



ReView

管理员操作指南

杭州比特瑞旺电脑有限公司

杭州市文三路 259 号昌地火炬大厦 2 号楼 301

P:0571-88994438

F:0571-88994328

Welkin@chinakvm.com.cn



版权声明

杭州比特瑞旺电脑有限公司©2013 版权所有 保留一切权利

非经本公司书面许可任何单位和个人不得擅自摘抄复制本档内容的部分或全部
并不得以任何形式传播



目录

Review 管理软件简介	5
Review 集中管理平台介绍:	6
Review 管理软件安装服务器最低系统配置要求	7
Review 管理软件客户端最低系统配置要求.....	7
入门	8
许可-基本信息.....	8
许可-许可购买、许可升级.....	9
基本概念	10
系统典型拓扑结构图	11
Review 管理软件界面	12
JAVA 运行环境安装	13
Review 审计回放插件安装	14
基本操作	15
色彩方案配置及更改密码.....	15
添加装置	17
设备分组	19
用户组.....	22
抢占级别	25
管理用户账户	26
设备操作界面	28
对装置的操作	31
目标设备和装置物理对应关系	33
事件管理	34
固件与插件的管理	36



插件管理	37
高级操作	38
访问控制列表	38
TCP/UDP 端口	39
代理服务器	40
二次口令认证	42
系统全局参数	43
权限及安全功能	47
多域设置	50
认证服务与用户锁定登录的问题	55
Review 审计功能介绍	56
Review 审计最低系统配置要求	56
审计策略的添加、删除、禁用、启用和修改	57
用户 KVM 会话审计	61
KVM 会话审计查询	62
审计存储策略配置	65
KVM 会话操作	69
会话窗口的功能键	69
鼠标同步设置	73

Review 管理软件简介

杭州比特瑞旺电脑有限公司的 Review 管理软件，为数据中心提供了一个管理所有连接在网络上的硬件和软件的安全和集中的方案。Review 软件可以帮助管理员访问、诊断和变更全球范围内任意地点的任意网络资产，为用户提供一个安全、方便的后台认证管理系统平台，同时在用户权限设置、日志管理、定期任务各方面提供给用户全面、快捷、周到的管理。



Review 可管理的设备如下：

AS 系列 KVMA over IP 交换机：AS2008、AS2016、AS2032、AS4008、AS4016、AS4032、AS4064、AS8016、AS8032、AS8064。

ACM 高级串口服务器：ACM4、ACM8、ACM16、ACM32、ACM48。

APM 智能电源管理设备：APM8、APM16、APM20。



Review 集中管理平台介绍:

1. **一主多备:** 分布式后台集中主备认证体系, 保证认证的安全性和认证系统的负载均衡;
2. **高可扩充性:** 不论是服务器还是用户的扩容都不需要修改 KVM 结构、布线系统。
3. **高安全性:** 通过使用现有的内部或外部的标准认证服务, Review 软件不需要额外的安全过程。所有的流量都需通过加密并且该软件还将提供详细的活动日志, 为问题的解决和法规符合性的问题提供关键的审计踪迹。通过尽可能减少数据中心内对本地访问需求, 该软件的远程管理能力可以帮助您以物理方式锁闭敏感的机器, 进一步提高安全性水平。
4. **高级权限管理功能:**

能做到针对不同的用户操作 KVM 的时候, 可以针对每台服务器进行设置, 可以把键盘、鼠标左键、鼠标右键和视频、音频信号的权限分开单独设置, 以实现不同的权限分配功能。
5. **服务器画面巡检功能:** 能够指定几台服务器进行巡检, 能够设定巡检的间隔时间, 停留时间, 并可以在巡检画面上直接切换到指定服务器进行操作。
6. **支持二次口令认证功能:** 支持管理员二次口令认证, 更高安全级别;
7. **支持界面定制功能:** 可以根据用户熟悉的方式, 来进行 KVM 摆放分组及显示, 支持用户个性化显示。
8. **报警功能:** 支持当出现异常现象(如 KVM 离线等), 能实现报警。
9. **日志系统:** 具备日志系统, 能够针对各种事件进行统计。日志能记录用户登录系统时间、退出系统时间。
10. **支持审计平台扩展:** 与 Review 审计平台集合, 可以实现对 KVM 会话的视频审计和键盘审计功能。
11. **支持二次开发功能:** 可以根据用户的一些特定要求, 进行二次开发。



Review 管理软件安装服务器最低系统配置要求

2 GHz Pentium 或相当的处理器

4GB 内存

100BT 网卡（建议使用 1 GB 局域网）

10 GB 可用磁盘空间

下列操作系统中的一种：

- Microsoft Windows Server 2003 Standard、Enterprise 和 Web Edition
- Windows XP Professional，带 Service Pack 2 或更新的服务包
- Windows 2003 Server Standard、Enterprise 或 Web Edition
- Windows 7 Professional，Enterprise 或 Ultimate
- Windows 2008 Server Standard、Enterprise 或 Web Edition

Review 管理软件客户端最低系统配置要求

2 GHz Pentium 或相当的处理器

2GB 内存

100BT 网卡

10 GB 可用磁盘空间

下列操作系统中的一种：

- Microsoft Windows Server 2003 Standard、Enterprise 和 Web Edition
- Windows XP Professional，带 Service Pack 2 或更新的服务包
- Windows 2003 Server Standard、Enterprise 或 Web Edition
- Windows 7 Professional，Enterprise 或 Ultimate
- Windows 2008 Server Standard、Enterprise 或 Web Edition

入门

许可-基本信息

- 许可基于在 Review 管理软件中配置的目标设备节点数。

授权目标机器数：决定了 Review 管理软件最多可以有效使用目标设备的数量。

- 你购买的许可是否包含**审计授权**许可决定了是否可以进行 KVM 会话审计。

审计许可：分审计最大并发数和回放最大并发数；

审计最大并发数：决定同一个时间有多少路 KVM 会话可以被审计；

回放最大并发数：决定同一个时间有多少路审计录像可以被打开回放。

- 授权截止日期：表示授权的有效期限，超过这个有效期限，授权失效软件无法进入。

- 授权类型：分文件证书和加密狗两种。

文件证书：跟机器绑定，需要用“机器码生成工具”生成机器码，发回厂家生成专用文件证书，邮件请发 license@chinakvm.com.cn。

加密狗：不跟机器绑定。

- 在 Review 管理软件里面授权信息如下：



- 如有多台主备 Review 管理软件服务器，则需要对应数量文件证书或加密狗。



许可-许可购买、许可升级

基本许可	
Review-stand	Review-stand – 1 hub, 64devices
Review-advance	Review-advance – 1 hub, 1 spoke, 512 devices
附加许可	
Review-16	Review device license – 16-pack
Review-32	Review device license – 32-pack
Review-64	Review device license – 64-pack
Review-128	Review device license – 128-pack
Review-256	Review device license – 256-pack
Review-512	Review device license – 512-pack
Review-1024	Review device license – 1024-pack
Review-unlimited	Review device license-unlimited
审计许可	
Review-record-5	Review-record-5 并发录像及键盘审计通道数：5 通道
Review-record-10	Review-record-10 并发录像及键盘审计通道数：10 通道
Review-record-20	Review-record-20 并发录像及键盘审计通道数：20 通道

譬如贵公司有 100 台左右服务器，但不超过 128 台，购买的时候可以先购买基本许可 Review-stand，再购买附加许可 Review-64，这样总共有 $64+64=128$ 个许可。

许可升级：

如果原来采用的是文件证书，则我方会 email 一个新的文件证书给贵公司，只要替换即可。

如果原来采用的是加密狗模式，则需把加密狗寄回我处升级，在此期间，我公司会给一个临时的文件证书，以保证业务不中断。



基本概念

KVM: 对目标设备（服务器类），通过键盘（Keyboard）、视频（VGA）、鼠标（Mouse）接口，通过一个小板设备，用网线连接到 KVM 设备的端口实现管理（监控屏幕、远程控制）；

（适用于本管理软件的 KVM 为 AS 系列 KVM，包括 AS2008、AS2016、AS2032、AS4008、AS4016、AS4032、AS4064、AS8016、AS8032、AS8064）

ASIQ: AS KVM 系列配套使用的接口模块，有 PS2、USB 等接口类型，可以将服务器的键盘、鼠标、显示器、音频信号转换成 RJ45 接口后，通过 CAT5e 网线连接到 AS KVM 主机。

ACM: 高级串口管理设备，用来对各类设备的 console 输入输出信号（RS232 协议）进行汇聚、交换和 OVER IP 的转换；

（适用于 ACM4、ACM8、ACM16、ACM32、ACM48）

APM: 高级电源管理设备，通过网络可以实现对智能 PDU 的远程管理，可以实现开关电源、温湿度检测等功能。

（APM8、APM16、APM20）

装置: 指 KVM、ACM、APM 系列硬件。

目标设备: 只连接在 KVM、ACM 下的设备，及连接在 APM 下的电源口名称。

设备: 包括装置与目标设备。

设备组: 把有相同属性的设备进行分组，便于管理及统一权限分配。

用户: 指 Review 里创建的用户，默认管理员用户为 admin。

用户组: 指用户分组，譬如信息科技处，包含张三、李四等，便于管理及统一权限分配。

系统典型拓扑结构图

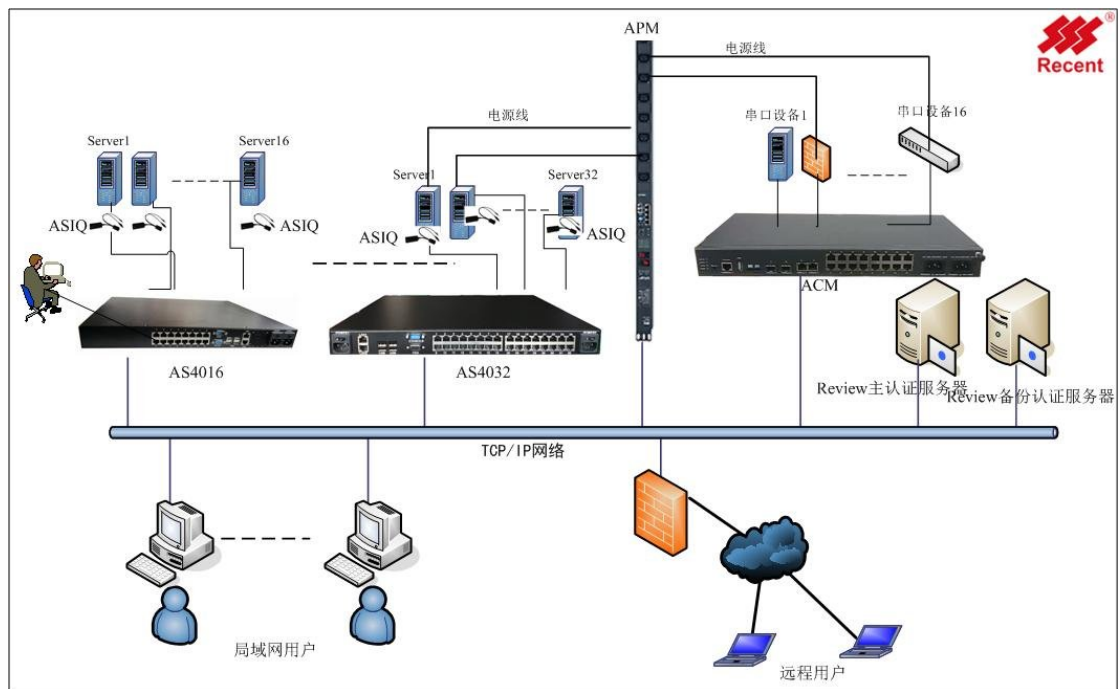
如图：

服务器通过 ASIQ 连入 AS KVM 管理，各类串口设备的 CONSOLE 通过网线连入 ACM 管理，服务器或串口设备的电源口连入 APM 管理；

AS 系列 KVM、ACM、APM 均通过网络连入到 TCP/IP 网络；

在 TCP/IP 网络中连入 2 台服务器，分别安装 Review 主认证服务器和 Review 备份认证服务器；

客户端连入 TCP/IP 网络，在与 Review 服务器、KVM、ACM、APM 等设备能互通的情况下，通过 IE 浏览器来访问和控制。



Review 管理软件界面



编号	名称	说明
1	顶部选项栏	使用顶部选项栏为 Review 软件窗口刷新窗口显示、注销软件会话或调出专用界面显示、以及界面风格切换按钮。登录的用户名会显示在顶部选项栏。
2	选项卡栏	使用选项卡栏显示和管理设备、审计、用户、报告、系统设置。
3	顶部导航栏	根据选项卡栏中的活动选项卡的不同，顶部导航栏中的选项会有所不同。与这些选项相关的主题会在侧面导航栏中显示。
4	内容区域	由选项卡栏、顶部导航栏和侧面导航栏选项指定的信息会显示在此区域，并且这些信息可在此区域进行更改。
5	告警事件窗	该窗口提供一些紧急告警事件通知，在有告警的时候会弹出显示。
6	侧面导航栏	使用侧面导航栏选择要在内容区域显示或编辑的系统信息。侧面导航栏包含有控制其显示状态的箭头。

JAVA 运行环境安装

在 KVM 会话之间，远程访问的控制机，需要安装一个 JAVA 运行环境才能正常打开 KVM 会话，JAVA 的版本要为 1.6 以上。

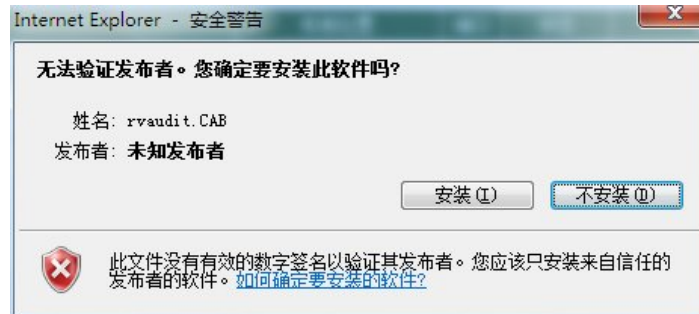


备注：如果没有安装 JAVA 运行环境，则无法打开 KVM 会话，JAVA 运行环境简称 JRE，可从 www.java.com 上免费下载。

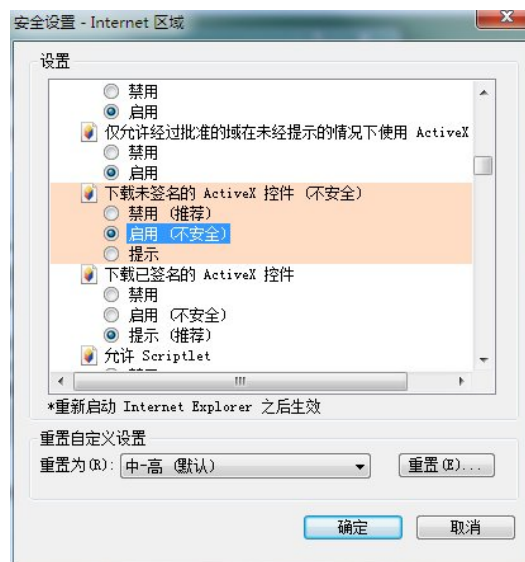


Review 审计回放插件安装

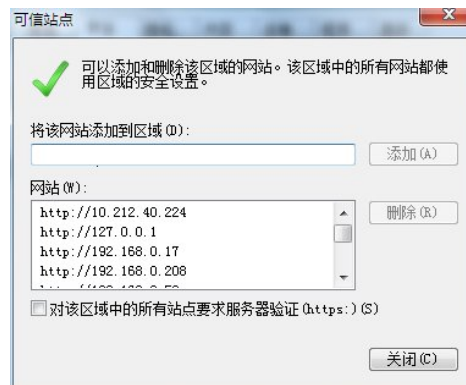
首次登录进 Review 管理软件后，会出来一个安全警告，提示安装 rvaudit.CAB 软件，该插件用来对已审计内容进行回放。



需要对该控件进行安装，需要对 IE 的安全选项进行设置，如下图



并把 Review 管理服务器的 IP 地址，加入到可信站点，这样就不会每次登陆都出来安装提示。



基本操作

色彩方案配置及更改密码

- 色彩方案:

系统内建两套颜色方案，一套为青绿色，一套为天蓝色。可以通过顶部选项栏右侧的两个对应颜色的按钮来进行切换。 对应颜色按钮切换到对应颜色方案。

- 更改密码:

在“选项卡栏”里选择“系统”，再选择“顶部选项栏”里的“更改密码”，出来以下窗口：



输入当前的密码，输入并确认新密码，按保存以确认更改密码。

“重置”按钮用来清空输入框里的内容。

如果是普通用户忘记密码，需要管理员去修改的话，管理员进入“用户”选项栏，勾选需更改用户前面的勾选框，并“重置密码”，如下图：



重置后的密码为 review。

也可以修改成指定密码，点击“用户名”进入用户属性修改

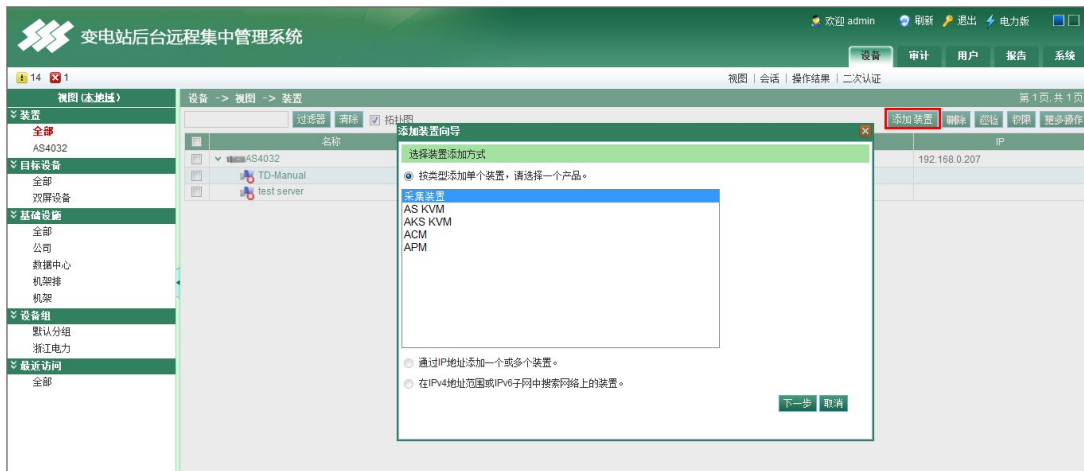


在“密码框”里直接对密码进行修改，重复输入密码，按保存。

添加装置

添加设备（kvm）步骤方法

在“设备”视图，点击“添加装置”，出来如下界面：



选中装置类型，点击下一步



填入对应 KVM 等类型装置的 IP 地址，ReView 自动在网络内寻找对应 IP 地址的 KVM 等类型装置等，选“下一步”出来以下对话框：



备注:

“禁止单机版登录”，意味着只能通过 Review 集中管理软件访问，直接访问 AS KVM 单机版会提示“**Err:授权失败 失败: kvm 已被集成管理服务服务器安全托管**”。

“允许有相同名称的目标设备合并成一个目标设备”，表示如果新添加的目标设备名称与 Review 里的目标设备名称相同的话，则可以合并成一个“目标设备”，否则根据系统规则，会给新的目标设备名称加上~1 以示区别。

添加装置完成后，为如下图显示



备注：添加 ACM、APM 同 AS KVM 添加步骤。

设备分组

Review 管理软件可根据装置的类型（AS KVM 交换机、ACM 串口服务器、APM 智能电源管理设备等）对受管理的装置进行自动分组。目标设备会按照其所分配的类型自动分组。

也可以添加和更改“个人和全局设备组” — 全局设备组允许所有用户查看，而个人设备组仅允许创建该组的用户查看。从“侧面选项栏”里点击“默认分组，出来下图所示界面。

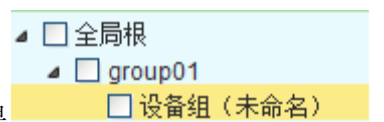


从图中“组导航”的右侧点击“+”号，出来“维护设备组”界面：



图中“+”和“-”分别对应“增加组”和“删除组”操作：

增加组操作：选中某个组，注意是使组名称背景变成黄色，则在该组下新建一个组；如



选中 group01，点击“+”，则出来以下效果

删除组操作：选中某个组，注意是勾选对应组前的勾选框，可以多选，点击“-”后，

会出现删除确认对话框，，按确定执行删除组操作。

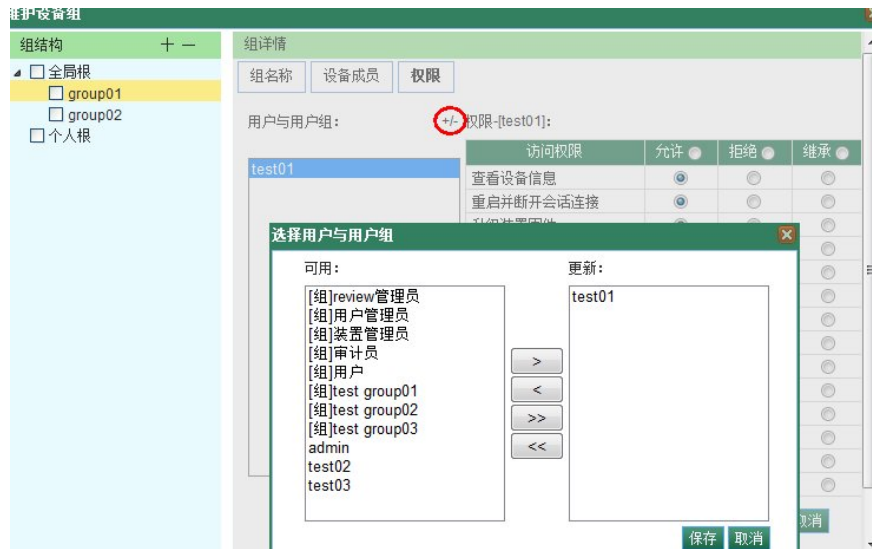
设备组成员分配

设备组建好以后，需要进行对设备组成员进行分配，该分配为了更好的权限管理，譬如 group01 里含 test server 和 h3c router 两个设备，则对应对 group01 有权限的 user01，就对应访问 test server 和 h3c router 两个设备的权限，其存在权限继承关系。



设备组权限分配

对应“设备组”设置权限分配，可以对应分配“用户”或“用户组”，如下图，先选择“权限”，再点击图中红色圈圈标注的“+/-”符号，出来“选择用户和用户组”对话框，对话框左边为可用的用户和用户组，右边是选中的用户和用户组。





用户组

添加到 Review 管理软件的用户可添加到如下两种类型的用户组：

内建 — Review 管理软件附带了五个预定义的用户组：Review 管理员、用户管理员、装置管理员、审计员、员和用户。用户添加到 Review 管理软件系统后，所有这些用户将会被自动纳入“用户”用户组。可将用户添加到其他任何用户组。用户在 Review 管理软件系统执行操作的权限取决于用户所属的内建用户组。

用户定制 — 也可以基于任何需要的标准定义定制组。例如，可以基于具备只读访问权限的用户管理员定义组，定义特定部门的软件开发者，基于职位定义全局网络基础设施人员，等等。

内建组操作权限说明：

内建组名	说明
Review 管理员	集控平台的管理员，拥有最高权限及所有设备的操作权限。
用户管理员	负责账户组、账户、认证服务的管理职能，审计策略配置
装置管理员	负责装置及目标设备的管理职能。
审计员	负责审计工作，回看会话视频。
用户	普通操作员，通常用会话（KVM、ACM、APM 等）方式对拥有权限的目标设备进行日常管理。

内建组操作权限说明：

操作	Review 管理员	用户 管 理 员	装 置 管 理 员	审 计 员	用 户
系统配置	√				
添加、更改、导入和删除 ReView 软件	√	√			
备份和恢复 ReView 软件数据库	√	√			
添加、更改和删除设备	√		√		
添加、更改和删除设备组	√	√	√		
配置访问权限	√	√			



添加、更改和删除地点、部门和位置属性	√		√		
添加、更改和删除外部认证服务	√	√			
添加、更改和删除用户账户和自定义用户组	√	√			
所有与事件相关的操作	√			√	
更改密码	√	√	√	√	√

自定义组操作说明:

如下图,可以通过图中红色方框标注的按钮来完成“新增”、“删除”、“权限分配”操作。



用户组“权限”操作里含以下几个内容:

- 名称修改: 更改用户组名称。
- 成员分配: 分配属于该用户组的成员。注一个用户可以属于多个用户组。
- 访问权限分配: 对应分配“设备”和“设备组”权限。







抢占级别

在创建帐户或组时，**ReView** 软件管理员和用户管理员可以为用户帐户或用户定制的用户组指定抢占级别。抢占级别可稍后进行更改。

用户的抢占级别决定了他们是否能够中断或断开另一个用户与目标设备的会话（**KVM**、**ACM** 等）。抢占级别从低到高定义为 **1-4**。一个用户所拥有的抢占级别，是其所属组（允许多个）拥有的抢占级别中最高的一个级别。所以，帐户组同样允许有抢占级别的设定。

用户和用户组的抢占级别：

抢占级别	说明
4	Review 软件管理员和装置本地账户的默认抢占级别。本地账户拥有最高的抢占访问级别。
3	帐户组 “装置管理员” 的默认抢占级别。
2	帐户组 “用户管理员” 的默认抢占级别。
1	帐户组 “用户” 及 “审计员” 的默认抢占级别。

抢占级别的使用方式如下：

- **用户抢占级别** — 此级别是由 **ReView** 软件管理员或用户管理员分配给用户的抢占级别。如果此值大于用户所属的用户组的最高抢占级别，则该值将被用作有效用户抢占级别。
- **组抢占级别** — 此级别是分配给用户所属的用户组的抢占级别。如果用户被分配到多个不同抢占级别的用户组，则最高抢占级别用户组的抢占级别将会成为用户组的抢占级别。例如，如果用户分属管理员（级别 2）和审计员（级别 1）用户组，则该值将会被定义为 3。如果该值大于用户的最高抢占级别，则该值会被用作有效用户抢占级别。
- **有效用户抢占级别** — 该级别是用户和组抢占级别之间的最大值，也是当用户试图抢占另一用户会话时 **ReView 3** 软件所认可的实际抢占级别。例如，如果用户属于审计员组（级别 1）但所分配的用户抢占级别为 4，则用户的有效用户抢占级别为 4。尽管此用户是审计员组的成员，但是此用户也可以抢占属于管理员或装置管理员用户组的用户的会话。

管理用户帐户

您可以通过 ReView 3 软件：

- 添加、更改和删除用户帐户
- 解除用户帐户锁定
- 指定用户帐户限制
- 更改用户组成员资格
- 显示用户和用户组对目标设备及受管理的装置的访问权限
- 添加和删除用户定制的用户组
- 从内建或用户定制的用户组中显示、指定和移除用户组成员

用户帐户窗口

通过“用户”窗口显示和管理用户帐户。

要显示“用户”窗口，请：

1. 单击“用户”选项卡。将会打开“用户 — 全部”窗口。
2. 要显示内建或用户定制的用户组的用户名称，请单击侧面导航栏中“用户”下的组名链接。将打开此组的“用户”窗口并列此组所有用户。
3. 要选择一个人用户，请单击“用户帐户”窗口内的用户名。

“用户”界面如下图所示：



可以对用户进行如下操作：



“新增”：新增加一个用户，用户可以属于不同的认证服务体系，默认属于“review 内部认证”；

“删除”：删除指定用户；

“**权限**”：针对该用户进行权限设定，分配其允许或拒绝访问的设备或设备组；

“**重置密码**”：把用户的密码重置成 review；

“**解锁**”：当用户由于密码多次输错导致被封锁的情况下，进行解锁操作，使得用户账号重新启用。

更改用户帐户属性

如果具有 ReView 软件管理员或用户管理员的权限，您可以更改下列用户帐户属性：

- 用户（登录）名和全名
- 登录属性：仅以操作员身份登录、需要二次认证、需要访问控制列表；
- 登录密码
- 帐户登录限制和到期期限设置
- 用户被分配到的用户组
- 用户的抢占级别
- 家庭和公司地址
- 家庭电话、公司电话、移动电话和寻呼机号码
- 主电子邮件地址和另外可多达五个电子邮件地址
- 希望添加的有关此用户的注释
- 多达六个定制字段

某些属性仅当该用户帐户使用 ReView 软件内部认证服务时才可更改。



The screenshot shows the ReView user management interface. At the top, there are tabs for '设备' (Devices), '审计' (Audit), and '用户' (Users). Below the tabs, there is a breadcrumb trail: '帐户 | 帐户组 | 认证服务'. The main content area is divided into two sections. On the left, there is a sidebar menu with the following items: '名称', '密码', '限制' (highlighted in yellow), '用户组', '抢占级别', '地址', '电话', '电子邮件', '注释', '定制字段', '访问权限', and '访问控制列表'. The right section is titled '限制' (Limits) and contains several checkboxes: '禁用用户账户', '用户在下次登录时必须修改密码', '用户不能更改密码', and '密码永不过期'. Below these checkboxes, there is a '结束于:' (Expires on) field with the value '2013-11-30 16:14:28' and a calendar icon. At the bottom of the '限制' section, there are two buttons: '保存' (Save) and '重置' (Reset).

设备操作界面

界面的拓扑显示



如上图：

1、下拉小箭头。小箭头如果展开，则会列出 AS KVM 下连了哪些服务器，也可以收拢，只看到 AS KVM 本身；

2、拓扑图按钮。如果拓扑图选项不勾选的话，就只显示 AS KVM 等装置，而不显示目标设备（装置所管理的对象，如：KVM 所管理的是服务器类设备。）

备注：默认下拉小箭头展开、拓扑图选项勾选。

界面的内容显示

默认 Review 软件设备页面显示以下这些内容，包括“名称”、“机柜位置”、“端口”、“状态”、“类型”、“操作”、“IP”，如下图所示：

名称	机柜位置	端口	状态	类型	操作	IP
AS4032			空闲	KVM		192.168.0.207
TD-Manual		6	无电源	目标设备	KVM会话	
test server		20	无电源	目标设备	KVM会话	

如果想多显示内容的话，需要到“系统”菜单下“全局属性”的“管理列”里进行定制，如下图：



勾选需要显示的内容，则相关内容就会自动在“设备”视图中进行显示了。

过滤器的作用



Review 软件窗口允许您过滤列表信息，在过滤文本框中输入文本字符串，即可检索匹配的项目。如果有大量 kvm 装置或者其他项目扩展到多个页面，那么过滤功能就会非常有用。允许过滤的窗口在内容区域有一个文本字段和一个“过滤器”按钮。如上图所示。

过滤是对整个列表中的项目或指定列执行操作，过滤后，项目列表的范围将更小更精确。执行过滤时，将在各行各列搜索指定的文本字符串。

目标设备设置

点击一台“服务器名字”：

<input type="checkbox"/>	AS4032			空闲	KVM		192.168.0.207
<input type="checkbox"/>	TD-Manual	6	无电源	目标设备		KVM会话	
<input type="checkbox"/>	test server	20	无电源	目标设备		KVM会话	

出来如下界面：

设备属性 - TD-Manual

- 设备
 - 概述
 - 属性
 - 标识
 - 位置
 - 联系人
 - 定制字段
 - 注释
 - 网络
 - 活动的会话
 - 连接

概述

名称:

类型: 目标设备

工具

①在上图的属性中，可以对服务器的名称进行定义，并根据自身需要对服务器进行各项描述，从而在设备视图中进行显示。其中“位置”字段需要预先定义好，才可以在下拉菜单中显示。

②在上图中可以自己定制所需要的标签，如购买时间，维保年限，维保联系人等。

设备属性 - TD-Manual

- 设备
 - 概述
 - 属性
 - 标识
 - 位置
 - 联系人
 - 定制字段
 - 注释
 - 网络
 - 活动的会话
 - 连接

定制字段

定制字段 1:

定制字段 2:

定制字段 3:

定制字段 4:

定制字段 5:

定制字段 6:

定制字段 7:

定制字段 8:

定制字段 9:

定制字段 10:

对装置的操作

在添加装置以后，需要对装置进行改名、重启、升级、重新同步等操作，在“设备”视图下，点击 KVM 等装置名字（以 KVM 举例）“

名称	机柜位置	端口	状态	类型	操作	IP
AS4032			空闲	KVM		192.168.0.207
TD-Manual		6	空闲	目标设备	KVM会话	
test server		20	无电源	目标设备	KVM会话	

如上图，点击 AS4032 的装置名称之后，出来以下窗口：



在这里可以更改 AS4032 的名称、网络 IP 地址、升级固件、重新同步等等操作。

最重要的就是重新同步、设备更改 IP、升级固件。下面分别介绍

重新同步：

当 AS4032 下所接的服务器有所变化（增加或减少）的时，而在目标服务器列表没有更新的时候，按下“重新同步”按钮进行手动同步，ReView 会把 AS4032 下的设备进行准确的跟新列表出来。

设备更改 IP

更改 AS4032 IP 的时候，需要在 Review 里面更改两个地方的 IP 地址

“装置-属性”中的“网络”，这里的“地址”是 ReView 去通讯的 AS4032 的地址，是一个 IP 指向地址，如下图：



“装置设置”中的“网络信息”，这个是 AS4032 的**实际 IP 地址**，如下图：



更改顺序，先更改 AS4032 实际 IP 地址，再更改 IP 指向地址。

升级固件：

前提是先往 ReView 系统中已经添加了 AS4032 的固件升级文件，点击“升级固件”按钮，按照提示选择合适固件版本进行升级操作。

目标设备和装置物理对应关系

当添加了一个服务器以后，我们要知道该服务器和 **KVM** 装置的物理连接关系，也就是说要知道哪台服务器是连着哪台 **KVM** 的哪个口。同时我们也需要知道哪台 **KVM** 装置下面连着哪些服务器。

名称	机柜位置	端口	状态	类型	操作	IP
AS4032			空闲	KVM		192.168.0.207
TD-Manual		6	空闲	目标设备	KVM会话	
test server		20	无电源	目标设备	KVM会话	

由上图我们可以知道，服务器后面跟着端口号，十分容易查找。

另一种方法，是直接点击目标设备名称，如下图



点击“连接”后能清楚的显示整个物理拓扑结构。

事件管理

事件泛指广义的事件，是指触发自装置、认证、平台管理等一些记录。

事件配置的设置

在 ReView 软件里面开启事件记录功能，报告——〉配置事件：



如上图，可以日志的以下选项进行设置：

- 日志保留时间；
- 事件的开关：用户、认证、设备、会话、装置、任务、系统、状态、审计、访问控制，使得相关日志是否启用；
- 告警设置：使得“装置离线”或“目标设备离线”告警是否启用并弹出告警窗。

事件配置的查看

The screenshot shows the '事件日志' (Event Log) section of the ReView software. The interface includes a navigation bar with '设备', '审计', '用户', '报告', and '系统' tabs. Below the navigation bar, there are filters for '全部' (All) and '过滤器' (Filter). The main area displays a table of events with the following columns: 状态 (Status), 严重性 (Severity), 时间 (Time), 用户 (User), 装置 (Device), and 描述 (Description). The table contains 14 rows of event data.

状态	严重性	时间	用户	装置	描述
新	信息	2013-08-28 14:29:51	admin		修改账户基本信息'test03'成功
新	信息	2013-08-28 14:29:38	admin		解锁账户'4'成功
新	信息	2013-08-28 14:29:31	admin		修改账户基本信息'test03'成功
新	信息	2013-08-28 14:23:27	admin		修改认证服务'Review内部认证'成功
新	信息	2013-08-28 14:12:56	admin		登录账户'admin(192.168.0.17)'成功
新	信息	2013-08-28 14:12:53	test03		登出账户'test03'成功
新	信息	2013-08-28 14:12:09	test03		登录账户'test03(192.168.0.17)'成功
新	信息	2013-08-28 14:12:05	admin		登出账户'admin'成功
新	信息	2013-08-28 14:12:03	admin		修改账户基本信息'test03'成功
新	信息	2013-08-28 14:11:55	admin		登录账户'admin(192.168.0.17)'成功
新	非紧急	2013-08-28 14:11:46			登录账户'test03(192.168.0.17)'失败:您当前网络地址不允许登录
新	信息	2013-08-28 14:11:42	admin		登出账户'admin'成功
新	信息	2013-08-28 14:11:39	admin		修改装置权限'7'成功
新	信息	2013-08-28 14:11:37	admin		新建账户权限'4'成功
新	信息	2013-08-28 14:07:03	admin		修改账户基本信息'test03'成功
新	信息	2013-08-28 14:04:29	admin	70A5D9-36G008	同步采集装置'70A5D9-36G008(70A5D9-36G008)'成功

如上图，可以根据“严重性”或“事件类别”来进行事件查看，默认是查看全部事件。

事件的导出

事件导出分部分导出和全部导出：

- 如果勾选了某些信息，则为部分导出；
- 如果没有勾选任何信息，则为全部导出；

The screenshot shows the '事件日志' (Event Log) section of the ReView software. The interface includes a navigation bar with '事件日志', '配置事件', and '数据信息记录' tabs. Below the navigation bar, there are filters for '全部' (All) and '过滤器' (Filter). The main area displays a table of events with the following columns: 状态 (Status), 严重性 (Severity), 时间 (Time), 用户 (User), 装置 (Device), and 描述 (Description). The table contains 5 rows of event data. The '导出' (Export) button is highlighted in red.

状态	严重性	时间	用户	装置	描述
新	信息	2013-08-28 14:29:51	admin		修改账户基本信息'test03'成功
新	信息	2013-08-28 14:29:38	admin		解锁账户'4'成功
新	信息	2013-08-28 14:29:31	admin		修改账户基本信息'test03'成功
新	信息	2013-08-28 14:23:27	admin		修改认证服务'Review内部认证'成功
新	信息	2013-08-28 14:12:56	admin		登录账户'admin(192.168.0.17)'成功

事件的查找

可以根据事件的起始时间来定义搜索事件。

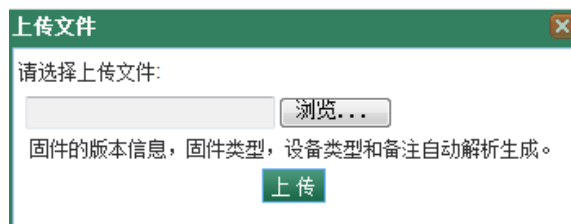
固件与插件的管理

固件管理

在“系统-固件与插件”窗口中可添加、删除 kvm 装置固件文件，添加固件文件之后，您可使用这些文件升级受管理的装置。如图：



单击“添加”。将会出现“添加固件文件向导”：



浏览需要添加到ReView 软件装置文件库的固件文件的目录和文件名（或者浏览到其位置），然后单击“上传”。

固件信息查看

- 1、单击“设备”选项卡
- 2、勾选“kvm装置”，点击“更多操作-获取固件版本”
- 3、如下图所示



插件管理

插件可在 **ReView** 软件中为特定类型(型号)的装置提供支持,用于 **Applet** 升级。
applet 组件目前有: **kvm** 会话, 巡检、审计播放器。

插件封装放在一个单独的存档文件中,可独立于ReView 软件提供和添加,您可以将插件添加至ReView 软件

添加插件

- 1) 单击“系统选项卡”
- 2) 单击左侧导航栏中的“插件”。
- 3) 单击“添加”。将会打开“添加插件向导”。



- 4) 选择插件类型,输入插件版本、备注,浏览至插件文件位置后,点击上传。

高级操作

访问控制列表

用户通过 WEB 来访问 Review 管理软件，不仅仅是通过用户名和口令进行限定，同时还可以通过 IP 地址来进行限定，在 Review 管理软件里面可以设定，某某用户只能从某 IP 地址的主机进行远程访问。

打开“系统”选项里的“服务器”菜单，再在侧面栏里选择“访问控制列表”，出来如下图所示界面：



通过 **新增** **删除** **启用** **禁用** 来完成相关操作：

- “新增”：新增一条访问控制列表；
- “删除”：一条访问控制列表；
- “启用”：启用一条访问控制列表；
- “禁用”：禁用一条访问控制列表；

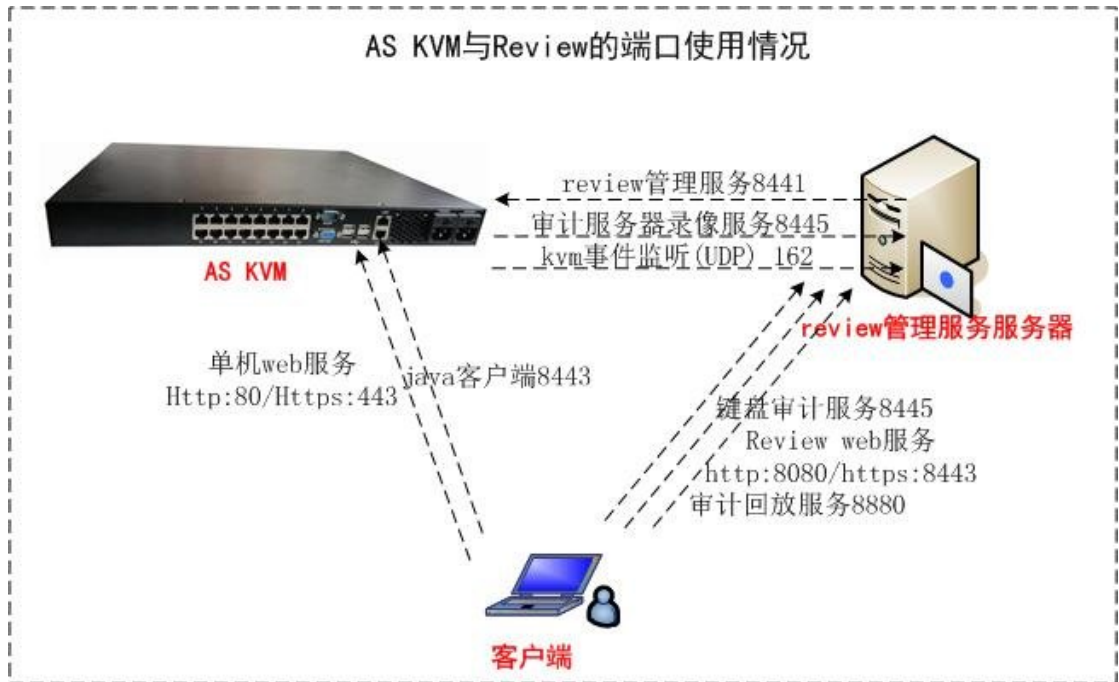
新增好一条访问控制列表后，需要指定该条访问控制列表作用于某个用户。



注：一条访问控制列表可以作用于一个用户或多个用户。一个用户可以被作用多条访问控制列表。

TCP/UDP 端口

如图：



- AS KVM 单机 web 访问可通过 http（80）或 https（443）端口访问；
- 客户端通过 IE 页面里 JAVA 客户端与 AS KVM 进行通过，所有键盘、鼠标、显示器、音频信号均通过 8443 端口进行传输。
- Review 管理软件通过 8441 端口对 AS KVM 进行管理；
- Review 审计服务器通过 8445 端口与 AS KVM 进行通信，并通过 8445 端口从客户端这边接收审计数据。
- Review 管理软件 Web 访问可通过 http（8080）或 https（8443）端口访问；
- 客户端通过 8880 端口调阅审计服务器的审计数据。
- AS KVM 通过 UDP 161/162 与 Review 管理服务器进行通讯。

代理服务器

当客户端能访问到 Review 服务器，但客户端与 KVM 等装置不在同一个网段，即客户端与装置网络不通的情况下，需要有 Review 管理软件来代理，进行数据转发。此时 Review 服务器起的作用为“代理服务器”，类似于网络中的路由器。

代理服务器的设置

打开“系统”菜单下的“服务器”，找到“代理服务器”，如下图：



代理服务器有 4 个选项：

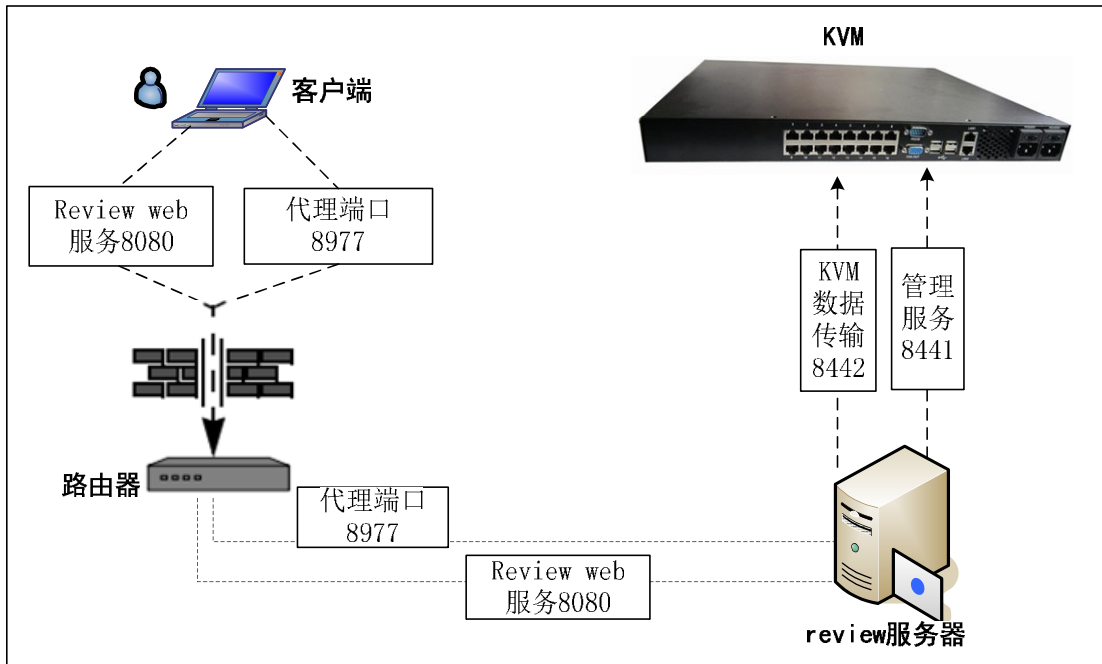
- 禁用代理服务器，此为默认选项；
- 将代理服务器用于所有 KVM、串行和虚拟媒体会话；
- 仅将代理服务器用于与此 Review 服务器处于不同网络的客户端；
- 仅将代理服务器用于连接到以下地址的客户端。（指定 IP 的客户端使用代理模式）

代理服务器参数有如下几项：

- 服务器地址，此地址一般就填 Review 服务器的 IP 地址；
- 服务器端口，默认为 8977，可自行修改，建议端口用大一些；
- 内存分配，默认为 64M，可自行修改，但不能小于 64M，内存大小根据代理的 KVM

会话并发数量来进行调整，(注：占用内存跟 KVM 会话的内容存在一定的关系，简单的说一个是 word 文档修改，另一个是网页浏览，占用内存会有区别，一般情况下 1 路 KVM 会话按 20M 来计算，可适当大些)；

- 启动线程，默认 10 个，2 个线程可以代理 1 路 KVM 会话代理，即可以同时 5 路 KVM 会话代理。



用于与 KVM 交换机代理服务器连接(KVM) 的端口

二次口令认证

用户可设定为是否需要二次口令认证；

需要二次口令认证的用户在打开 KVM 会话的时候，会跳出一个窗口，要求再输入二次口令密码才能继续操作，否则不能打开远程服务器进行操作；



二次口令密码有系统管理员管理，在管理界面有专门页面显示二次口令，并与哪个用户访问哪台服务器一一对应。

序号	申请时间	申请人	申请理由	访问设备	装置名称	认证码	有效期	剩余时间	状态	操作	备注
1	2013-08-28 14:12:23	test03	11	TD-Manual		0397	2013-08-28 14:24:23	12分钟	正常	告知	

二次口令密码的过期时间可以自定义，在过期时间以内，该用户如果还是继续对此服务器申请操作，则用同一密码，如果过期了，则需向管理员重新申请。



系统全局参数

打开“系统”——“全局属性”——“系统参数”，出来关于全局的一些系统参数配置，现就“系统参数”进行一一解释说明：



自动推送名称：启用自动推送名称后，如果 Review 软件中的名称发生了更改，则名称推送操作将会自动执行，对应 AS KVM 等装置上的名称会跟随变化。（默认起作用）

自动抽取装置：启用自动抽取名称后，如果装置名称发生了更改，则名称抽取操作会自动执行。（默认起作用）

自动拓扑更新：指装置上物理端口的目标设备发生变化（譬如原来有插设备，现在被拔了；原来插第 1 口目标设备，现在插第 5 口了）的时候，对应的更新策略。

- 来自设备的拓扑更改来自动更新 Review；（默认开）
- 允许有相同名称的目标设备合并成一个目标设备（默认开）
- 删除不再连接的设备；（默认关）

删除脱机设备：

作用于在设备视图中删除设备使用该属性。

- 仅删除连接；（默认开）
- 删除连接，同时删除目标设备；（默认关）



添加设备向导:

- 禁止单机登录; (默认关)
- 删除连接, 同时删除目标设备; (默认关)

重新同步向导:

当 KVM 装置下所连的目标设备发生变化时, 由于自动拓扑更新需要有一段时间的轮询, 如需马上看到装置下目标设备连接的变化, 需要手动进行同步向导。

- 删除脱机的连接;
- 删除不再连接的目标设备;
- 允许有相同名称的目标设备合并成一个目标设备;

轮询设置:

- 启用状态轮询; (默认开)
 - 两个轮询周期之间的延迟(秒): 默认 5 秒。
 - 要并行轮询的设备数: 默认 10 个。

二次认证设置:

- 二次认证码有效期(分钟): 默认 12 分钟。

严肃审计设置:

严肃审计启用的效果是, 如果审计服务器由于故障或某个原因无法连接的时候, 为保证审计的必要性, 需被审计的 KVM 会话会自动关闭, 而不予打开。

- 严肃审计默认关闭;

串口开关:

用于对于串口服务器 ACM 的相关设置:

- 启用串口密码验证; (默认启用, 进入串口会话需经过 Review 认证体系)



- 启用串口的端口状态检测；（默认关，自动对每个串口进行状态检测，结果为在线和脱机两种）

版本设置

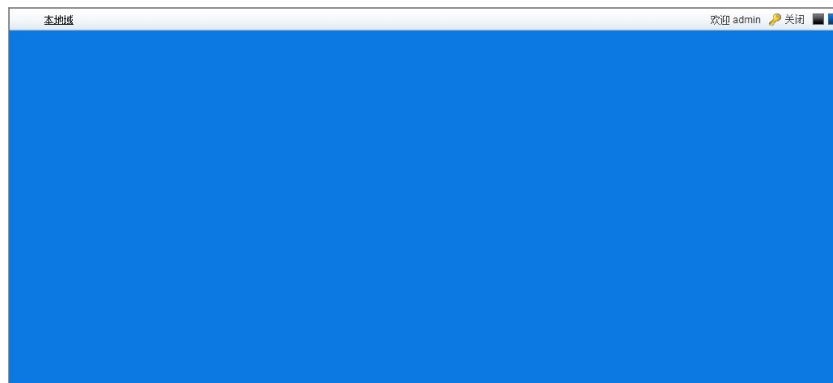
用于版本切换，如果启用并更改名称的话，在“顶部导航栏”会多出一块，并可以点击链接出来图形化菜单，以更方便的进行 KVM 会话操作。



比如启用并填写“地税机房”后，上图会变成下图



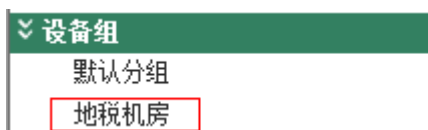
点击“地税机房”后出来以下界面



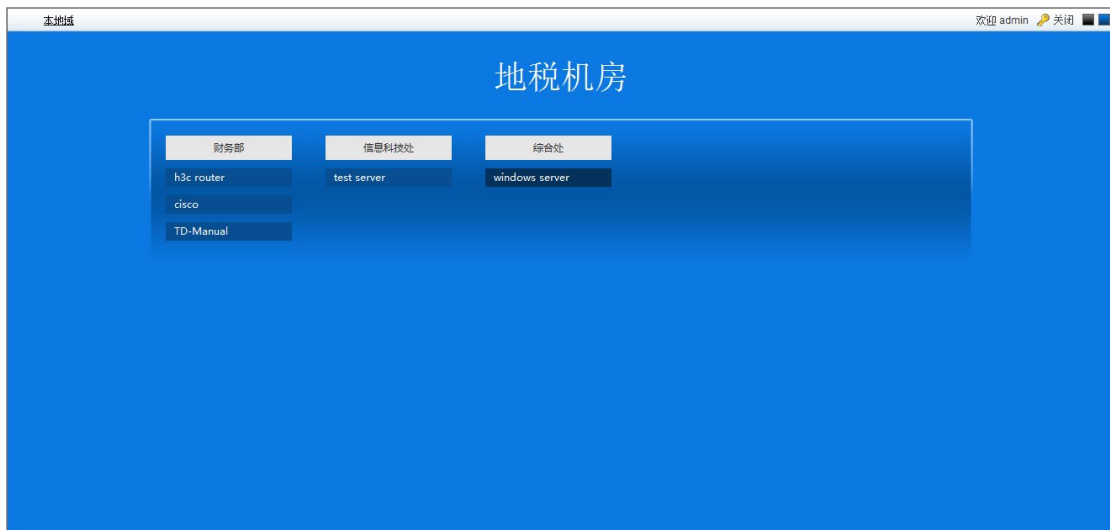
图中为空白，需要启用自定义组，在“全局属性”——“自定义设备组”，勾选“开启自定义设备组”，在“自定义名称”框里填入相应名称，譬如“浙江电力”。



在“设备”菜单栏下的“设备组”里就会多出来“地税机房”设备组，如下图所示



通过对该组进行组成员配置后，可以出来以下效果图：



点击 **h3c router** 等图标，可以直接进行 KVM 会话，不影响二次口令和审计操作。

注：本界面可以通过设定用户身份，使用用户的身份限定为“操作员”，在该用户登录 Review 软件后直接出来如上界面，具体设定在用户属性里面：



勾选“仅以操作员身份登录”。

权限及安全功能

关于访问权限的设置

访问权限指明那些用户和用户组可以访问 ReView 软件系统中的设备。访问权限也会指明所允许的操作。

对于目标设备，可以指定用户或用户组是否可进行下列操作：

- 查看“设备视图”窗口中的设备
- 配置设备信息
- 建立会话（目标设备支持的视频查看器或建立会话审计）
- 会话键盘操作
- 会话鼠标左键操作
- 会话鼠标右键操作
- 会话音频
- 查看数据记录-仅可对连接到支持数据记录的装置的目标设备设置此访问权限。



对于特定的受管理的装置，您可以指定用户或用户组成员是否可进行下列操作：

- 查看“设备视图”窗口中的设备

- 重启并断开会话连接
- 升级装置固件
- 配置设备信息
- 配置装置本地账户用户（对于不支持本地用户账户的受管理的装置，此选项将不会显示）

访问权限					
设备: +/- 权限-[AS4032]:					
TD-Manual		访问权限	允许 <input type="radio"/>	拒绝 <input type="radio"/>	继承 <input type="radio"/>
AS4032		查看设备信息	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
test server		重启并断开会话连接	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		升级装置固件	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		配置设备信息	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
		配置装置本地帐户用户	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

关于 kvm 会话和 ReView 客户端超时的设置

KVM 会话超时

由 KVM 设备本身控制，点击 AS4032 进入装置属性配置，在“装置设置”里的“用户与登录显示”里，不活动超时设定为 0 的时候，意味着 KVM 会话一直打开，不会自动关闭，设定时间为 1—120 的话，则在对应时间后 KVM 会话会自动关闭。

装置属性 - AS4032

装置设置-用户与登录显示

Admin的密码:

确认密码:

登录超时设定:(0为不启用) 10 [0-120]分钟

不活动超时设定:(0为不启用) 0 [0-120]分钟

保存 取消

Review 客户端会话超时

由 Review 管理软件控制，在“系统”——“服务器”——“客户端会话”下，设置会



话超时时间，默认 30 分钟，时间设置范围为 5—600 分钟。





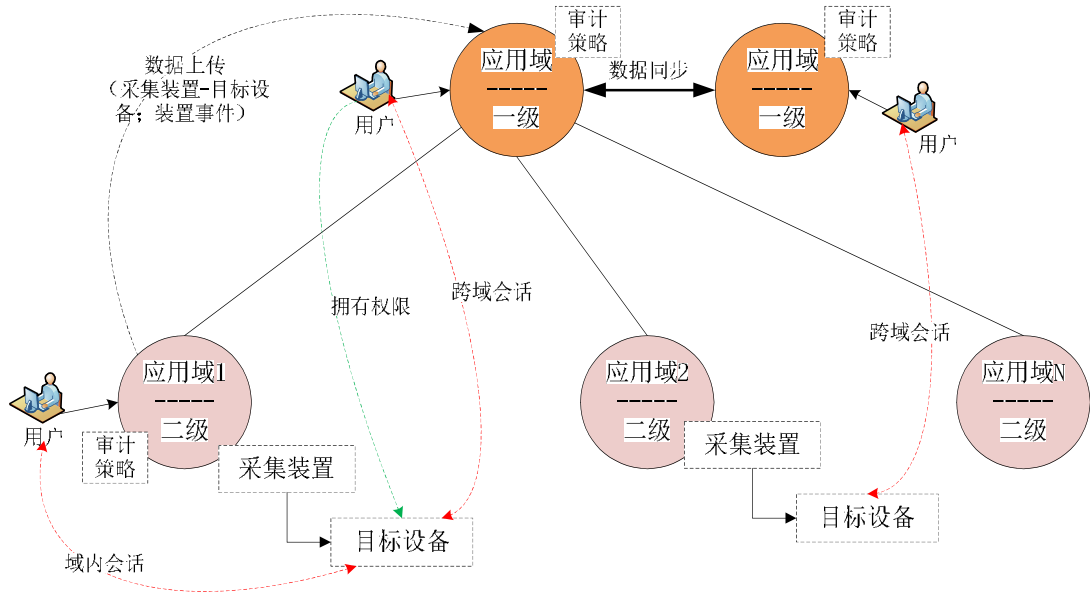
多域设置

域的定义

在 Review 软件中存在着域的概念，“域”代表一个独立的 Review 管理软件系统，“域”通常应用于有着多套 Review 管理软件系统并且他们的关系是上下级的关系，因此“域”常分为上级域和下级域。

域的特性

- 下级域通过接口与上级域上传数据，如：装置—目标设备信息；上级域可以查看到下属域的装置与目标设备；
- 上级域用户需要操作下级域的目标设备时，首先需要上级域管理员分配其相应权限；
- 下级域用户能且仅能访问自己域内设备，不能访问上级域及其他同级域设备；
- 上级域用户可以对下级域的目标设备，创建会话进行远程管理；此类跨域会话将直接连接下级域的装置，而不需要通过装置所在域的集中管理平台中转；
- 跨域会话时，审计策略将基于用户所在域的策略，如上述场景中，以上级应用域中的审计策略为参考，审计资源限制策略基于装置所在域，审计数据库信息将入库到所在域，通过域之间数据接口上传。
- 作为装置设备要求支持：单机会话、域内会话、跨域会话，且支持共享会话及抢占控制。当用户的抢占级别一样时，上级域用户的级别不会高于下级域用户，此时，依旧按照统一的抢占级别控制；



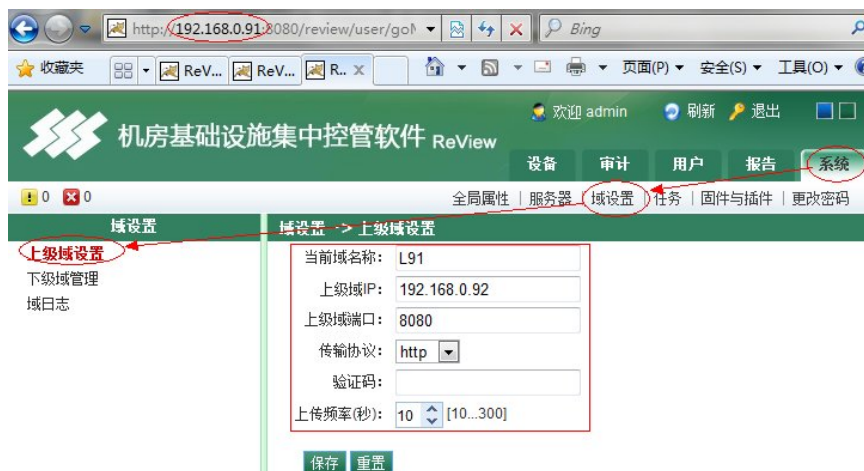
域拓扑结构示意图

建立上下级域步骤

单独运行服务器

按照部署文档，分别部署好上级域 ReView 平台和下级域 ReView 平台，分别运行。

下级域(192.168.0.91)配置上级域信息，打开“系统”菜单下的“域设置”，如下图



上级域(192.168.0.92)允许下级域的请求

查看下级域的请求



允许下级域的请求



在下级域中更新验证码，如下图



在上级 192.168.0.92 中，确认连接成功。



上下级域效果

下级域设备信息

机房基础设施集中控管软件 ReView

设备 -> 视图 -> 装置

名称	机柜位置	端口	状态	类型	操作	IP
KVM_LS_1			空闲	KVM		192.168.0.229
TD-Master		2	空闲	目标设备	KVM会话	

上级域中查看下级域设备信息

机房基础设施集中控管软件 ReView

设备 -> 视图 -> 装置

名称	机柜位置	端口	状态	类型	操作	IP
KVM_LS_1			空闲	KVM		192.168.0.229
TD-Master		2	空闲	目标设备	KVM会话	

跨域会话

上级域配置审计策略

序号	账户组	设备组	状态	修改人	修改时间	操作
1	所有账户	所有设备	启用	admin	2013-08-17 14:30:33	修改

上级域发起跨域会话

名称	机柜位置	端口	状态	类型	操作	IP
KVM_LS_1			空闲	KVM		192.168.0.229
TD-Master		2	空闲	目标设备	KVM会话	

审计数据存放在上级域中

查看跨域审计数据

开始日期-时间	结束日期-时间	持续时间	账户	目标设备	会话类型	操作
2013-08-17 15:00:06	2013-08-17 15:00:35	00:00:29	admin	(L91)TD-Master	kvm	审计 键盘 导出视频

认证服务与用户锁定登录的问题

Review 内部认证服务，是对用户认证的密码策略、封锁策略进行定义，如下图，在“用户”菜单中，选择“认证服务”，再点击编辑：



密码策略：

- 最小密码长度；
- 密码到期时间；
- 密码必须同时包含字母和数字；
- 密码必须同时包含大小写字母；

封锁策略：

- 在多次登录失败后锁定：默认 3 次；
- 在封锁期后自动对用户解锁，最长封锁期：默认 1 分钟；

如果普通用户锁定的话，我们可以通过 review 管理员帐号进去，到“用户”的“帐户”下，选择对应用户，点“解锁”按钮，就可以完成对目标用户的解锁。

	账号	姓名	认证服务	状态	抢占级别
<input type="checkbox"/>	admin	系统管理员	Review内部认证	正常	4
<input type="checkbox"/>	test01	王小明	Review内部认证	正常	1
<input type="checkbox"/>	test02	李四	Review内部认证	正常	1
<input checked="" type="checkbox"/>	test03	王五	Review内部认证	禁用	1



Review 审计功能介绍

Review 审计模块是配合 Review 平台一起使用的 KVM 审计功能模块，其可以独立安装在一台服务器，也可以安装在与 Review 平台一起的服务器。由于审计数据是以视屏回放和键盘按键记录的形式，导致所需硬盘容量比较大(平均存储数据 1 分钟 8M)，因此审计服务器硬盘要求较大，建议至少 1T 以上，并根据并发用户数、每天的访问次数、访问时间、保留时间来计算存储空间。

Review 审计最低系统配置要求

2 GHz Pentium 或相当的处理器

2GB 内存

100BT 网卡（建议使用 1 GB 局域网）

1TB 可用磁盘空间

下列操作系统中的一种：

- Microsoft Windows Server 2003 Standard、Enterprise 和 Web Edition
- Windows XP Professional，带 Service Pack 2 或更新的服务包
- Windows 2003 Server Standard、Enterprise 或 Web Edition
- Windows 7 Professional，Enterprise 或 Ultimate
- Windows 2008 Server Standard、Enterprise 或 Web Edition

审计策略的添加、删除、禁用、启用和修改

审计策略的添加

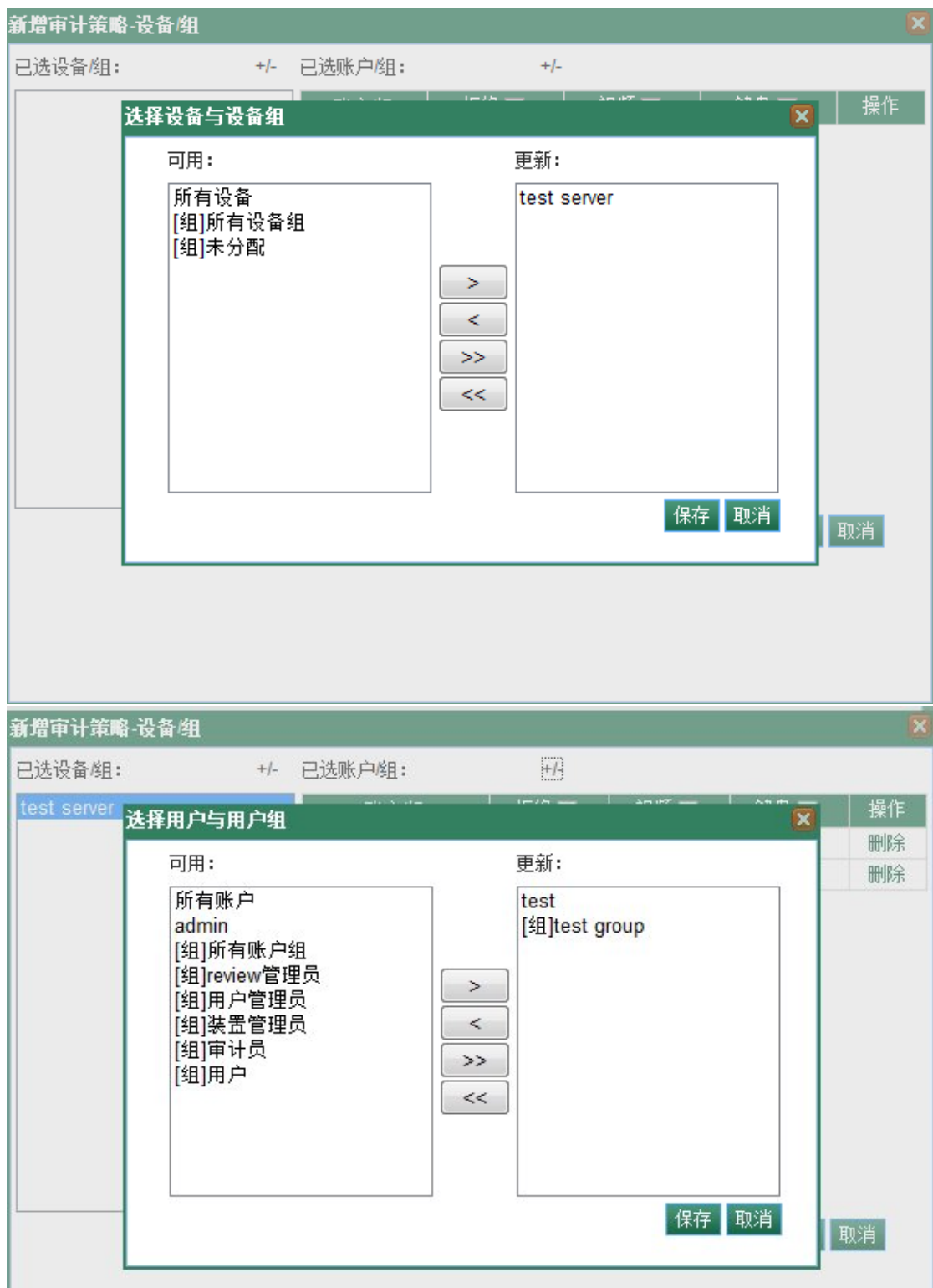
找到“审计” ——> “审计配置” ——> “设备/组策略”；



打开设备/组策略如下图所示：

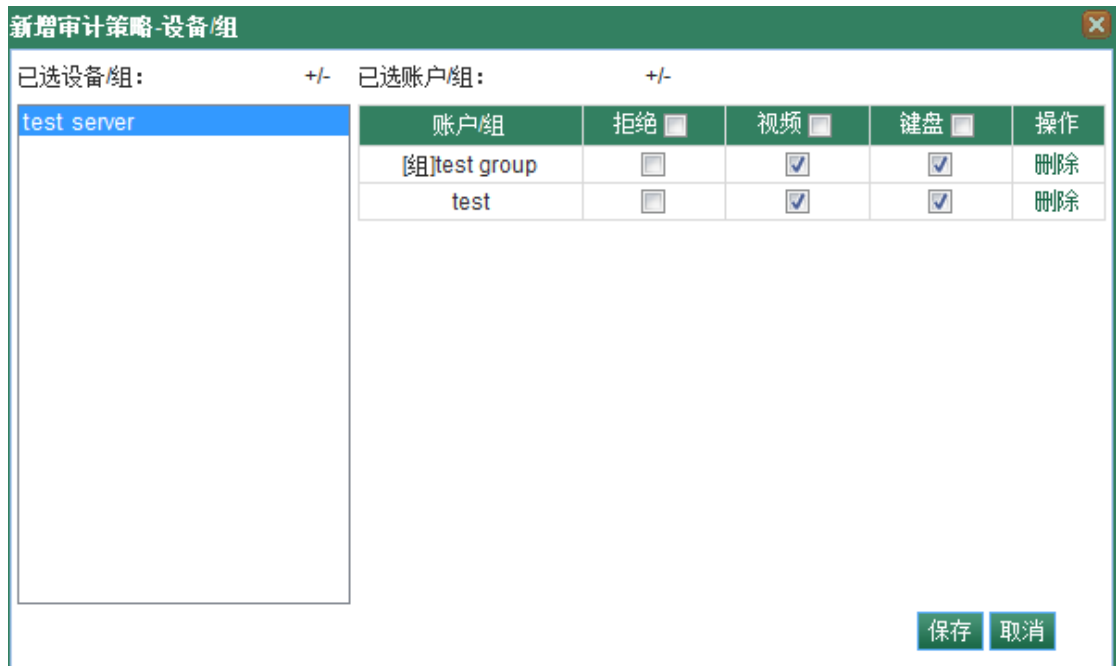


分别点击上图中红圈圈中的“+/-”符号，选择需要审计的设备和设备组，以及需要审计的用户或用户组。

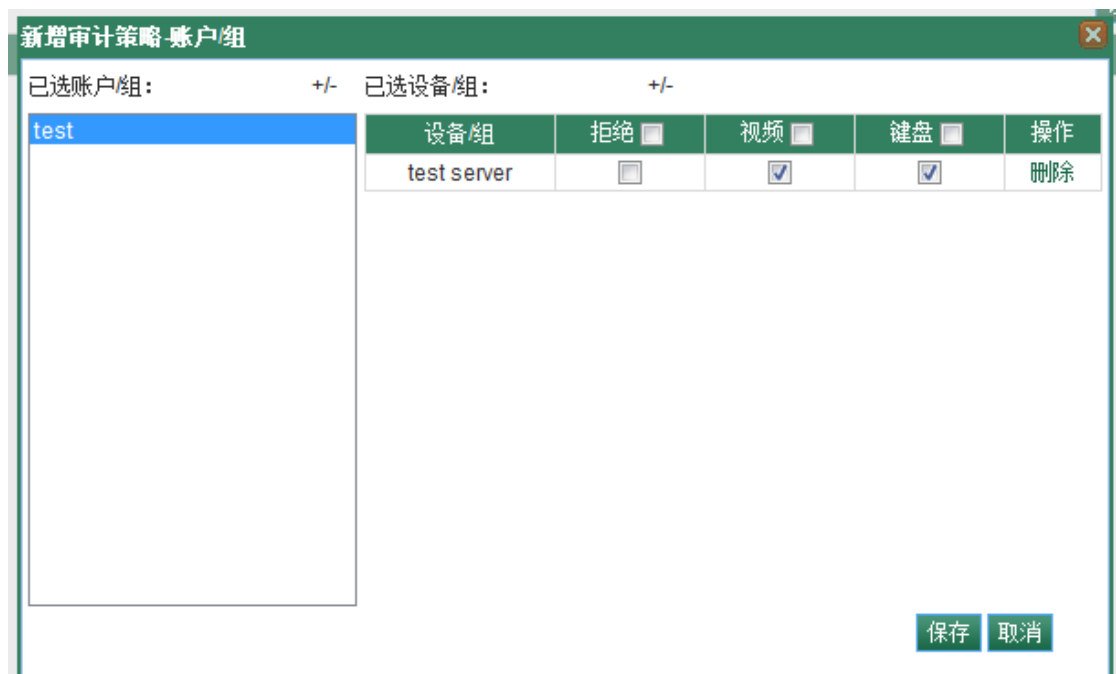


当选择好设备/设备组，用户/用户组之后，出来下图后，我们可以单独对用户或用户组来设定进行哪类审计，视频是指对 VGA 输出画面的审计，即视频录像审计；而键盘是指对键盘输入指令的审计，记录文件为文本文件。

备注：键盘为最底层的输入审计，不管用户输入什么字符都会被记录下来，因此包括用户在输入密码的时候，也会被审计，请慎用。



同“设备/组策略”，我们同样可以对“用户/组策略”进行设定



设定好之后，审计策略会显示结果：



审计策略的删除、修改、禁用和启用：

选择对应序号的审计策略后，审计配置中的“删除”、“禁用”、“启用”按钮，就会原来的灰色变成可以操作，如下图：



分别点击对应按钮来进行对审计策略的“删除”、“禁用”、“启用”操作。

“删除”，指删除该条审计策略，结果该审计策略失效，并无法恢复；

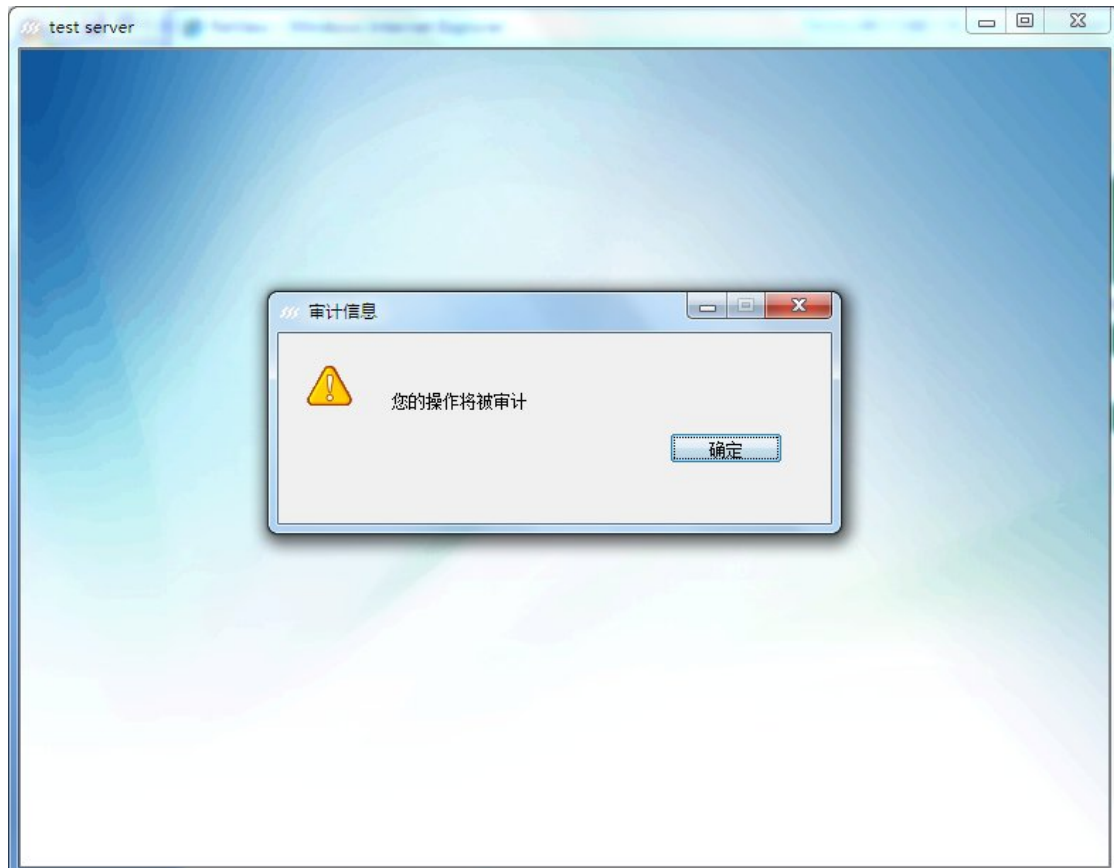
“禁用”，指临时禁用该条审计策略，结果该审计策略失效，可通过“启用”恢复；

“启用”，可把临时禁用的审计策略重新生效；

另外，先勾选某条审计策略，可以点击“修改”，对该条审计策略进行修改，并按“保存”生效。

用户 KVM 会话审计

如下图，当用户点击 KVM 会话时，如果该用户对该服务器的访问，在审计策略里是需要审计的时候，会跳出“您的操作将被审计”提示框，以提醒用户接下去对服务器的操作会被审计。



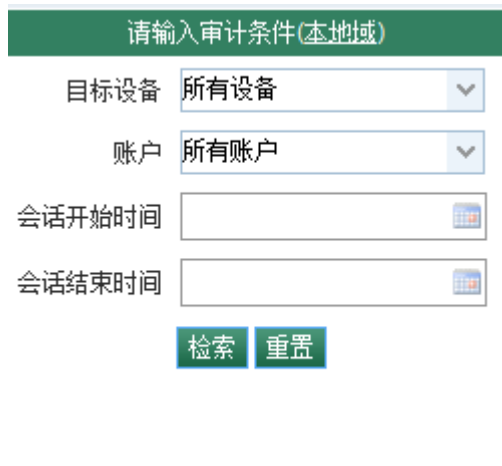
审计信息窗口，可以点击“确定”按钮直接关闭，或过 6 秒钟会自动关闭。

KVM 会话审计查询

如下图，点击“审计”——》“新审计”，出来以下窗口：



在窗口左侧，可以通过“目标设备”、“用户”和“会话的开始、结束时间”来快速查找所需查找的审计记录，如下图所示

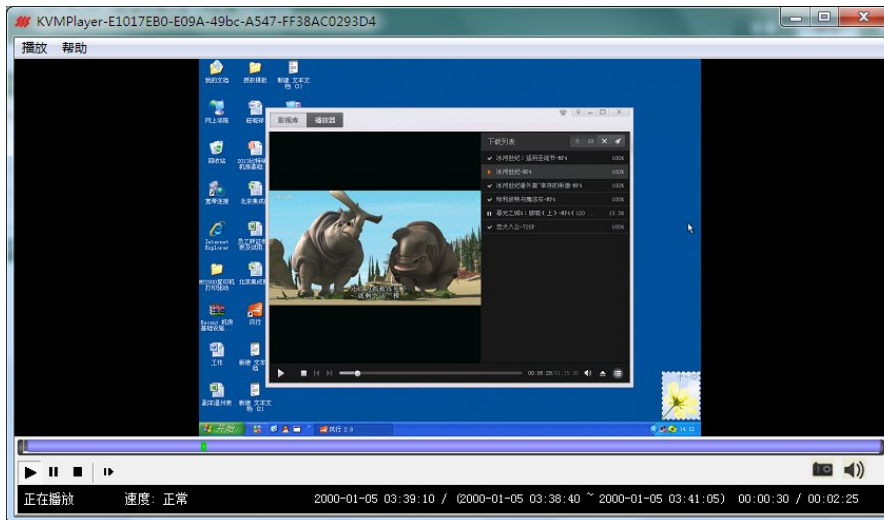


在“会话列表”框里，在“操作”一栏里点击“审计”、“键盘”、“导出视频”可以分别完成不同的操作：

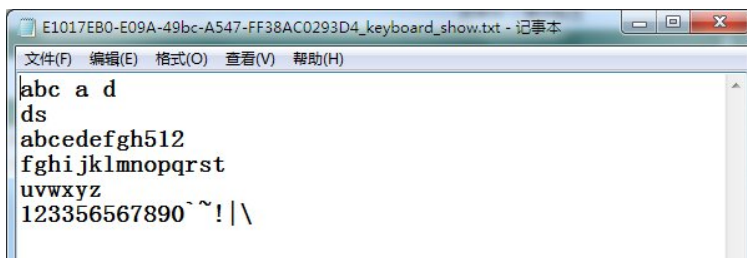
- “审计”：调出视频审计窗口，在该窗口可以对 KVM 会话整个过程进行查看：
 - ◇ 可以对播放过程进行拖拉，播放速度可以调节为“1/2，正常速度，2 倍，3 倍，4 倍”速度来进行播放；



- ◇ 可以通过“暂停”按钮或在屏幕上单击，对播放过程进行暂停操作；
- ◇ 可以通过鼠标“双击”或窗口最大化按钮进行全屏查看；

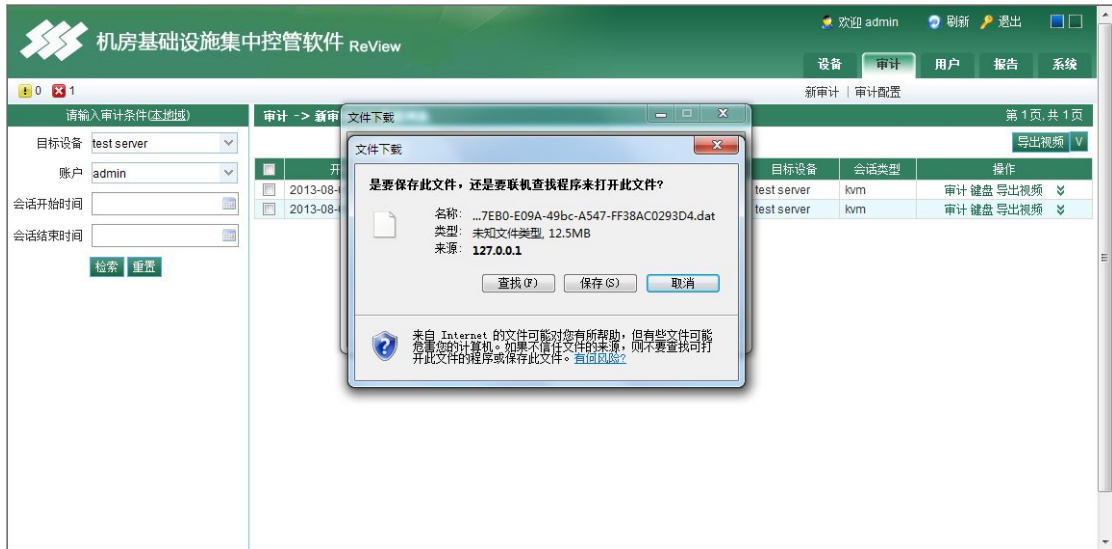


- “键盘”：调出该 KVM 会话过程，键盘的输入指令记录：



- “导出视频”：把该 KVM 会话视频审计导出成文件：

该文件必须用软件自带的播放工具播放，其视频编码格式为独有。



审计存储策略配置

存储路径相关设置

找到“审计”——>“审计配置”——>“存储策略”，如下图



说明：

- “中间栏”表明审计服务器的表示和 IP 地址，可以有多个，127.0.0.1 的服务器地址表明该审计服务器与 web 服务器安装在同一台服务器。
- “右侧栏”表明该审计服务器的物理存放位置，以及磁盘的使用情况，如果空间过满，可以添加另外的存储目录；

		存储路径	数据维护	备份与恢复			
序号	存储路径	状态	磁盘容量	修改人	修改时间	操作	
1	C:/work/StreamData	正常	86.57%(42.27G/48.83G)		2013-08-05	手动维护 删除	
2	d:\	正常	70.73%(449.05G/634.86G)	admin	2013-08-05	手动维护 删除	

- 如果存储路径里有审计数据，则会提示“不能删除包含审计数据的存储路径”，需要手动清空存储路径里的审计数据后才能删除。
- “手动维护”按钮，作用是马上执行一次数据维护（见下）。



数据维护设置

存储路径	数据维护	备份与恢复
------	-------------	-------

审计数据管理策略：

存储容量达到硬盘存储的 %，删除审计数据，使得磁盘容量保持在 %。

保留最近 天的审计数据。

- 可以设置譬如当存储所在磁盘容量达到该盘符容量的 90%，删除审计数据，使得磁盘容量保持在 80%，以上两个数值可以自己设定；
- 或者是保留最近多少天的数据，一旦审计数据的时间超出这个时间，则会自动进行数据的自动删除。

数据备份与恢复

存储路径 数据维护 **备份与恢复**

添加 删除

序号	备份名称	备份内容	备份存储	修改人	修改时间	操作

新增审计数据备份

备份名称
审计数据备份1

数据备份范围

备份所有数据(2013-08-05至2013-08-05)

备份该服务器以下时间段内的数据

2013-08-01 至 2013-08-06

备份文件存储地址
D:\TEMP

开始备份 取消

- 可以选择备份“所有审计数据”或“指定时间段审计数据”到审计服务器的目录,或者是网络目录(支持NAS目录直接备份,如\\192.168.0.181\share\shenji)上。
- 当审计服务器数据被误删或其他原因,导致审计数据丢失,可以通过“还原”操作来还原审计数据:

存储路径 数据维护 **备份与恢复**

添加 删除

序号	备份名称	备份内容	备份存储	修改人	修改时间	操作
1	审计数据备份1	2013-08-01至2013-08-06	D:\TEMP	admin	2013-08-05	还原记录 还原 删除

并可指定还原至哪台目标审计服务器。



添加 删除

序号	备份名称	备份内容	备份存储	修改人	修改时间	操作
1	审计数据备份1	2013-08-01至2013-08-06	D:\TEMP	admin	2013-08-05	还原记录 还原 删除

审计数据还原

备份名称: 审计数据备份1

备份内容: 2013-08-01至2013-08-06

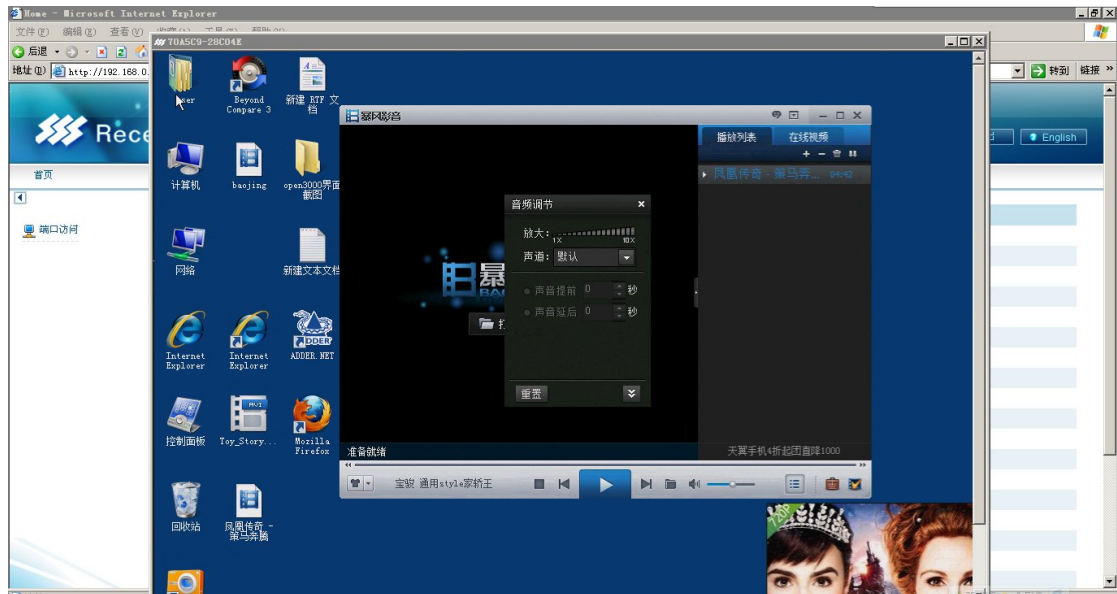
备份存储: D:\TEMP

目标服务器: (reviewServer01)127.0.

开始还原 关闭

KVM 会话操作

选中需要访问的服务器模块，点击“connet”，跳出会话窗口，



会话窗口的功能键

当你把鼠标移到窗口的上面部位时，会跳出一个控制菜单，如下图：





“文件”菜单：

是用于对目标服务器的画面进行全屏截图或指定区域截图的一个工具，所截的图存在本地硬盘。

“视图”菜单：

常用子菜单的主要有三个：



- 1) “刷新视频”：用于消除屏幕上一些不均匀的色块，等同于  按钮。
- 2) “全屏”：在全屏的时候，当控制机和被控制机的分辨率不同的情况下，被控制机的画面会按比例自动缩放已填满屏幕。（注： 该按钮等同于全屏操作）
- 3) “比例缩放”：

“自动缩放”，选择后，可以任意对 KVM 会话窗口进行缩放，视频会根据窗口大小自动填充；

“全尺寸缩放”，选择后，KVM 会话窗口会根据被控制机的实际分辨率来显示，如果被控制机的分辨率大于控制机分辨率，则会出现滚动条来显示不可见区域。

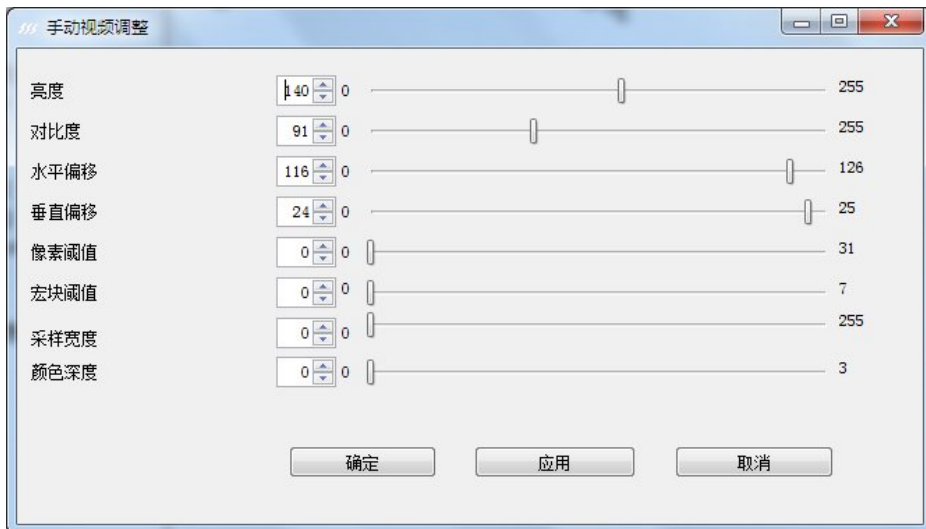
“宏”菜单：

由于一些特殊的组合键无法分别是对控制机操作还是对被控制机操作，这个时候就会出现控制机和被控制机的冲突，因此在这里用“宏”来解决这个问题，将一些常用的组合键做成“宏”命令直接发送到被控制机，常用“宏”有：“Ctrl+Alt+Del”、“Alt+Tab”、“Alt+F4”、“Print Screen”。

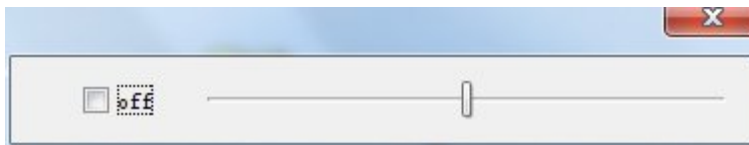
“工具”菜单：

此菜单为重要功能：

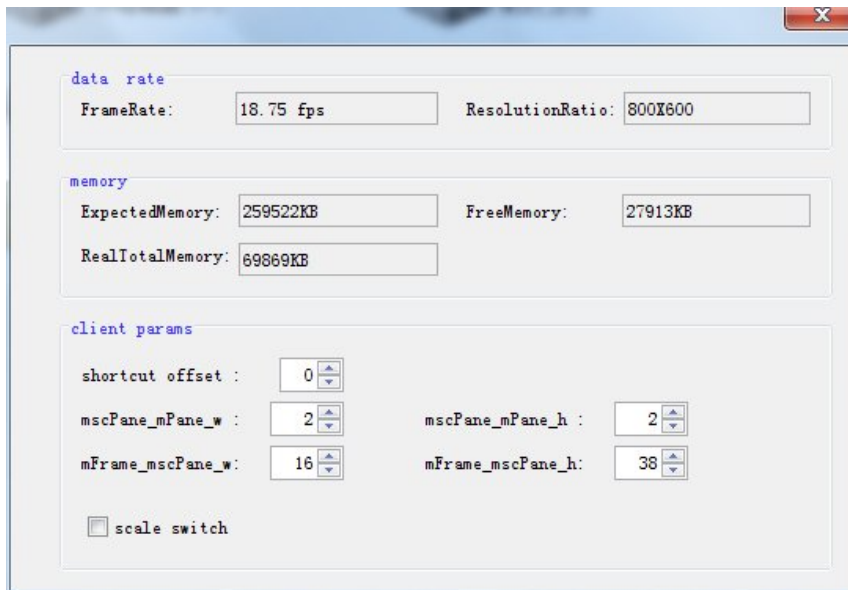
1. “自动视频调整”：让 KVM 对视频重新采样，重新初始化。
2. “手动视频调整”：手动调整视频画面的质量。
 - a) “水平偏移”：用来调整画面的左右偏移位置，这个较常见。
 - b) “像素阈值”：默认为 0，通过调高，一般不建议超过 5，用来适应不良的视频信号源。
 - c) “亮度”和“对比度”：分别视频亮度和对比度，偶尔会用。



3. “音频控制”：如若被控制机连接的是带音频的模块，则该功能可用，默认“音频输出”是关的，打开后可以将音频信号通过 KVM 传输到控制机。



4. “语言”，可以选择中文和英文。
5. “运行时信息”，可以查看打开会话时的帧率和分辨率，用来判断 KVM 会话是否正常。
 - 帧率 (FrameRate)：该数值一般在 15-20 左右为正常，如果帧率很低，则代表着鼠标移动缓慢，需调高“像素阈值”或进行“自动视频调整”，如不起作用，则需查明是否为视频源问题。
 - 分辨率 (ResolutionRatio)：该数值一般情况下显示为 KVM 获取到被控制机的分辨率。如果该数值出现如“768X576”，与被控制机实际分辨率(如 1024X768)不符，则问题出在被控制机的显卡驱动未安装，需安装正确的驱动程序，也有可能由于视频源干扰过于严重。而 KVM 会话窗口一直显示“视频调整中”。



“鼠标”菜单：

由于打开 KVM 会话，窗口内会出现两个鼠标（控制机和被控制机），这个时候会出现两个鼠标的同步问题。

“单鼠标模式”，隐藏掉控制机的鼠标，此时窗口内只有一个鼠标为被控制机的，此鼠标不能画出会话窗口，退出按 F9（该快捷键可修改）。

“相对鼠标模式”，这种模式下必须对被控制机的鼠标设置，见**鼠标同步设置**。

“绝对鼠标同步”，在此模式下被控制机不需要进行任何设置即可同步，仅适用于 WINDOWS 系统，同时必须有相应的带绝对鼠标功能的模块支持。

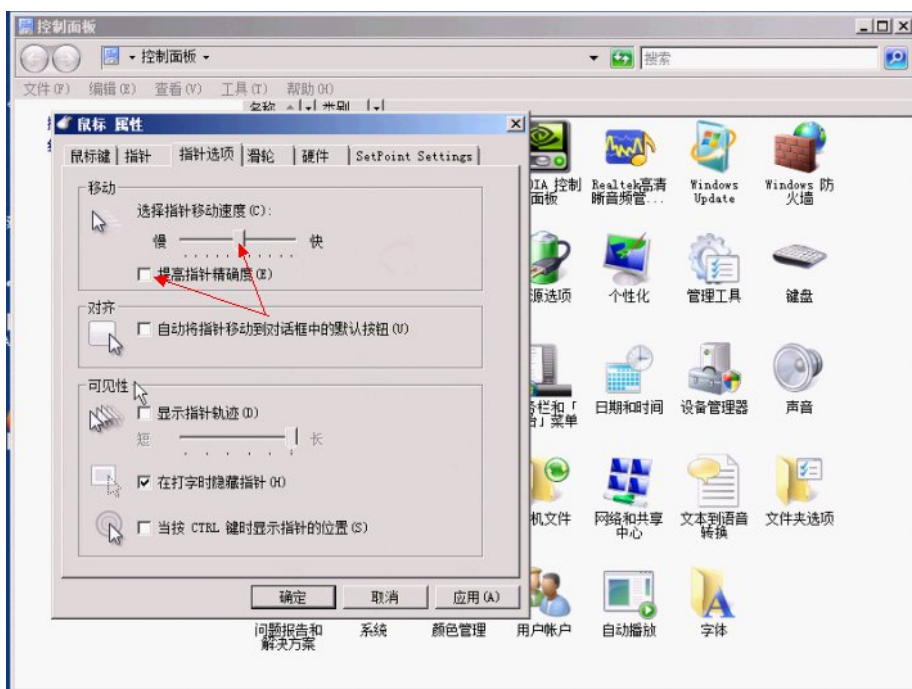
鼠标同步设置

目的：由于打开服务器控制界面以后，会出现两个鼠标，其中一个是本机的鼠标，另一个是被控制电脑的鼠标，由于某些原因，两个鼠标一般都没有同步一起，对操作影响很大，所以需要把两个鼠标同步。

不同的操作系统需要对鼠标进行不同的设置，分别设置如下：

1. Windows 2003、windows 2008、windows XP、windows 7

- 单击开始菜单-设置-控制面板
- 选择鼠标图标
- 选择 Pointer Options（指针选项）标签
- 确认指针速度，滚动条在中间位置
- Enhance Pointer precision（提高指针精确度）选项不被选中
- 使用重新同步按钮重新同步鼠标。

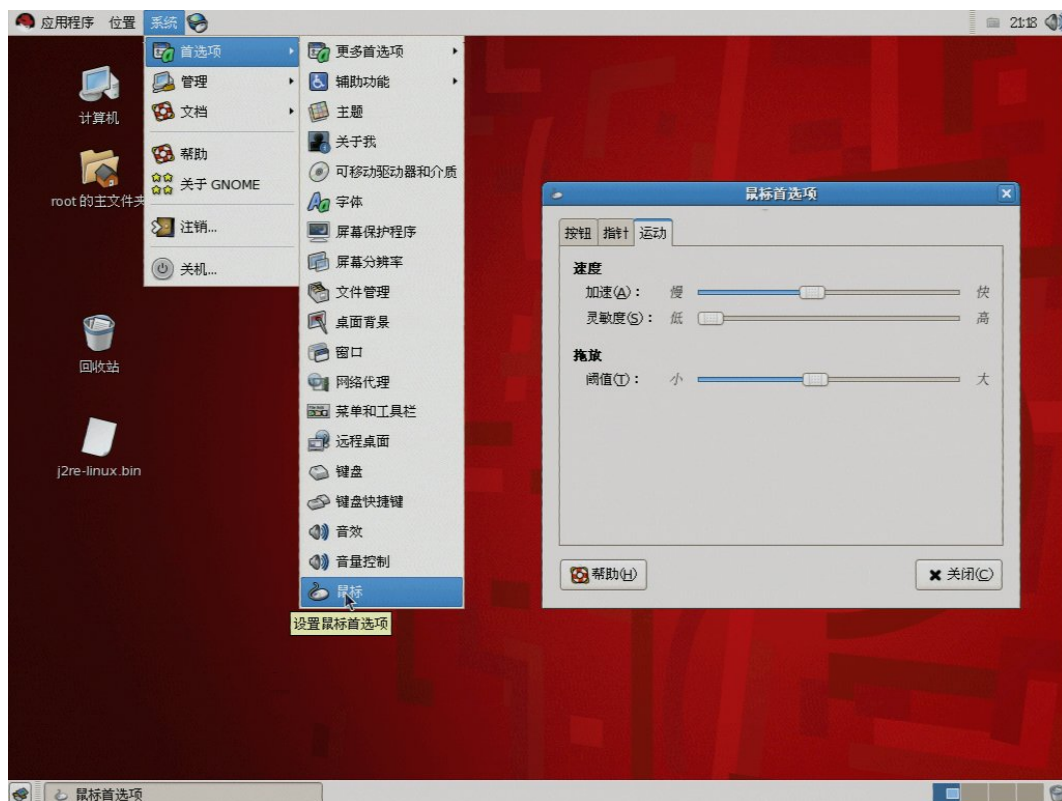


2.RedHat enterprise Linux: (Versions5.x)

- 更改加速为“中间”；
- 灵敏度为“最低”；
- 阈值为“中间”；

以上选项改过之后，在服务器重启以后还是可以同步的。

也可以用 `xset mouse 1 1` 的同步命令去同步的，但服务器重启之后同步失效，需要重新输入命令。



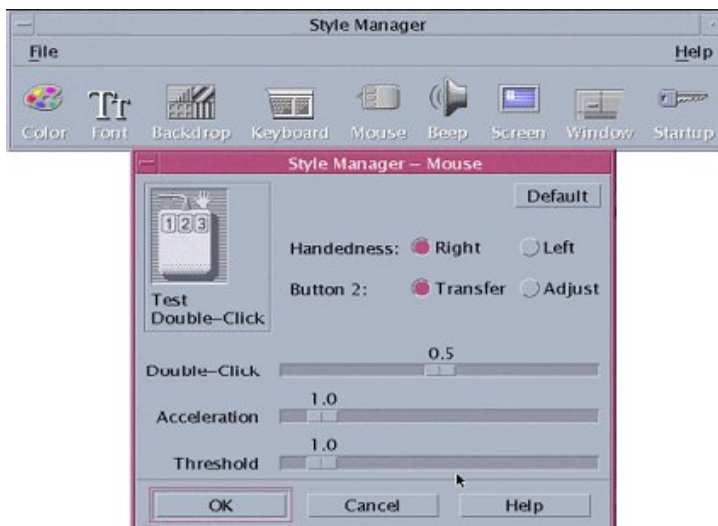
3.Red Hat Linux (Versions 8.0 and above)

- 打开“Red Hat”GNOME 桌面
- 选择 Preferences
- 选择鼠标
- 选择移动标签
- 把鼠标灵敏度滚动条拉至左边（低）
- 将加速滚动条，设置到中间



4.Sun Solaris

- 在 Solaris CDE 中打开 Style Manager
- 选择 Desktop Settings 打开鼠标程序
- 设置加速度为 1.0



5.AIX version 5.x

- 在 AIX 图形界面中打开 Style Manager 选择鼠标设备
- 在鼠标设置里，将鼠标加速度设置为 1.0
- 设置 Threshold 为 3.0。

