

# 金万维 TSAuditor 技术白皮书

——安全接入审计系统白皮书

## 版权声明

本白皮书中的内容是 TSAuditor 解决方案产品说明书。本材料的相关权力归北京金万维科技有限公司所有。白皮书中的任何部分未经本公司许可，不得转印、影印或复印。

© 2010 北京金万维科技有限公司所有

All rights reserved.

### 安全接入审计 (TSAuditor) 系统

### 技术白皮书[第二版]

本资料将定期更新，如欲获取最新相关信息，请访问金万维网站 [www.gnway.com](http://www.gnway.com)

北京金万维科技有限公司

Beijing GNWAYTechnology CO.,LTD

北京金万维科技有限公司，100070

电话(TEL): 010-51266543-8123

传真 (FAX ): (8610) -63704110-8088

电子信箱: [tsa@gnway.com](mailto:tsa@gnway.com)

# 目 录

一、 准备工作： .....	- 4 -
1. 环境准备.....	- 4 -
2. 程序下载： .....	- 4 -
二、 安装 TSAuditor_Server.....	- 4 -
1. 程序安装.....	- 4 -
2. 注册试用帐号.....	- 5 -
三、 配置 TSAuditor 属性.....	- 6 -
1. TSAuditor 管理员配置.....	- 6 -
2. TSAuditor 录像调度.....	- 7 -
3. TSAuditor 在线用户监控.....	- 9 -
4. TSAuditor 录像文件管理.....	- 9 -
四、 安装 TSAuditor Player.....	- 9 -
1. Player 安装.....	- 9 -
2. 播放录像.....	- 11 -
五、 后记.....	- 11 -
1. 关于录像空间说明.....	- 11 -
2. 关于策略配置说明.....	- 11 -
3. 关于最简化配置的若干方案.....	- 11 -
4. 注意事项.....	- 11 -
5. 关于服务.....	- 12 -

## 一、 准备工作:

### 1. 环境准备

- i. 操作系统环境要求为 32 位 Windows 2003 、 2008 服务器。建议为 2003Server。
- ii. TSAuditor 服务器需要与审计的服务器[远程接入或远程桌面服务器]为同一服务器。
- iii. 建议 TSAuditor 所在的服务器安装终端服务并激活。

### 2. 程序下载:

可直接访问 <http://www.gnway.com/prod/tsauditor/> 至安全接入审计主页进行相关下载;

程序分为两部分: 主配置程序 及 专用播放器。

本文针对程序版本为 TSAuditor V1.7.1

## 二、 安装 TSAuditor\_Server

### 1. 程序安装

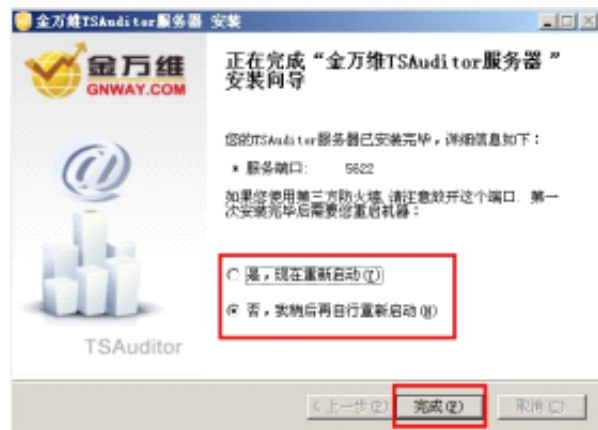
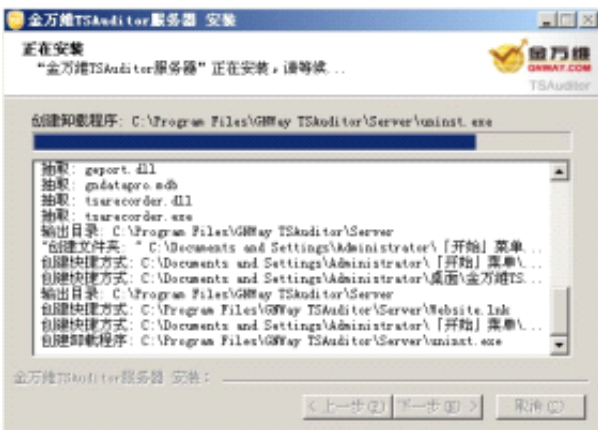
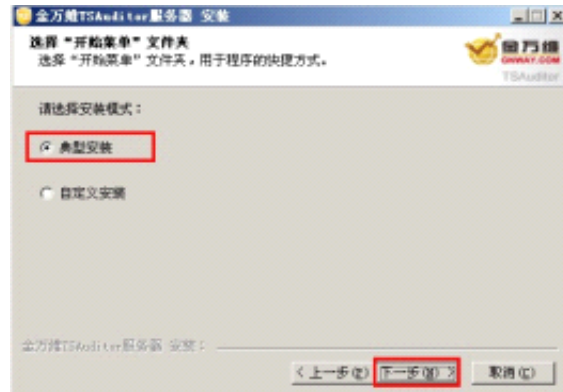
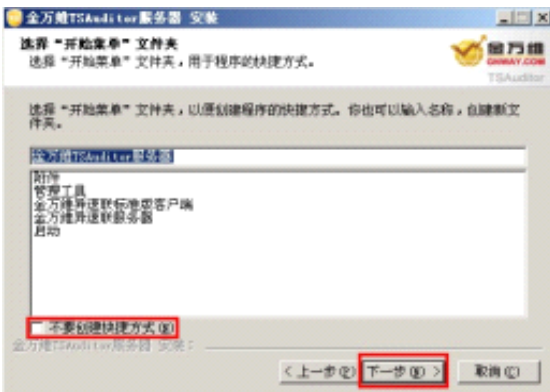
TSAuditor\_Server 的主程序为:



双击主程序, 进行安装



按提示进行安装, 选择下一步;

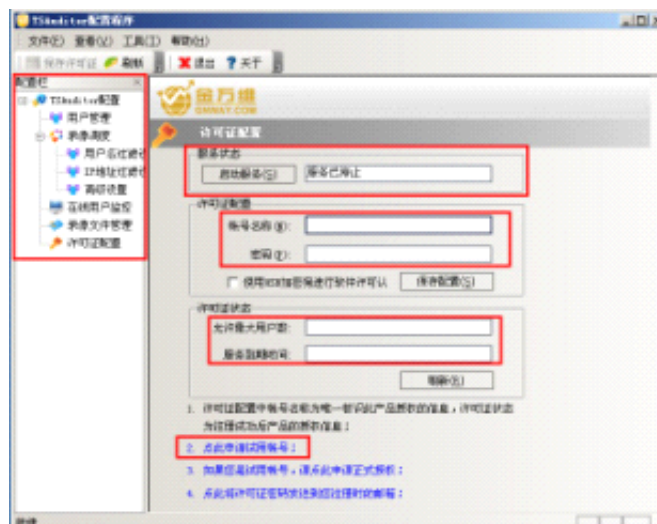


**\*重要提示: TSAuditor\_Server 安装后需要进行重启才会生效;**  
安装完成后, 桌面上会生成 TSAuditor\_Server 的程序图标:



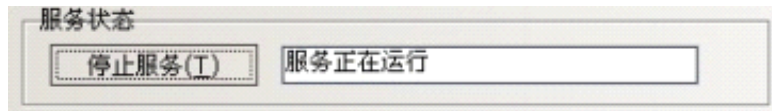
## 2. 注册试用帐号

打开 TSAuditor 服务器:



如果没有 TSAuditor 系统的注册帐号，请选择 **2. 点此申请试用帐号；** 重新注册 申请一个新的 TSAuditor 的测试帐号，如果有，请直接在许可证配置里 输入原有的 TSAuditor 的帐号即可。 并选择 “保存配置” 和 “刷新”， **直至许可证状态有显示状态为正常。**

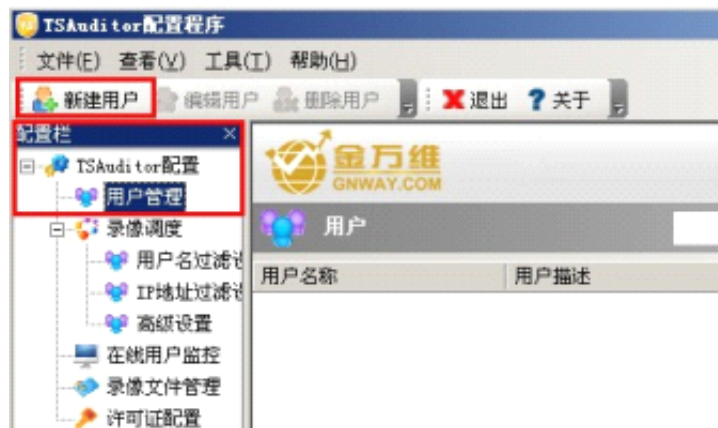
同时点选 “启动服务”，将 服务状态 改为



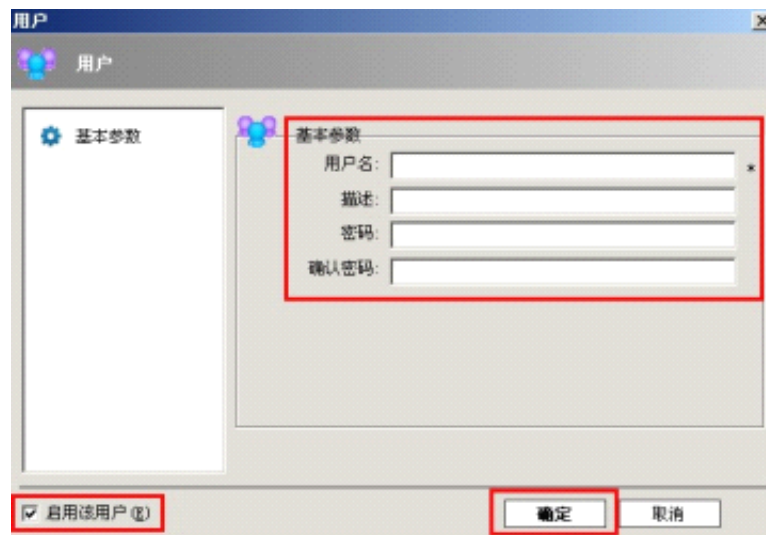
### 三、 配置 TSAuditor 属性

#### 1. TSAuditor 管理员配置

- i. 新建 TSAuditor 管理员帐号；



首先点选 “用户管理” 然后 选择 “新建用户”。



直接输入 “用户名”，“描述” 项可写可不写，“密码” 与 “确认密码” 可以是空白，但如果配置密码，要求值必须一致。

**\*注：**可以建多个管理员帐号，如果想暂时停用哪个帐号，不需要删除，只需要将 “启用该

用户”前的默认对勾，去掉。

帐号建立成功后，会在“用户管理”项下面显示，管理员帐号状态：



\*注：用户管理下的帐号可以不需要设置，不设置时，打开 TSAuditor 配置程序时，不需要帐号和密码，而如果有“用户”存在时，在登录时，就会提示登录框，需要输入相应的帐号和密码才可以进行 TSAuditor 配置。



## 2. TSAuditor 录像调度



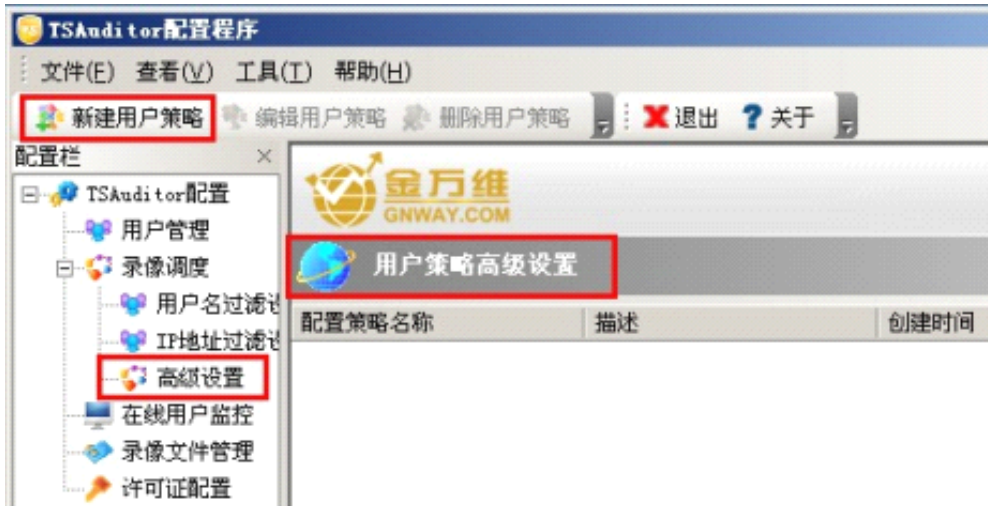
**用户名过滤:**

设置录像对象，可以引出系统对象客户，可以指定录像，也可以排除录像。

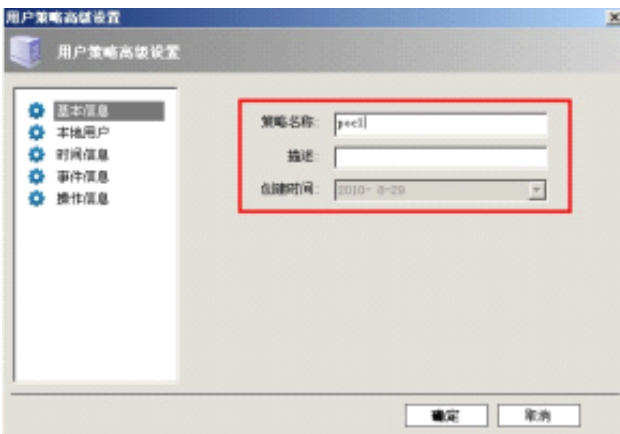
**IP 地址过滤:**

设置录像对象，可以针对指定的 IP 地址范围，做为录像或排除对象。

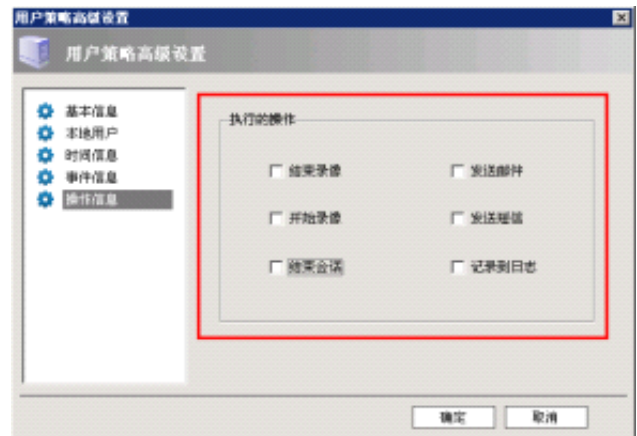
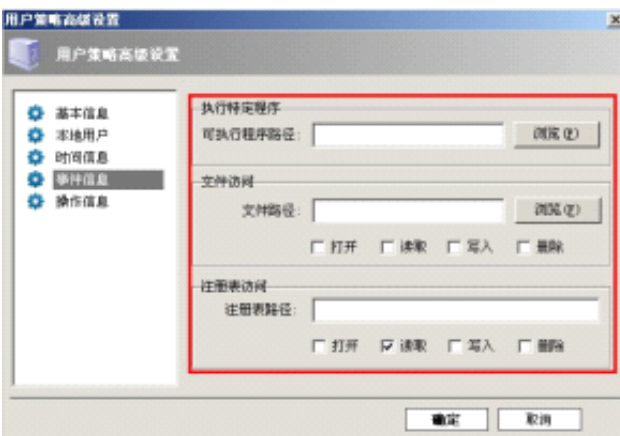
**高级设置:**



选择 **高级设置** 然后 “**新建用户策略**”



\*注：本地用户选择是策略所要针对性的客户



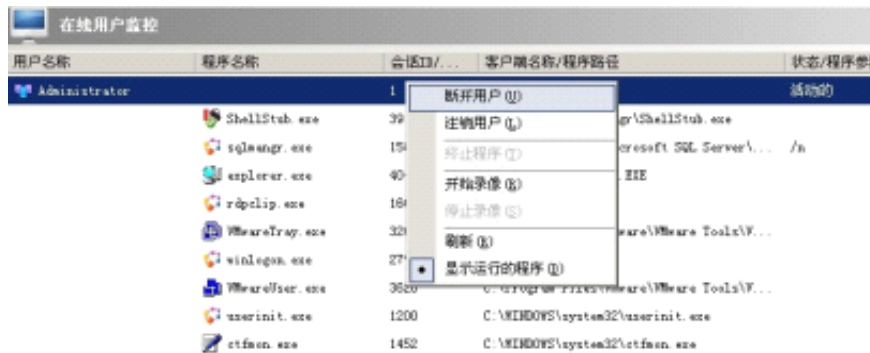
**事件信息:**

可以针对可执行程序路径，或特定文件或文件夹事件、注册表路径配置详细的“事件触发”策略。

### 操作信息：

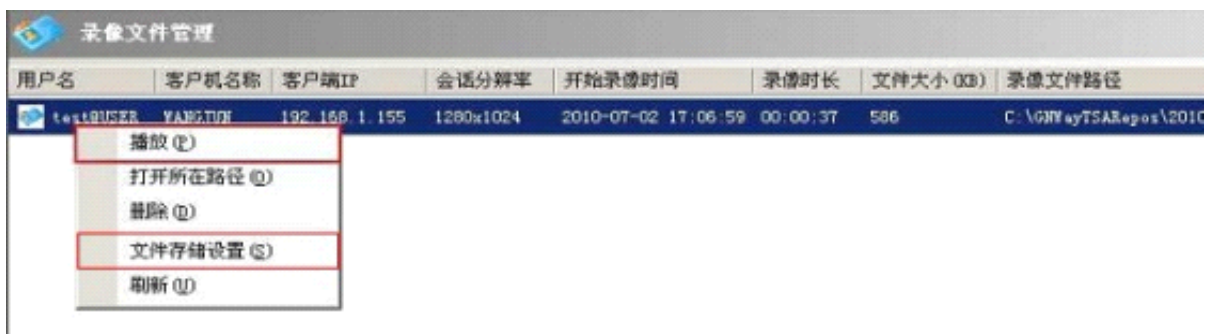
可以针对所制定的“事件触发”策略，来执行相应的动作，比如结束录像，开始录像，结束会话，等。

## 3. TSAuditor 在线用户监控



在线用户监控，可以实现对所有远程登录到服务器的用户，及所有附带启动的程序进行管理，同时可以配置用户断开及注销操作。并可以针对特定用户，开始录像。

## 4. TSAuditor 录像文件管理



所有的录像文件，全部可以在此时显示，并且，如果安装过播放器的话，可以直接双击播放，同时也可以修改录像文件的存储位置。

## 四、 安装 TSAuditor Player

### 1. Player 安装

TSAuditor\_Player 的主程序为：



双击安装主程序；



选择“完成”即可完成安装，并且不需要重启，直接就可以使用。



## 2. 播放录像

- i. 直接在 TSAuditor\_Server 程序里面看，可以直接双击所对应的录像文件即可。
- ii. 直接找到 TSAuditor\_Server 所对应设置的录像目录位置，直接双击每个录像文件，也可播放。

# 五、 后记

## 1. 关于录像空间说明

标准说明： 操作较少时，一天可以录 23M

操作较多时，一天可以录 119M

一年单人最大录像空间不超过 30G 同时如果对录像文件压缩，压缩比例为 1/20 .

录像所占大小与实际所录的内容有关，屏幕不发生变化时，录像文件大小也不变，但当在录图片操作时，录像空间占用很大。

## 2. 关于策略配置说明

目前策略中的“高级配置”可以组合使用，可以发布多个策略。

## 3. 关于最简化配置的若干方案

- i. 什么用户都不需要建，直接安装上，注册好用户后，直接就可以对所有操作进行录像。
- ii. 可以手工改动 过滤设置，设置成 对下列用户录像全为空。
  1. 然后通过策略设置，针对某些操作事件来激活录像，或关闭录像。

## 4. 注意事项

- i. 如果通过远程桌面方式安装 TSAuditor，建议至少应该在控制台模式下安装，或直接在服务器前进行本地安装。
- ii. TSAuditor 通过远程桌面查看录像延迟较大时，可以直接把需要查看的录像文件复制到本地，直接安装 TSA 播放器进行观看。
- iii. TSAuditor 在首次安装时，请重启电脑后再启动服务。
- iv. 短信功能软件内默认没有开启，因为费用及延迟问题；也可以直接通过手机邮箱方式实现短信提醒。

## 5. 关于服务

### 全国服务网络:

审计服务咨询热线: 010-51266543-8123

**北京办事处:**010-63704105 地址: 北京市丰台科技园总部基地 12 区 5 号楼 6 层

**济南办事处:**0531-55500787 地址: 济南市历下区窑头路友谊苑北区 2 号楼 4 单元 502

**上海办事处:**021-51876651 地址: 上海市闵行区珠城路 99 弄 20 号 402

**南京办事处:**025-85262543 地址: 南京市玄武区玄武大道 88 号阳光聚宝山庄 7 栋 805

**苏州办事处:**0512-67593243 地址: 苏州市相城区阳澄湖西路御苑家园 121 栋 402 室

**杭州办事处:**0571-88992213 地址: 杭州市都市水乡水曲苑 3 幢 2 单元 301 室

**郑州办事处:**0371-60151518 地址: 郑州市黄河路 131 号新迪商务 619 室

**武汉办事处:**027-87641712 地址: 武汉市洪山区名都花园 105 栋 1 单元 7B

**长沙办事处:**0731-82469785 地址: 长沙市芙蓉区马王堆中路惠泽园 D7 栋 501 室

**广州办事处:**020-85533462 地址: 广州市天河区科韵路 62 号五华大厦 209

**深圳办事处:**0755-86297735 地址: 深圳市南山区新塘街一坊 3 号 908

**东莞办事处:**0769-23367346 地址: 东莞市东城区八达路和兴街 116 号和兴花园 A 座 609

**佛山办事处:**0757-82283609 地址: 佛山市禅城区建设二街 6 号 405

**福州办事处:**0591-88051970 地址: 福州市晋安区福马路大景城 19 号楼 1004 室

**西安办事处:**029-85458410 地址: 西安市草场坡骊马豪城 F 座 907 室

**甘宁办事处:**0931-2183448 地址: 兰州市城关区科技街 121 号 302

**西宁办事处:**0971-8127471 地址: 西宁市胜利路茂源水岸星光 4 号楼 16 层

**成都办事处:**028-85585850 地址: 成都市高新区沙子堰西巷 2 号 2 单元 510

**沈阳办事处:**024-62466247 地址: 沈阳市沈河区杏林街 38 号 242 室

**旗下网站:** 主站: [www.gnway.com](http://www.gnway.com) 中国软件分类网 [www.saas8.com](http://www.saas8.com) 帮我吧 [www.bangwo8.com](http://www.bangwo8.com)

伙伴平台: [agent.gnway.com](http://agent.gnway.com) 问吧平台 [ask.gnway.com](http://ask.gnway.com)