终端行为管理产品(标准版)

安装及使用手册

[版本号: TCM-1.5]

北京金万维科技有限公司

http://www.gnway.com/

金万维 GNWAY

【版权声明】

终端行为管理产品(标准版)安装及使用说明

2014 年 04 月 28 日

北京金万维科技有限公司
Beijing GNWAYTechnologyCO.,LTD
北京金万维科技有限公司，100070
电话（TEL）:010-63701717-8137
传真（FAX）:010-52285616
电子信箱：tsa@gnway.com

本手册将定期更新，如欲获取最新相关信息，请访问金万维网：www.gnway.com 或者发送邮件到：tsa@gnway.com

目录

1. 文档说明

1.1. 关联文档

文档名称	说明
TCManager_help.chm	TCM 管理端帮助文档
终端行为管理-TCM(高级版)安装使用手册	与标准手册类似，不同之处是引用了第三方软件

1.2. 术语与缩写解释

本文档中的约定俗成的术语：

术语	英文	说明
客户端	Client	与代理同一个含义,都指安装在被审计的服务器或者终端电脑上的程序.
服务器	Server	指所有客户端需要保持连接的同一个服务器,该服务器对这些客户端进行统一管理的服务.
管理端	Manager	指管理终端,管理员通过该终端程序,连接到服务器,对客户端进行统一管理.

1.3. 文档中使用图列说明：

[ ] ：[ ] 中内容指的是系统平台中用的程序模块功能名称；

【】 ：【】中的内容指在程序安装的过程中下一步安装的指示；

2. 产品介绍

2.1. 终端行为管理产品简介

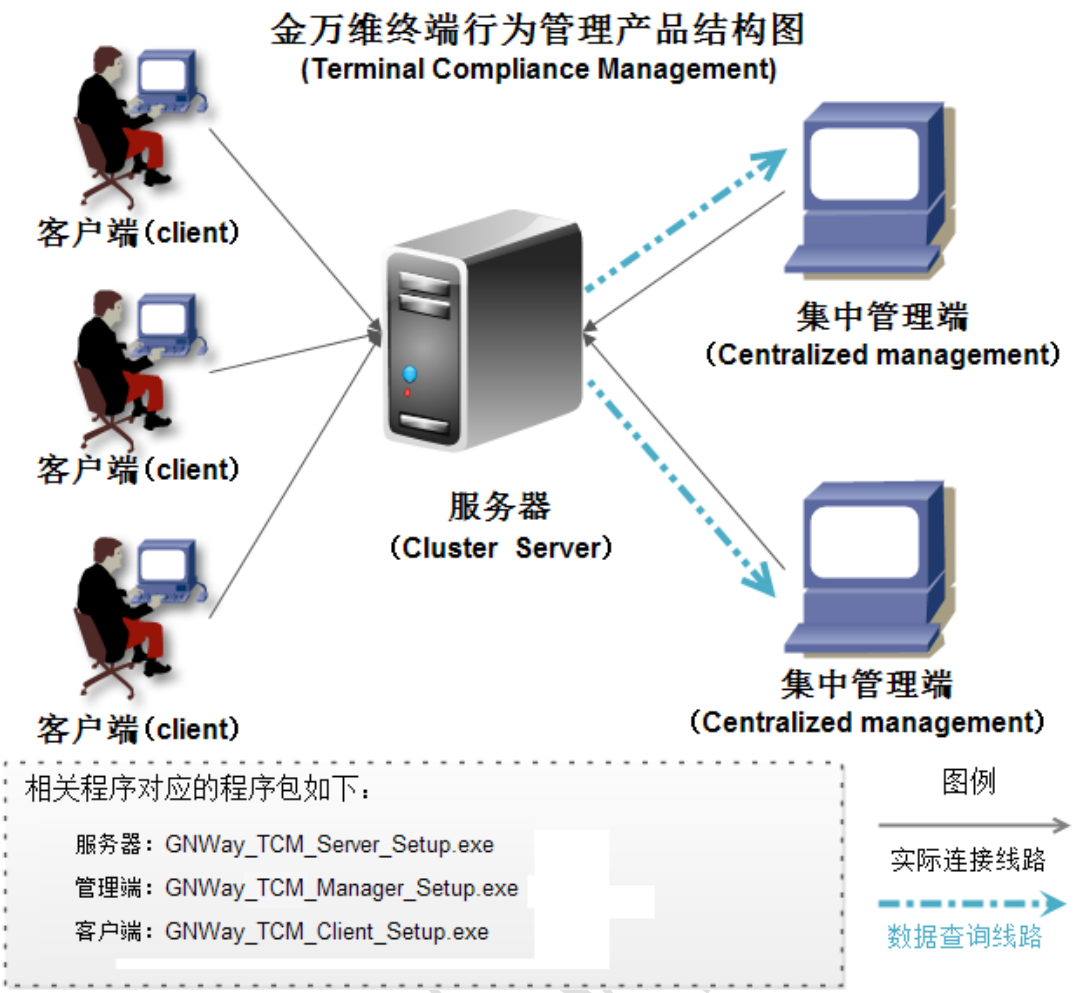
终端行为管理产品，通过对主机本地操作行为的录像,实现主机行为审计。

终端行为管理产品是一款软件产品,它提供以“截屏”方式来进行选择性操作监控，进而对用户在计算机上的所有操作行为审计。

该产品部署后,可以选择性监控、录像、审查、回放用户在计算机上的操作行为，从而可帮助客户洞悉员工是否符合信息访问、操作规范性和知识产品保护的既定要求。该产品简单,稳定,具有良好的可靠性和易用性,可广泛应用于需要加强员工行为控制、加强责任认定和完善授权管理的部门和领域。

2.2. 产品结构

终端行为管理产品包括三个安装程序，分别是：服务器端、客户端、管理端。三个程序在系统中的配合,分别如图所示:



服务器：

此程序安装在一台服务器上。被客户端必须与汇总服务器通过网络连通，所有的数据都会被传送到汇总服务器端。此程序主要是进行对截屏录像的管理、对截屏录像的查询检索，采取分布式部署对截屏录像的汇总而进行集中管理。

客户端：

此程序安装在每个被监控的主机上，用于对这些主机上的行为进行监控和记录。

管理端：

此程序安装在管理人员的机器上，管理端通过与服务器端的交互，来对各个被审计的主机进行管理，主要作用是对各个客户名单上面的录像信息进行检索、播放。

2.3. 产品 License 授权说明

授权	说明
标准版	1、主要是 windows 环境下的运维审计或者操作监管
	2、用户数量不多,对性能要求不高,够用即可
高级版	1、主要是 windows 环境下的运维审计或者操作监管
	2、用户数量比较多,因而对性能有要求
	3、 对 24 小时不间断运行要求苛刻

备注：

1、 高级版需要配置数据库接口(所有符合 ODBC 接口标准的数据库均可适用)

2、 关于高级版的数据库软件安装及配置请参考《终端行为管理-TCM(高级版)安装使用手册》

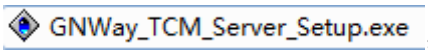
3. 准备工作、安装步骤

3.1. 准备工作

在准备安装程序之前，我们需要做如下的准备工作：

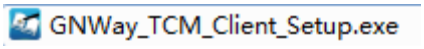
1、 服务器端：准备一台服务器作为服务器，并安装有 Windows 系列操作系统，强烈建议采用 server2003 或者 2008-32 或 2008-64 位的系统作为服务器；

准备服务器安装包：GNWay_TCM_Server_Setup.exe

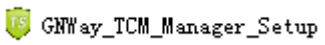


；

2、 客户端：在被审计的电脑上所要安装程序是：GNWay_TCM_Client_Setup.exe



3、 管理端：在管理端需要安装的程序是：GNWay_TCM_Manager_Setup.exe



准备好以上工作就可以进入安装配置阶段。接下来，针对服务器端、客户端、管理端的安装步骤将给予详细的讲解。

3.2. 服务器安装步骤

双击金万维 TCM 安装程序 GNWay_TCM_Server_Setup.exe，进入“金万维 TCM 服务器安装向导”界面，如下图：

点击【下一步】进入 TCM 服务器安装界面，按照安装向导提示进行 TCM 服务器的安装，

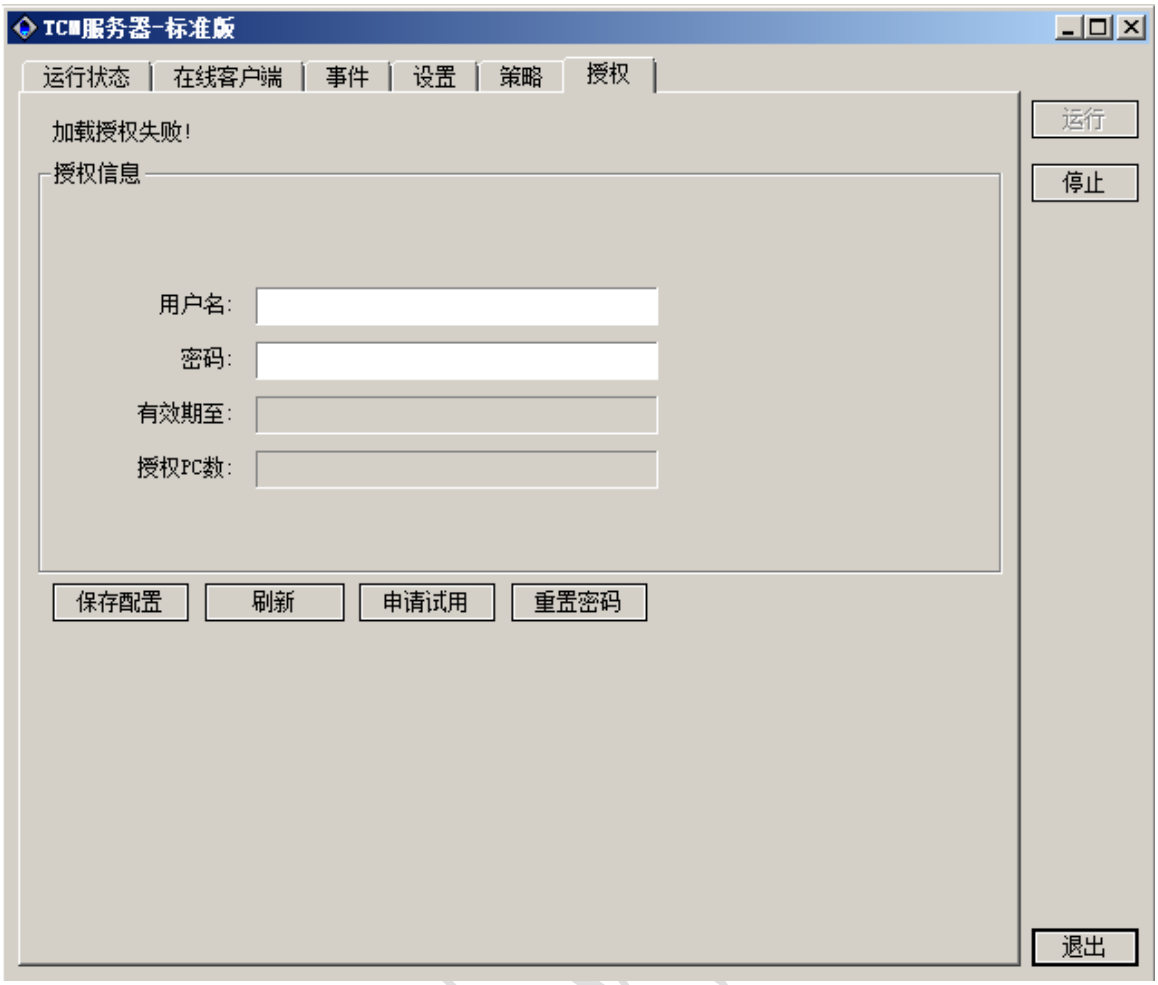
点【完成】就完成了 TCM 服务器的安装，如下图：

3.2.1. 服务器端配置操作

对服务器的相关的配置操作，可以通过 TCM 服务器端界面程序进行相关的配置操作。关于此部分的配置操作见手册中的 TCM 服务器端使用说明。(跳转至使用说明)。

3.2.2. 申请 TCM 程序免费试用账号

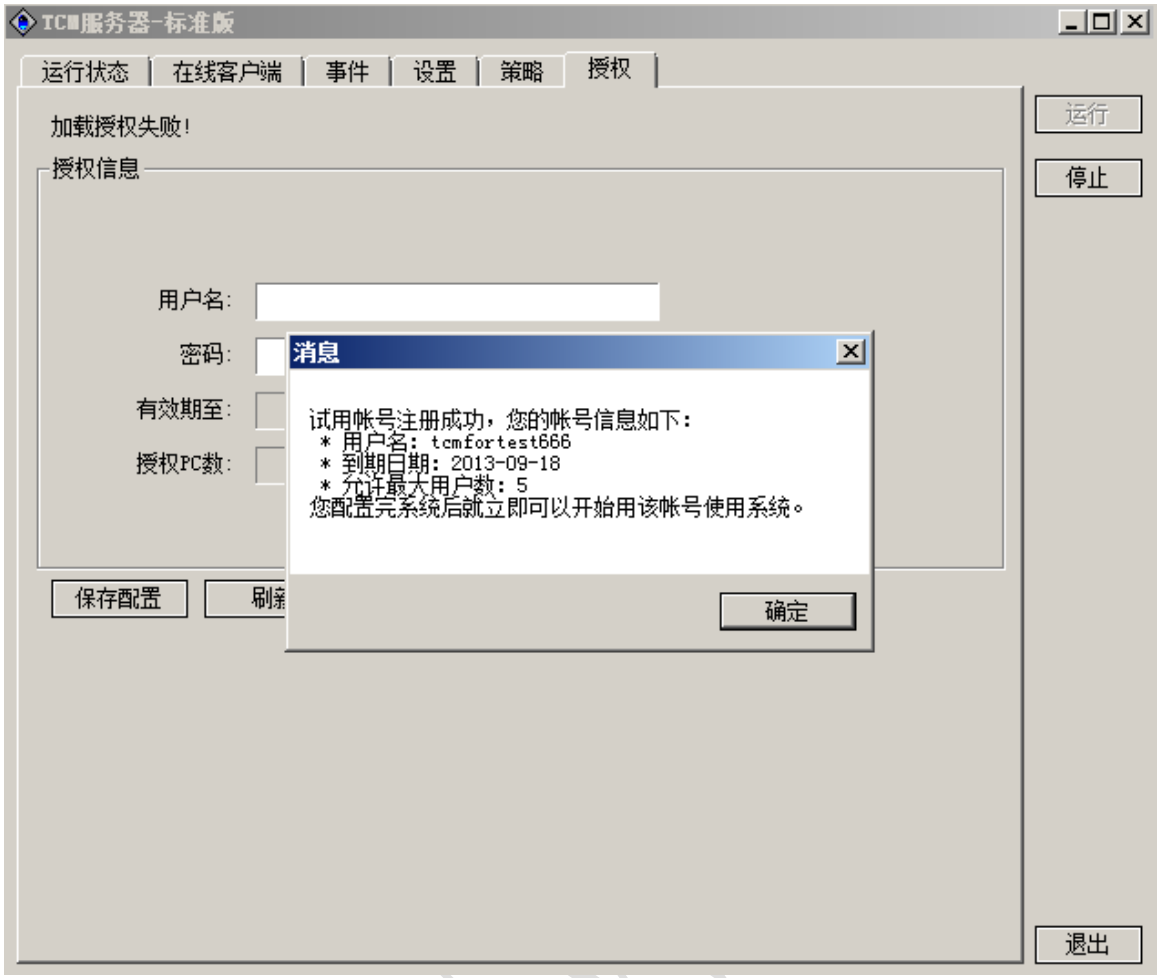
双击 TCM 服务器快捷方式，点击“授权”到如下图界面：


TCM服务器-标准版
运行状态
在线客户端
事件
设置
策略
授权
加载授权失败!
授权信息
用户名:
密码:
有效期至:
授权PC数:
保存配置
刷新
申请试用
重置密码
运行
停止
退出

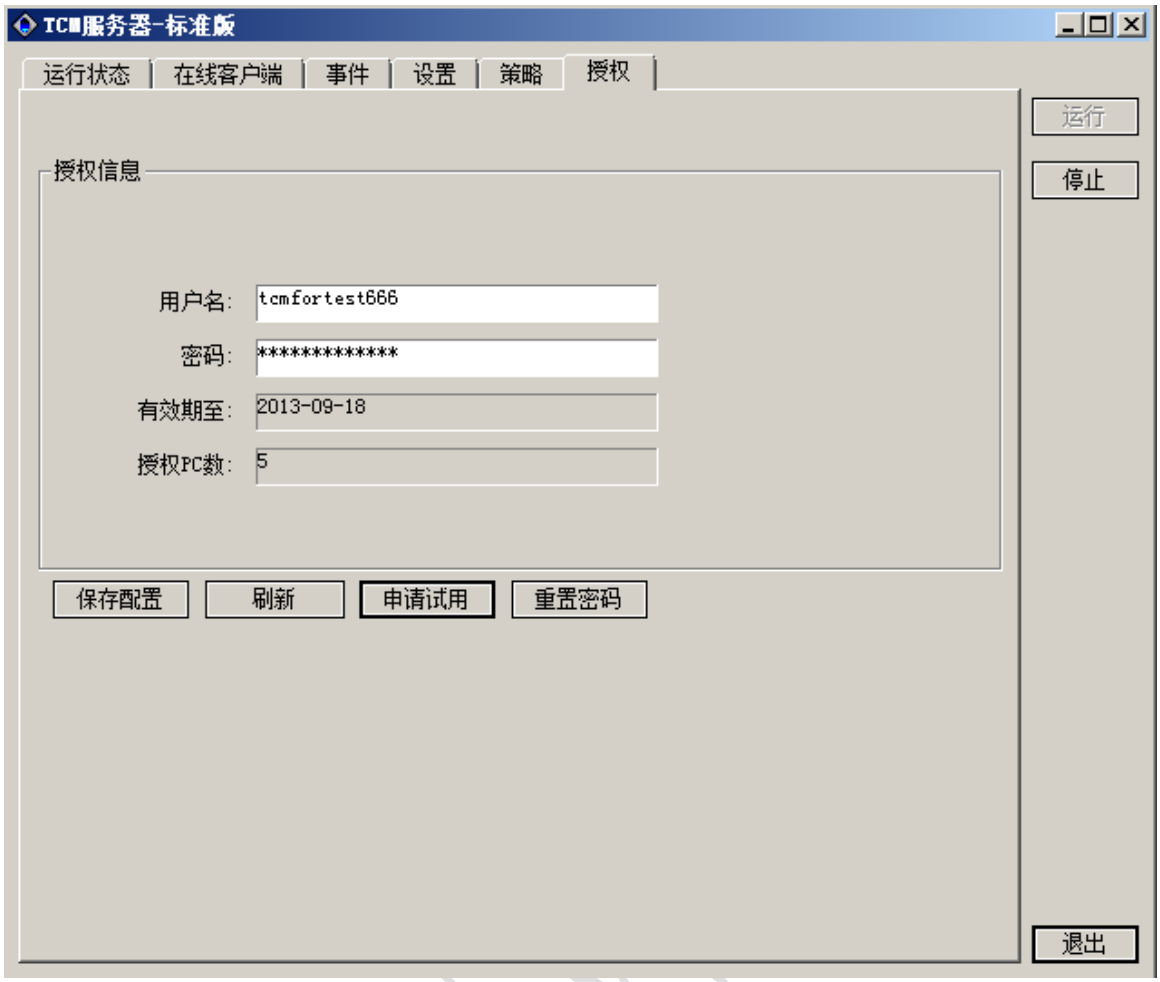
点击【申请试用】如下图，

输入注册试用账户的相关合法信息(用户名：字母数字组合，大于六个字符；密码长度大于七个字符；E-mail 地址便于遗忘账号密码时候找回账号密码)，如下图。

点击“注册”，如果填写合法且网络完好，将给予如下注册成功的提示信息：

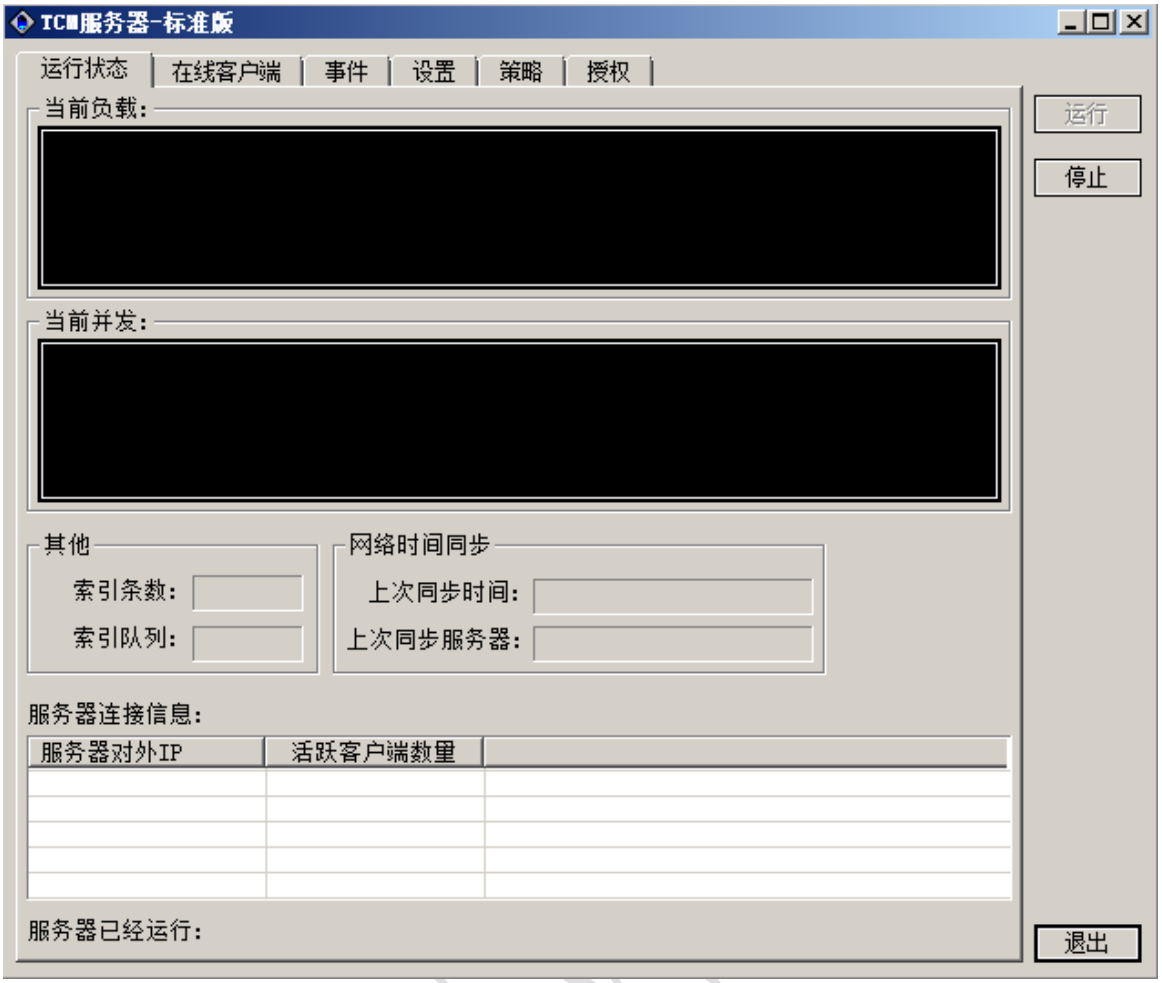


点击“确定”，就成功申请了试用期为 15 天，最大用户数为 5 的免费账号，如下图：



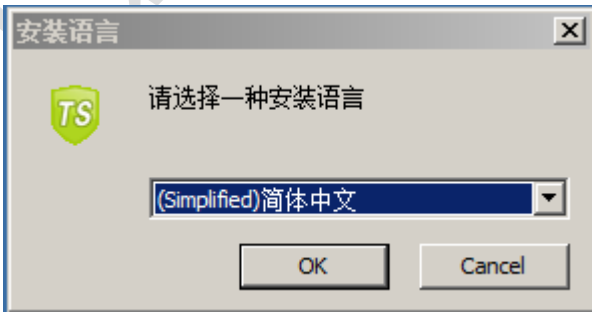
3.2.3. 启动服务

找到 TCM 服务器，双击即可执行程序，如下图：



3.3. 集中管理端(金万维 TCM 管理端)安装步骤

双击金万维 TCM 安装程序 GNWay_TCM_Manager_Setup.exe,选择安装语言，如下图：



点击【OK】，进入“金万维 TCM 管理端安装向导”界面，如下图：

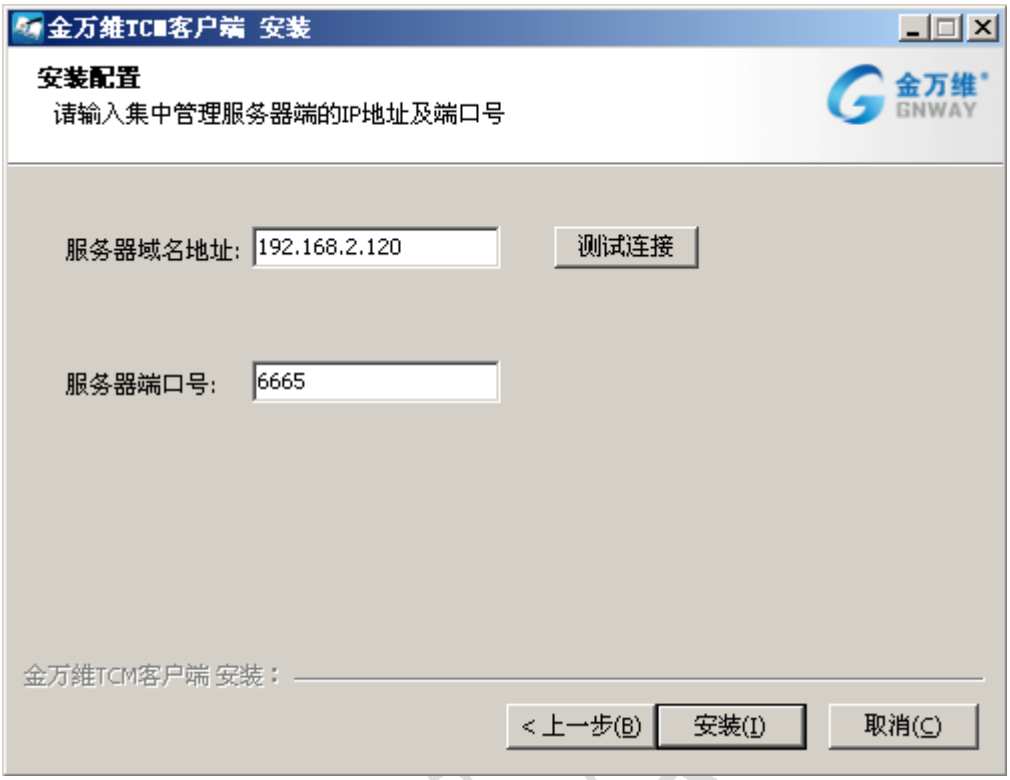
点击【下一步】进入 TCM 管理端安装完成界面，点【完成】就完成了 TCM 管理端的安装，如下图：

3.4. 客户端安装步骤

双击金万维“TCM 客户端”程序，进行【下一步】安装，如下图：

继续选择【下一步】，进入到安装路径选择页面，如下图：

继续选择【下一步】，进入“安装配置”界面，如下图：



说明：

[服务器域名地址]：指要连接到服务器的地址，包含服务器的固定 IP 或者服务器上装的域名解析软件地址；

[服务器端口号]： 指“TCM 客户端”与“TCM 服务器”端的通信端口号，此端口号默认为：6665

选择【安装】，TCM 客户端自动安装到完成，点击【完成】即可，如图：

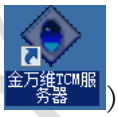
4. 使用手册

4.1. TCM 服务器端使用说明

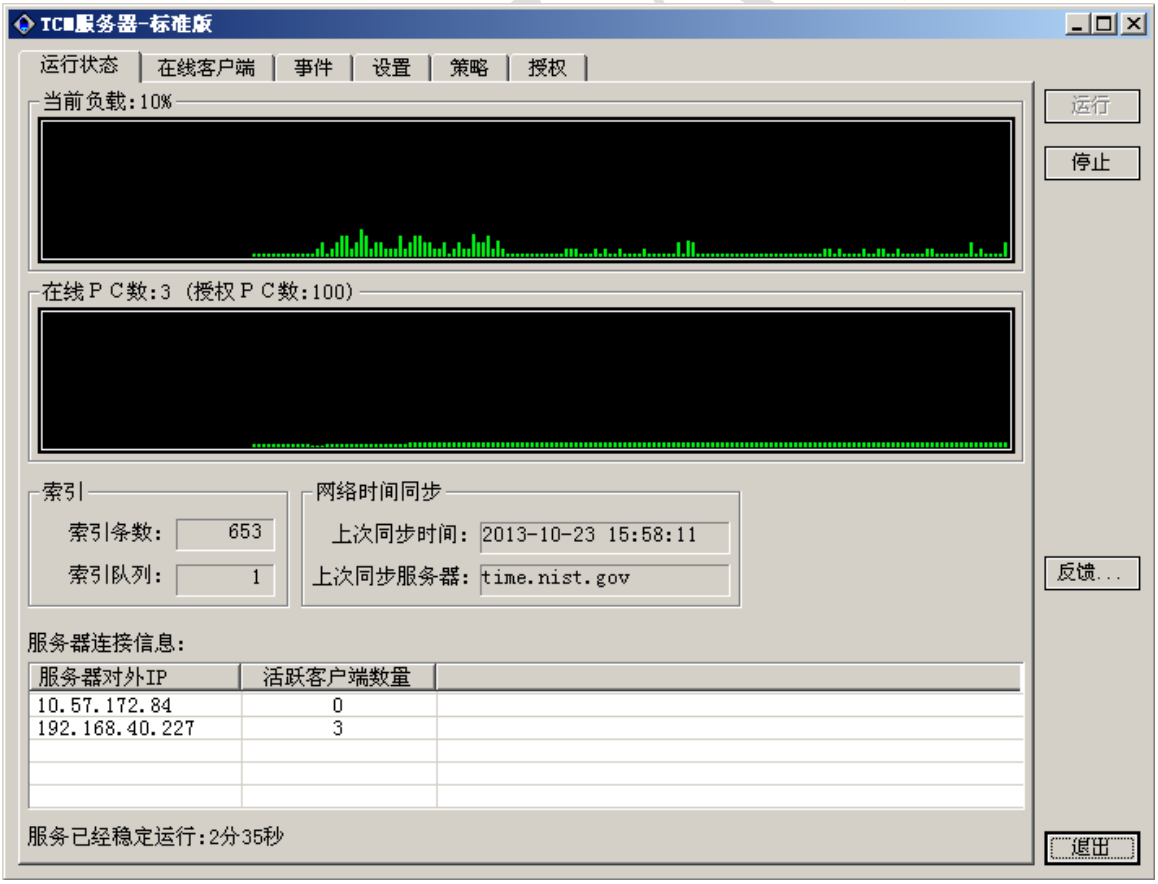
客户端必须与服务器通过网络连通，所有的数据都会被传送到 TCM 服务器端。

在 TCM 服务器端，可以通过 TCM 服务器界面进行相关信息的配置，配置后的参数应用在 TCM 客户端和 TCM 管理端上，关于 TCM 服务器界面配置说明如下文所述。

服务器 TCM 服务器界面说明及使用

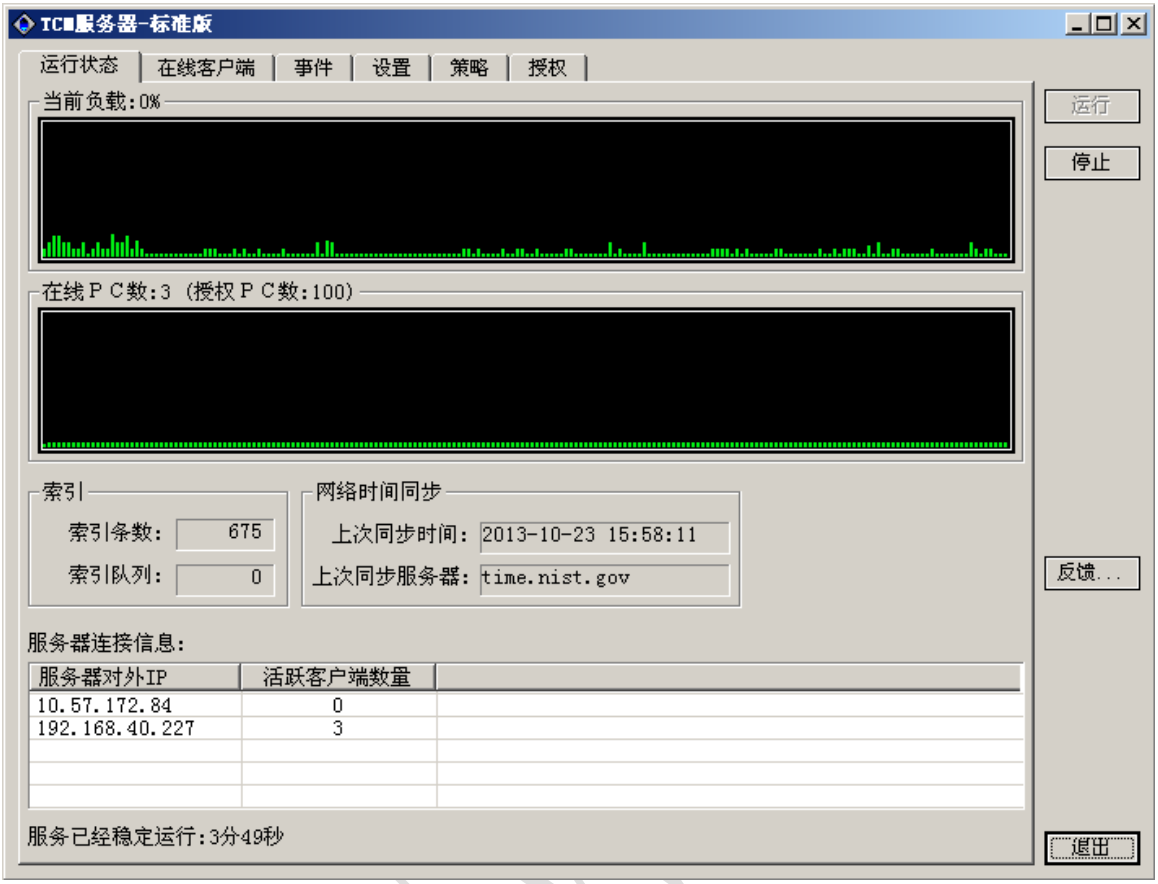
安装好 TCM 汇总服务的程序后，双击 TCM 服务器(快捷方式： 

)就会弹出如下的界面，此时已启动了服务，如下图：



TCM 服务器有六部分组成：运行状态、在线客户端、事件、设置、策略、授权，每一块的说明如下。

【运行状态】



显示当前负载、当前并发、索引条数、索引队列、网络时间同步、服务器连接信息以及当前服务器运行的时间。

说明：当前并发(在线并发/授权并发)，默认的授权并发为 5 个(通过申请试用获得)。

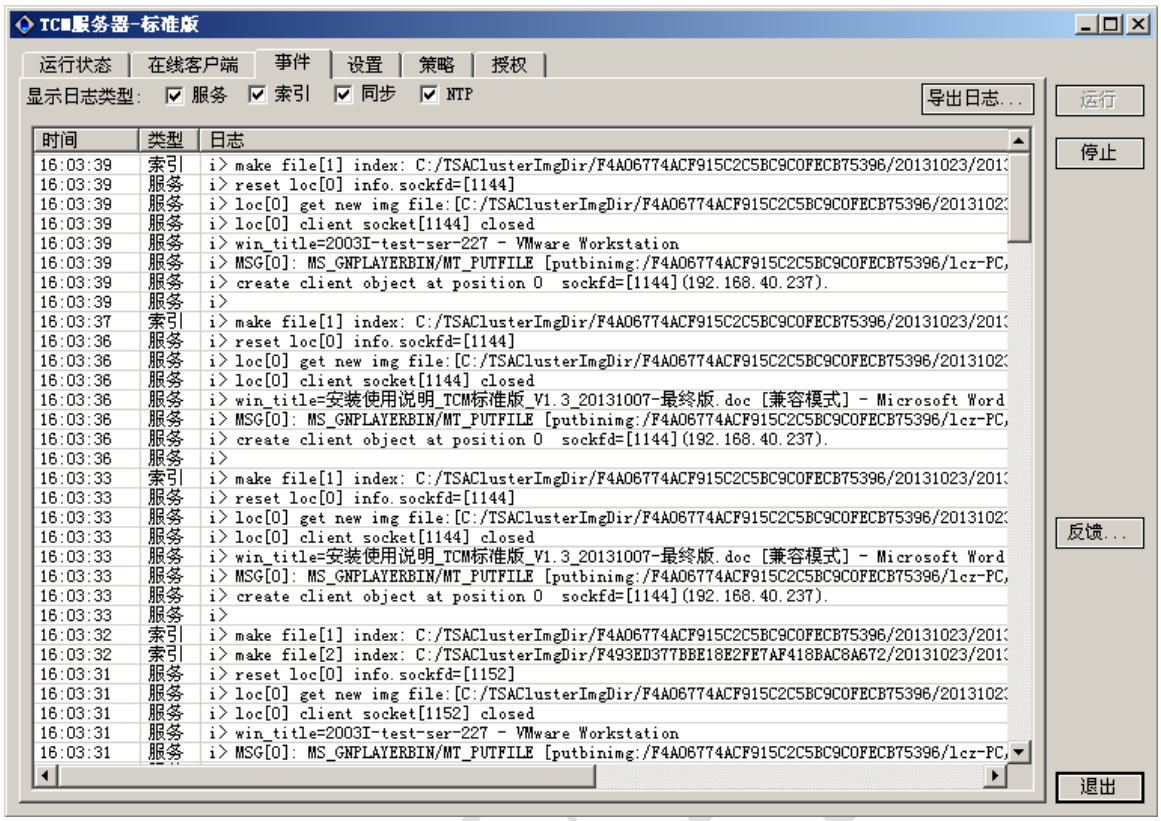
【在线客户端】

在线客户端：显示的当前在线的“TCM 客户端”的相关信息，包括主机 ID、主机 IP、主机名、当前登录的用户名、启动时刻、时间误差及等待队列等，并在状态栏显示当前在线“TCM 客户端”的 PC 数目，如上图。

说明：时间误差在 60s 之下说明为正常的。

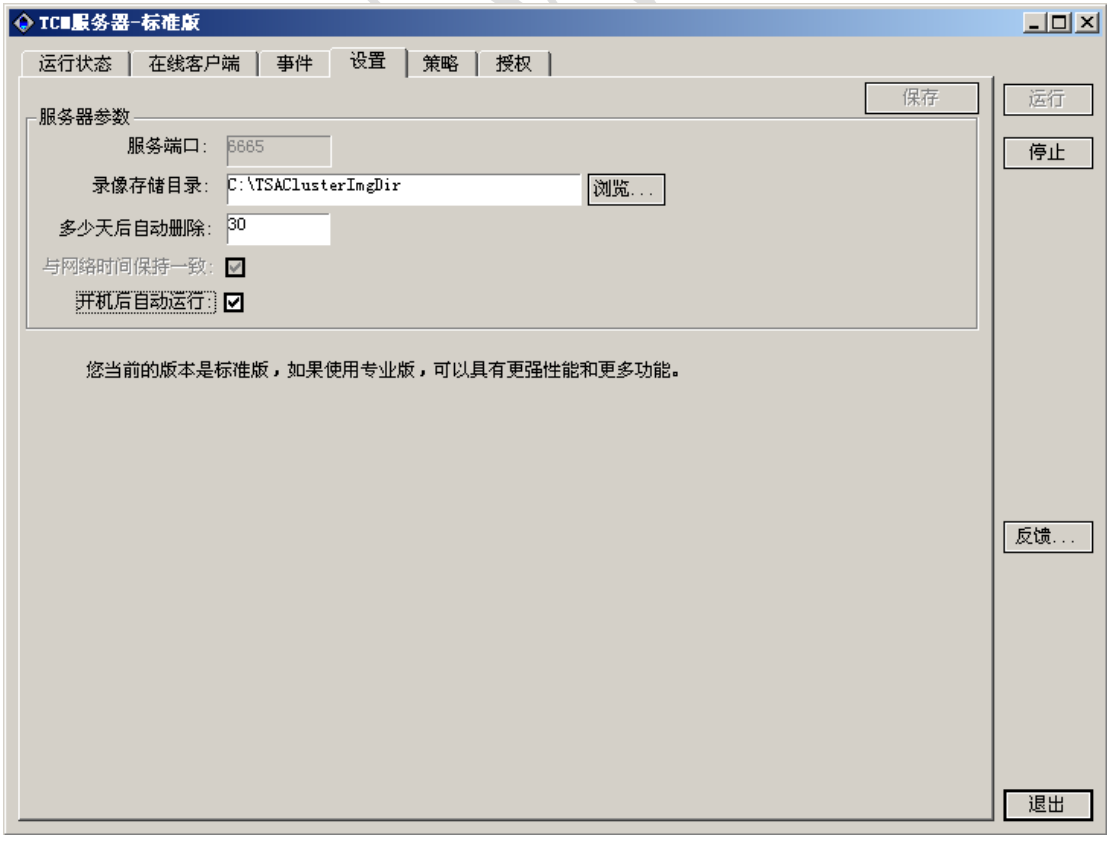
【事件】

显示的是“TCM 客户端”与“TCM 服务器”端进行交互的日志信息，见下图：



【设置】

客户端与服务器端的交互信息的配置页面，如下图：



服务器参数：

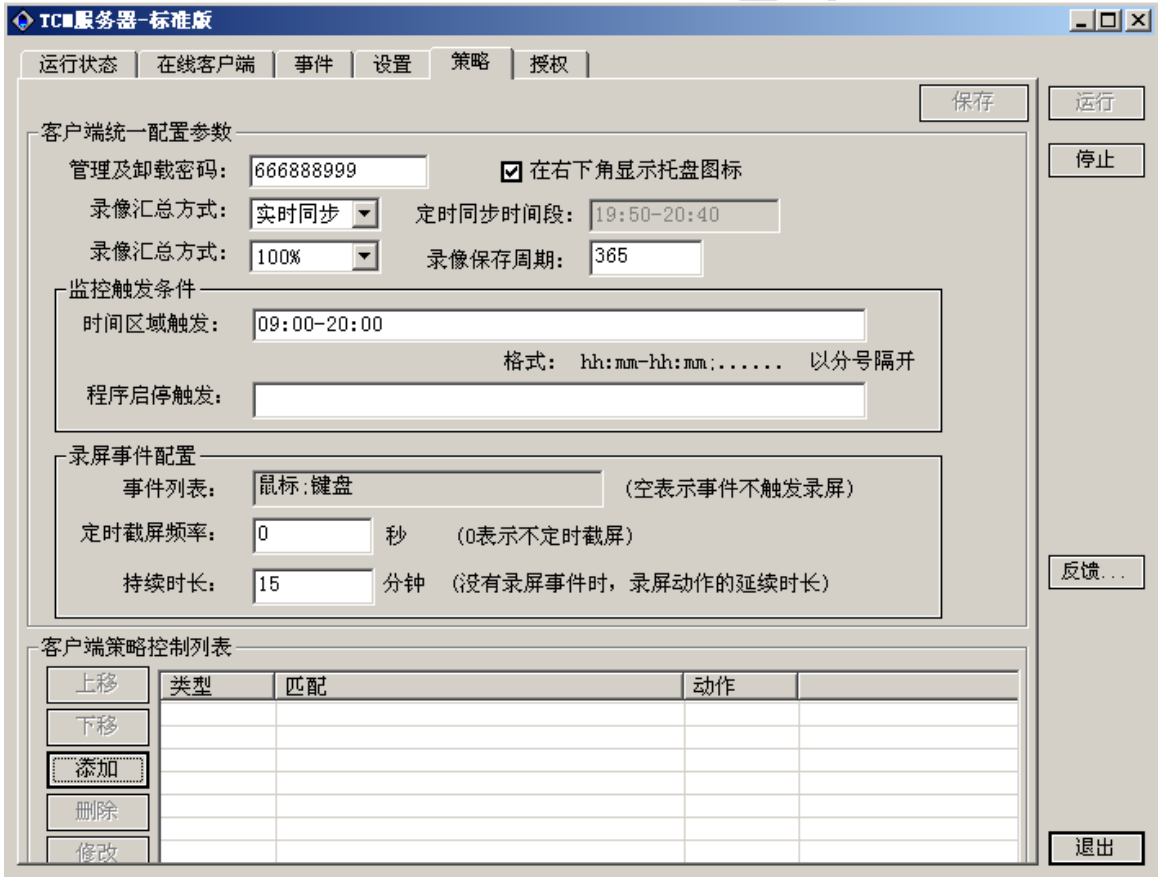
服务端口：指“TCM 客户端”与“TCM 服务器”端的通信端口号，此端口号默认为：6665。

录像存储目录：指“TCM 客户端”的图片汇总到“TCM 服务器”端中的位置。

多少天后自动删除：指“TCM 客户端”的图片汇总到“TCM 服务器”端中后，多少天(如图中默认 30 天)之后删除已上传到服务器文件夹“TSAClusterImgDir”中的“TCM 客户端”图片；

开机后自动运行：指服务器端开机后是否自动运行。

【策略】



[客户端端统一参数配置]

管理及卸载密码：指客户端程序卸载的时候或者打开客户端程序的时候需要输入的密码

录像同步方式：指客户端的监控录像信息，通过何种方式进行汇总同步；

录像保存周期：指客户端录像在本地电脑上的保存时间；

[监控触发条件]

时间区域触发：指在设定的时间段范围之内，如果有鼠标键盘录屏生成，这些录屏信息则会上传到服务器中，反之，录屏信息不会传到服务器中；

为“空”时—不监控；00:00-00:00 表示：24 小时循环监控；

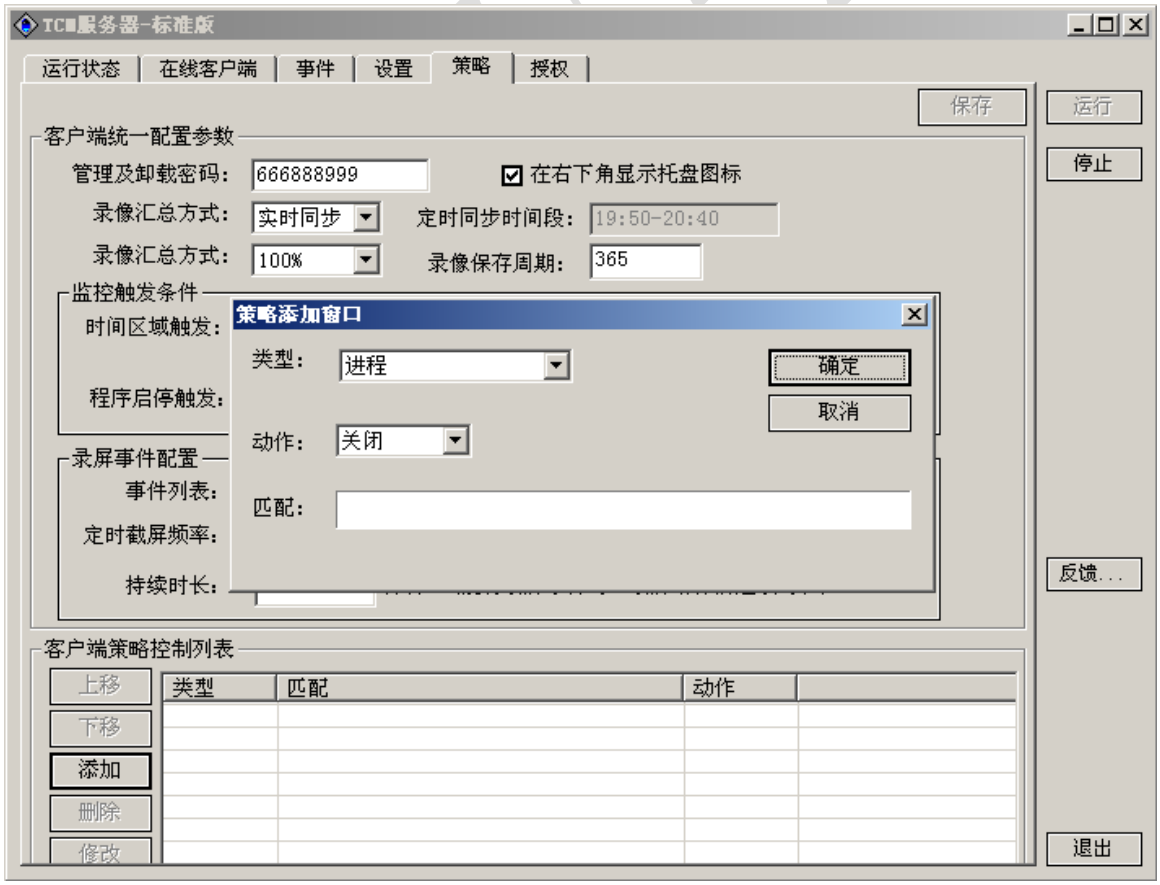
程序启停触发：根据程序的进程启停，来控制是否进行监控录像，这个目前一定要配合【定时截屏频率】和【持续时长】一块使用；需要注意的是目前当监控的程序进程退出之后，监控还会继续进行截屏，截屏的时长就是设定的持续时长；

定时截屏及持续时长：在没有“程序”的情况下，如果设定了定时截屏和持续时长，则按照设定的定时频率及持续时长进行截屏；持续时间到截屏结束。

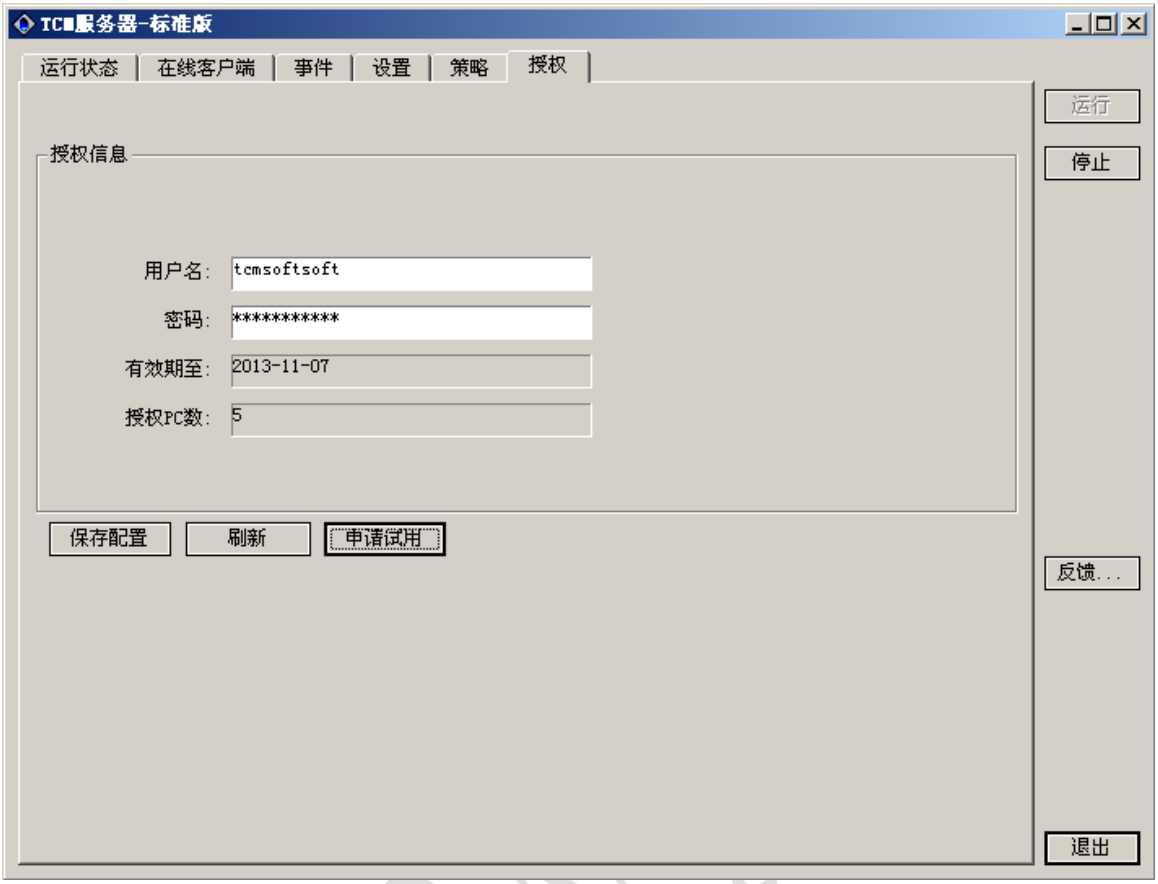
持续时长为“空”或者“0”时，代表按照设定的时间频率持续截屏

[客户端策略控制列表]

策略控制即黑名单问题，通过策略类型、动作、匹配进行对策略控制；其中，类型包括进程和标题关键字；动作包括关闭。如下图：



【授权】



如上图，此页显示的是 TCM 服务器授权信息，新程序可以通过点击“申请试用”试用时间为 15 天，监控 PC 数为 5 的免费试用账号，具体如何申请试用可参考“申请 TCM 程序免费试用账号”；正式使用用户则通过联系我司进行激活(相关账号密码或者使用密码狗激活，这些信息由我司提供，为收费版)。

调回至：服务器端配置操作

4.2. 集中管理端(金万维 TCM 管理端)使用说明

集中管理端登录页面如下：

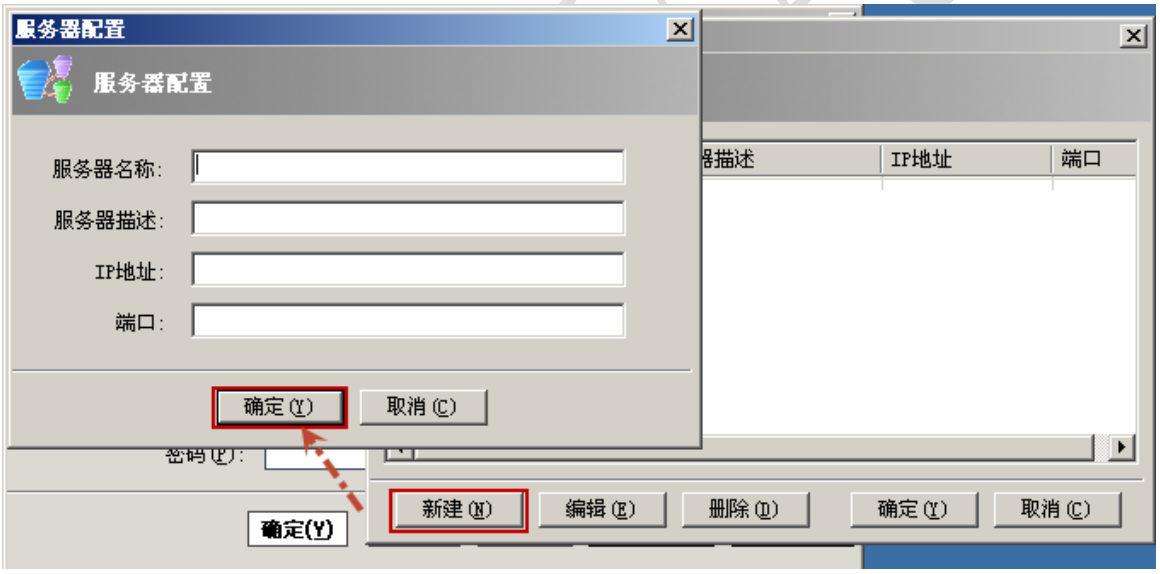
说明：

[高级]：点击配置可以进行连接服务器的相关配置，具体操作见下文；

[密码找回]：找回“用户”的密码，这里通过给创建用户时填写的邮箱地址发送邮件，进行找回密码，具体操作见下文。

点击【配置】进行下一步配置，

点击【新建】如下图：



说明：

服务器名称：即 TCM 服务器的名称；

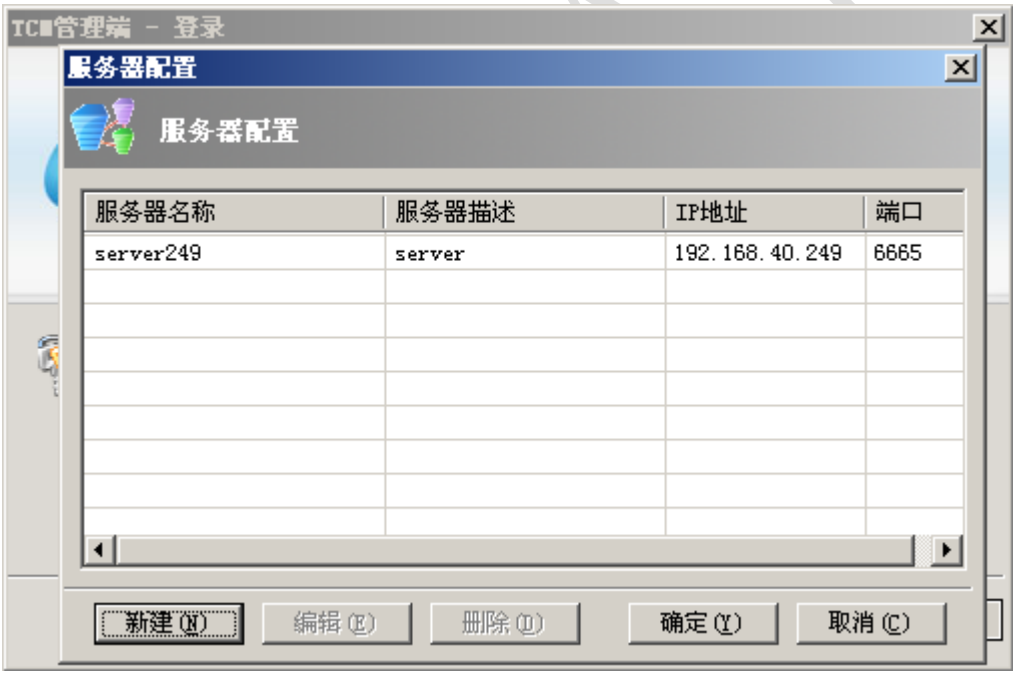
服务器描述：对 TCM 服务器进行的描述；

IP 地址：TCM 服务器的 IP 地址；

端口号：TCM 服务器的端口号；

实例如下图：

点击“确定”，如下图：



再次点击“确定”，如下图：

说明：

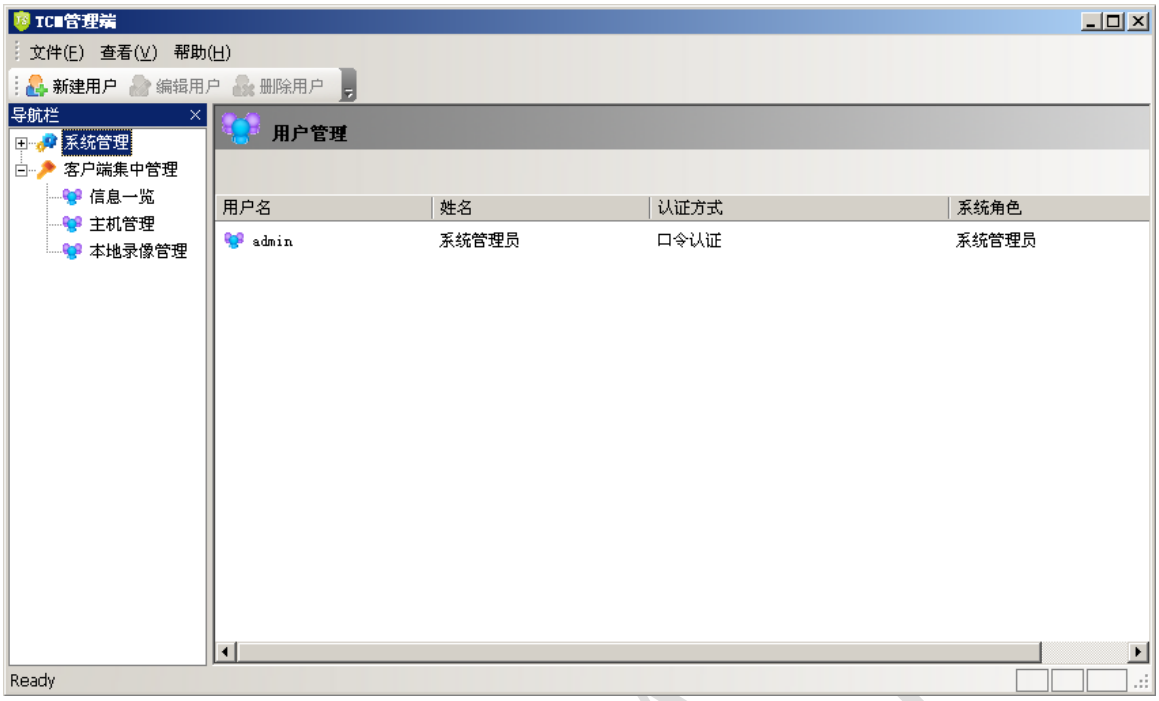
服务器：选择通过“高级”进行配置的服务器；

用户名：TCM 服务器的用户名，默认的是 admin 用户；

密码：TCM 服务器的用户名密码，默认的 123456；

如下图，以 202 服务器为例，连接到 TCM 服务器

连接到服务器的界面如下：

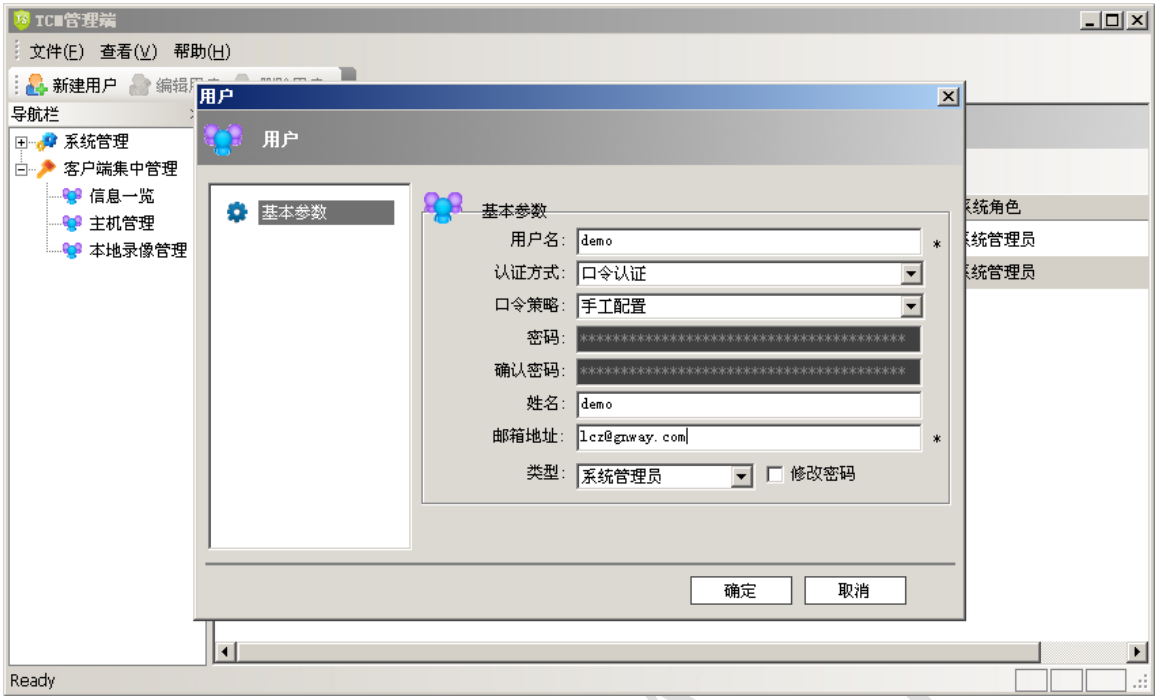


界面中，主要包括“系统管理”和“客户端集中管理”两个模块，关于管理端的两个模块说明与使用，见以下详解。

4.2.1. 系统管理——用户管理

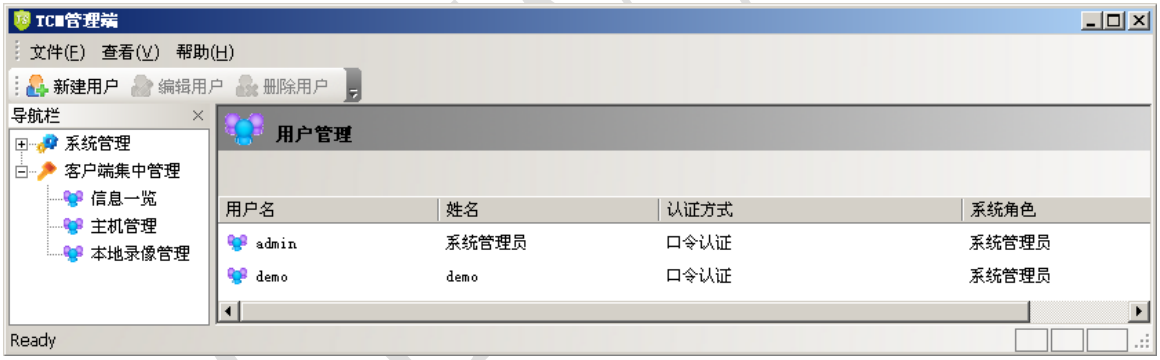
用户管理：主要是对能够登陆 TCM 管理端程序的用户进行创建、编辑和删除的管理；

在用户管理页面，右击可以新建用户，如下图：



说明：邮箱地址就是“找回密码”时发送邮件的邮箱地址。

点击确定就可以完成用户添加，如下图；



编者提醒：在创建用户的时候，需要填写“邮箱地址”主要是为了防止因为登陆密码的忘记而无法进入 TCM 管理端程序的问题；

密码找回步骤：

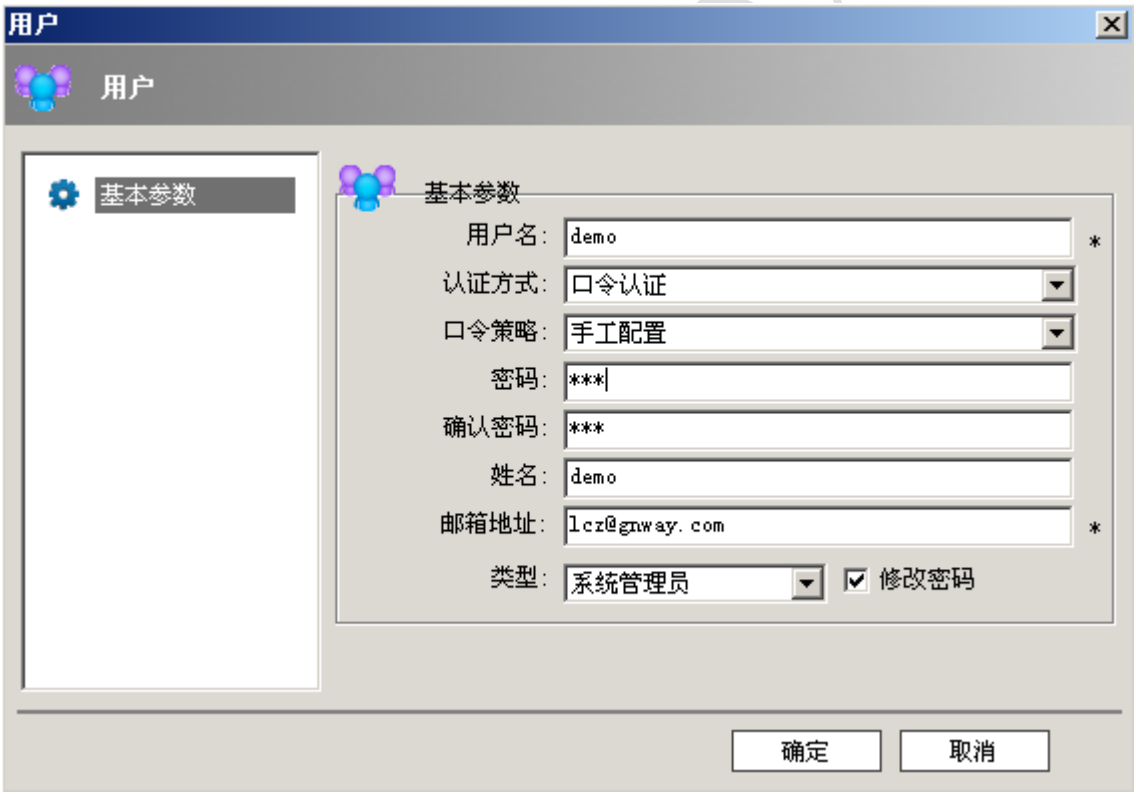
点击“找回密码”，弹出找回密码框，输入用户名，如下图：

点击“确定”，账号密码将被发送到预设的邮箱中，如下图：

邮箱信息：

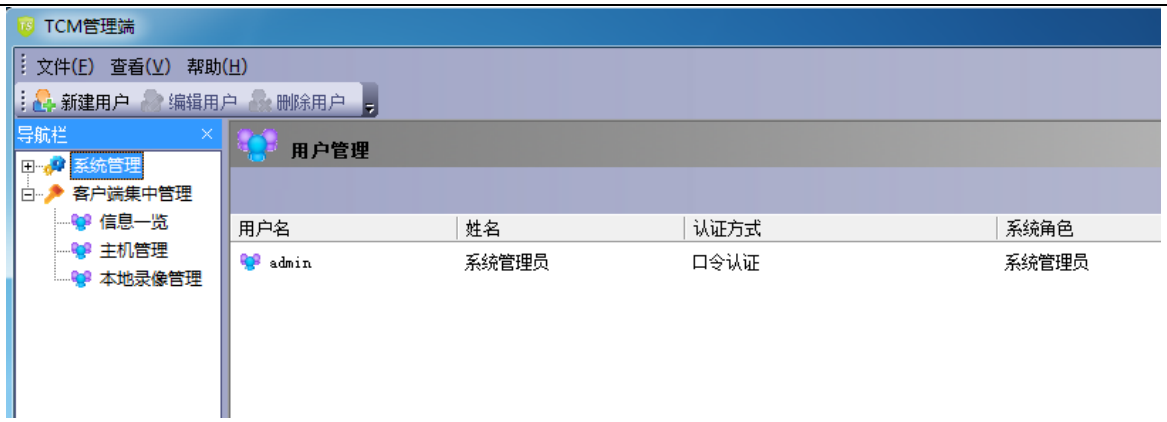
找回的密码是一个随机密码，以新密码登录到客户端，最好重新设置一下。

密码修改：选中“修改密码”，密码与确认密码框为可修改状态，重新输入新密码即可，如下图：



4.2.2. 客户端集中管理

客户端集中管理中，有三部分组成：信息一览、主机管理、本地录像管理，如下图：



先分别对三项进行如下介绍。

4.2.2.1 信息一览

信息一览，即全面展现当前 TCM 客户端的连接情况的信息界面；

说明：

主机类型：目前主要是 TCM 主机；

主机数量：所有与汇总服务器交互过的监控主机数量；

当前活跃数：指正在被监控的主机的个数

截屏图片数量：被监控主机的截屏图片个数

4.2.2.2 主机管理

主机管理，即对 Client 的主机进行相关操作管理，如下图，显示的就是 Client 的主机相关信息：

说明：

主机 ID：表明此 Client 主机唯一性的标识

主机名称：此 Client 主机的计算机名称

主机 IP：此 Client 主机的 IP 地址

端口号：与 TCM 服务器端通信端口

主机类型：表明此主机审计的类型是 img 类型

在线状态：表面该主机是在线还是离线；

监控状态：显示的是当前的主机状态，有在线、离线、unregister

描述：此 Client 的备注信息

是否注册：表明该主机是否写入到数据库中，如果是未注册，那么在“信息一览”中“主机数量”不会加入该主机的数量；

主机管理页面相关操作的说明，如下几个方面。

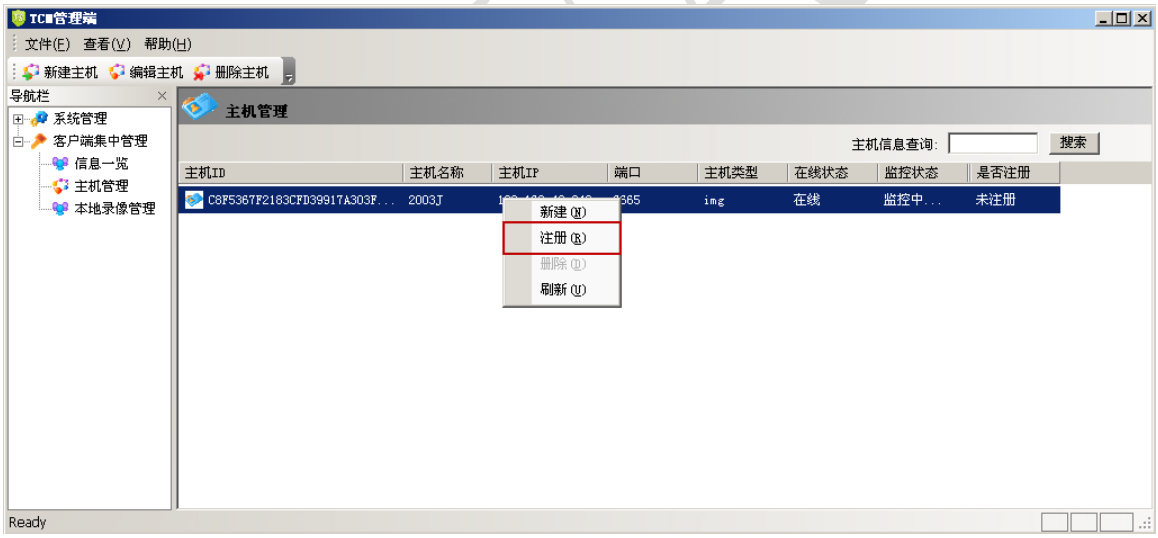
1.在主机管理页面，可以通过两种方式进行“Client”主机的管理，如下操作：

a)、手动添加主机，如下图，在主机管理页面右击“新建”就可以通过手动添加主机。

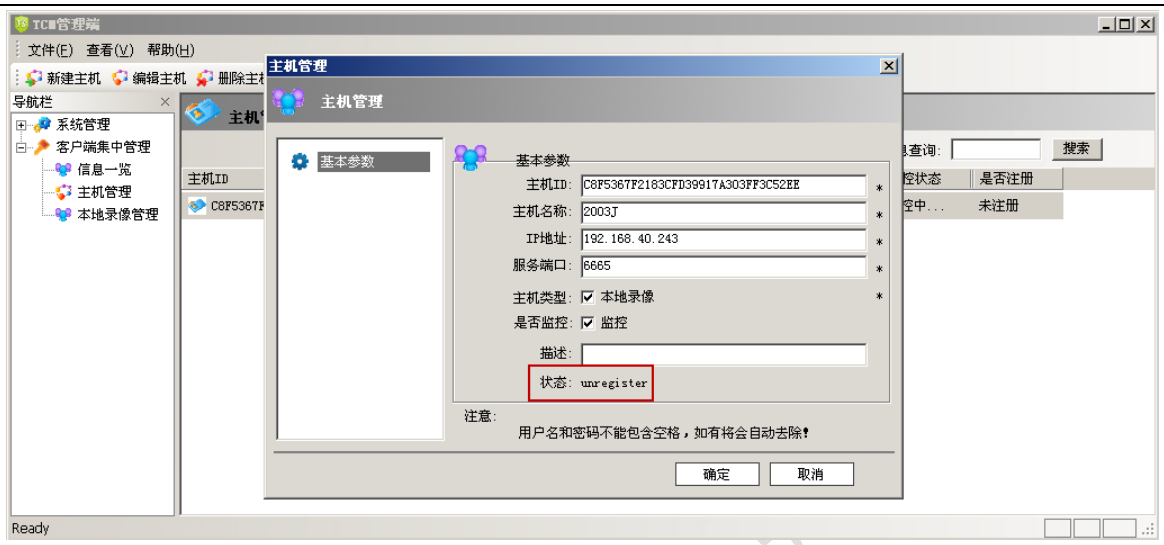
b)、直接获得主机信息，在主机管理页面，右击“刷新”便可以通过刷新获得 Client 的主机信息。

2. 把未写入数据库的“Client”主机，写入到数据库。

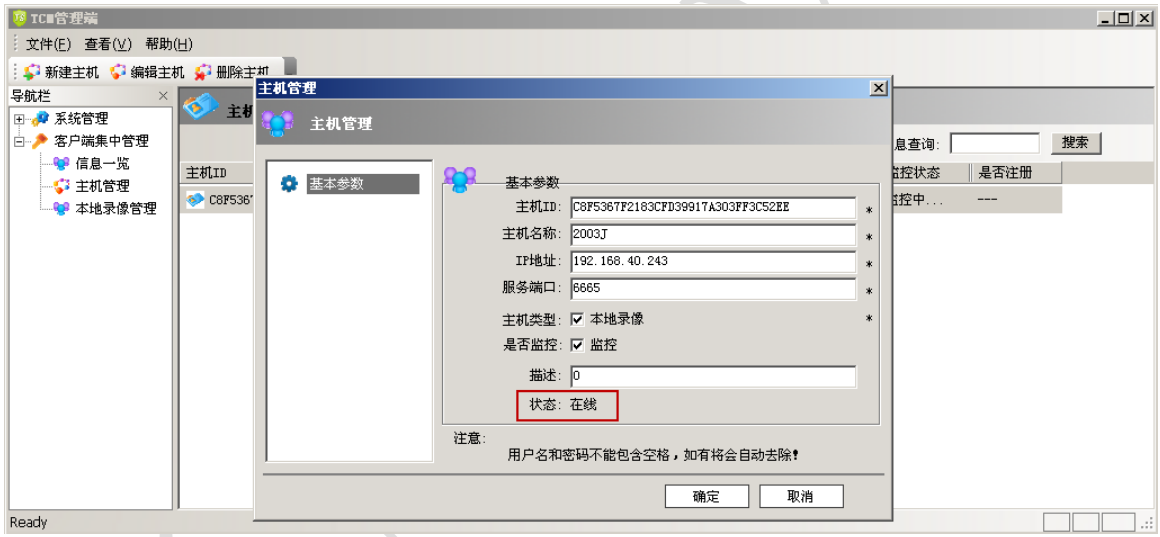
未写入数据库的“Client”主机是“未注册”的监控状态，右击“注册”如下图：



点击“注册”进入如下界面：



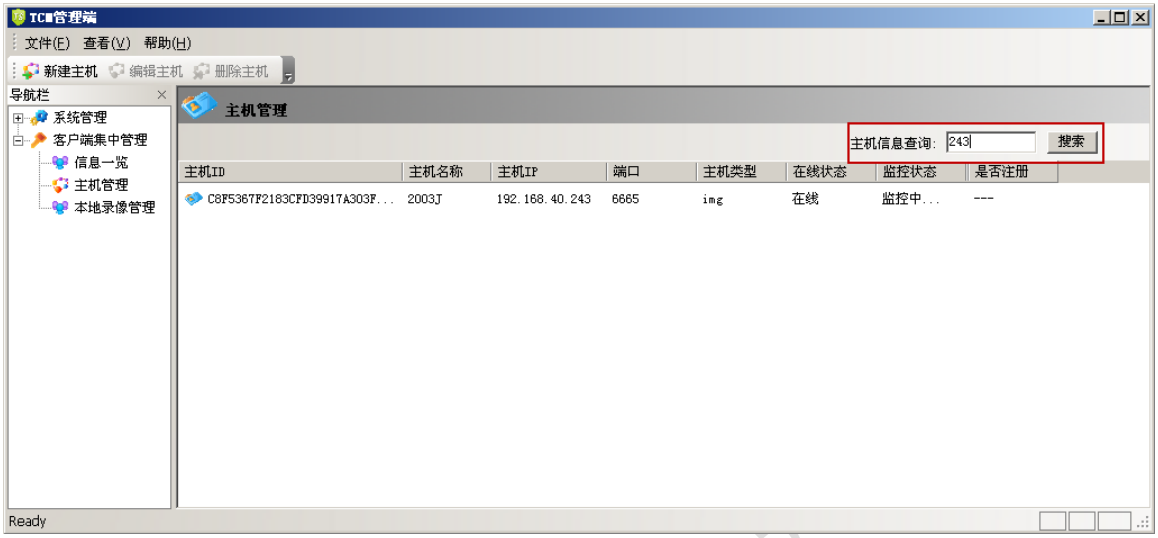
点击“确定”就可以把新在线的主机写入数据库，如下图：



3. 可对主机信息查询

对主机信息查询，包括主机 ID、主机名称、主机 IP 的查询。

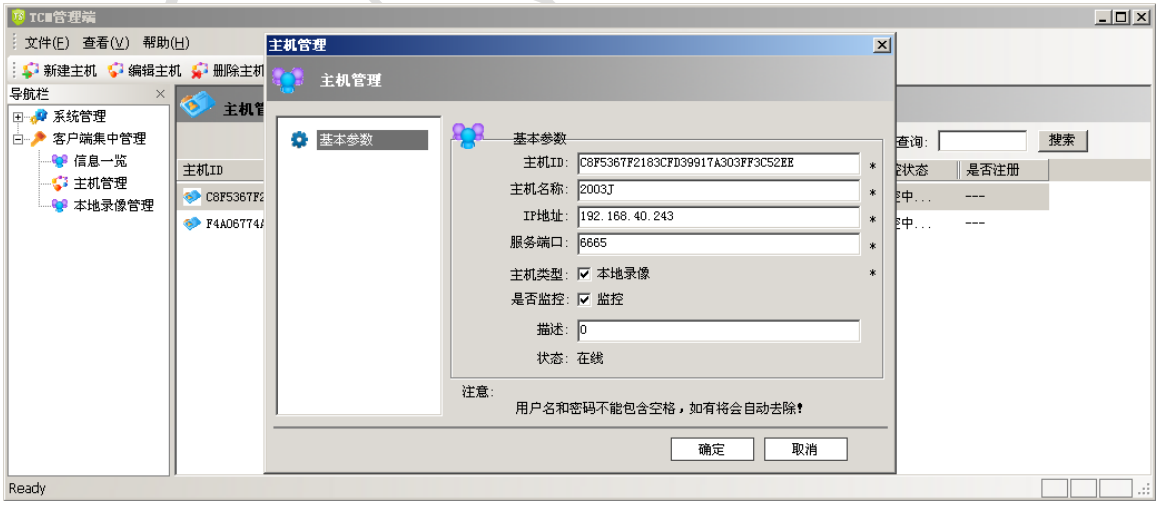
比如我对主机 IP 为“243”的用户进行检索，如下：



4. 主机相关管理操作

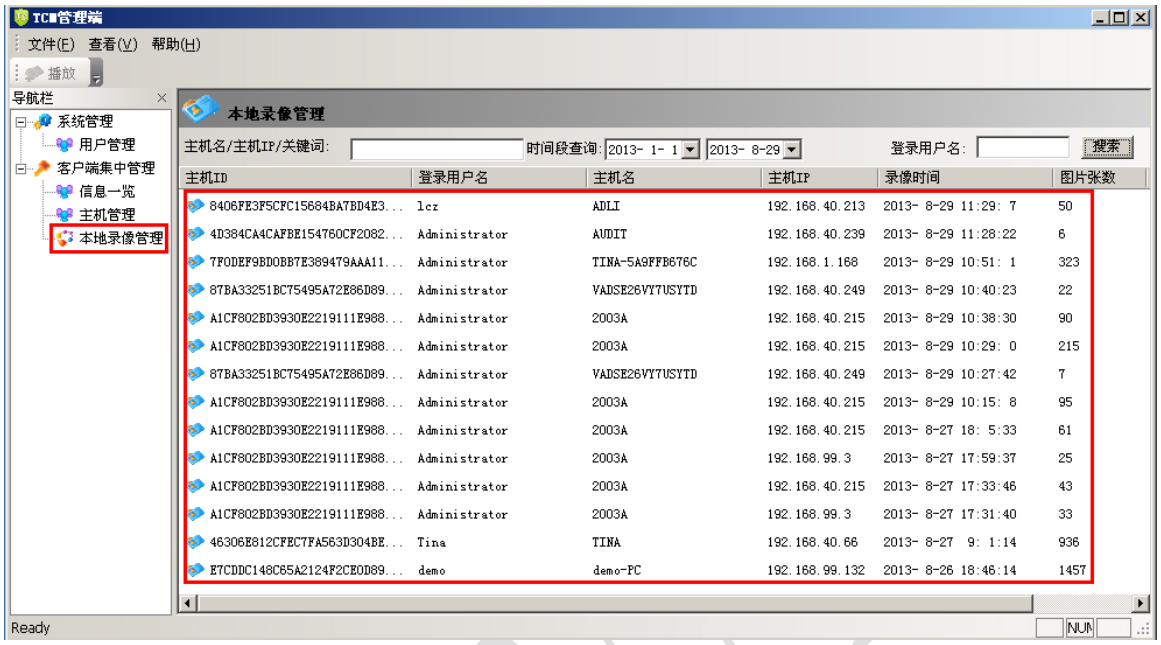
对主机进行管理，如编辑、删除操作，如下图：

点击“编辑”，弹出如下框，可对相关可编辑信息进行编辑：

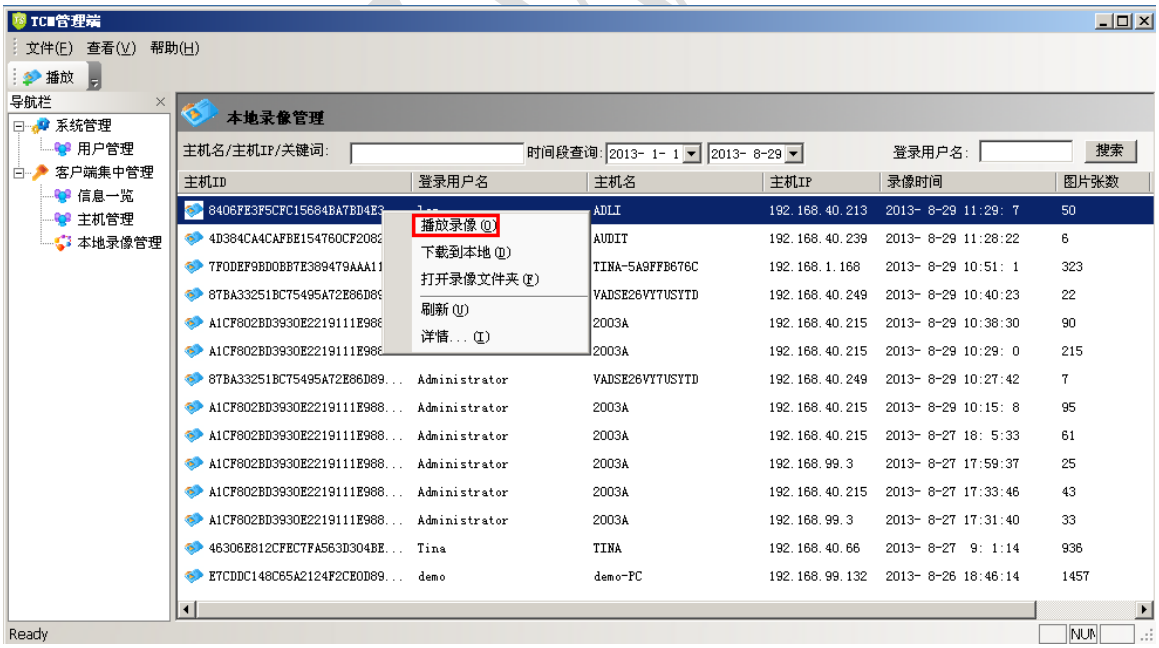


4.2.2.3 本地录像管理

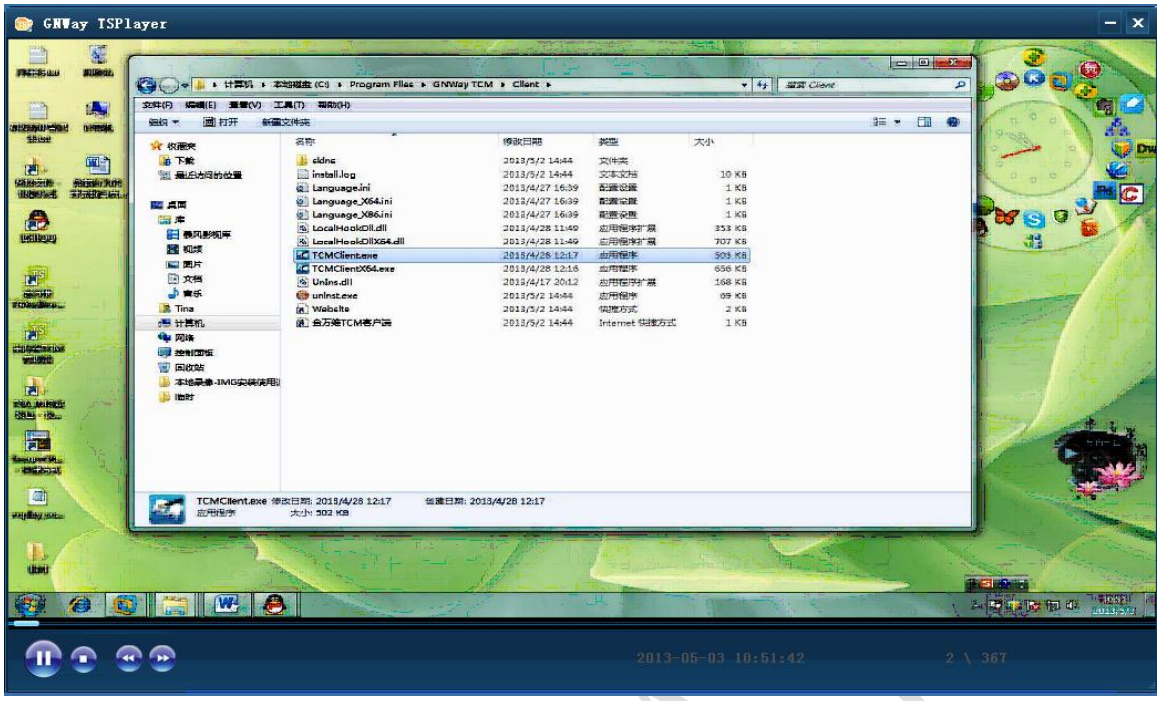
本地录像管理：是对 Client 端录像的播放、下载、查询等操作。如下图：



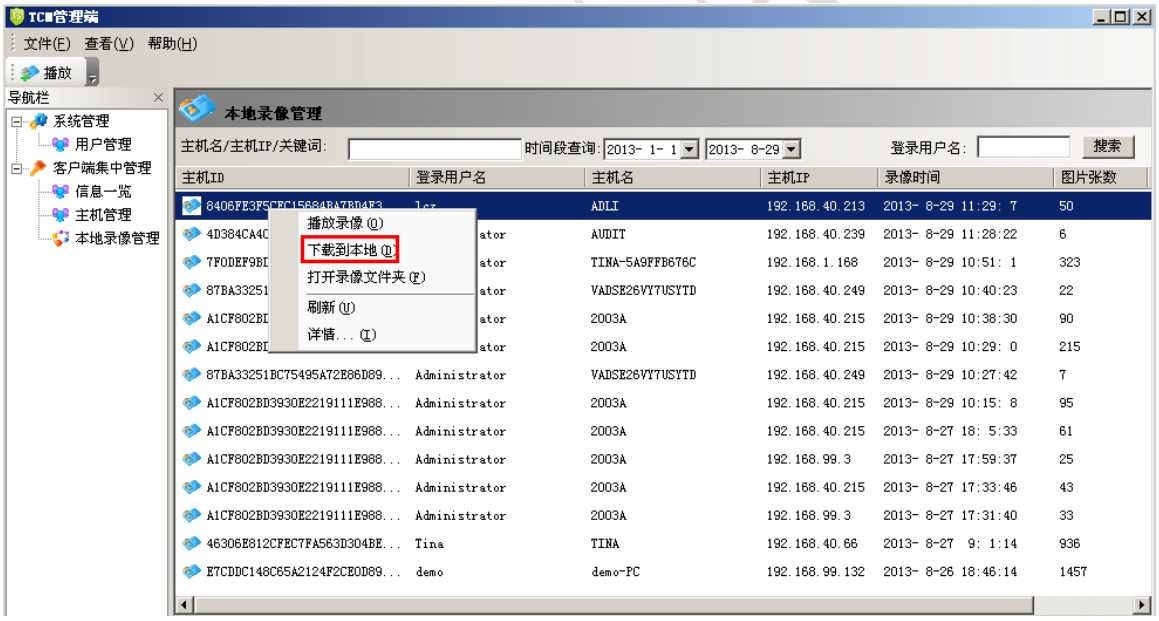
[录像播放]



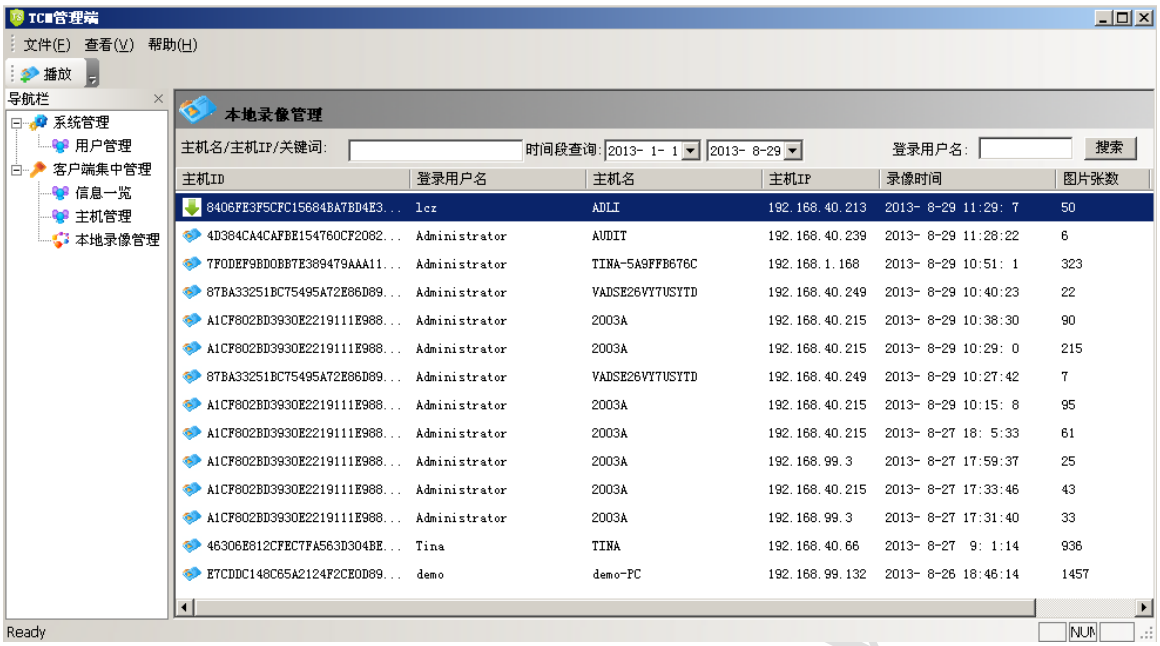
如上图，在录像文件上右击，选择“播放录像”，就可以打开如下播放窗口：



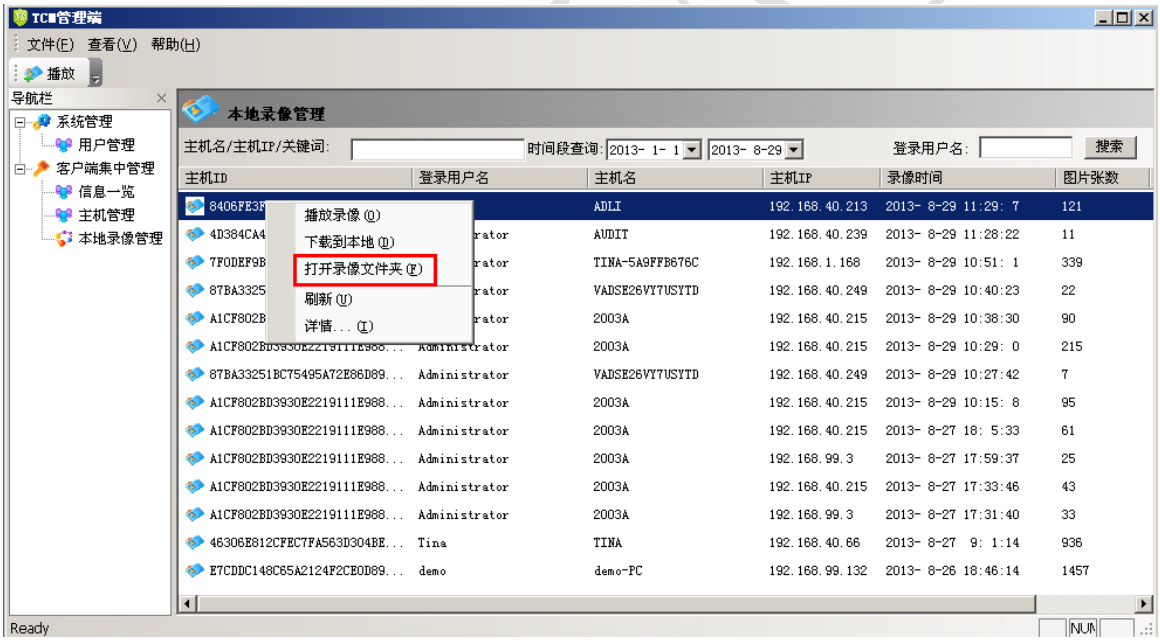
[下载录像到本地]



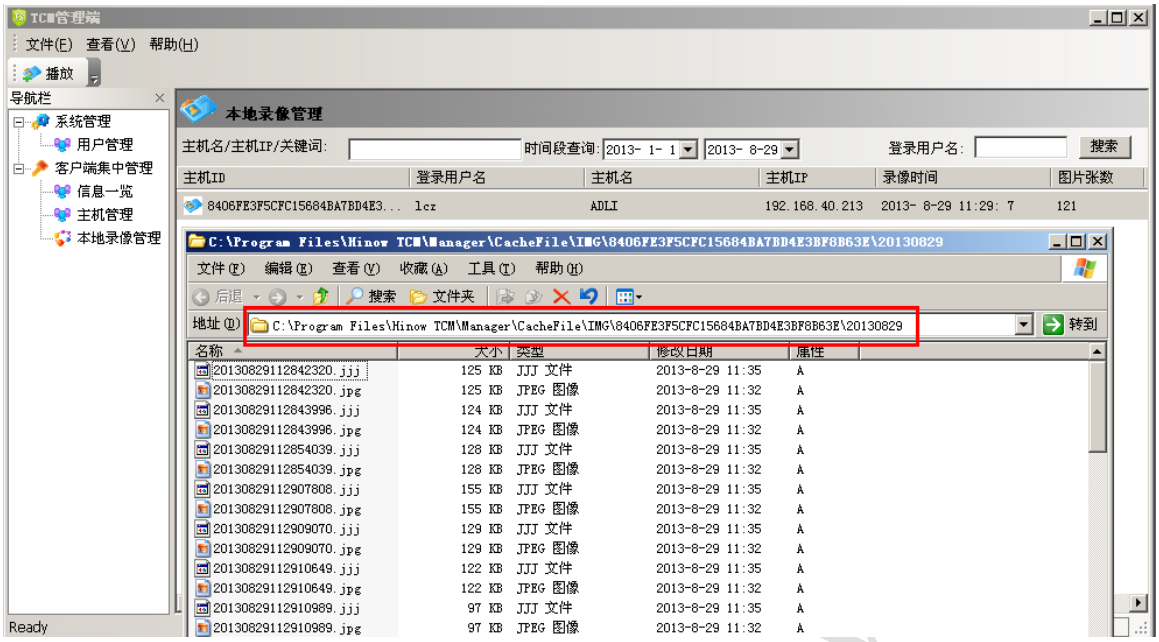
如上图，在录像文件上右击，选择“下载到本地”，就可以下载录像到本地，如下图是下载过程：



[打开录像文件所在的目录]



如上图，在录像文件上右击，选择“打开录像文件夹”，就可以查看录像文件所在的文件夹了，如下图：

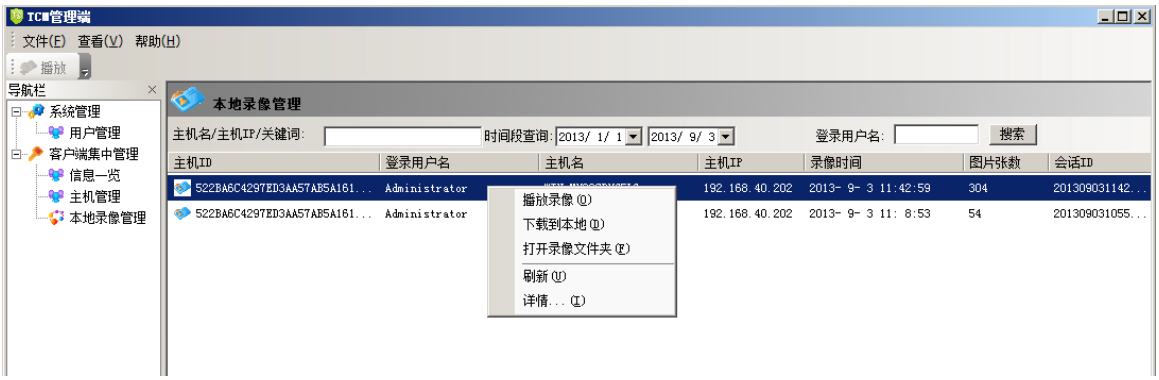


[录像信息查询]

录像信息查询，包括查询主机名、主机 IP、关键字、登录用户名以及对录像时间查询，以关键字【百度】为例，如下图：

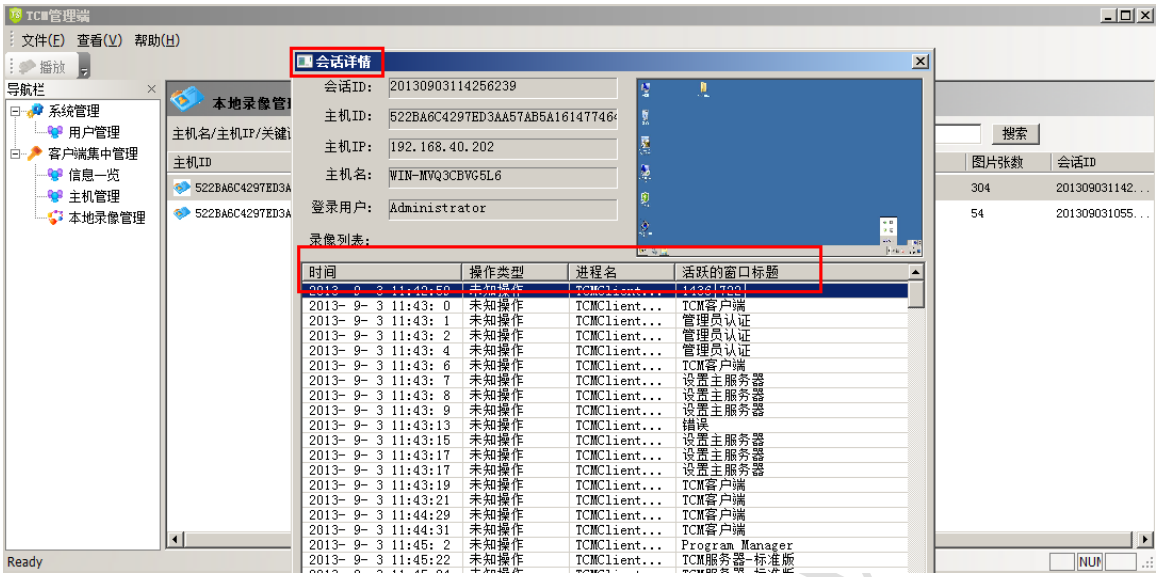
[详情]

详情，即录像会话详情，如下图：

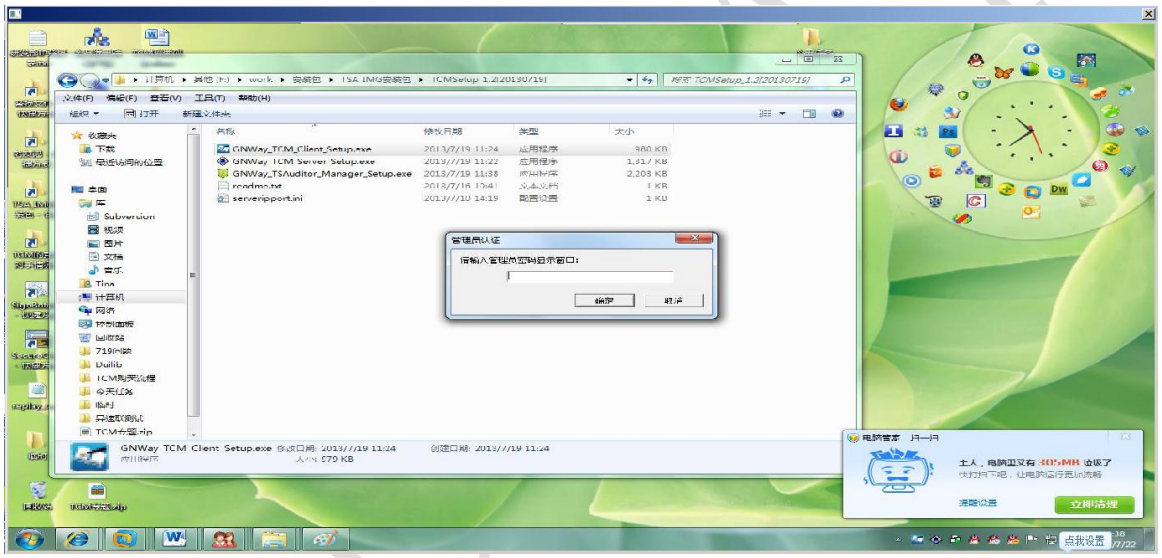


点击“详情”，弹出了会话详情的框，从这个会话框可以看到当前会话的所有详细信息及

当前录像图片的缩略图



双击任意一项就可以看到录像的放大图片，在上面单击可以切换到下一张图片，如下图：



4.3. 集中管理 Client 使用说明

启动 TCMClient.exe(64 位系统下启动 TCMClientx64.exe)则开始进行桌面监控。

启动后的 TCM 客户端的窗口如下：

4.1.TCM 客户端页面说明

[服务器连接配置]

服务器：当前客户端所连接的服务器 IP 地址与端口号详情；

服务器名：当前客户端所连接的服务器的主机名；

设置服务器：如果服务器的 IP 地址、端口号发生改变时，可以通过这里重新设置使得客户端再次连接到服务器；

查看策略：可以查看当前服务器端配置了哪些策略。

[配置参数]

同步策略：指的是“客户端”与“TCM 服务器”之间“监控审计信息的同步规则，包括不同步、定时同步、实时同步；

不同步：则客户端的图片将不会向服务器端上传；

定时同步：设置“定时同步时间段”后，客户端图片将在这个时刻定时上传到服务器端；

实时同步：设置了“实时同步”后，只要客户端有图片就会上传到服务器端。

监控时间段：在服务器端设置不同监控的时间短后，客户端的图片会根据所设置的时间段进行上传图片。

时间区域触发：指监控的时间段，在这个时间段之内对鼠标、键盘的操作进行监控录像；

程序启停触发：指根据显示的程序进程进行监控；

查看更多：指显示全面的策略配置；

[本机信息]

本机信息：指的是能够标识此“客户端”本机身份和此“客户端”与“TCM 服务器”连接情况的状态信息，给予如下介绍。

本机 ID：“客户端”的 ID，换而言之是“客户端”的“身份证”；

本机 IP：“客户端”的 IP 地址；

本机名称：“客户端”的主机名称；

在线状态：分为在线、离线；在线：“客户端”与服务器正在进行交互，反之不交互；

管理状态：对当前所录制的图片的计数；

[设置密码]

设置密码：点击“设置密码”可以设置客户端的卸载密码及客户端离线时候的显示密码

一、 注意事项

4.4. TCM 管理端用户密码问题

默认的 TCM 管理端的登陆用户名与登陆密码分别是 admin，123456

4.5. 客户端的管理密码

为了方便管理，客户端的管理密码分为两种，客户第一次安装离线的密码和客户端在线后的密码问题。

如果客户第一次使用并安装 TCM，当第一次安装后客户端是离线状态，默认的客户端管理密码与客户端的卸载密码是 123456，这个密码是只是暂时保留的，如果需要更改该密码，请联系我们售后技术支持。

如果客户端在线，管理客户端的默认密码是 666888999，管理员可以通过 TCM 汇总服务器的【设置】页面进行更改“客户端管理密码”。