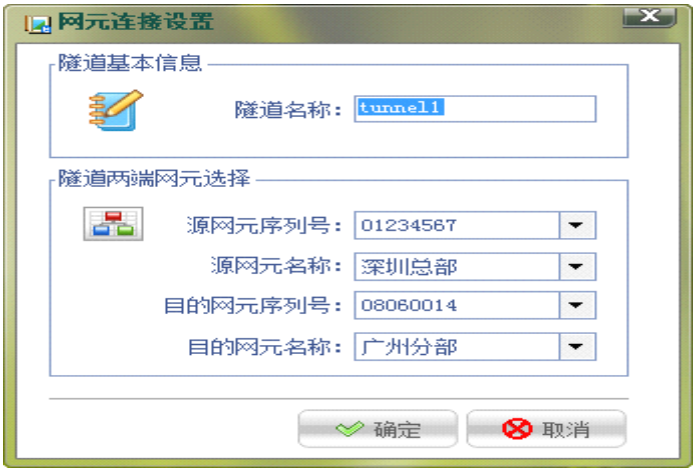


图 4

中心点配置完成。

- **VPN 节点配置**

1. VPN 认证服务器配置下，填写 VPN 中心的地址；

2. 其它设置与中心点相同，只要设置本节点相应信息即可与中心点建立 VPN。

实现 VPN 互联的网络内网地址不能是同一个地址段。比如：总部的地址是 192.168.1.0/24 的地址分部的地址就不能是这个地址，可以是 192.168.2.0/24,也可以是 10.0.0.0/24。如果是同一地址段，VPN 建立后，会导致设备无法上网。对于多个网段的网络，也存在同样的问题，互通的网段中，两个网络的地址段不能冲突。

7 用户管理

用户管理界面主要提供添加用户、选择认证模式给予用户授权，可以为授权用户设置上网行为管理、桌面行为管理，使用户有访问网络资源的权限。

NETSYS AC 提供企业→部门→员工的二层逻辑层次管理模式。一般情况，可以为企业设置详细信息、添加部门、将企业所要管制的员工通过手动添加编辑其中，同时需要填写员工的基本信息（从属部门、姓名、工号、联系电话、Email）和选择认证模式进行捆绑。

7. 1 用户类型

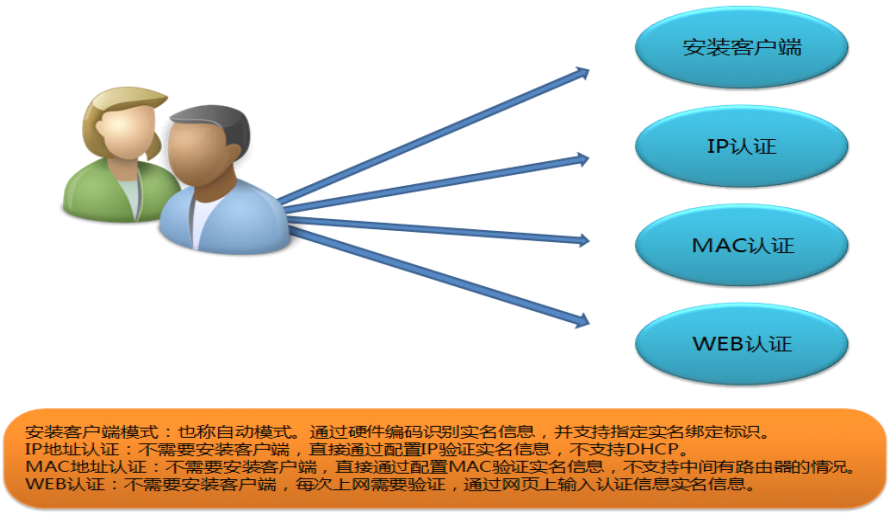


图 7.1 用户类型

7.1.1 用户认证方式

安装客户端模式——需要在计算机上安装客户端，可以对计算机最全面的管理和基于用户使用计算机的权限。

IP 地址认证模式——该网络环境使用手动分配 IP 地址，如果企业不想为计算机安装客户端，可以选择 IP 地址认证模式，通过该用户与配置该 IP 地址的计算机进行绑定，也能达到管理计算机和给予用户使用计算机的权限。此认证模式不适合使用 IP 地址动态分配（DHCP 服务器/DHCP 中继）的网络，由于动态分配 IP 地址无法与指定用户进行捆绑。

MAC 地址认证模式——通过获取计算机网卡的 MAC 地址和指定用户捆绑的验证模式。此认证模式适合只有一个网段的网络环境，如果网络中含有多个网段的情况，将无法使用 MAC 地址认证模式。

WEB 认证模式——该模式是用户通过以网页形式输入用户名和密码验证的方式，此模式较为适合移动办公用户。

使用安装客户端模式，可以对该计算机进行最全面的管理操作，至于选择 IP、MAC、WEB 认证模式的计算机，只能得到[网络审计]、[视频监视]、[网络功能]、[网络日志审计]的管理操作，所以按照企业的需求，选择合适自己的管理方式，从而得到更为有效的结果。

企业可以根据实际需求，选择认证模式，下表为客户端的安装、不安装的功能对比：

功能列表		安装客户端	不安装(IP,MAC,WEB)
日志审计	实时监视	√	×
	屏幕录像	√	×
	聊天日志	√	×
	工作业绩日志	√	×
	资产告警日志	√	×
	文件操作日志	√	×
	详细工作日志	√	×
	详细工作日志	√	×
	记录QQ,MSN传文件传输日志	√	×
网络审计	上载文件限制	√	√
	应用层过滤	√	√
	URL 过滤	√	√
	论坛言论限制	√	√
文档加密	文档加密	√	×
视频监视	视频监视	√	√
网络功能	网络诊断	√	√
	带宽控制	√	√
	企业防火墙	√	√
	VPN	√	√
资源审计	终端资产管理	√	×
	资产变更告警	√	×
本地日志审计	屏幕录像查看	√	×
	聊天记录	√	×
	工作业绩	√	×

	上下线日志	√	×
	屏幕录像查看	√	×
	聊天记录	√	×
	文件操作日志	√	×
	文件传输日志	√	×
	进程审核	√	×
网络日志审计	上网日志	√	√
	WEB 邮件	√	√
	POP/SMTP 日志	√	√

表 7.1.1

7.2 修改企业信息

该界面主要是更改企业名称，选择企业背景图。设置方法如下：

图 7.2 修改企业信息

【1】 编辑企业名称
【2】 更改企业背景图（当桌面行为实时监视使用拓扑管理时生效）
【3】 办公位置图样例(单击图也可以更改背景图)
【4】 把企业背景图上传到 NETSYS AC(通过同步图片信息可以更换拓扑)

7.3 添加企业部门

企业内有多个的部门，划分部门主要是企业员工的工作职责不同。该界面主要添加企业

部门以至于部门员工的归属，设置方法如下：

点击[用户管理]→[部门配置]→右下角[添加]→弹出[部门配置]对话框，将信息填写完整，也可以更改部门背景图：

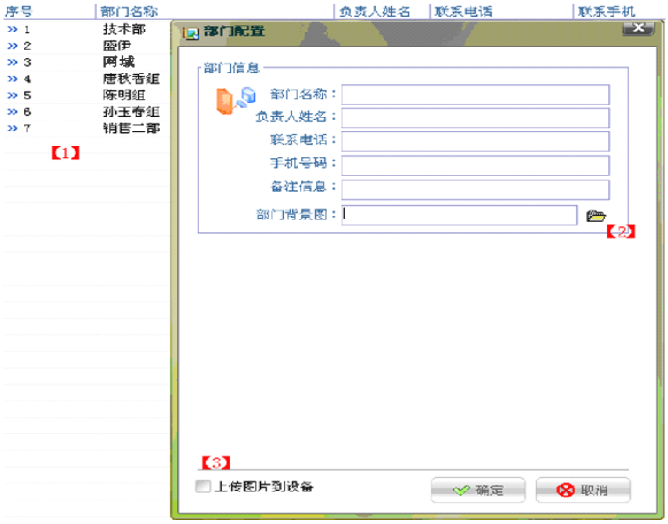


图 7.3 添加企业部门

【1】 已添加的部门信息

【2】 修改部门背景图（当桌面行为实时监视使用拓扑管理时生效）

【3】 打勾上传图片到设备

7.4 手工添加员工

如果需要对企业员工进行信息录入，可以通过手动添加用户，在添加过程中主要遇到的就是员工基本信息的填写，选择认证模式，实名绑定等设置。

如果要对已设置好的对象进行编辑，可以点击右下角的[修改]，这里弹出的对话除了对象姓名无法修改以外，其余的信息都能更改。

如果要删除对象，选择对象点击右下角的[删除]。

图 7.4 手工添加员工

【1】选择新添加员工所属的部门

【2】双击此处修改员工头像（照片）

【3】选择认证模式

【4】在使用客户端认证模式下，选择实名绑定的类型

7.4.1 自定义格式导入

当企业的电脑多达数百台的时候，一个个地手动添加员工明显很繁琐、费时。这样我们可以通过“自定义格式导入”功能添加。首先我们点击“自定义格式导入”按钮，弹出对话框后点击“运行采集工具”启动“局域网查看工具”（如下图）。

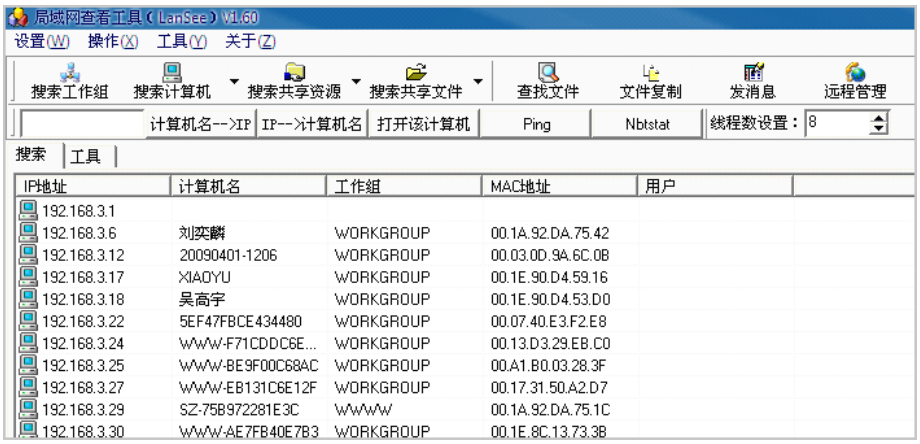


图 7.4.1 导入工具

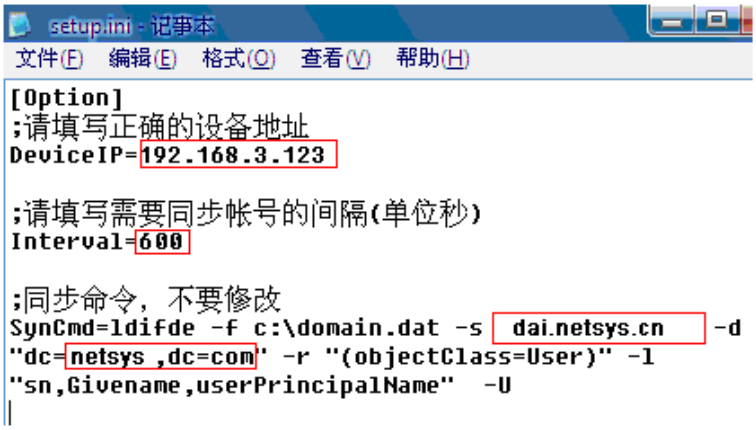
点击搜索计算机，工具会搜索网段内所有在线的 PC，扫描完毕后右键点击保存搜索列表。再返回 NETSYS AC“自定义格式导入”对话框点击“打开”选择保存的列表（如下图）：

选择导入后的用户，修改部门、姓名以及选择认证模式，完成自定义导入。

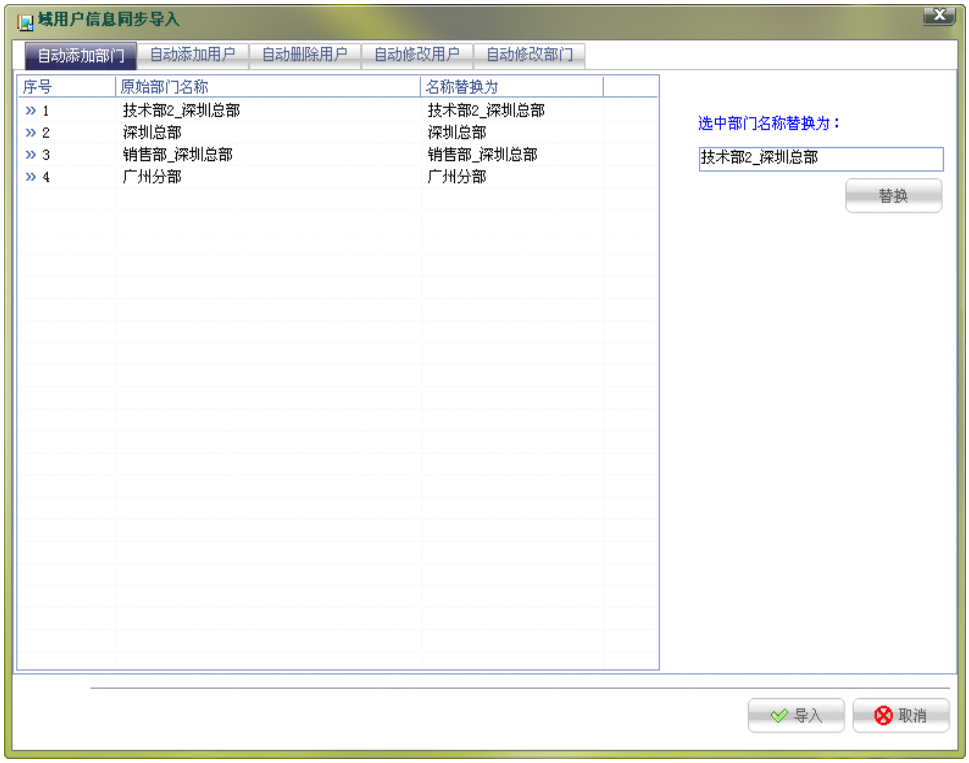
7.4.2 域用户手工同步

[域服务器同步]用户将 LADP 服务器的用户和组织结构同步到 NETSYS AC 中，可以实现 LDAP 服务器上的用户和组织结构自动同步，此功能只支持微软的 Active Directory。

设置方法：在域服务器上安装“域服务器同步”，在启动程序前需要修改 setup.ini 配置（设备地址，同步帐号的间隔，域服务器计算机名和域的名称）；修改完后启动 DomainService.exe（如下图）。



管理员登陆 NETSYS AC 点击“域用户手工同步”，弹出对话框（如下图）：



“导入”完成域内用户信息登陆。

7.5 修改用户姓名

在管理过程中经常会遇到员工工作位置变动，员工离职等情况，那么该用户不再会使用与其捆绑的计算机，新用户使用计算机时，又要重新添加除了用户名不同，其余设置相同的操作，这时可以通过更改用户名来简便添加新用户的操作过程。

用户姓名作为 NETSYS AC 整个系统关键索引信息，修改用户姓名将删除所有保存在 NETSYS AC 内的相关用户日志信息，所以要特别注意。相关设置：

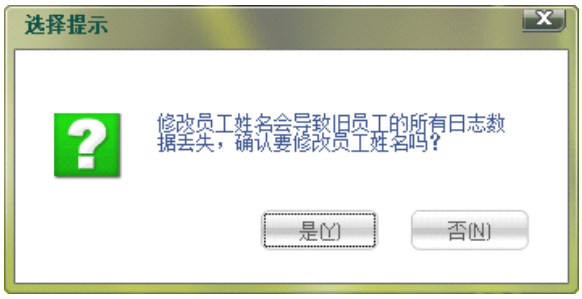


图 7.5 修改用户姓名

7.6 新认证用户

当没有配置员工信息，直接在员工机器安装主机加固时，员工机器相关的信息就会上报到新认证用户列表中，管理人员可以对等待申请的用户进行编辑，将其生成为员工。其操作过程与添加新用户类似。

序号	申请时间	计算机名称	MAC地址	计算机IP
» 1	2009-05-22 16:14:17	20090309-1659	00-05-4E-46-AF-70	192.168.3.102
» 2	2009-05-22 16:14:17	kh-978688c4...	00-16-D3-C8-42-D3	192.168.3.238
» 3	2009-05-22 16:14:17	20090309-0851	00-19-E0-75-AA-63	192.168.1.111
» 4	2009-05-22 16:14:17	cstd-user	00-1D-0F-0C-4A-07	192.168.3.141
» 5	2009-05-22 16:14:17	cstd-user	00-1E-8C-02-C5-80	192.168.3.141
» 6	2009-05-22 16:14:17	ecde440cf01...	00-1E-90-D4-3C-A3	192.168.2.170
» 7	2009-05-22 16:14:17	20081205-1809	00-50-56-C0-00-01	10.10.10.1

图 7.6 新认证用户

设置方法：

点击[生成员工]，弹出员工基本信息[对话框]，填写基本信息和实名绑定

7.7 免监控 IP

企业网络内有一群用户是无需对其进行行为监控等控制，那么可以将这类用户的 IP 地址添加进免监控列表中。（免监控用户姓名不得与已有的员工姓名重复）

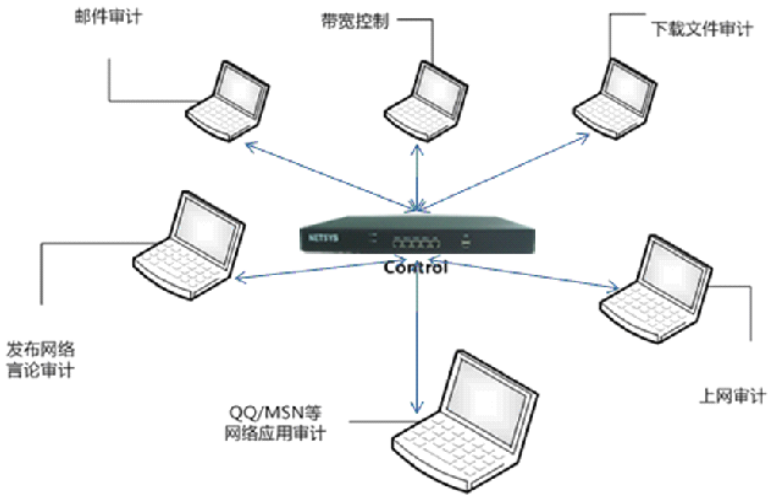
点击[添加]→填写用户名称和 IP 地址，确定后在列表中生成该免监控用户的信息

7.8 认证定制

该功能的主要意义是可以人性化定制企业上网认证提示页面，可以设置网页标题、公司版权信息、点击下载上网验证终端提示的文字，网页的总体背景图，企业 LOGO 图片。

图 7.8 企业认证定制

8 上网行为管理



目前，互联网已经成为企业高效运营，提高企业竞争力的平台。互联网的开放性、交互性、延伸性、廉价性为人们快速获得知识，即时沟通，跨地域的业务往来提供了极大的便利。但是，廉价的互联网资源也给企业网络带来如下的风险：

网络堵塞：企业不注重网络管理，带宽严重消耗，核心应用得不到应有的保障。

病毒泛滥：员工不经意地传播病毒、蠕虫、木马等恶意代码导致网络瘫痪，严重影响网络的正常使用。

工作效率降低：互联网丰富的内容总是在分散员工注意力，炒股、聊天、购物、游戏、与工作无关的视频、语音、图片、文档的上传和下载，导致员工工作效率下降。

信息泄密：通过 MSN、QQ 传文件、外发邮件等方式，导致内部机密信息泄漏，给企业带来巨大损失。

员工不当的网络行为引发的诸多问题，对企业网络带来巨大的影响，甚至威胁到企业的生存。所以对员工的网络行为进行有效、统一的管理对企业刻不容缓，如何有效的规范员工的网络行为呢？

“NETSYS AC”系列产品包含上网行为管理功能，为企业规范员工的网络行为提供一套有效的解决方案。比传统的防火墙、入侵检测系统、邮件防御系统更具有优势不但能对外网攻击进行防御，而且能对内网的员工的上网行为进行有效的管理，能让企业随时了解员工的网络行为。

8. 1 文件过滤

互联网上的共享资源非常丰富，数之不尽。员工经常会在网上下载各式各样的文件，不知不觉地把病毒、木马等恶意程序下载到本地计算机，从而导致计算机崩溃、数据遗失的损失。NETSYS AC 通过对文件后缀名定义配置，限制用户下载匹配定义策略的文件。

8.1.1 文件后缀对象

文件后缀对象主要是抓取文件的类型，通过文件名后缀识别文件类型在审计策略中限制了用户下载文件的类型。默认出厂时已在对象中添加常用的后缀对象，企业还可以按自己的需求自行添加。设置方法：点击[添加]按钮，在对话框中配置文件的类型，后缀定义和后缀解释。

序号	后缀分类	后缀定义	后缀解释
1	执行文件	.exe	EXE文件
2	执行文件	.bat	BAT文件
3	压缩文件	.rar	rar文件
4	压缩文件	.zip	zip文件
5	压缩文件	.tgz	tgz文件
6	压缩文件	.tar	tar文件
7	压缩文件	.gz	gz文件
8	压缩文件	.bz2	bz2文件
9	镜像文件	.iso	ISO文件
10	镜像文件	.img	IMG文件
11	音频文件	.wav	WAV文件
12	音频文件	.mp3	MP3文件
13	音频文件	.ogg	OGG文件
14	音频文件	.mpc	MPC文件
15	音频文件	.wma	WMA文件
16	音频文件	.ape	APE文件
17	视频文件	.avi	AVI文件
18	视频文件	.mpeg	MPEG文件
19	视频文件	.mov	MOV文件
20	视频文件	.asf	ASF文件
21	视频文件	.wmf	WMF文件
22	视频文件	.rm	RM文件
23	视频文件	.rmvb	RMVB文件
24	视频文件	.3gp	3GP文件
25	视频文件	.amv	AMV文件

图 8.1.1 文件后缀对象

8.2 网页过滤

Web 是互联网上内容最丰富、访问量最大的应用，但是网页内容有许多反动、暴力、色情以及其它不健康的信息。这样的网页有可能携带病毒、恶意软件，为内网用户带来安全风险。NETSYS AC 通过预分类 URL 策略模版设置，对违反国家法律、危害企业安全的内容进行过滤，避免用户有意无意访问包含非法内容的网页，净化网络，减少病毒进入局域网的几率，降低企业法律风险，创造文明健康的上网环境。

8.2.1 网址审计对象

网址审计对象主要是禁止用户访问互联网的某些网站，通过 URL 过滤在审计策略中阻止用户访问。默认出厂时已在对象中添加了对象，企业还可以按自己的需求自行添加。设置方法：点击[添加]按钮，在对话框中配置相关属性。

图 8.2.1 网址审计对象

8.3 应用层过滤

现今，各种互联网应用层出不穷，如即时通讯、网络游戏、在线炒股以及在线音乐视频等等。未加管理的使用，不可避免地影响员工的工作效率。这些不当的网络活动大大降低了员工的工作效率，造成了企业人力资源的严重浪费。因此我们通过 NETSYS AC 的应用层过滤，有效地限制了员工上班时间使用各种影响工作效率的应用程序。

8.3.1 应用层策略对象

应用层策略对象主要是禁止用户使用指定软件，通过软件特征过滤在审计策略中阻止用户使用。默认出厂时已在对象中添加了对象，企业还可以按自己的需求自行添加。设置方法：点击[添加]按钮，在对话框中配置相关属性。

图 8.3.1 应用层策略对象

8. 4 审计策略模版和配置

上网审计基于审计模版定义各项策略，启用限制、过滤等策略动作。模版配置有以下五个功能 ：

8.4.1 下载文件限制

通过对指定文件的后辍名进行过滤下载链接地址（如下图 8.4.1）；

图 8.4.1 下载文件限制

8.4.2 网络应用层过滤

通过对网络应用程序的数据包做分析，提起特征码的进行过滤屏蔽特定应用。这个屏蔽只能是对网络应用程序（如下图 8.4.2）；

图 8.4.2 网络应用层过滤

8.4.3 URL 过滤

分为黑白单模式（对指定的网址进行屏蔽）和白名单模式（对指定的网址允许上网，其它网址屏蔽），支持网址模糊匹配（如下图 8.4.3）；

图 8.4.3 URL 过滤

8.4.4 论坛言论过滤

通过屏蔽搜索引擎关键字和论坛关键字来过滤。关键字需严谨匹配，其中不能包含空格或其它字符，否则过滤不生效（如下图 8.4.4）；

图 8.4.4 论坛言论过滤

8.4.5 日志审计

查看记录的上网日志、网页发送邮件、邮件工具的接送记录（如下图 8.4.5）。

图 8.4.5 日志审计

8. 5 带宽控制

目前，企业经常反映网速慢的问题，集中反映在企业网络应用过程中，发送邮件，企业 OA, ERP 或者财务系统等应用中。网络应用对带宽资源的占用也越来越高，特别是以 P2P 为代表的下载软件，如果不加限制，会严重消耗企业的带宽资源，从而影响正常的业务数据的传输。NETSYS AC 支持针对用户的带宽分配与流量管理。

在启用带宽控制功能后，企业网络就可以得到一个良好的上网环境，网络业务都可以正常的使用。但是对于企业的某些特定应用或者特定的人群，NETSYS AC 同时提供带宽控制和带宽保证的功能来实现。带宽控制和带宽保证，是为了保证特定应用的带宽需要来设计的。比如：企业的某个服务器是对外开发的，必须保证这个服务器的带宽，或者，企业的财务软件需要保证带宽等，这样的应用就可以通过带宽保证来实现，从而让企业的网络更好的服务企业应用需求。

8.5.1 带宽配置

打勾启用带宽控制，只有启用带宽控制，对带宽控制所配置策略才能生效。启用带宽控制后，NETSYS AC 会实现基于 IP 的流量转发，保证网络中用户都可以比较好的上网，消除 P2P 等软件造成的应用造成的网络带宽占用的不公平性。

必须启用带宽控制并且正确配置上行、下行带宽，否则在上网行为配置的带宽控制全部失效。带宽单位为 KB，电信等运营商提供的都是 Kbit。例如：电信标准上行带宽 512Kb=512/8KB。

<突发流量优先处理>是 NETSYS AC 针对突发流量的网络应用的优化处理，比如上网，在每次打开网页的时候产生一个比较大的流量，在不点网页的时候，没有网络流量。针对这种应用，NETSYS AC 可以优先转发，保护这类网络应用的速度优先。打勾表示启用此功能 。

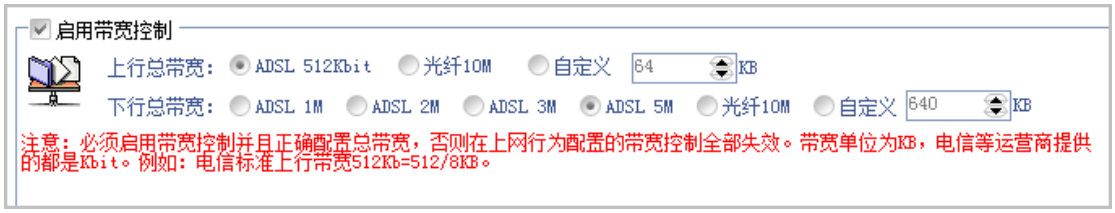


图 8.5.1 带宽配置

8.5.2 员工策略

可以对用户进行策略设置，分配网络带宽，从而使用户、服务、业务等用网需求得到保障。

带宽限制——对某些 IP 或者应用的数据流量做限制，限制后流量不得超过限制数值。

带宽保证——对某些 IP 或者应用的数据流量保证带宽，如果被保证的用户使用网络，带宽流量可以达到保证的带宽数值，如果该用户没有占用带宽，带宽会被其他的用户使用。

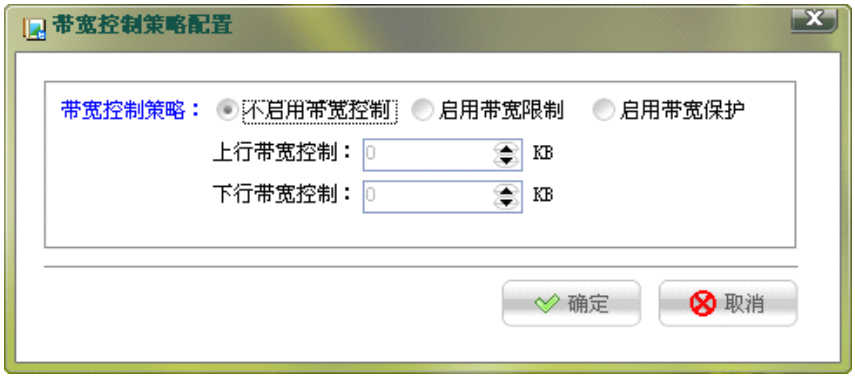


图 8.5.2 带宽控制策略配置

8.5.3 高级策略

高级策略设置主要还是带宽的限制和保证进行配置。点击添加按钮，在对话框中添加本端IP

地址段、目的IP地址段、目的端口、上行带宽和下行带宽。

图 8.5.3 高级策略界面

高级策略中，配置上行、下行带宽时，设置的数值为一个总量，即1个IP分配下行100KB，此时该IP所拥有的下行总带宽为100KB；如果一个IP地址段，开始地址192.168.1.200，结束地址192.168.1.210，分配下行500KB，那么这个地址段的下行带宽总量为500KB，即一个IP为50KB带宽（如下图）。

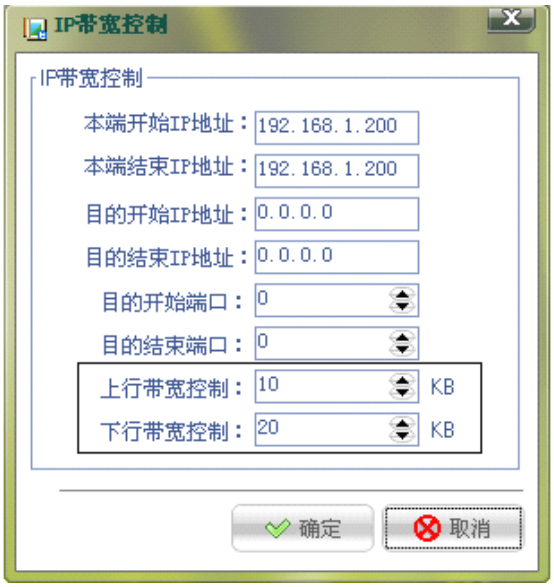


图 8.5.4 IP 带宽控制配置对话框

8.6 流量监视

基于每个用户进行流量监控，通过直观的走势图展现流量，使网络流量完全透明可视。同时，通过提供快捷的视图为管理员展示异常流量的原因，更改终端速率限制，同时提供限制、保证终端带宽，为快速消除网速缓慢提供有力的保障。

8.6.1 终端实时流量

监视网络内部用户的流量，以曲线图的显示方式实时的采集用户终端数据流量。可以选择监视用户对象，采样周期，也可以通过配置设置对象的带宽等设置（如下图 8.6.1）。

序号	终端员工	终端IP	采集次数	发流量(K)	收流量(K)	当前发(K)	当前收(K)	平均发(K)	平均收(K)	最大发(K)	最小发(K)
19	戴	192.168.3.111	41	595.72	8.44	0.00	0.00	14.53	0.21	590.01	0.00
20	柳	192.168.3.112	41	5.43	6.24	0.07	0.17	0.13	0.15	2.10	0.00
21	盛	192.168.3.114	41	783.04	1.94	0.00	0.00	19.10	0.05	782.66	0.00
22	潘	192.168.3.118	41	0.13	0.24	0.00	0.00	0.00	0.00	0.07	0.00
23	192	192.168.3.119	41	1.20	2.68	0.00	0.00	0.03	0.06	0.28	0.00
24	孙	192.168.3.140	41	7.76	13.66	1.20	1.71	0.19	0.33	1.93	0.00
25	刘	192.168.3.141	41	109.08	14.39	98.50	4.20	2.66	0.35	98.50	0.00
26	贾	192.168.3.146	41	382.80	3.05	0.00	0.00	9.34	0.07	382.28	0.00
27	谢	192.168.3.151	41	373.16	1.49	0.00	0.00	9.10	0.04	372.33	0.00
28	姚	192.168.3.158	41	3.10	4.92	0.00	0.00	0.08	0.12	1.41	0.00
29	郝	192.168.3.170	41	12.80	42.58	0.23	0.43	0.31	1.04	1.47	0.23
30	192.168.3.190	192.168.3.190	41	0.39	0.13	0.00	0.00	0.01	0.00	0.39	0.00
31	192.168.3.229	192.168.3.229	41	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

图 8.6.1 终端实时流量

8.6.2 终端最近流量

记录了用户得计算机最近一段时间的访问流量（如下图 8.6.2）。

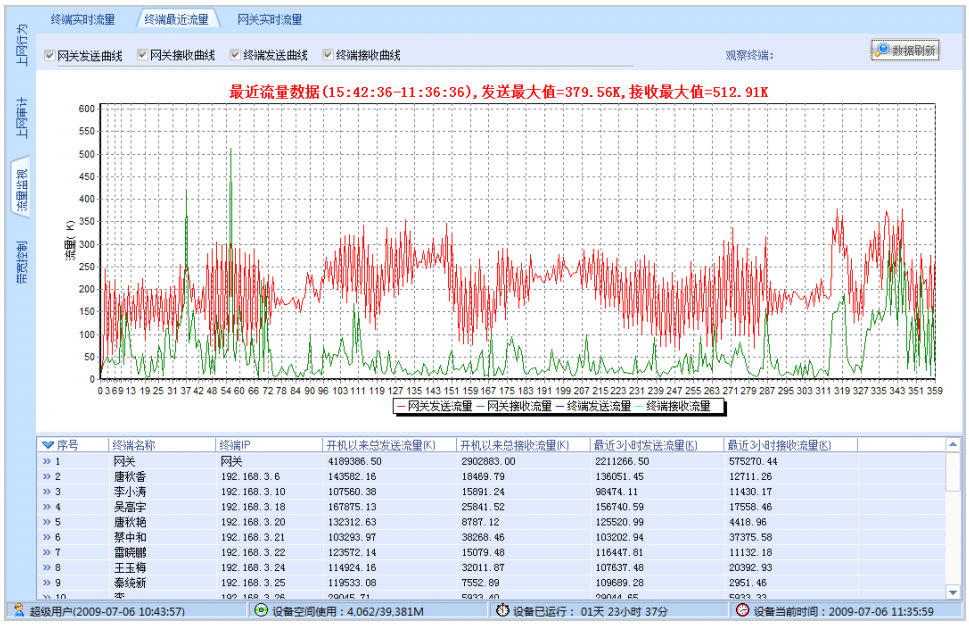


图 8.6.2 终端最近流量

8.6.3 网关实时流量

记录外网接口实时数据流量，通过曲线图显示（如下图 8.6.3）。

图 8.6.3 网关实时流量

8.7 配置实例

8.7.1 基于 IP 带宽流量限制

某公司网络带宽资源上行128K下行512K，公司某些人员经常使用P2P软件占用大量带宽资源，为保障公司业务正常传输和公司其他工作人员正常工作，需对此类用户网络流量进行限制。

方法及配置步骤如下：

1.高级策略界面，添加带宽限制策略元素

[本地IP地址]中输入要限制的终端IP如：192.168.3.213；

[目的起始IP地址]中输入0.0.0.0（0.0.0.0代表所有地址）；

[目的端口]中输入0；

[上行带宽控制]和**[下行带宽控制]**分别限制为10和20（如果把上下行带宽限制为“0”并不等于拒绝本IP的所有流量，只是此IP占用的带宽流量非常少）。

2.保存配置（如下图8.7.1）。

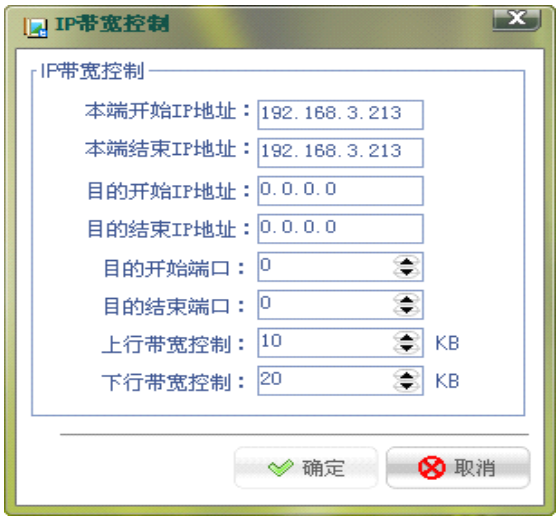


图 8.7.1 流量带宽限制

8.7.2 基于 WEB 流量带宽保证

某公司有一台公网WEB服务器，这台服务器对公司的业务有关键作用，公司要求即使在网络繁忙的时候也要充分保障公司和WEB服务器的正常通讯。采用“CSTD—NETSYS AC”设备带宽保障功能对WEB服务器的流量进行保障，公司上行带宽为521K,下行带宽为2M。

方法及配置步骤如下：

1.高级策略界面，添加带宽保障策略元素

[本地IP地址]中输入0.0.0.0（0.0.0.0代表所有地址）；

[源端口]为0（0 代表所有端口）；

[远端IP地址]中输入服务器IP如：126.42.57.31；

[目的端口]为80（WEB服务端口）；

[上行带宽控制]和**[下行带宽控制]**保障为100、200。

2.保存配置（如下图）。

图 8.7.2 流量带宽保证

8.7.3 上网审计快速配置

例如：张三是装有客户端程序的普通员工，禁止下载 RAR、EXE 文件，禁止看风行、天人、九品网络电视，只允许登录 www.sohu.com 网址，禁止搜索六合彩关键字和发表有关法轮功的帖子。李四是 IP 认证的财务经理，禁止下载 MP3、WAV 文件，禁止玩 QQ 游戏、联众世界，禁止登录 www.51job.com，www.chinahr.com，禁止发表有关法轮功的帖子。

添加上网审计模板：

在[上网审计]→[审计策略模板]列表中[添加模板]→依次添加[员工模板][管理层模板]后即可保存。

定义对象上网审计模板：

- 张三的模板

1. 在[上网审计]→[审计策略模板]→[员工模板]→[下载文件限制]→启用并设置（图 1）；

图1

2. 在[上网审计]→[审计策略模板]→[员工模板]→[应用层过滤]→启用并设置（图 2）；

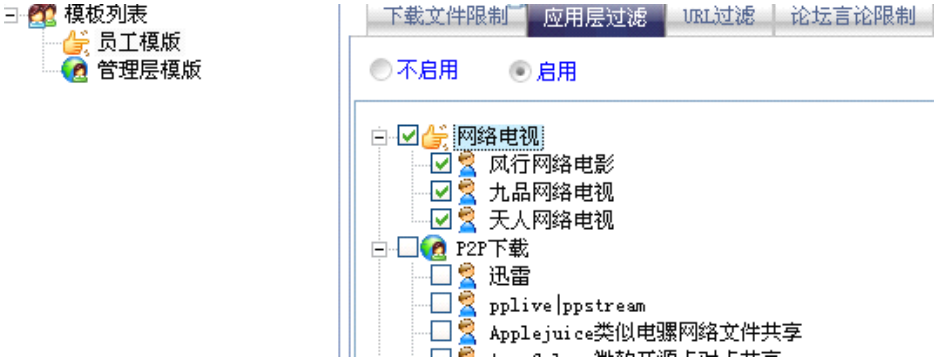


图2

3. 在[上网审计]→[审计策略模板]→[员工模板]→[URL 过滤] →启用并设置（图 3）；

图3

4. 手动添加网址进行过滤，[上网审计]→[网址审计对象配置]即可在相应的对象中添加网址（图 4）；

图 4

5. 在[上网审计]→[审计策略模板]→[员工模板]→[论坛言论限制] →启用并设置（图 5）；

图5

● **李四的模板**

6. 在[上网审计]→[审计策略模板]→ [管理层模板] → [下载文件限制]（图 6）；

图 6

7. 在[上网审计]→[审计策略模板]→ [管理层模板] → [应用层过滤]（图 7）；

图 7

8. 在[上网审计]→[审计策略模板]→ [管理层模板] → [URL 过滤]（图 8）；

图 8

9. 在[上网审计]→[审计策略模板]→ [管理层模板] → [论坛言论限制]（图 9）；

图 9

9 桌面行为管理

桌面行为管理就是对电脑的使用人员在电脑上的行为进行管理。和网络行为管理相对应，网络行为管理关注的是和上网相关的行为，桌面行为管理是对电脑上操作的行为，进行监控和管理。其核心目的是规范电脑的使用，提高工作效率，通过避免员工在电脑上做和工作无关的事情，及时的指正员工的不良行为，规范工作行为，帮助员工和企业提高效率。另外，桌面行为管理通过对企业所有电脑的软硬件管理，帮助企业净化网络环境，减少病毒感染。通过文件操作记录，辅助的保护公司重要信息，保护公司重要无形资产。

桌面行为管理模块是 NETSYS AC 产品中的重要模块，这个模块对企业的管理非常重要，也是企业管理层主要应用和关注的模块。良好的应用桌面行为管理，不仅是对员工的一个监督作用，管理层加强对员工在实际工作中的了解，能更真实的了解员工，这样能更有效

的帮助员工改进工作中的不足，从而提升企业的效率。

桌面行为管理的实现，需要在被管理的 PC 机上安装“客户端”程序。只要电脑和 NETSYS AC 在网络上联通，就可以进行管理。桌面行为管理总体包括如下功能：

实时监控——随时记录电脑软硬件资产的变化信息以及电脑屏幕画面；

桌面行为审计——限制员工使用 USB 移动硬盘、应用程序进程等电脑操作对象；

桌面行为日志——详细记录聊天工具内容、文件操作日志等电脑操作内容；

软硬件资产管理——准确获取电脑软硬件信息，并管理其共享目录及插件信息。

本章所有功能的实现需要安装“客户端”程序。

9.1 桌面行为

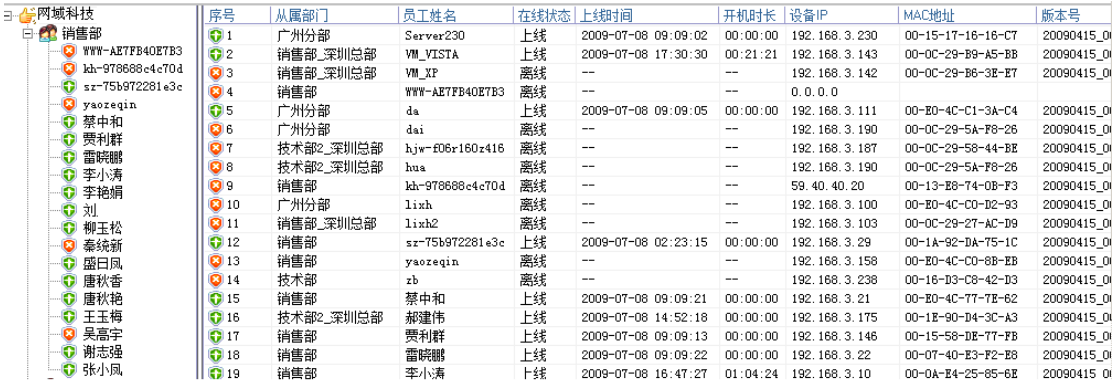
在桌面行为界面下，可以查看员工所使用计算机的工作状态、资产信息，给当前员工发送通知信息、监控当前员工屏幕画面，查看屏幕日志、IM 聊天日志、业绩分析、工作流水记录。

9.1.1 界面说明

在桌面行为界面可以看到左侧以树形结构表示已添加的员工，右侧是以拓扑和列表两种显示方式，通过右键点击弹出的菜单选择显示方式。

拓扑显示方式——通过拓扑编辑，在界面中以拓扑形式显示，该方式较为直观。

列表显示方式——以详细的信息列表样式显示。



9.1.2 基本信息

显示员工的所属部门、姓名、设备是否在线、用户认证方式、配置的上网行为和桌面行为的模版类型、最近登录时间、连续在线时间、实名绑定信息、终端 IP 地址、终端版本号等信息（见图 9.1.2）。

图 9.1.2 基本信息

9.1.3 工作状态

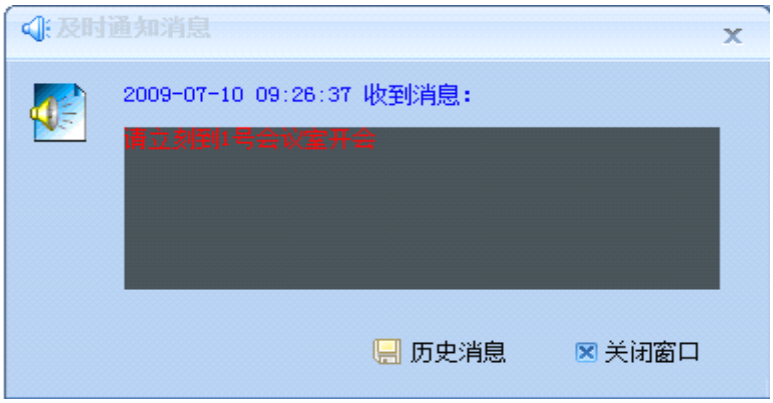
工作状态可以查看员工计算机的硬盘信息、内存信息、网卡信息、系统当前以开的窗口进程和系统进程（如下图 9.1.3）。

在窗口、系统进程界面中，通过右键点击或右下角的功能按钮，企业对员工当前已开启的进程进行强行关闭和加入进程对象配置中。

图 9.1.3 工作状态

9.1.4 发送通知

发送通知可以对当前员工发送消息，在对方的计算机上弹出通知内容，也可以编辑常用短语，方便日常选择使用。



9.1.4.1 通知信息广播

对多个用户发送即时通知消息（如下图 9.1.4.1）。

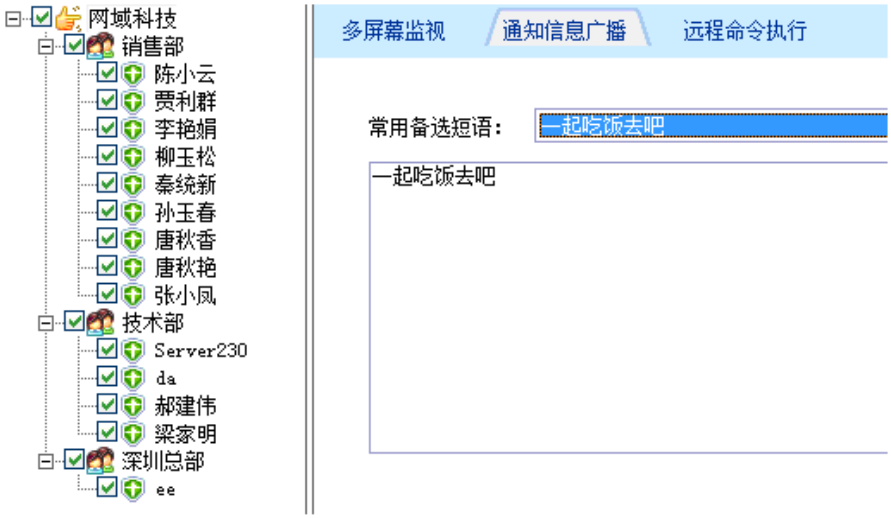


图 9.1.4.1 通知信息广播

9.2 资源审计

当今，无论是台式机又或者是笔记本都带有丰富的外设接口。这些接口为用户日常使用带来便捷，但方便的同时也会不经意地带来潜在的危害。像移动存储介质的 U 盘、移动硬盘是传播病毒、木马的途径；同时也会为企业重要数据、文件带来隐患。因此我们为企业用户提供解决方案，NETSYS AC 可以自定义地关闭计算机的外设接口，禁止员工使用外设接口，有效防止病毒传播、企业机密泄漏。

9.2.1 本地硬件资源审计

关闭员工计算机的外设接口，光驱、串口、并口、USB 接口的 U 盘和移动硬盘、红外接口和 1394 接口。（如下图 9.2.1）。

图 9.2.1 资源审计

9.3 模块审计

现阶段，企业老板、网管在管理公司网络时，最头痛的是反复听到某员工的计算机系统崩溃，某员工的 IP 地址冲突，企业网络不知为何缓慢、不稳定。种种故障问题为管理者带来烦恼。此时只要在桌面行为的模块模版中开启相应审计功能，即可有效地防止以上故障的发生。

9.3.1 功能模块说明

开启模块审计中的功能，可以对员工的操作进行控制，禁止员工启动进程名单内的应用程序，禁止修改计算机的 IP 地址和注册表，绑定网关 IP/MAC 地址；从而强行关闭影响员工工作效率的应用程序，防止内网计算机 IP 地址冲突，防止企业计算机系统崩溃。（如下图 9.3.1）。

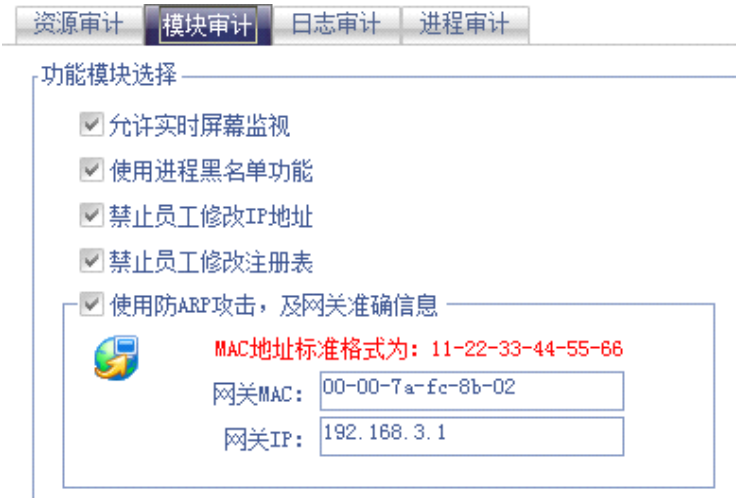
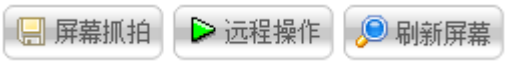


图 9.3.1 模块审计

9.3.2 屏幕监视

企业老板、管理层想了解员工的工作状况，可以对员工的计算机进行抽查、监视、记录。NETSYS AC 的屏幕监视可以实时地查看员工的屏幕信息。通过屏幕抓拍和远程操作按钮，还可以截取员工的当前屏幕图像和当前窗口、进程程序。



使用方法：首先在模版中开启[允许实时屏幕监视]（即开启了桌面行为的当前屏幕功能和多屏幕监视功能），员工配置模版后即可点击该员工查看当前屏幕（如下图 9.3.2）。

9.3.2.1 抓拍日志

当前屏幕界面的右下角有一个屏幕抓拍按钮，通过此按钮可以对当前用户的桌面截屏取

证，此时抓取的图片都被保存在设备中，浏览图片需要到桌面行为的高级日志中查询。

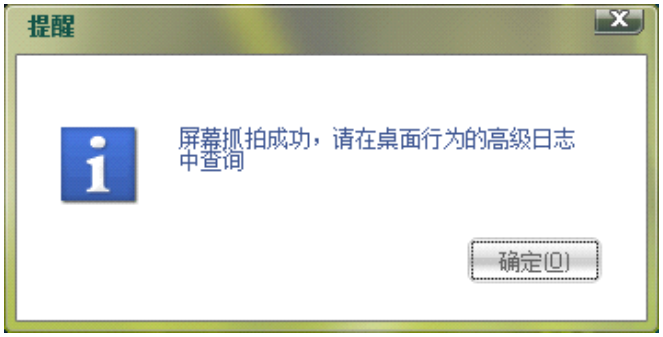


图 9.3.2.1 屏幕抓拍日志

9.3.2.2 多屏监视

在多机操作界面下，可以通过多屏幕监视查看最多 4 个用户的屏幕（如下图 9.3.2.2）。

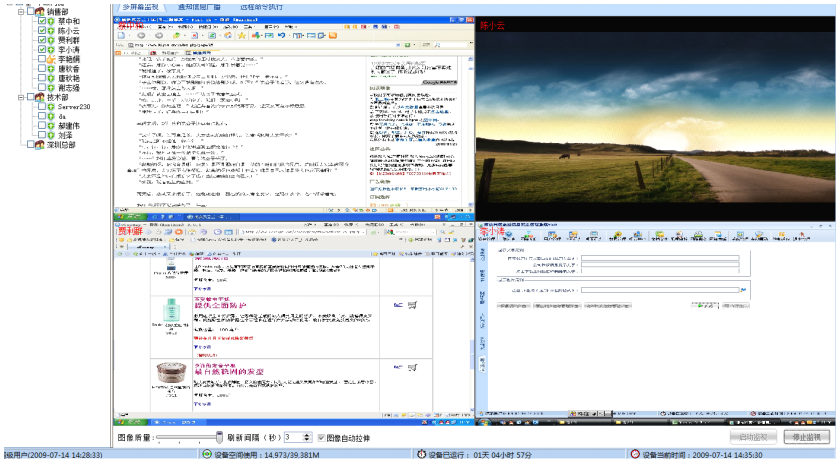


图 9.3.2.2 多屏幕显示

9. 4 日志审计

图 9.4 日志审计

- 记录工作业绩日志：勾选后即开启业绩分析，通过图表了解员工日常应用操作；
- 记录资产告警日志：勾选后即开启资产告警，如计算机硬件有变更将会有告警通知；
- 记录详细工作日志：勾选后即开启工作流水，员工在使用计算机时记录的所有操作；
- 记录屏幕录像日志：勾选后即开启屏幕日志，记录计算机当前屏幕图像；
- 记录聊天日志：勾选后即开启聊天日志，保存当前主流通讯软件的聊天记录。

9.4.1 业绩分析

业绩分析是统计在一段时间内计算机常用程序的活动比率，NETSYS AC 自动生成分析图，形象的概括了用户的操作记录。

在策略模版中勾选开启[记录工作业绩日志]功能后，即可在桌面界面中查看该员工的业绩分析饼图，从图中就可了解该员工日常应用操作（如下图 9.4.1）。

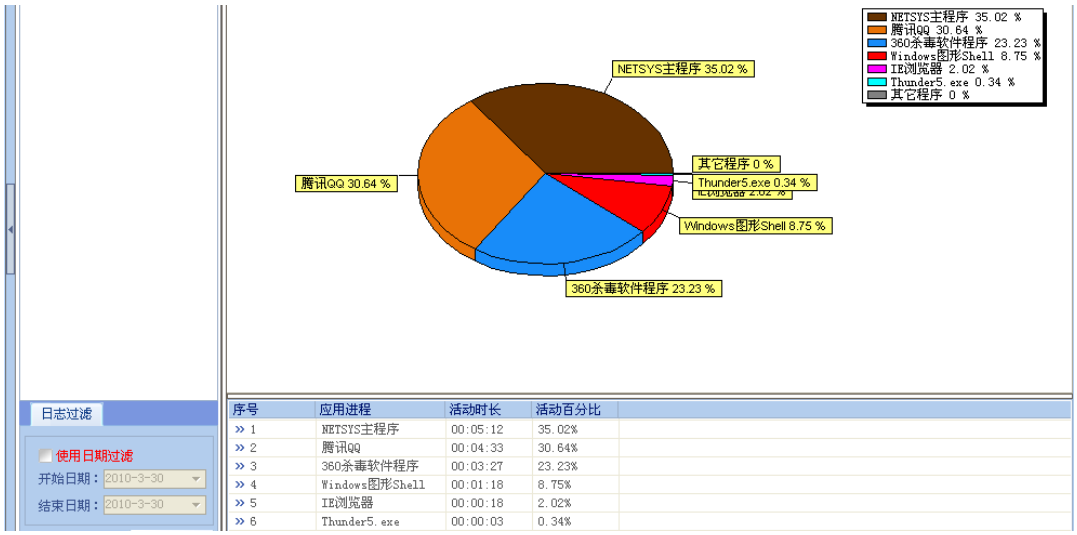


图 9.4.1 业绩分析图

还可以对列表内的应用进程进行查看和设置，未知进程进行编辑解释。

9.4.2 资产告警

企业计算机属于企业固定资产的一部分，总有一些员工对公司资产垂涎，CPU、内存、硬盘被偷换更是难以发现。NETSYS AC 附带的资产管理功能就可以方便管理者通过查看该界面，浏览员工的计算机相应的硬件信息。资产警告中显示用户的计算机硬件被更改，与注册时的硬件信息不符，即在界面中显示计算机的变更信息（如下图 9.4.2）。

图 9.4.2 资产管理

9.4.3 工作流水

工作流水是员工在使用计算机时记录的所有操作，管理者通过记录的日期可以查询当日完整的操作记录。同样，工作流水是要在策略模版中勾选开启[记录详细工作日志]功能（如下图 9.4.3）。

图 9.4.3 详细工作日志

9.4.4 屏幕日志

除了详细工作记录、即时通讯软件聊天记录，NETSYS AC 还对计算机的桌面屏幕进行屏幕抓拍记录。

员工配置的模版开启了[记录屏幕录像日志]，同时设置屏幕抓取间隔、录像质量，这样屏幕的快照就会被保存到 NETSYS AC 中，在屏幕日志界面可以查看员工的屏幕图像日志（如下图 9.4.4）。

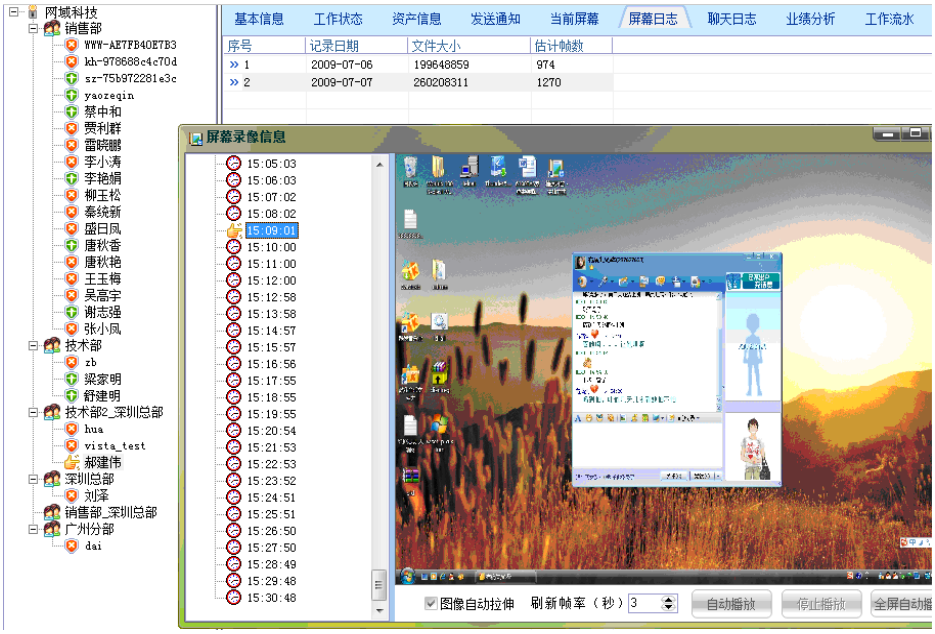


图 9.4.4 屏幕日志

9.4.5 聊天日志

随着互联网技术的不断发展，基于 Internet 的即时寻呼软件更是各种各样。有的企业是需要这类通讯软件为其商务业务带来便利，但员工是否规范自己的行为操作，是利用这类资源工作还是在上班时间聊天。NETSYS AC 的记录聊天日志能记录当前主流即时通讯软件的聊天日志。

在策略模版中勾选开启[记录聊天日志]功能后，即可对 QQ、MSN、Skype 等即时聊天工具进行侦听，获取聊天日志（如下图 9.4.5）。

图 9.4.5 聊天日志

9.4.5.1 聊天内容全库检索

NETSYS AC 为用户提供了聊天记录搜索库，使用方法是在搜索前首先点击同步数据按钮，让服务器上的聊天记录与本机同步（同步时间数秒至数分钟不等，同步完毕会有对话框），输入搜索的关键字、词，点击全库检索按钮即可，如要指定日期只需定义搜索日期。

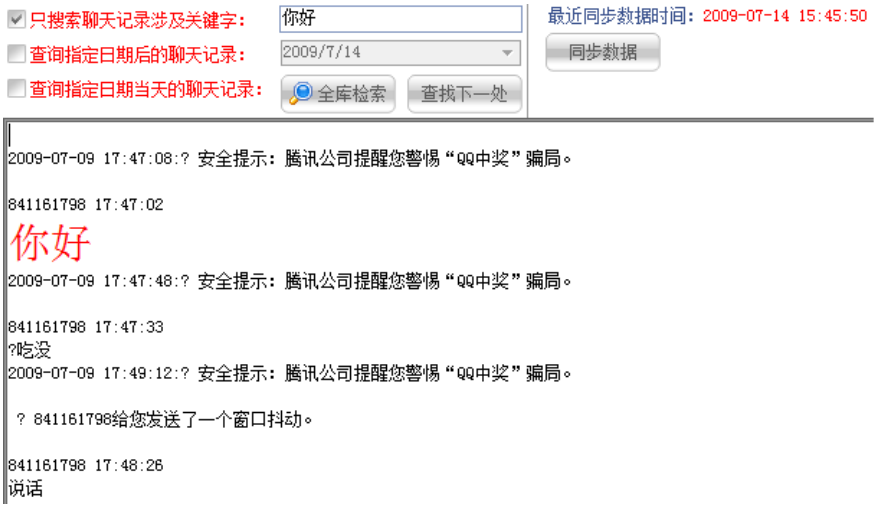


图 9.4.5.1 聊天搜索库界面

9.5 进程审计

启用审计模块中的进程黑名单功能，即可在进程审计中勾选进程对象，策略通过匹配应用软件的进程名、命令行等特征进行强行关闭，从而限制员工使用某类软件（如下图 9.5）。

图 9.5 进程审计

9.5.1 进程对象配置

进程对象在出厂默认状态下不能满足企业的需求，那么可以手动添加进程对象。手工添加：点击“添加”按钮（如下图 9.5.1）

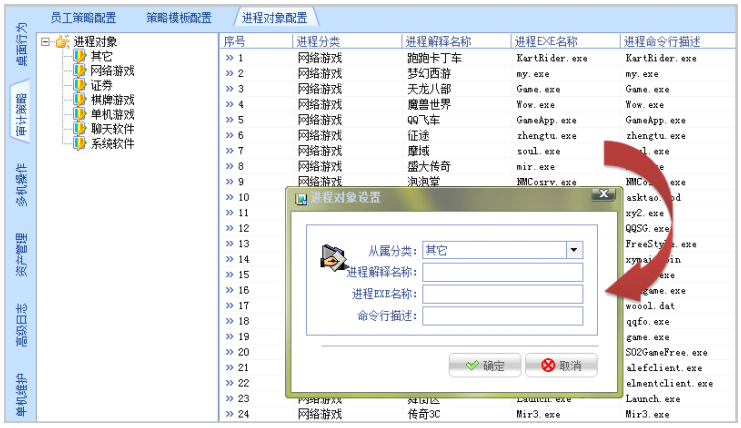


图 9.5.1 进程对象配置

从属分类：进程的应用类型，方便以后查找，类型可在左下方点击按钮添加；

对象名称：一般填写产生该进程的应用程序名或者其它容易理解的文字信息；

进程对象：填写进程名，通过“任务管理器”查看，注意大小写；

命令行描述：一般填写产生该进程的应用程序名或者其它容易理解的文字信息。

9.6 单机维护

单机维护是为用户提供关于桌面行为管理相关的维护功能。例如查看员工的基本信息、检查员工配置的审计策略模版、对计算机执行远程命令和查看计算机的外部链接等，对网络内所有连接的计算机统一维护管理。

9.6.1 桌面审计策略

在日常维护工作中，经常性的需要检查员工的策略模版是否配置正常，此时可以用到桌面审计策略查看配置信息。

图 9.6.1 桌面审计策略

9.6.2 远程命令执行

远程命令执行是通过 NETSYS AC 管理系统向员工客户端发送命令，从而对计算机下达某些动作的远程操作。

点击按钮对计算机执行相应操作命令：

- 远程关机——对计算机进行关机指令；
- 重启机器——对计算机进行重启指令；
- 网络隔离——对网络内指定计算机进行隔离指令，使其无法与网络通信；
- 重启客户端程序——重启计算机的客户端程序，是程序服务重新加载运行；
- 安装/卸载文档加密——安装和卸载文档加密程序，使计算机激活文档加密功能；
- 卸载客户端程序——卸载 NETSYS AC 客户端程序。

9.6.2.1 多机远程命令

可以对多个员工进行远程命令操作。

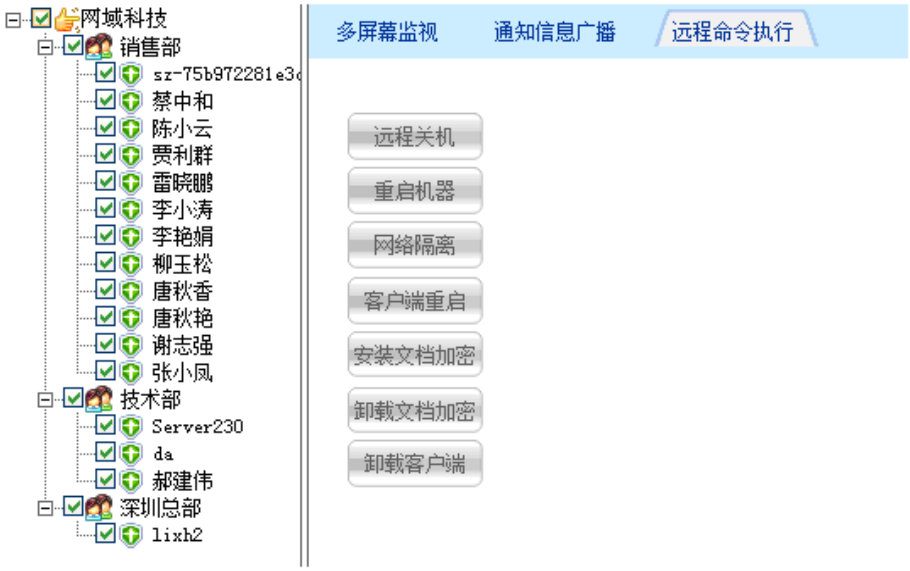


图 9.6.2.1 多机远程命令

9.6.3 共享目录管理

查看用户计算机上所共享的文件夹，可以手动停止用户共享的文件夹。

序号	共享名称	共享目录路径
» 1	121	C:\Documents and Settings\Administrator\桌面\121
» 2	TEST22	F:\TEST22
» 3	IPC$	
» 4	解决局域网共享	C:\Program Files\装机人员工具\解决局域网共享
» 5	卡巴斯基360豪华版 v7....	E:\sy\卡巴斯基360豪华版 v7.0.0125
» 6	test	F:\test
» 7	软件安装包	D:\软件安装包
» 8	软件程序	D:\软件程序
» 9	dat	C:\Documents and Settings\Administrator\桌面\dat
» 10	bin_ManagerUI	F:\test\bin_ManagerUI

图 9.6.3 共享目录管理界面

9.6.4 网络连接跟踪

NETSYS AC 追踪当前用户所访问的外部链接，此功能类似 Windows 内部命令 netstat –an，以更加直观、详细的方式体现。 同时也可以对未知的进程修改进程名称。

序号	进程名称	使用协议	源信息	目的信息	目的地址分析
» 1	MpCmdRun.exe	TCP	192.168.3.175:49678	65.55.94.222:443	美国 Microsoft公司
» 2	IE浏览器	TCP	192.168.3.175:49680	121.14.89.14:80	广东省中山市 电信
» 3	IE浏览器	TCP	192.168.3.175:49681	74.55.154.134:80	美国 CZ88.NET
» 4	IE浏览器	TCP	192.168.3.175:49682	74.55.154.140:80	美国 CZ88.NET
» 5	IE浏览器	TCP	192.168.3.175:49683	74.55.154.140:80	美国 CZ88.NET
» 6	IE浏览器	TCP	192.168.3.175:49684	74.55.154.140:80	美国 CZ88.NET
» 7	IE浏览器	TCP	192.168.3.175:49685	74.55.154.140:80	美国 CZ88.NET
» 8	IE浏览器	TCP	192.168.3.175:49686	74.55.154.140:80	美国 CZ88.NET
» 9	IE浏览器	TCP	192.168.3.175:49687	74.55.154.140:80	美国 CZ88.NET
» 10	IE浏览器	TCP	192.168.3.175:49688	58.222.19.67:80	江苏省泰州市 电信
» 11	IE浏览器	TCP	192.168.3.175:49689	58.222.19.67:80	江苏省泰州市 电信
» 12	IE浏览器	TCP	192.168.3.175:49690	74.55.154.154:80	美国 CZ88.NET
» 13	IE浏览器	TCP	192.168.3.175:49702	207.66.153.91:80	美国 CZ88.NET

图 9.6.4 网络连接跟踪界面

9.7 拓扑编辑

可以对企业员工办公拓扑结构进行自定义编辑，重新编排图标位置。

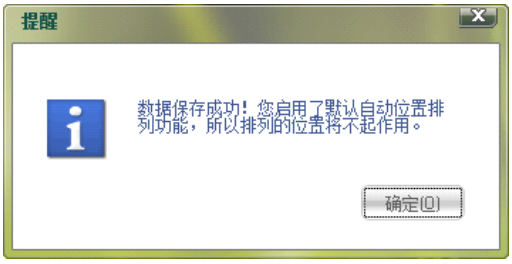
背景图的自定义方法是：用图片制作工具制作一张与企业办公结构相符的拓扑图，图片类型只支持 BMP 格式，且大小不超过 3M。然后依次打开[NETSYS AC] → [用户管理]→[企业信息]，在企业背景图中选择已设计好的图上传保存即可。

拓朴编辑方法是：打开[NETSYS AC] → [桌面行为] → [拓扑编辑]，在拓扑图界面中右击选择[申请拓朴编辑]或直接点击右下方的[申请编辑]按钮，然后用鼠标拖动的方式可对员工图标进行任意位置拖放。完成后单击右键，选择[保存]或直接点击右下方的“保存”按钮（如下图 9.7）。

图 9.7 拓扑编辑菜单

常见错误解决方案：

在点击“保存”按钮时弹出如下图错误提示：



解决方法：在“申请拓朴编辑”后单击鼠标右键，在弹出菜单中选择[取消自动排列并获取设备中的位置]或[取消自动排列并保留现在的位置]，然后在进行重新编辑并保存。

9.8 配置实例

员工策略配置：

例如：一家企业分类为 2 层，一是管理层（领导级别，经理、主管、主任等）、二是普通员工。这样在桌面行为管理配置 2 个模版，普通员工受限制要比管理层要多，权限也相对较少。

添加审计策略模板：

在[审计策略]→[审计模版配置]列表中[添加模板]→依次添加[普通员工模板]和[管理层模板]后即可保存。

定义对象上网审计模板：

- 普通员工的模板

1. 在[审计策略]→[审计模版配置]→[普通员工]→资源审计（图 1）；

图 1

2. 在[审计策略]→[审计模版配置]→[普通员工]→配置模块审计（图 2）；

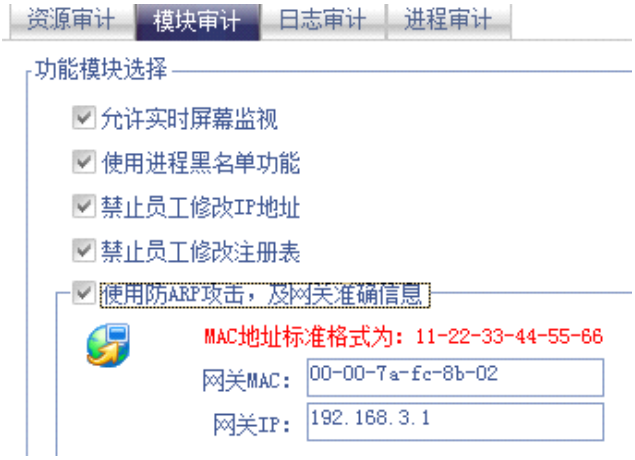


图 2

3. 在[审计策略]→[审计模版配置]→[普通员工]→配置日志审计（图 3）；

图 3

4. 在[审计策略]→[审计模版配置]→[普通员工]→配置日志审计（图 4）；

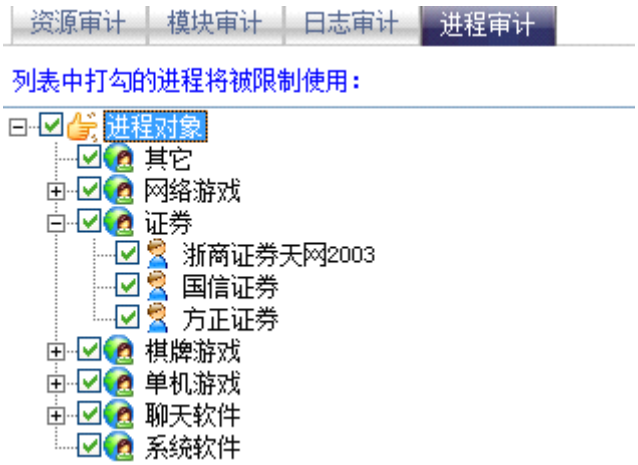


图 4

5. 在[员工策略配置]为员工添加[普通员工]模版（图 5）；

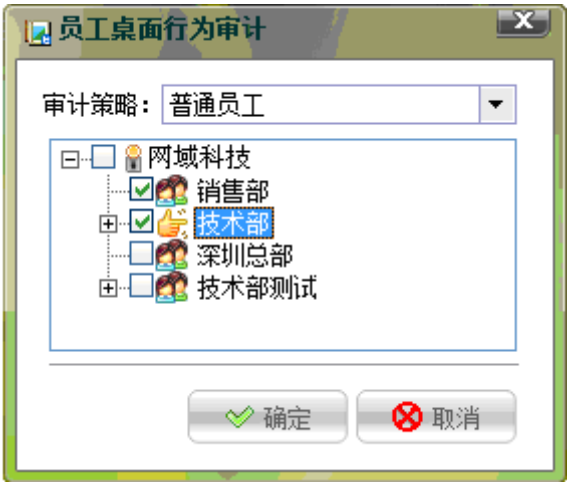


图 5

- 管理层的模板

1. 在[审计策略]→[审计模版配置]→[管理层]→资源审计（图 1）；

图 1

2. 在[审计策略]→[审计模版配置]→ 管理层]→配置模块审计（图 2）；

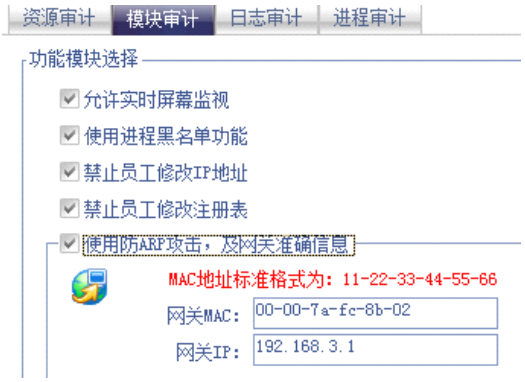


图 2

3. 在[审计策略]→[审计模版配置]→[管理层]→配置日志审计（图 3）；

图 3

4. 在[审计策略]→[审计模版配置]→[管理层]→配置日志审计（图 4）；

图 4

5. 在[员工策略配置]添加[管理层]模版（图 5）；

图 5

10 数据管理

数据存储的容量总是有限的，而数据存储的环境又是不可预测的。自然灾害、操作系统破坏、人为操作失误等等，都有可能导致原有数据的不可恢复性损坏。因此，从安全保护角度来讲，定期备份已有数据十分有必要。

NETSYS AC 提供将设备里的数据通过网络完整的拷贝到本地电脑硬盘中，或者删除指定日期前的指定数据，以节省不必要的空间浪费。同时提供将日志形成报表打印功能，提供有针对个人的日志数据打印和针对整个企业或某个部门的报表打印。

10.1 界面说明

打开[NETSYS AC]→ [数据管理] （如下图 10.1）：

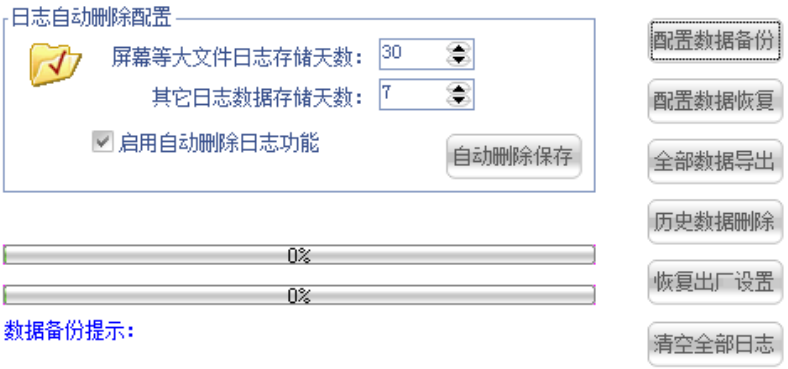


图 10.1 数据管理界面

- 日志自动删除——定义日志记录的存活时间，并让系统自动删除日志。
- 配置数据备份——备份设备的配置数据；
- 配置数据恢复——恢复备份的配置数据；
- 全部数据导出——导出设备中的所有数据，通过离线查看工具查询；
- 历史数据删除——删除指定用户对象和时间对象的数据记录；
- 恢复出厂设置——还原至设备出厂时的默认设置；
- 清空全部日志——是指删除所有员工的各种日志记录。

10.2 功能说明

10.2.1 日志自动删除

屏幕日志、聊天日志、工作业绩日志、资产告警日志、详细工作日志等，系统记录的数据保存到设备中，然而设备的存储空间又是有限的，通过日志自动删除配置，定义日志的存活时间，过期则让系统自动删除数据（如下图 10.2.1）。

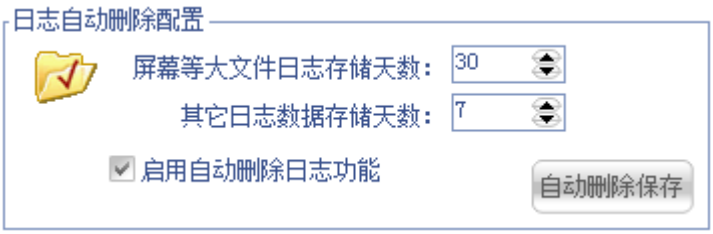


图 10.2.1 数据管理界面

10.2.2 历史数据删除

历史数据删除是基于成员，时间，历史数据记录三个条件因素构成的管理功能。通过选择一个或多个员工，日志类型和时间，删除相应的记录数据（如下图 10.2.2）。

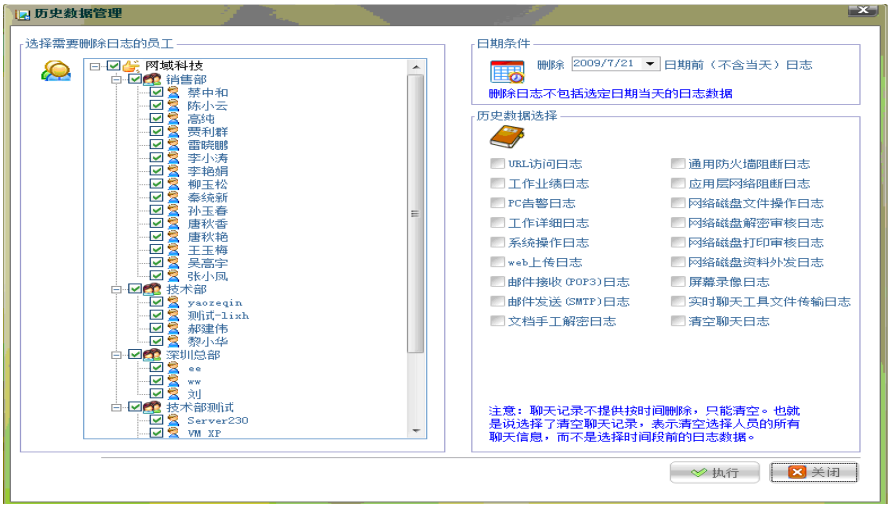


图 10.2.2 历史数据管理

10.3 报表中心

NETSYS AC 为企业管理层提供强大的交互式构建报表，报表数据来源于 NETSYS AC 设备所产生的所有日志，而报表的数据源可以灵活选择，报表的结构格式及排版由 NETSYS AC 相应工具自动生成并提供打印和保存功能。

10.3.1 企业报表

企业报表可以选择打印整个企业或某个部门的数据，也可以选择打印某段时间内的数据，同时还可以选择需要打印的日志信息。选择好查询条件后，点击[数据准备]进行数据下载，在数据下载完成并提示后点击[打印预览]。

[报表中心] → [企业报表]：

图 10.3.1 企业报表

10.3.2 个人报表

在这个窗口中可以选择待打印员工的数据，也可以选择打印某段时间内的数据，同时还可以选择需要打印的日志信息。选择好查询条件后，点击[数据准备]进行数据下载，在数据下载完成并提示后点击[打印预览]进行个人报表预览和打印。

[报表中心] → [个人报表]：

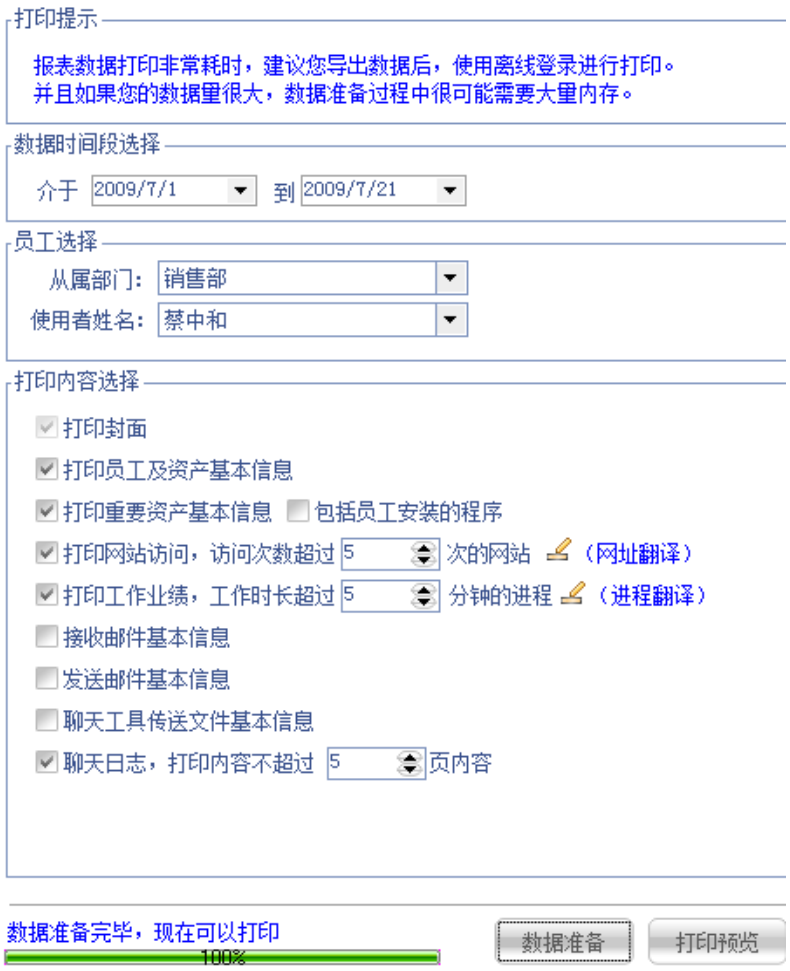


图 10.3.2 个人报表

11 文档安全

文档安全是为企业机密文件信息提供一套安全的加密管理方法。通过定制终端用户加密策略，使用透明加解密等一系列技术方案，在不改变终端用户任何使用习惯的基础上，防止内部重要数据文件被有意或无意的泄露，实现企业信息安全。

随着信息化的发展，越来越多的文件以电子文档的形式进行传输。我国计算机安全防护能力处于发展的初级阶段，许多计算机基本上处于不设防状态。据中国国家信息安全测评认证中心调查，信息安全的现实威胁主要为信息泄露和内部人员犯罪，而非病毒和外来黑客引起。

保证内部信息的安全性，往往首先想到的是外部攻击，因此会考虑到防火墙、入侵检测、内部网和外部网物理隔离等技术，而内部的信息泄露往往不受重视。据调查显示由于内部人员泄密导致的经济损失，是黑客造成损失的 16 倍，是病毒造成损失的 12 倍。众所周知，电子文档是极易复制和传播的。

因此，要彻底保护企业文件安全，不仅仅要加强内部安全管理，还要部署文档加密。

文档加密领域是一种新兴的安全技术，只有拥有雄厚的技术实力，才能跟得上技术发展的趋势，进而提供持续的服务。透明加解密技术是近年来针对企业文件保密需求应运而生的一种文档加密技术。所谓透明，是指对使用者来说是完全觉察不到的，完全不改变其使用习惯。当使用者在打开或编辑指定文件时，系统将自动对未加密的文件进行加密，对已加密的文件自动解密，实现透明加解密。

NETSYS AC 所嵌入的文档加密功能，基于 Windows 底层文件驱动过滤技术，通过计算机底层操作系统对数据严格的加解密控制。结合 NETSYS AC 强大的管理功能，实现对机密信息的加密，控制，保证文档安全。

11.1 基本原理

透明加解密技术是与 Windows 紧密结合的一种技术，它工作于 Windows 的底层。通过监控应用程序对文件的操作，在打开加密文件时自动对密文进行解密，在写文件时自动将内存中的明文加密写入存储介质。从而保证存储介质上的文件始终处于加密保护状态。

在文档加密领域，透明加密技术主要分为驱动技术和 Hook 技术两大流派。就开发难度而言，驱动级加密的开发难度要大的多，但由于收到 Windows 保护，稳定性好，兼容性高，速度快。Hook 透明加解密技术开发容易，但存在技术缺陷，容易被反 Hook 所破解。市场上，能开发基于驱动级的文档加密产品只有少数厂商。

A. 应用层加密

通过 Windows 的钩子技术，HOOK 程序监控所有应用程序对文件的打开和保存，当打开文件时，先将密文转换后再让程序读入内存，保证程序读到的是明文，而在保存时，又将内存中的明文加密后再写入到磁盘中。

B. 文件驱动加密

基于 Windows 的文件系统（过滤）驱动（IFS）技术，工作在 Windows 的内核层。文件驱动就是把文件作为一种设备来处理的一种虚拟驱动。当应用程序对某种后缀文件进行操作时，文件驱动会监控到程序的操作，并改变其操作方式，从而达到透明加密的效果。

优势和特点

技术优势

- 基于 Windows 内核驱动的高效加解密技术

NETSYS AC 文档加密对系统缓存进行了大量的优化，同时采用独有的 3 层过滤判断的技术，将系统的资源进行了最优化，使加密文件的打开和保存速度大幅度提高。实际测试结果证明，使用文档加密透明打开或保存大于 100M 的加密文件，时间延迟不超过 2 秒。

- 极高的安全性

定义 160 位的企业加密密钥。采用 RC4 算法与 AES 算法同时加密（AES 由于速度较慢，只加密小部分数据，但是足以让纯粹 RC4 算法安全性提升一个档次）。这样文档安全性极高，若没有正确的企业密钥，从时间上看要破解一个文件根本不可能。从数学上看由于 AES 目前国际上尚无人能破，RC4 也没有确切的解密方案，因此从数学角度看,使用暴力破解该加密文档成为不可能的事情。

技术特点

- 全程加密采用“新建与覆盖加密”方式，保证文件从创建即被加密。
- 保证内存读取软件无法从缓存中获取任何明文内容。
- 灵活的加密策略模板配置。从而实现对不同用户选择不同加密策略的加密处理。
- 提供对离开网络后的加密客户端进行有选择的安全处理。
- 不改变企业用户原有工作习惯和工作流程。
- 提供对指定的应用程序和指定后缀的文件进行自动加解密密处理。
- 不需要人工输入加解密密码。
- 加密后的文件在非授权的情况下，在其他客户端不能访问。

11.2 基本部署步骤

NETSYS AC 文档加密基本部署（如下图 11.2）：

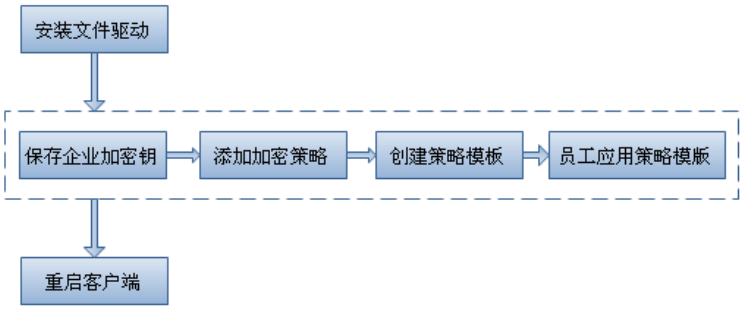


图 11.2 部署步骤

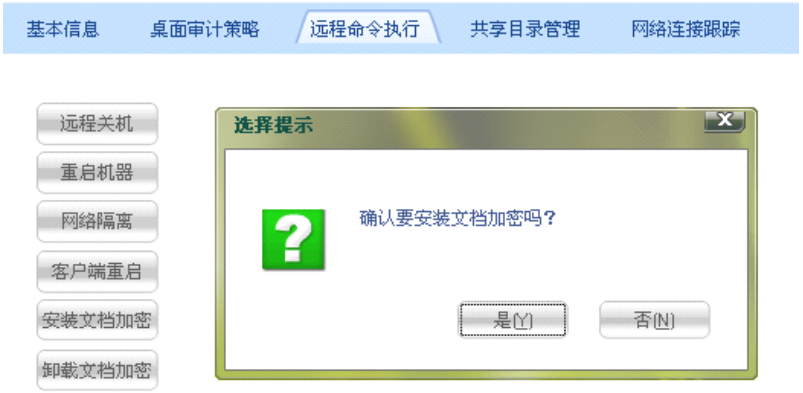
11.2.1 准备工作

1. 保证安装客户端的计算机已经接入网络中，并能与 NETSYS AC 设备正常通讯；
2. 安装文件驱动。

NETSYS AC 提供有 2 种安装文件驱动的方法：

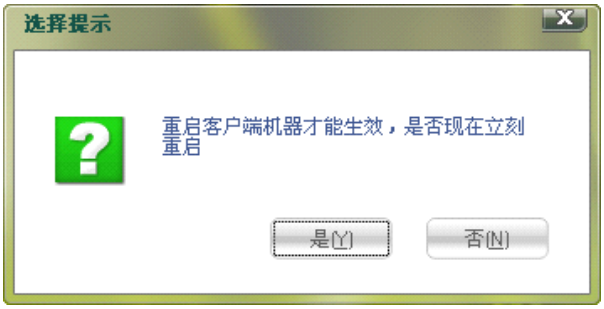
方法一：在 NETSYS AC 管理系统内为客户端安装

点击 [桌面行为] → [单机维护]，双击主窗口中对应的员工。选择 [远程命令执行] 。



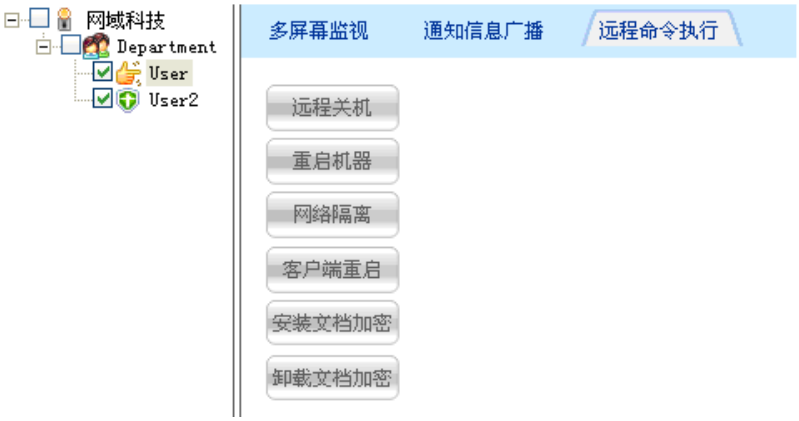
点击按钮 [安装文档加密] ，并在弹出的对话框，点击是，确认安装。

由于文档加密系统需要重启后才能生效。用户根据自己的当前需求，确定是否重启电脑 。



NETSYS AC 批量安装文件驱动：

点击 [桌面行为] → [多机操作]，勾选左侧需要安装的员工。选择 [远程命令执行] 。



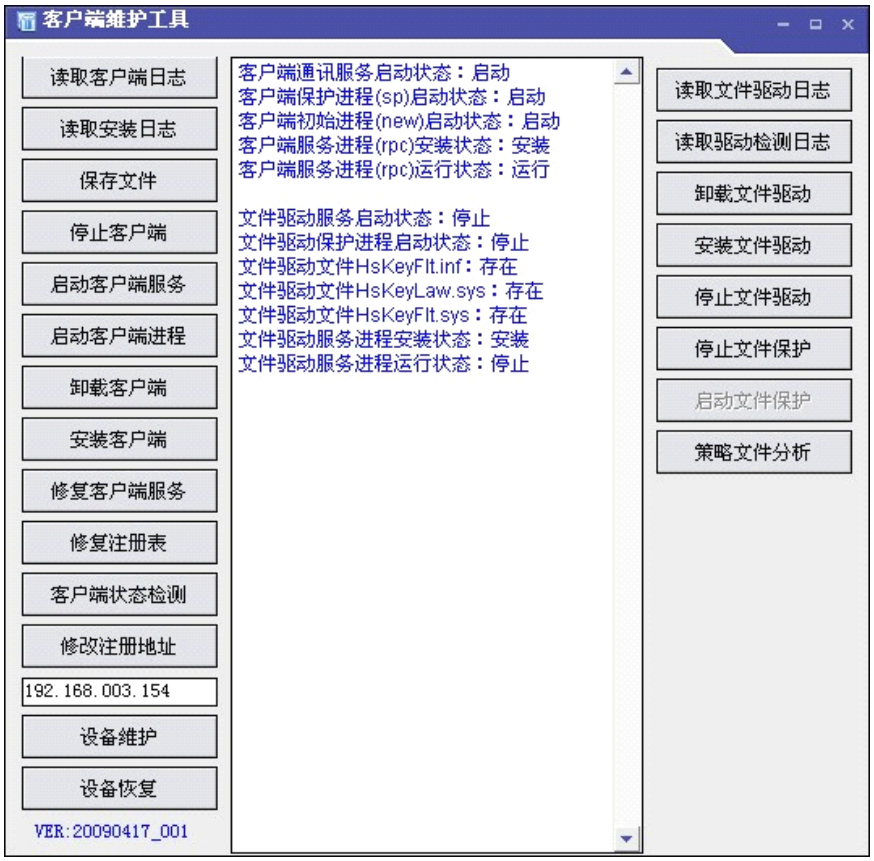
勾选对应的员工后点击 [安装文档加密] 即可。

通过 NETSYS AC 管理界面进行单机安装和多机安装，必须确保客户端上线方能对客户端进行远程安装。

方法二：客户端维护工具安装

注意：通过客户端维护工具安装文件驱动，只能针对单机进行安装。

在已安装客户端的基础上，点击安装客户端维护工具的 [安装文件驱动] 按钮即可完成文件驱动安装。



11.2.2 配置信息

当完成文件驱动的安装后，需要做好系列配置，就可以保证企业文件的安全性了。需要做得配置主要有：

- 配置企业密钥

企业密钥是 NETSYS AC 文档加密所采用的密钥，通过该密钥信息，使用底层算法来实现对文档的加密处理。

在该密钥配置中，必须强制输入 20 个字符的作为加密密钥（即 160 位加密密钥），点击 [保存] 。方能完成企业的统一加密密钥的配置。

注意：本密钥只能配置一次，请慎重填写。

➢ 配置加密策略

默认情况下，NETSYS AC 已为客户添加常用的文档加密策略。如因为默认提供的加密策略不能满足其需求，可自行添加分类和策略来完成策略的添加。

点击 [添加分类] [删除分类] ，可对左栏添加所需的类别的名称。

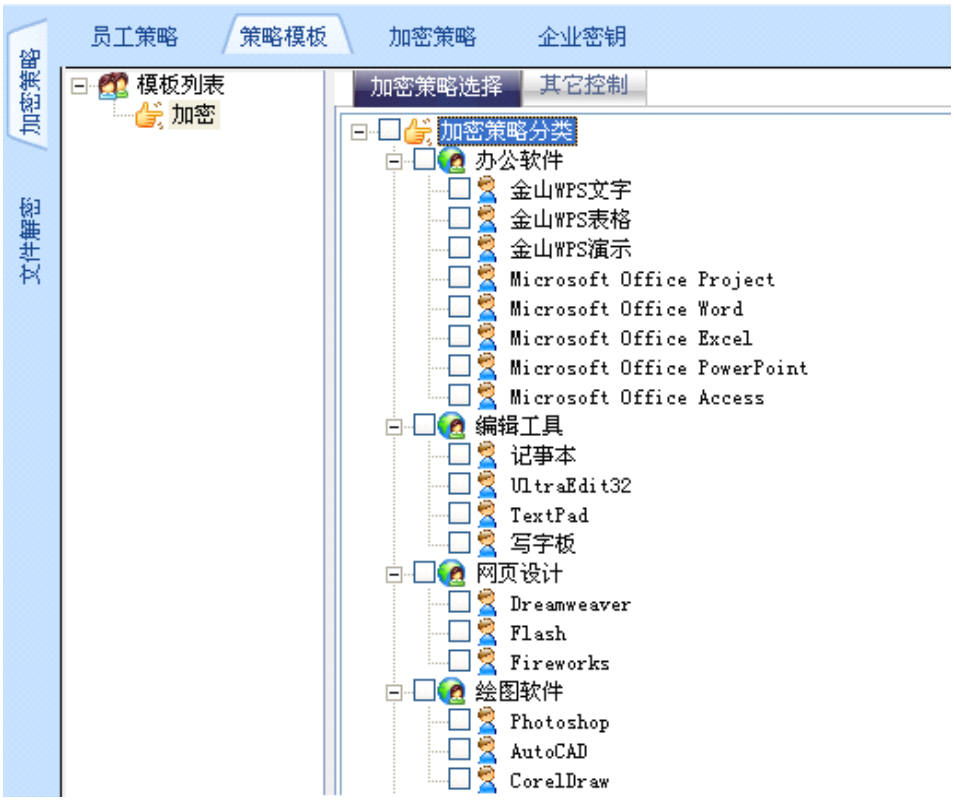
点击 [添加] 可在如下对话框中，添加加密策略。

通过输入加密受控程序的进程名，及其需要加密的后缀，钩选需要实施加密的动作及应用权限，则可完成对策略的编辑。

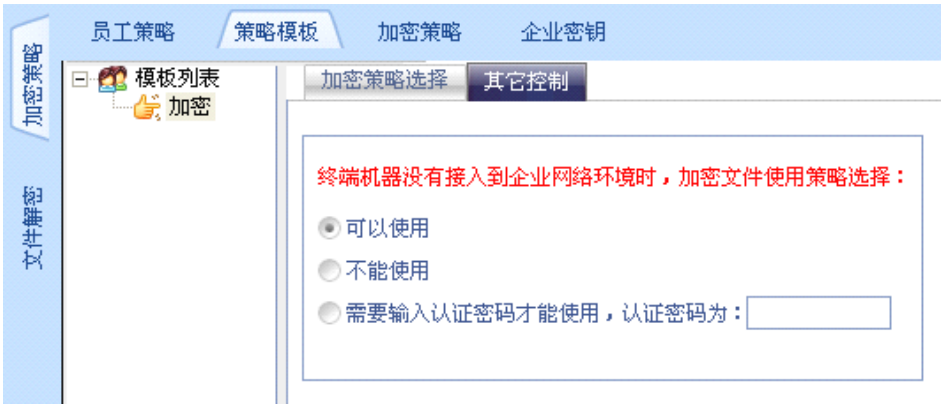
➢ 配置加密策略模板

点击[策略模板]，点击[添加模板] 可在弹出的“添加对象”对话框输入模板的名称：

通过定义模板名称，可见到模板提供了如下的策略选择。



[加密策略选择] 通过勾选以上复选框，点击[保存]，则可为所添加的模板加入所要加密的程序。



[其他控制] 提供了对文档加密的多个需求处理：

当受到加密的客户端没有接入到企业网络中的时候，针对加密的文件，提供如下对策：

- **可以使用** 对客户端应用策略生效后，加密客户端离开本地网络后，电脑重启后打开已加密的文件，该文件是可以被使用的。
- **不能使用** 对客户端应用策略生效后，加密客户端离开本地网络后，电脑重启后打开已加密的文件，该文件是不可以被使用的。
- **需要输入认证密码才能使用** 对客户端应用策略生效后，加密客户端离开本地网络后，电脑重启后打开已加密的文件，该文件是不可以被使用的。需要配合网域科技加载文档安全工具才能使用该加密文档。

➢ 配置加密策略

点击[员工策略]，在对应的窗口中点击[添加]按钮。

选择要实现加密的员工姓名，再选择要实现加密的策略模板。勾选“策略生效”，点击[确定]。再点击[保存]。

再选中所配置的员工，点击界面下按钮[重启客户端]，刷新显示。

当提示加载成功的时候，则文档加密的部署已完成

11.3 文档管理

11.3.1 全盘加解密工具

文件加解密驱动在正常工作后，每次保存文件会对文件进行加密。但是在第一次安装文件驱动后，原有的非加密文档不会自动加密，如果客户需要对终端机器所有需要加密的文件进行加密，需要配合“NETSYS AC 手工加解密工具”来实施加密。（如下图 11.3.1）。

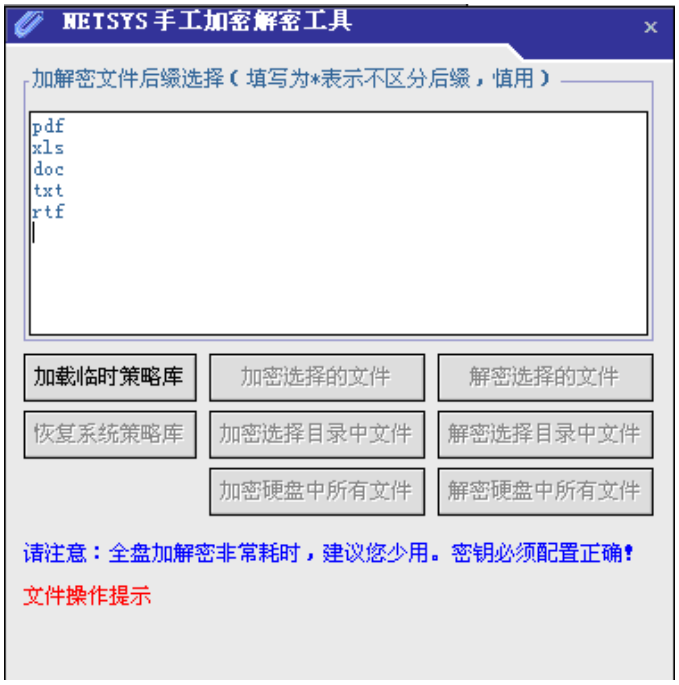


图 11.3.1 手工加解密工具

点击[加载策略库]，完成文件驱动及企业密钥的加载。对应需求，填入需要加解密的文件后缀，可以根据用户的需求，点击以下按钮，可针对文件，目录，硬盘进行加解密。

[加密选择的文件] **[解密选择的文件]**
[加密硬盘中所有文件] **[解密硬盘中所有文件]**
[加密选择目录中文件] **[解密选择目录中文件]**

- 注意：使用全盘加解密工具执行会比较耗时，不建议用户频繁使用。
- 切勿对系统文件，可执行文件等使用全盘加解密，否则会造成严重后果。

11.3.2 使用密码加密

当 NETSYS AC 在定义加密模板的时候，如在[其他功能]中启用了“需要验证密码后才能使用”，则终端的加密策略为：当终端离开公司的加密网络环境，重启电脑后。该电脑需要通过“密码加载文档安全”小工具，通过输入匹配的密码模拟启动公司的加密网络环境，方能能正常使用已加密的文件（如下图 11.3.2）。

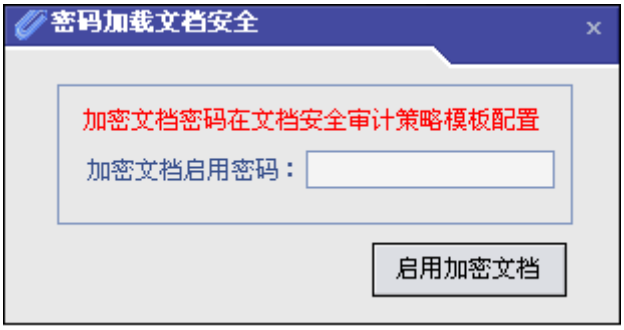


图 11.3.2 离线加密文件工具

11.3.3 文件解密

当企业的加密文件需要外发或者经过批准后允许带出企业时，需要对这些文件进行规范化管理。用户需要到文档管理人员处申请解密文件，系统自动记录下所有文件解密的日志，以备日后查询。

NETSYS AC 针对文件解密提供三种方式实施解密：

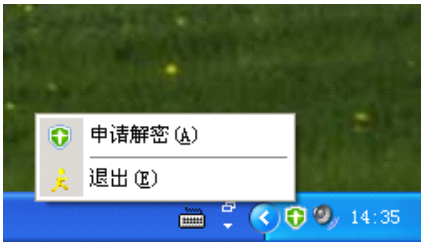
- 使用客户端在线同步解密工具解密
- 使用 NETSYS AC 手工解密工具解密
- 使用网络磁盘加密审核工具解密

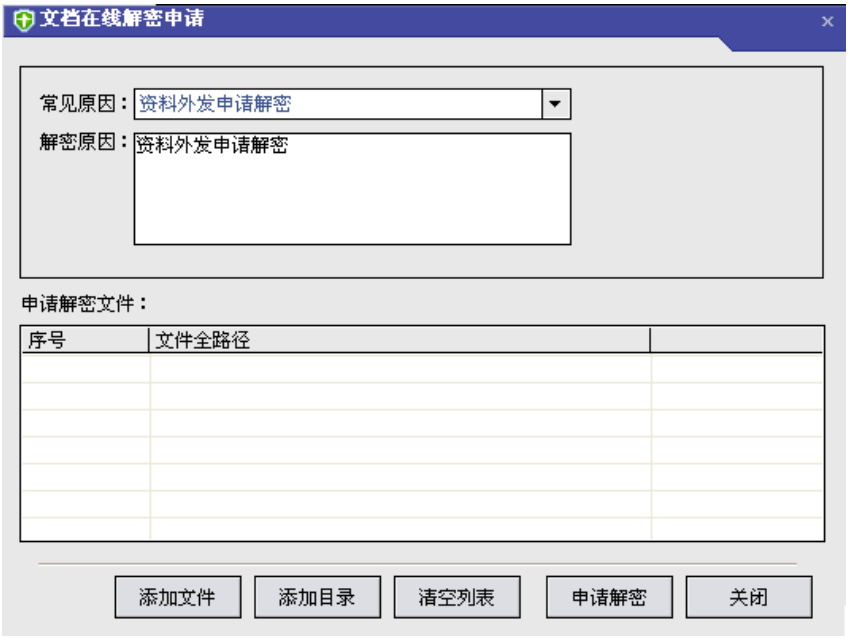
- 使用客户端在线同步解密工具解密

说明：在线同步解密工具要求解密申请端的申请工具和管理端的管理工具必须保持开

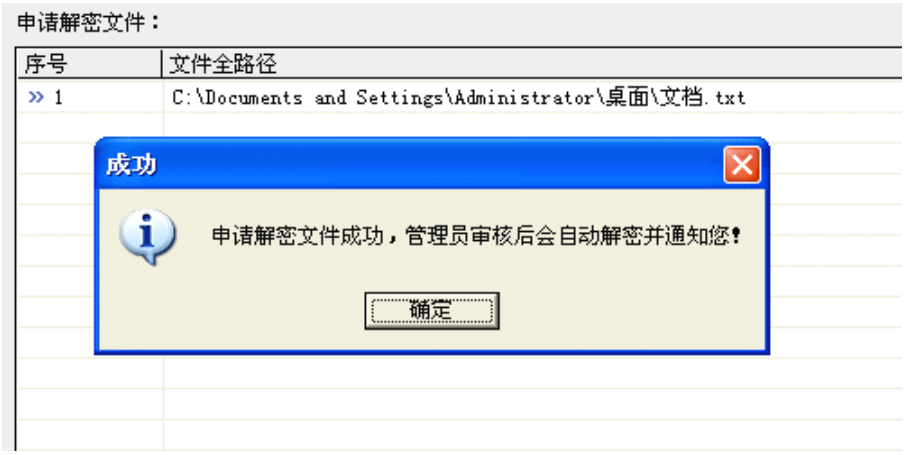
启，在线状态。客户端只需提交申请解密后，管理端则可响应申请，实施在线远程解密 。

启动在线同步解密工具后，可在任务栏右键点击该程序。点击 **[申请解密]**



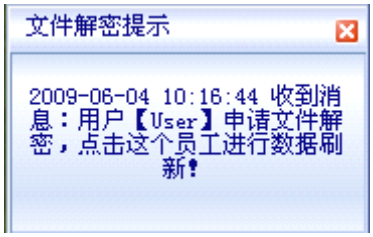


选择常见的原因、并填写解密原因。点击 [添加文件] 或 [添加目录]，选择被加密文件或目录。点击 [申请解密]，则为文档解密申请。



必须是 NETSYS AC 软件有开启的情况下，才可以实施在线同步远程解密。

点击申请后，有开启 NETSYS AC 的一端会再右下角有如下提示。

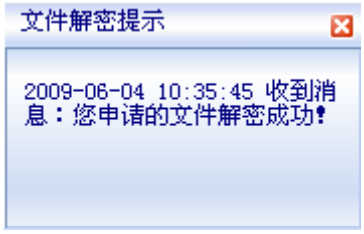


打开 NETSYS AC **[文档安全] → [文件解密] → [在线解密]**

选择对应的申请人员，可以看见申请信息

选中对应的申请信息，右键提供：
[同意解密所有文件]　[拒绝解密选中文件]　[拒绝列表所有文件]　[下载选中文件]

当点击同意解密所有文件的时候，NETSYS AC 则执行远程解密命令，对所申请的文件实施远程解密，并返回给申请人员审核后的信息。



- 使用 NETSYS AC 手工解密工具解密：

打开 NETSYS AC **[文档安全] → [文件解密] → [手工解密]**

选择相应部门、申请人员、原因，点击[添加文件]，选择被加密文件，点击[立即解密]，则为文档实现解密。解密文档后，通过点击[解密日志] ，可查看解密过文件的记录：

11.4 文档加密常见问题

- 客户端没有加密

  答：客户端不能加密有一下几个可能：

  1) 检查文件驱动是否正确安装成功
  2) 检查是否已经配置了企业加密密钥，已保存？
  3) 检查是否勾选了加密策略模板，已保存？
  4) 检查员工策略应用的模板，是否应用生效，且工作状态已加载成功？
  5) 配置后是否选中员工，重启了客户端

- 加密后的文件无法打开

答：

1) 加密后的文件如果是移植到其他非加密授权的主机，文件是无法打开的。
2) 如果启用本地客户端离开企业网络的加密策略，如离开网络后“不能使用”一项，或者“需要密码授权后才能使用”这一项。本地主机离开了企业网络后，文件是不能够被打开的。
3) 应用加密后，打开该加密的文件的软件或者插件，并未被定义到策略规则里面。

- 如何卸载客户端卸载文件驱动

  答：在桌面行为里，选择左栏的**[单机维护]** 或者 **[多机维护]** ，点击**[远程命令执行]**，选择对应的员工，点击按钮--- **[卸载文件驱动]**。或者使用客户端维护工具，点击按钮--- **[卸载文件驱动]。**则可以完成对文件驱动的卸载。

- 如何对对新的应用程序加密

  答：当用户需要加密的应用程序不在内置的控制应用程序列表时，需要增加新的应用程序加密策略来满足这个需求。需要在 [加密策略] 里手工添加。

12 网络磁盘

“网络磁盘”是 NETSYS AC 专属的存储空间，用户通过网络磁盘客户端登录的方式，可方便上传，下载文件，而独特的文件比较，权限管理，加密审批，邮件审批，打印审批功能更突破了传统存储的概念。

12.1 工作模式

NETSYS AC 的网络磁盘主要由 NETSYS AC 的管理软件与网络磁盘客户端构成。通过 NETSYS AC 主界面添加分配用户信息，磁盘信息。网络磁盘客户端通过用户名密码，登陆到 NETSYS AC 实现网络磁盘的应用。

12.2 基本功能

主要功能包括：

- 文件的上传/下载到网络磁盘的存储应用
- 用户权限管理的模版应用及其目录的访问控制
- 权限模板的定制，支持文件大小，后缀限制及审核权限控制
- 提供全盘文件搜索功能

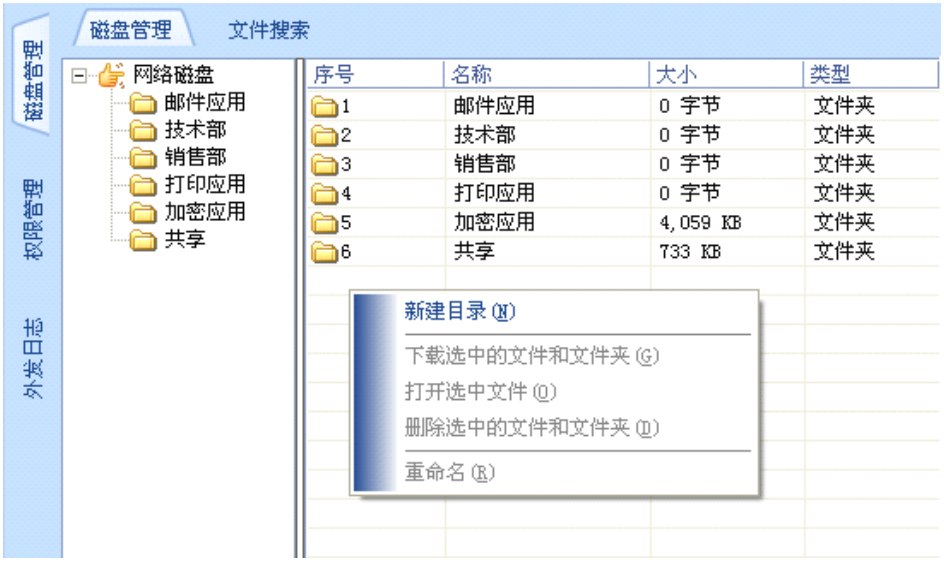
- 提供外发日志，磁盘的操作日志

12.3 基本配置

磁盘管理

点击 **[磁盘管理] → [磁盘管理]**

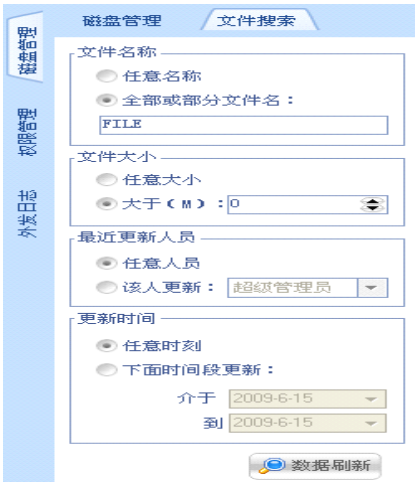
可以右键创建目录，删除目录或文件，重命名，并实现文件夹，文件的下载



文件搜索

点击 [磁盘管理] → [文件搜索]

可通过指定文件名称，文件大小，更新人员及更新时间来实现文件的搜索。如输入： file ，点击按钮 [数据刷新] ，则可在右栏显示搜索到的文件。



序号	文件名称	所在目录	最近更新时间	最近更新人员	文件大小
» 1	Filemon.exe	/共享/Filemon.exe	2009-06-10 16:30:39	TEST	724 KB

用户管理

点击 [权限管理] → [用户管理]，可右键添加用户，并支持批量添加。

通过输入用户信息，并选择对应的权限模板，可完成自定义网络磁盘用户的配置。

批量添加，NETSYS AC 支持对现有已经添加的员工批量添加进网络磁盘，并应用统一模板和密码，实现批量添加。

输入默认密码，选择权限模板，勾选要添加的员工，点击确定，可完成对员工批量添加到网络磁盘。

权限管理

点击 [权限管理] → [权限模版]

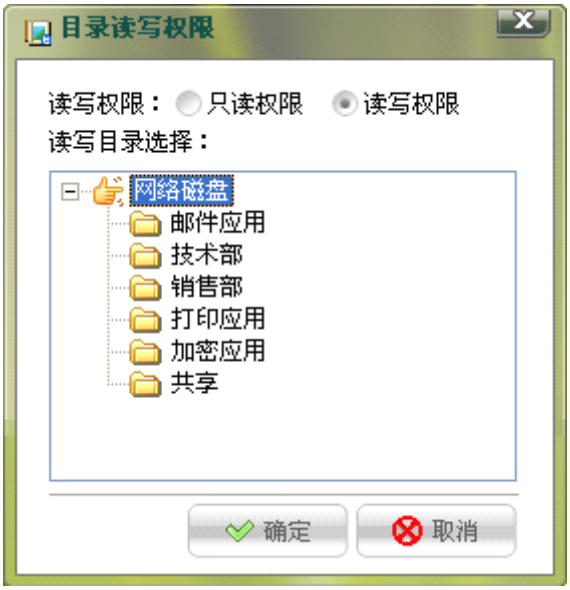
点击 [添加模板]，输入模版的名称后，可对该模版进行配置。

点击创建的模版，可在右栏对该模版进行功能定制。

包括：

- 支持对单个文件上传大小的限制
- 支持对上传文件的类型进行限制，并支持多种后缀
- 支持审核权限的定制
- 支持对指定目录进行操作机器读写的权限

注：审核权限控制的勾选应用，直接体现在网络磁盘客户端的功能界面上。用户可以根据实际操作需要，对模版分配不同的操作权限，并支持添加 可操作的目录，并指定读写权限



外发日志

NETSYS AC 网络磁盘，提供了对延迟审批的功能，包括：

加密审批：NETSYS AC 提供了文档加密功能，文件的解密，可依赖 NETSYS AC 网络

磁盘来中转，实现加密文件的提交，以便管理人员审核后实施解密后进行外发。

外发审批：针对某些企业对邮件外发的安全性，NETSYS AC 提供了对邮件审批，延迟代发功能。

打印审批：针对某些企业对文件打印的安全性，NETSYS AC 提供了对打印文件的审批功能。

通过网络磁盘客户端的应用申请，网络磁盘的针对审核后的动作，进行记录，其中包括：

- 文件解密日志
- 资料外发日志
- 文件打印日志

可以分别点击文件解密，资料外发，文件打印进行查看

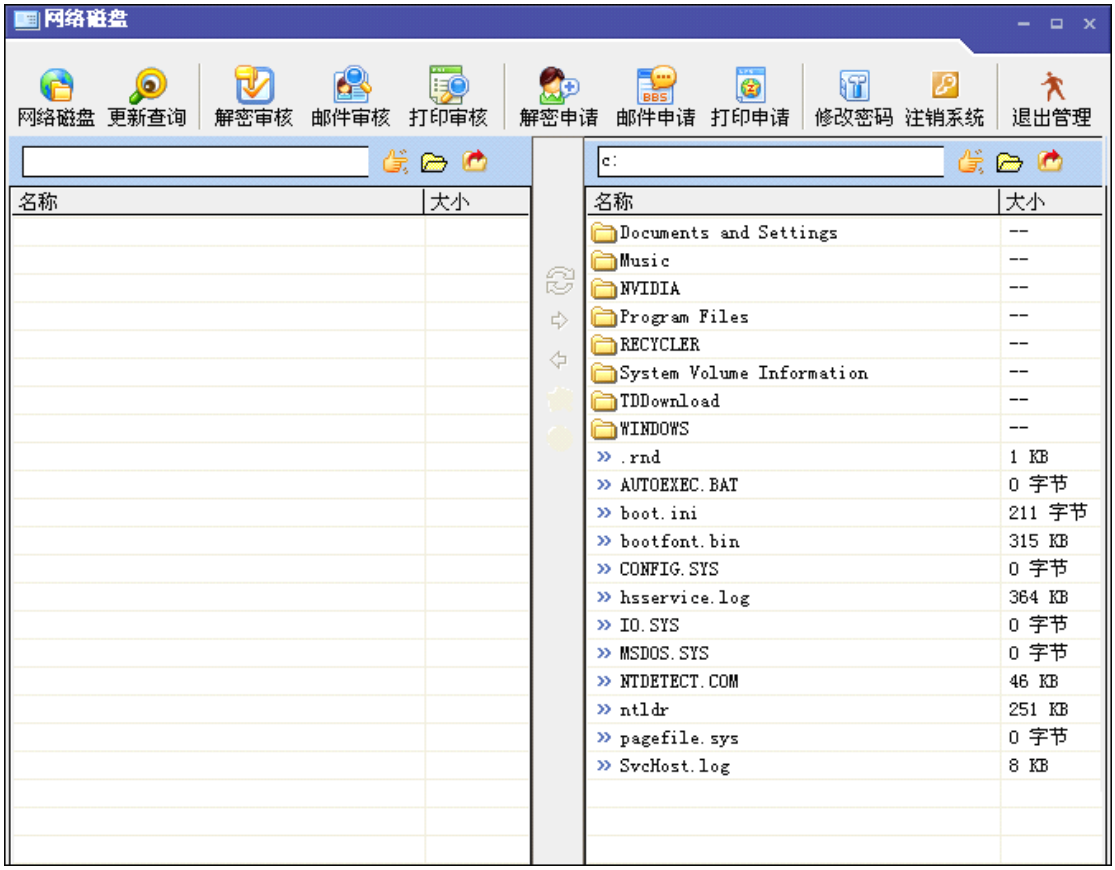
点击 [外发日志] → [磁盘操作日志]

可以查看到详细的对整个磁盘的使用情况

序号	记录时间	文件操作	操作人员	操作对象信息
1	2009-06-09 00:20:50	创建目录	系统 超级用户	/测试
2	2009-06-09 00:20:58	删除目录	系统 超级用户	/测试
3	2009-06-09 00:21:05	创建目录	系统 超级用户	/共享
4	2009-06-09 00:22:29	创建目录	系统 超级用户	/技术部
5	2009-06-09 00:22:40	创建目录	系统 超级用户	/销售部
6	2009-06-09 00:22:59	创建目录	系统 超级用户	/加密审核
7	2009-06-09 00:23:12	删除目录	系统 超级用户	/加密审核
8	2009-06-09 00:23:19	创建目录	系统 超级用户	/加密应用
9	2009-06-09 00:23:40	创建目录	系统 超级用户	/邮件应用
10	2009-06-09 00:27:45	创建目录	系统 超级用户	/打印应用

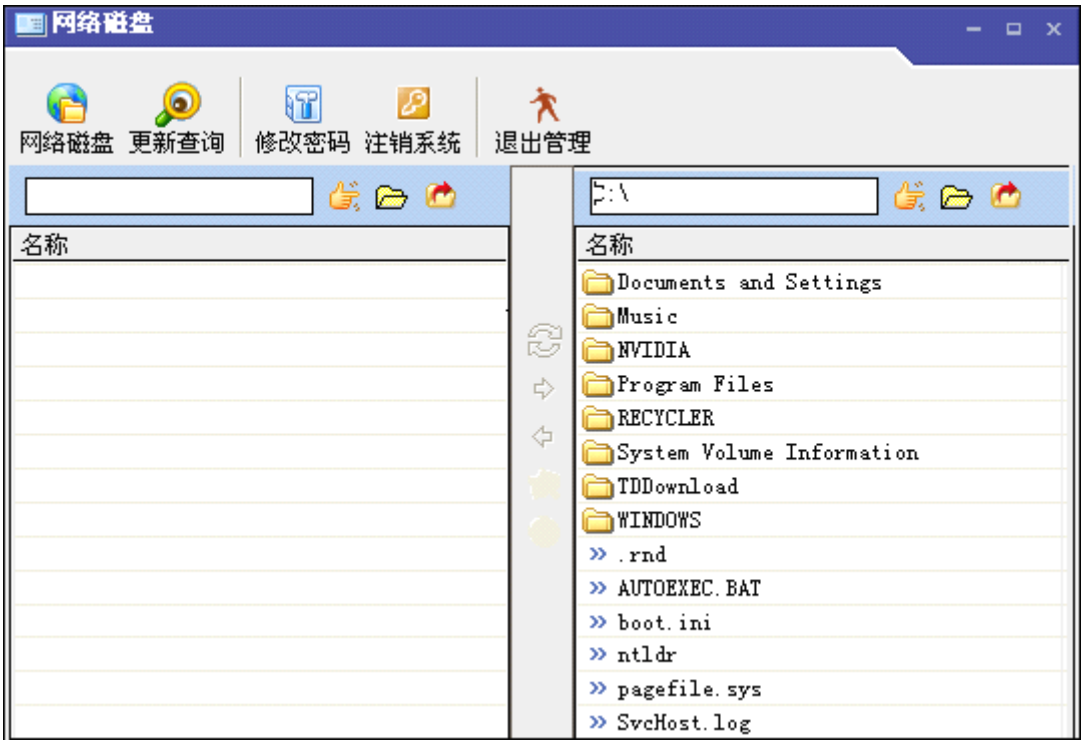
当配置网络磁盘的权限模版都勾选以下功能时候

网络磁盘的登录界面将根据勾选的选项，在界面上将功能模块显示出来。如下图：



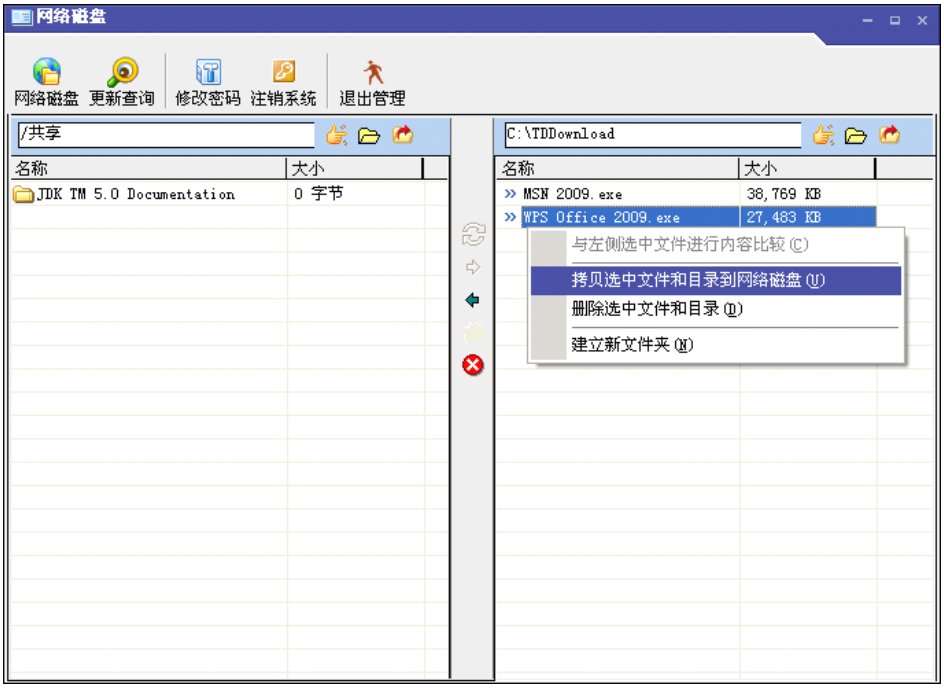
网络磁盘

点击 [网络磁盘] ，可见左栏为网络磁盘的操作目录，右栏为本地目录。



点击图标  可以选择用户对应的操作目录

通过点击左栏  选择需要上传文件的目录，选中文件右击，点击 [拷贝选中文件和目录到网络磁盘] 或者点击 中间按钮  ，则可实现到网络磁盘的上传。



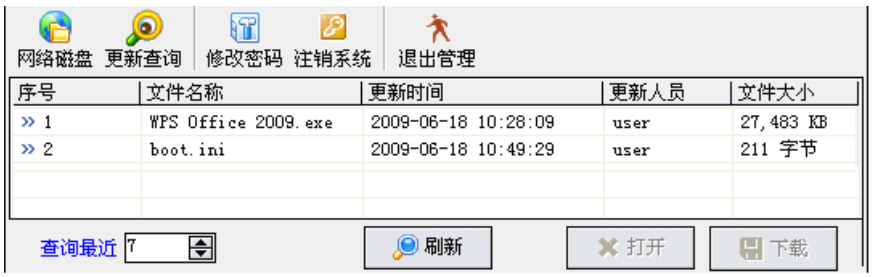
 文件内容比较 ，  下载文件到本地磁盘，  上传文件到网络磁盘，

 删除网络磁盘选中的目录或文件，

 删除本地磁盘选中的目录或文件。

查询更新

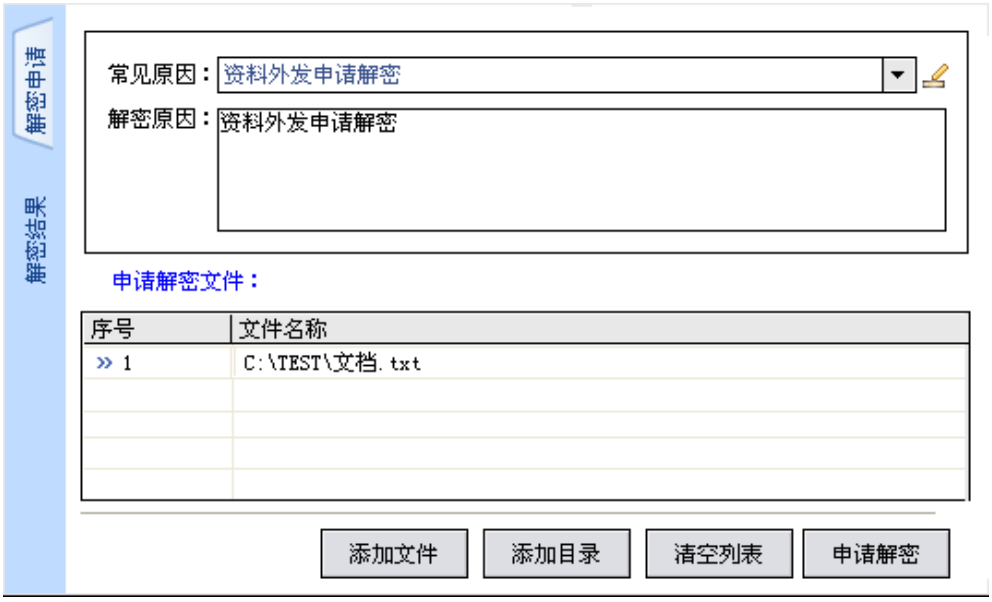
填写查询最近日期，可刷新显示网络磁盘的文件变动。并可以实现对文件的打开，下载 。

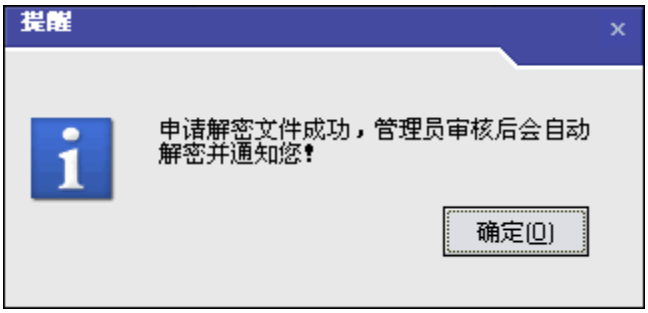


解密申请

网络磁盘客户端可供了文档加密解密申请功能，通过网络磁盘，可提供对已经加密的文件的提交解密申请，并实现界面提示和申请解密的结果日志。

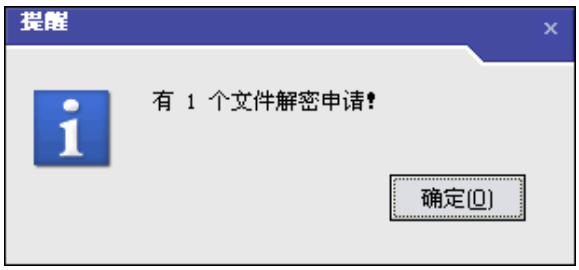
点击 **[添加文件]** 或 **[添加目录]** ，添加需要解密的文件，再点击 **[申请解密]**， 则完成对加密文件的解密申请。



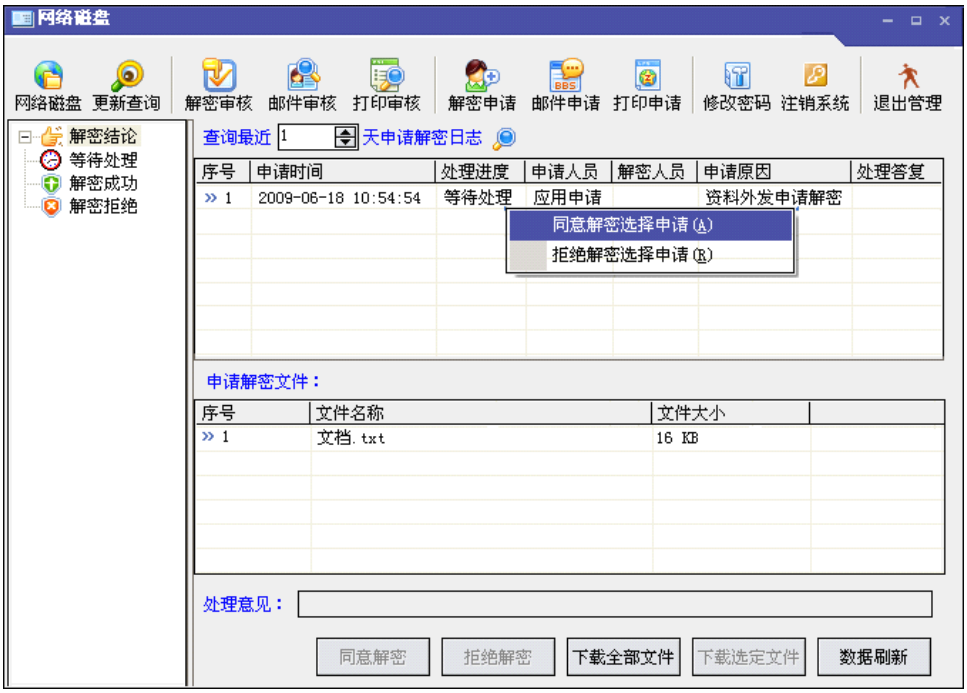


解密审核

使用网络磁盘客户端登陆到具备解密审核权限的账户后，若有解密申请，有如下提示：



点击[解密审核]进入解密审核的界面，可以看到由客户端机器发送而来的解密申请。



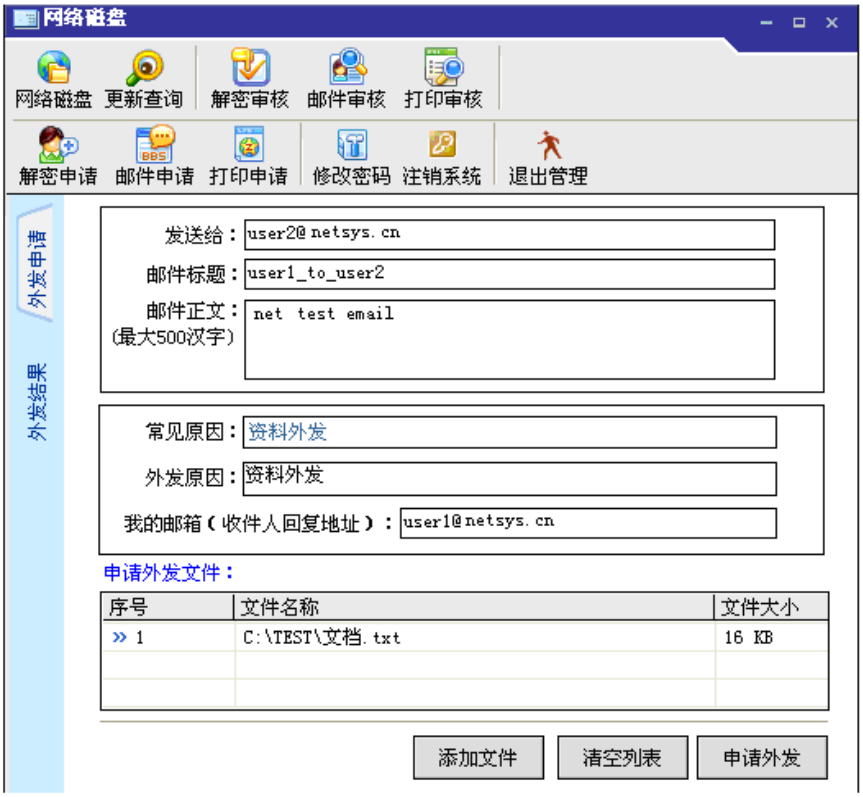
选中对应的审核请求信息，可实现该请求“同意解密”及“拒绝解密”。并且可以选中所申请的解密的文件，下载到本地进行查看。只需选中对应的文件，点击 [下载全部文件] 或者 [下载选定文件] 来实现对申请文件的查看。

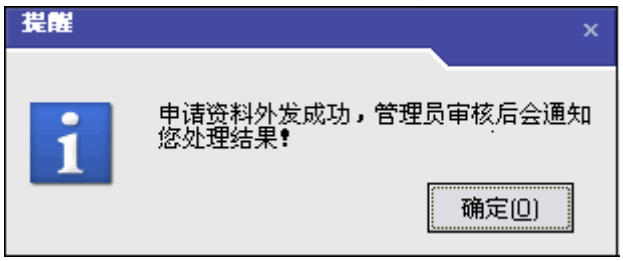
邮件申请

使用邮件申请，网络磁盘客户端需要填入以下参数

- 指定收件人的电子邮箱地址
- 邮件标题
- 正文
- 并且填入自己的电子邮箱地址
- 添加需要外发的附件

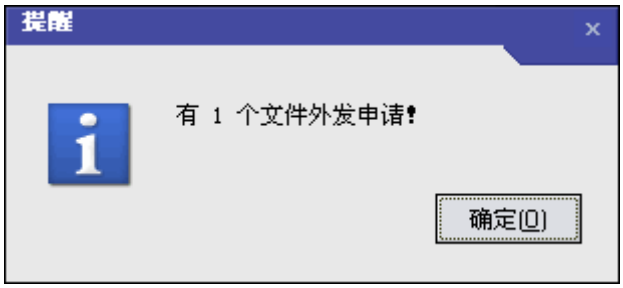
点击 **[申请外发]** 后 ，该邮件则自动上传到网络磁盘，等待邮件审核管理员的审批。



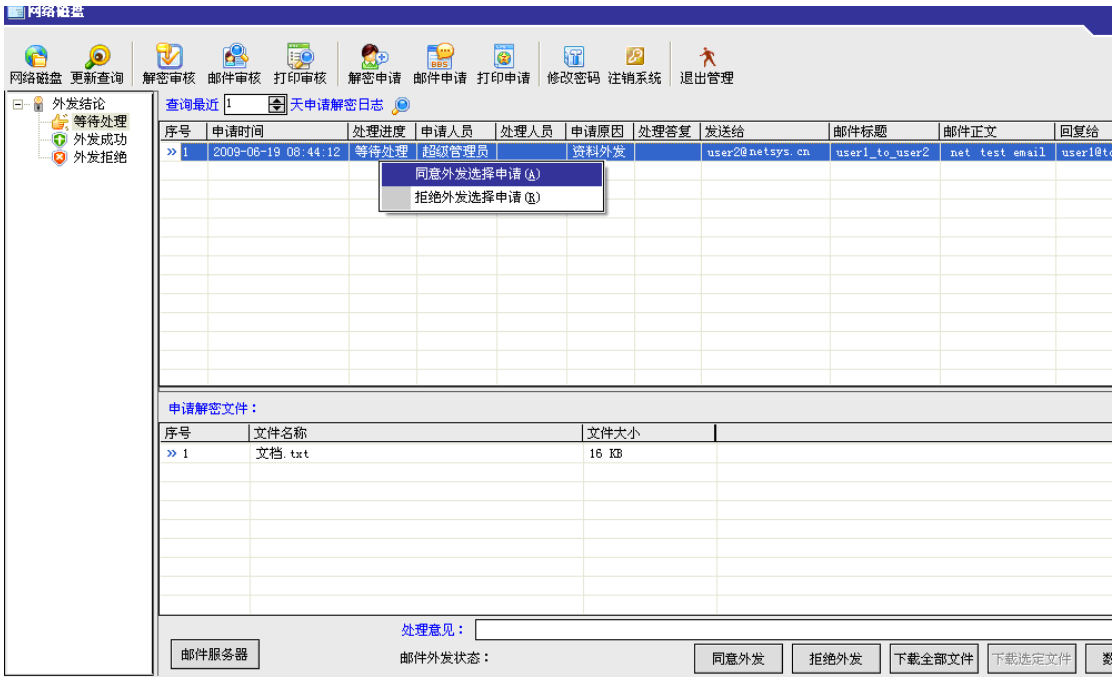


邮件审核

使用网络磁盘客户端登陆到具备邮件审核权限的账户后，若有邮件申请，有如下提示：



点击 **[邮件审核]** 进入邮件审核的界面，可以看到由客户端机器发送而来的邮件申请。



注：在同意外发前，我们需要对邮件服务器进行设置。

网络磁盘邮件审核功能，其功能主要是定义管理员邮箱进行代发，NETSYS AC 提供网络磁盘来延迟审核，从而代理发送邮件。以下，则是配置管理员邮箱的配置信息。

邮件服务器：为管理员邮箱对应的邮件服务器地址，如 mail.NETSYS AC.cn

由于主流的门户网提供的邮箱服务并不提供邮件服务器名来登录校验，需要配置成 smtp.xxx.yyy 进行登陆校验。如 smtp.sina.cn

当完成对邮件服务器的配置后，选中对应的审核请求信息，可实现该请求“同意外发”

及“拒绝外发”。并且可以选中所申请的邮件是附件，下载到本地进行查看。

只需选中对应的文件，点击 [下载全部文件] 或者 [下载选定文件] 来实现对申请文件的查看。

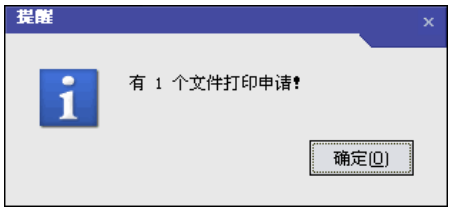
当完成了同意外发，或者是拒绝外发时，都将在外发结论中进行记录：

打印申请

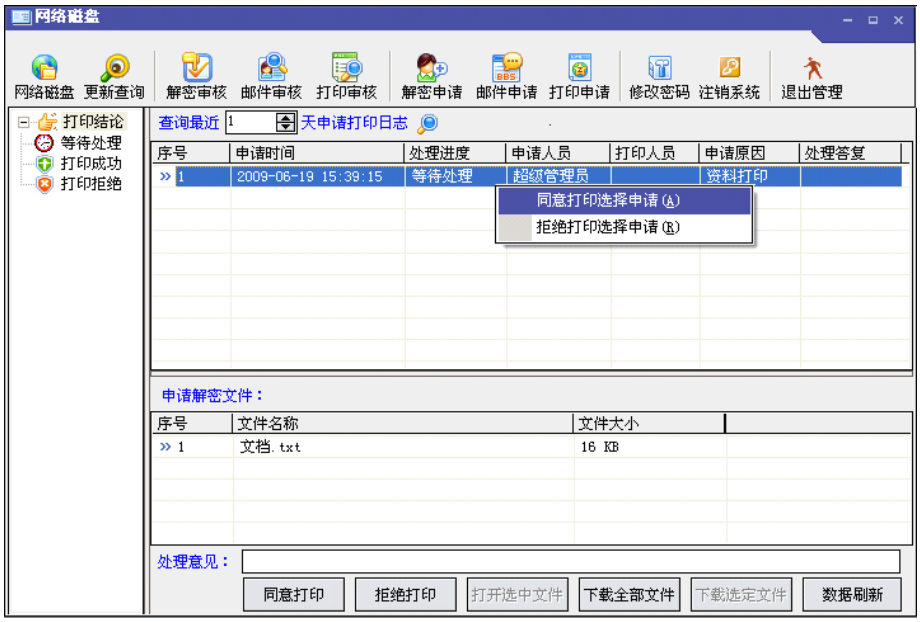
填入打印原因，点击 **[添加文件]** 需要打印的文件，点击 **[申请打印]** 后，需要打印的文件则会自动上传到网络磁盘，等待打印审核管理员的审批。

打印审核

使用网络磁盘客户端登陆到具备打印审核权限的账户后，若有打印申请，有如下提示：



点击 **[打印审核]** 进入打印审核的界面，可以看到由客户端机器发送而来的打印申请。



选中对应的审核请求信息，可实现该请求“同意打印”及“拒绝打印”。并且可以选中所申请的邮件是附件，下载到本地进行查看。

只需选中对应的文件，点击 **[下载全部文件]** 或者 **[下载选定文件]** 来实现对申请文件的查看。

当完成了同意打印，或者是拒绝打印时，都将在打印结论中进行记录：