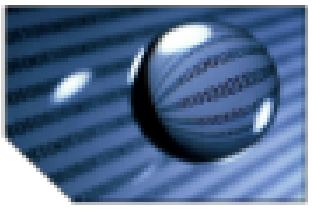
中软统一终端安全管理系统 8.0

使用手册

中国软件与技术服务股份有限公司

CHINA NATIONAL SOFTWARE & SERVICE CO., LTD.



版 权 声 明

◆ 非常感谢您选用我们的产品，本手册用于指导用户怎样使用中软统一终端安全管理系统 8.0（中文简称安全管理系统，英文简称 UEM8.0），请您在使用本系统前，详细阅读本手册。本手册和系统一并出售且仅提供电子文档。

Copyright © 2008 by CS&S，中国软件与技术服务股份有限公司版权所有。

◆ 中软统一终端安全管理系统 8.0 是中国软件与技术服务股份有限公司自主研发的受法律保护的商业软件。遵守法律是共同的责任，任何人未经授权人许可，不得以任何形式或方法及出于任何目的复制或传播本软件和手册，权利人将追究侵权者责任并保留要求赔偿的权利。

◆ 任何人或实体由于该手册提供的信息造成的任何损失或损害，中国软件与技术服务股份有限公司不承担任何义务或责任。

系统版权

中文名称：中软统一终端安全管理系统 8.0

开发单位：中国软件与技术服务股份有限公司

本系统的版权单位：

中国软件与技术服务股份有限公司

地址：北京市海淀区学院南路 55 号中软大厦，100081

电话：400-706-1810

邮箱：waterbox@css.com.cn

前　言

近年来，内网安全问题已经逐渐引起了各级单位的广泛重视，企业安全意识增强，安全投入增加，但是安全事件却不断在增多。分析其原因主要是因为安全解决方案存在缺陷，内网终端安全管理涉及多种基本的安全服务，是一个立体的、多方位、多层次的系统问题。为此，中软自主研发了统一终端安全管理系统。该系统采用了终端安全“一体化”的安全防护技术，整合了病毒防护监测、网络接入认证、终端健康检查、系统身份认证、资产查看、补丁管理、运行监控和失泄密防护等等终端软件的安全功能，以其全新的安全理念、强大的功能体系、完善的技术架构，改变了传统的内网安全管理模式，是终端安全的完整解决方案。

本手册详细介绍了中软统一终端安全管理系统 8.0 的使用方法和操作技巧，为用户在使用本系统时提供参考，全手册共分十四章。

- 第一章：系统概述
- 第二章：体系结构和运行环境
- 第三章：初识控制台
- 第四章：组织结构管理
- 第五章：安全管理中心
- 第六章：内网安全扫描
- 第七章：响应与知识库管理
- 第八章：统计审计分析
- 第九章：系统参数设置
- 第十章：服务器操作指南
- 第十一章：服务器级联
- 第十二章：客户端操作指南
- 第十三章：审计系统操作指南
- 第十四章：技术支持

为了方便读者阅读，我们在书中设计了两个小图标，它们分别代表：

注意： 告诉用户应特别注意的地方。

提示：给用户提个醒或介绍使用经验和心得。

本书内容全面，深入浅出，适合使用、配置安全管理系统的用户读者；检测、评估安全管理系统的技术人员和专家以及希望使用安全管理系统协助对其组织、机构或企业进行管理的管理人员等。

本手册适用于中软统一终端安全管理系统 8.0 的 8.0.19.326 版本的使用，随相应版本的产品光盘附带，对该产品的其他版本，如未作特殊说明或者更新，该手册同样适用。

本手册在编写过程中，尽管我们做了最大努力力求完美和准确，但由于水平有限，难免存在疏漏和缺陷之处。如果您对本手册有任何疑问、意见或建议，请与我们联系。感谢您对我们的支持和帮助。

中国软件与技术服务股份有限公司

2011 年 05 月

目　录

第一章 系统概述

近年来，内网安全问题已经逐渐引起了各级单位的广泛重视，企业安全意识增强，安全投入增加，但是安全事件却不断在增多。分析其原因主要是因为安全解决方案存在缺陷，边界安全很重视，内网安全的关注程度不够。同时国外的一项安全调查显示，超过 85%的网络安全威胁来自于内部，其危害程度更是远远超过黑客攻击及病毒造成的损失，而这些威胁绝大部分是内部各种非法和违规的操作行为所造成的,几乎没有一家企业管理人员不为企业终端的安全、管理等问题而苦恼。

为了解决这些问题，很多用户采购并部署了多个终端安全管理的安全产品，比如：身份认证、补丁管理、软件分发、防病毒软件等等。但是这一系列不同厂商的软件都是各自为政。每种软件都需要有其独立的服务器、独立的控制台、独立的客户端代理，最终结果是将终端个人桌面系统划分为一个个独立的信息安全孤岛，导致管理混乱和出现安全漏洞。同时客户端上不同的代理需要重复的占用很多系统资源，导致个人桌面系统运行速度变慢，系统性能严重下降。

内网终端的安全实施是一个系统工程。安全问题涉及身份认证、访问控制、数据保密性、数据完整性、抗抵赖、审计、可用性和可靠性等多种基本的安全服务。内网终端安全管理是一个立体的、多方位、多层次的系统问题。为此，中国软件与技术服务股份有限公司自主研发了中软防水墙系统,在历经了 7.0、7.0+、7.2、7.2R2 等版本的基础上，又推出了中软统一终端安全管理系统 8.0。

中软统一终端安全管理系统 8.0 围绕不同安全等级的关键业务,进行风险分析并形成对各种风险适度控制的安全策略,依据涉密系统的使命与目标和系统重要程度，将系统划分为不同的安全等级，并综合平衡考虑系统安全要求、系统所面临安全风险和实施安全保护措施的成本，进行安全措施的调整和定制，形成不同等级的安全措施进行保护，把各安全控制的功能模块融合在一个统一的管理、监控和响应的系统中。通过统一的桌面安全管理系统，提供综合的功能管理和安全的性能管理，从而降低系统的复杂度和维护管理成本。

中软统一终端安全管理系统 8.0 从以下几个方面对终端桌面系统进行管理：

终端安全管理：保证安全策略的合规性，保障终端的安全运行环境。它包括有安全策略管理、终端接入检查、终端出网许可、用户登录计算机的身份认证、网络进程访问控制、防病毒软件监测、系统补丁管理、安全操作管理等涉及主机安全管理、策略合规性管理的功能体系。

终端运维管理：监控远程终端的运行状况，管理内网的信息资产，为管理员的终端维护提供方便快捷的帮助。它包括有软件分发、资产查看、运行监控、远程管理等终端运行维护管理方面的功能体系。

用户行为管理：规范终端用户信息带出行为，防止企业敏感信息泄露。它包括有网络失泄密防护、存储介质泄密防护、打印机泄密防护、外设接口泄密防护等敏感信息失泄密防护方面的功能体系。

数据安全管理：从多个方面和多个层次实现对用户数据的安全管理。它包括：用户桌面安全保险箱，实现了终端用户对需要防护数据的主动加密要求；安全文档策略，该功能从底层实现了企业

对某类型的敏感数据的强制加密要求；可信移动存储介质管理，该功能帮助企业实现了移动介质数据的防护，实现了“外部的 U 盘进来使不了，里面的 U 盘出去不可用”。

终端接入管理：通过终端接入认证和非法主机扫描实现对接入网络的客户端进行认证，认证通过的可以连接网络，对通过其他非法途径进入网络的非法主机，通过扫描工具发现和告警，并及时进行阻断隔离。

系统管理与审计：集中统计、显示和分析各种受监控的用户行为日志、报警日志、主机状态日志、以及响应知识库的管理、系统角色和权限、用户的管理，同时为系统正常运行提供了相关参数的设置。

第二章　体系结构和运行环境

2.1 系统体系结构

系统分为三个组件：客户端、服务器和控制台，系统采用分布式监控，集中式管理的工作模式。组件之间采用 C/S 工作模式，组件的通信是采用 HTTP/HTTPS 加密传输方式。支持任意层级的服务器级联，上下级服务器之间采用 HTTPS 协议进行数据交换。体系结构如图 2-1 所示。

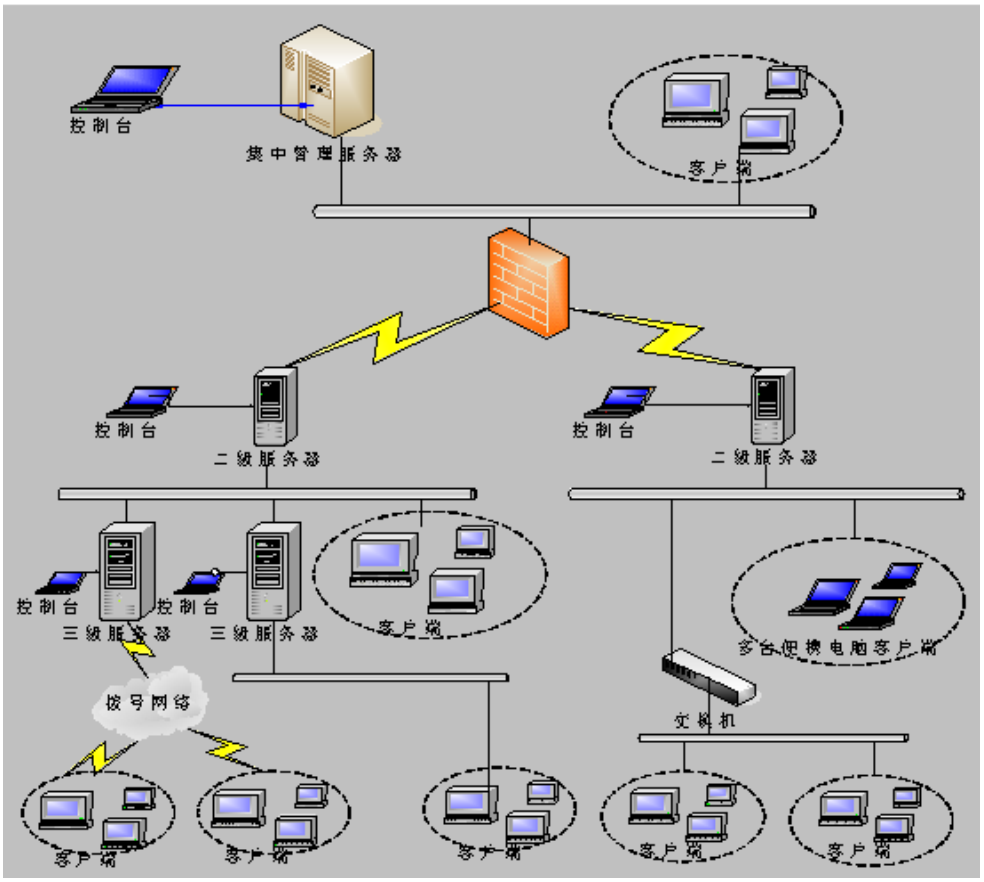


图 2-1　系统体系结构图

- **客户端：**安装在受保护的终端计算机上，实时监测客户端的用户行为和安全状态，实现客户端安全策略管理。一旦发现用户的违规行为或计算机的安全状态异常，系统及时向服务器发送告警信息，并执行预定义的应急响应策略。

- **服务器：**安装在专业的数据服务器上，需要数据库的支持。通过安全认证建立与多个客户端系统的连接，实现客户端策略的存储和下发、日志的收集和存储。上下级服务器间基于 HTTPS 进行通信，实现组织结构、告警、日志统计信息等数据的搜集。

- **控制台：**人机交互界面，是管理员实现对系统管理的工具。通过安全认证建立与服务器的信任连接，实现策略的制定下发以及数据的审计和管理。

  控制台、服务器、客户端之间的通信关系如图 2-2 所示。

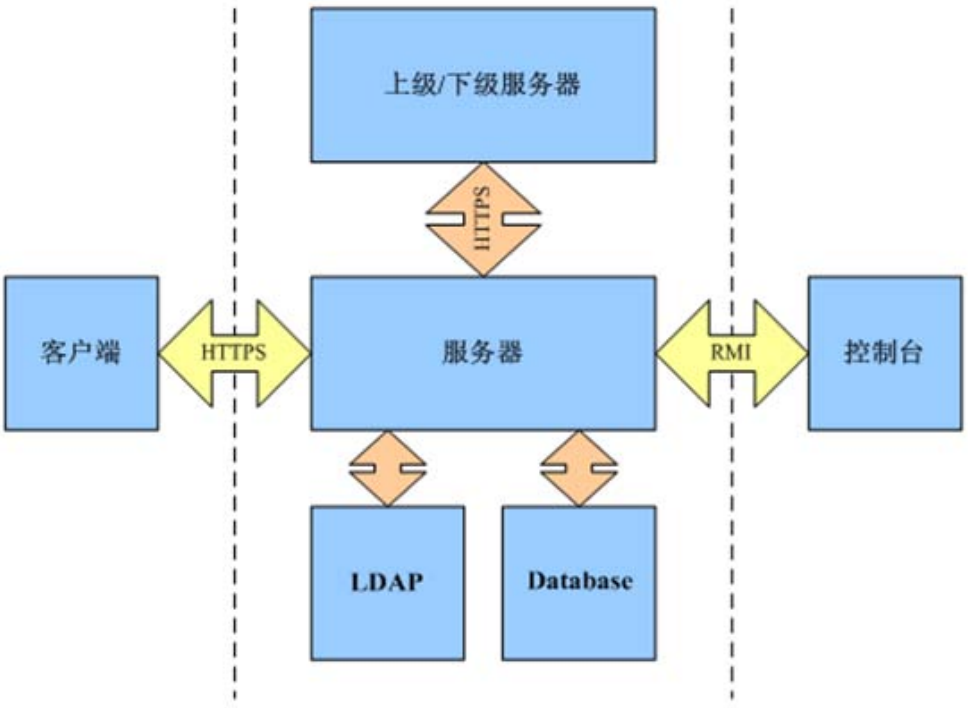


图 2-2　组件之间的通信关系图

2.2 推荐硬件需求

客户端个数	<200	200-500	500-1000	>1000
服务器主机个数	1	1	1	1+
服务器	CPU P4 3.0 RAM 1GB HDisk 120GB	CPU P4 3.0 AT RAM 2GB HDisk 240GB	CPU P4 3.0 AT RAM 4GB HDisk 480GB	CPU Xeon 1GB*4 RAM 4GB SCSI Disk 240GB RAID 5
控制台	CPU P4 2.0 RAM 512MB HDisk 40GB	CPU P4 2.0 RAM 1GB HDisk 40GB	CPU P4 3.0 RAM 1GB HDisk 40GB	CPU P4 3.0 RAM 1GB HDisk 80GB
客户端	CPU P4 2.0/ RAM 512MB/ HDisk 40GB			
审计系统	CPU P4 2.0/ RAM 512MB/ Hdisk 120GB （随服务器变化）			

表格 1　系统推荐硬件需求

2.3 推荐软件需求

	操作系统	所需其他软件支持
服务器	Microsoft Windows Server 2003 / Advanced Server	SQL Server 2000+SP4 SQL Server 2005 SQL Server2008或达数据库。 硬件“加密锁”驱动程序
控制台	Microsoft Windows Server 2003 , Microsoft Windows 2000 Professional / Server / Advanced Server, Microsoft Windows XP	
客户端	Microsoft Windows 2000 Professional / Server / Advanced Server, Microsoft Windows XP Professional，Microsoft Windows Server 2003，Microsoft Windows Vista (Ultimate / Business)，Microsoft Windows7（Ultimate / Enterprise / Business）（32/64 位）	
审计系统	Microsoft Windows 2000 Professional / Server / Advanced Server, Microsoft Windows XP, Microsoft Windows Server 2003	SQL Server 2000+SP4 SQL Server 2005 SQL Server2008或达数据库

表格 2　系统软件需求

提示：

- 安全管理系统服务器，包括服务器软件和后台支持数据库。建议在专用主机上安装安全管理系统服务器，并且关闭所有与安全管理系统无关的不必要的服务。支持操作系统为 MS Windows 2003 系列，推荐 Advanced Server 版本。
- 以上操作系统，没有特别说明，仅指 32 位操作系统。
- 安全管理系统客户端不支持 Linux 系统，不能在 windows 双系统下同时安装 UEM 客户端。
- 为保证用户正常使用安全管理系统，最好将安全管理系统服务器、控制台和客户端分别运行于独立的系统之上，同时用户安装前应将 Windows 版本进行升级，安装各自版本最高补丁。

第三章　初识控制台

3.1　登录控制台

3.1.1 普通用户登录

1. 首先将硬件“加密锁”安装在安全管理系统服务器上，然后双击控制台桌面上“WBConsole”图标，如图 3-1 所示。也可依次单击控制台的“开始→程序→CSS→WBConsole”，进入登录对话框。

图 3-1　控制台桌面图标

2. 在安全管理系统控制台登录对话框中，填写服务器地址、用户名和密码，然后单击“确定”按钮，进入安全管理系统控制台，如图 3-2 所示。

如果是第一次启动控制台或更换所登录的服务器，需要导入服务器证书验证身份，以后启动就不用再导入证书了。单击“选项”，输入服务器证书所在的路径，或者单击“浏览”按钮，选择存放证书路径。默认位置在服务器 C: \CSS\UEM\WBServer\server\default\conf\wbserver.cer 或 C:\program files\CSS\UEM\WBServer\server\default\conf\wbserver.cer，请用户注意做好备份（详见证书备份与恢复）。

图 3-2　控制台登录界面

注意：

（1）安全管理系统控制台首次登录时的“用户名”和“密码”，为服务器初始化时内置的“用户名”和“密码”，登录后可以修改密码，也可新增管理员角色和用户。

（2）系统内置管理用户有两个：管理员 admin，密码 1234567a；安全官 security，密码 1234567a。系统内置角色四个：管理员、安全官、操作员、审计员。

3.1.2 KEY 用户登录

当控制台设置某一个用户与指定的 KEY 关联时，该用户可以使用 KEY 登录。将 KEY 插入控制台，选择“身份认证 KEY”登录方式，如图 3-3 所示。选择 KEY 设备类型和身份认证 KEY，输入 KEY 密码，单击“确定”按扭，登录控制台。

如果与 KEY 关联的控制台用户，没有以“普通”方式登录过控制台，那么第一次用“身份认证 KEY”登录控制台时，也需单击“选项”按钮，导入服务器证书。

图 3-3　KEY 用户登录控制台

提示：控制台用户与 KEY 的关联，参见“关联 KEY”章节。如果设置 KEY 用户只能使用 KEY 方式登录时，该用户无法将使用用户名和密码的“普通”方式登陆，只能使用指定的 KEY 登录控制台。

3.1.3 控制台连接诊断

1．用户登录控制台连接服务器失败后，会弹出“无法连接服务器”消息框，如图 3-4 所示。同时，提示用户进行连接诊断，确认出错原因。

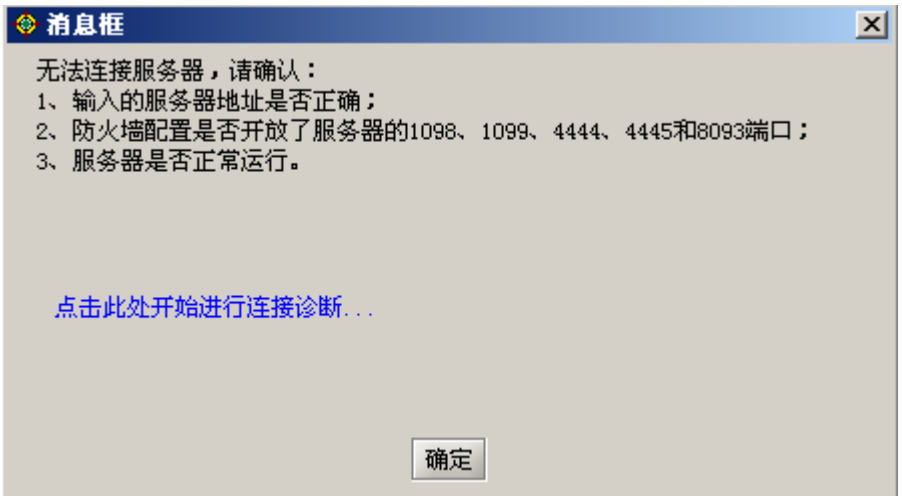


图 3-4　登录控制台失败消息框

2. 用户点击连接诊断后，对连接失败的原因进行分析，如图 3-5 所示。系统依次判断服务器 IP 地址连接状态、服务器端口是否打开、服务器是否启动、通信证书是否正确，并将每个步骤的诊断结果展示给用户，帮助用户查找问题。

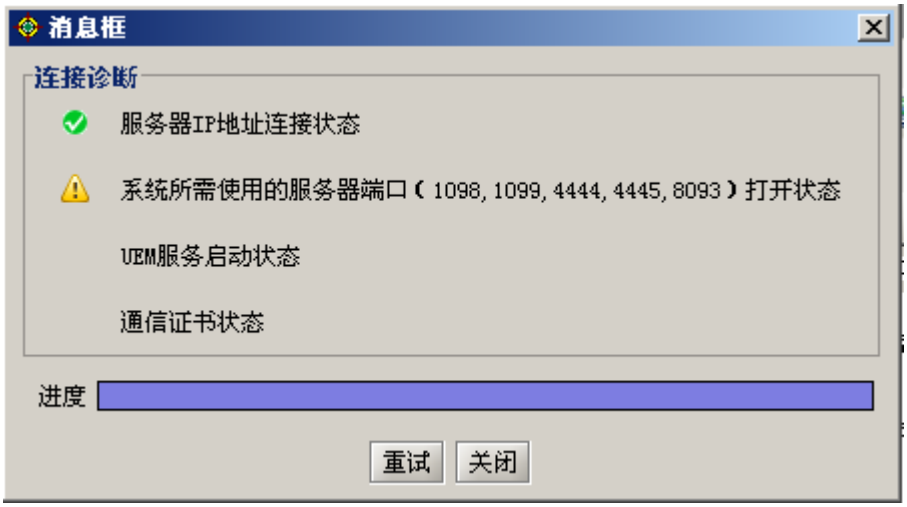


图 3-5　登录控制台连接诊断

3. 用户将查找的问题逐项解决后，以正确的方式登录控制台，连接服务器。

3.1.4 控制台使用控制

1. 当管理员登录时，已有相同的管理员用户在另一位置登录，会弹出提示框，如图 3-6 所示。管理员可以强制登录，也可换用其他帐户登录，保证不能有同名帐户同时登录。

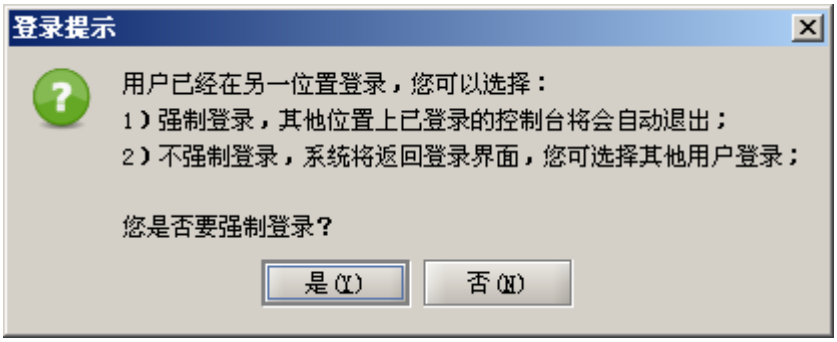


图 3-6　管理员单一登录控制

2. 控制台登录时，若版本与服务器所要求的不匹配，会提示用户“本控制台版本与服务器的版本不兼容，请升级到×.×.××.×××及以上版本!”，如图 3-7 所示。其中“×.×.××.×××”为服务器所要求控制台的最低版本。

图 3-7　服务器与控制台兼容性控制

3. 控制台登录时，如果密码尝试次数超过了服务器参数中帐户安全设置的次数，控制台将被锁定，如图 3-8 所示。超过锁定时间自动解锁，或者由系统管理员（默认 admin）解锁，详见帐户安全设置。

提示：控制台用户密码错误锁定功能只针对普通用户，不针对 key 用户，key 有自己的密码重试机制。

图 3-8　控制台帐户被锁定

4. 登录后，如果在指定的时间间隔内不操作控制台（详见帐户安全设置），则自动锁定，出现连接服务器失效提示框，如图 3-9 所示。重新输入密码后，才可重回原来的控制台操作界面，如图 3-10 所示。

图 3-9　控制台连接服务器失效

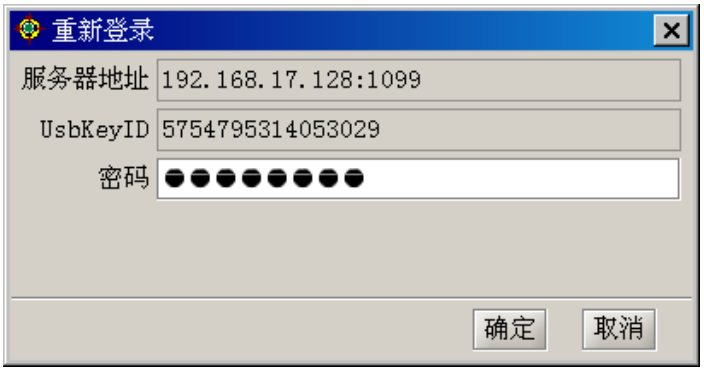


图 3-10　重新输入密码再次登录控制台

5. 控制台 KEY 用户在使用控制台的过程中，如果 KEY 被拔下，10 秒钟以内，控制台应该能够自动锁定，如图 3-11 所示。若插入正确的 KEY，并输入正确的密码，点击“确定”后可进行解密。点击“取消”，则退出控制台。

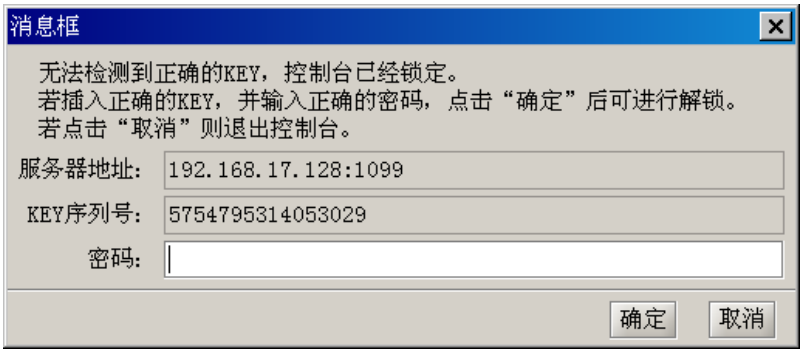


图 3-11　拔出 KEY 控制台自动锁定

3.2 快速入门

用户以 admin 初次登录控制台，可能感到无从下手。下面我们做几个例子，告诉用户如何添加组织和人员，怎样建立管理员帐户分配角色和权限，以及如何向客户端下发策略、查看日志信息等，这样用户就会对整个系统有个初步认识。

3.2.1 添加组织和人员

◆ **添加组织**

（1）用户初次以 admin 登录控制台后，看到的组织结构为空，只显示根组织。单击右键菜单“添加组织”，或者单击操作列表中的“添加组织”，如图 3-12 所示。

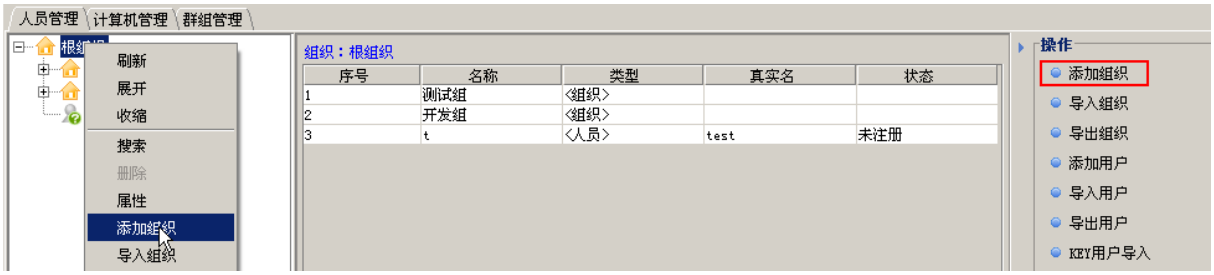


图 3-12　添加组织

（2）在弹出的添加组织界面中，输入组织结构名称和描述信息后，单击“确定”按钮，如图 3-13 所示。

图 3-13　输入组织信息

（3）在组织结构中能够看到刚添加的组织名称。用户可根据需要添加多个组织节点，建立自己的组织结构，如图 3-14 所示。

图 3-14　新建的组织节点

◆ **添加用户**

（1）建立了组织后，在组织下添加用户。在组织结构中选择节点，单击右键菜单，选择“添加用户”菜单项，或者单击操作列表中的“添加用户”，如图 3-15 所示

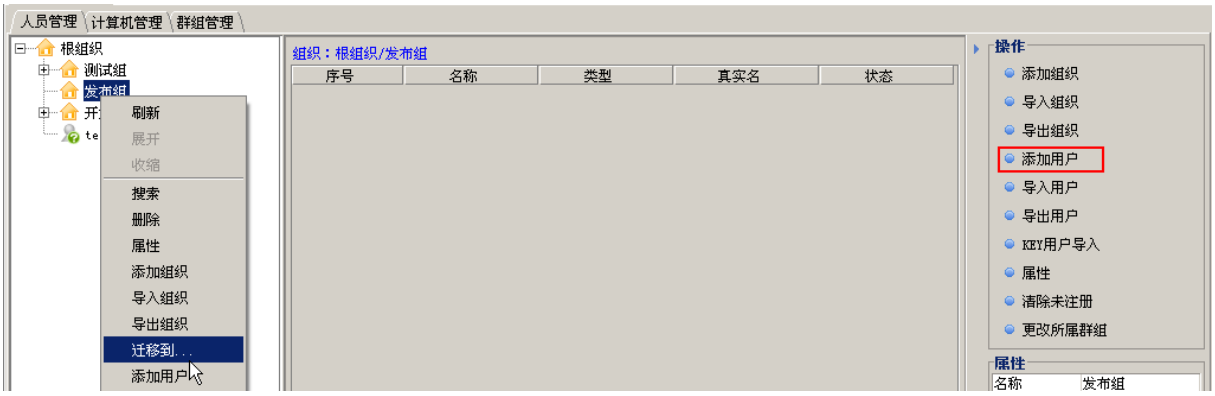


图 3-15　添加用户

（2）在弹出的添加用户界面中，输入用户名、真实名、性别、出生年月和密码等相关信息后，单击“确定”按钮，组织结构中显示出新增加的用户，如图 3-16 所示。

注意：密码项一定要输入，长度不小于 6 位。密码一定要记住，客户端注册时需要。

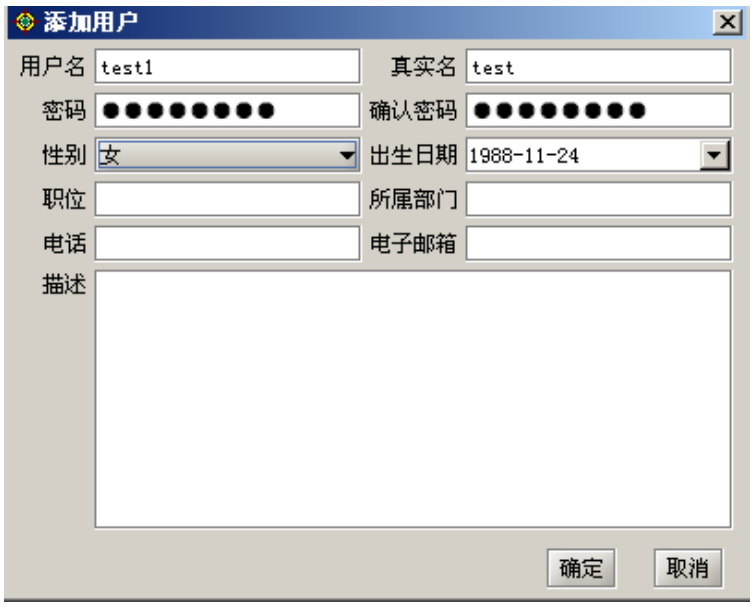


图 3-16　输入用户信息

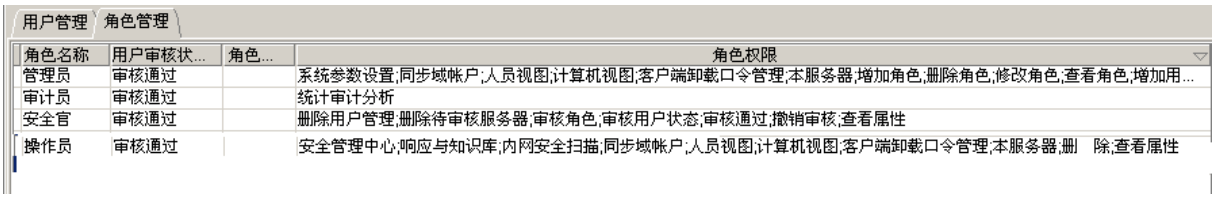
（3）同样方法，根据需要添加多个新用户，如图 3-17 所示。

提示：建立组织和用户后，参考安装手册，在其它机器上安装客户端，以上面建立的用户注册、登录。

图 3-17　新增的用户

3.2.2 添加管理员帐户

前面我们讲到，该系统提供了两个内置帐户：管理员 admin 和安全官 security。该系统是分级分权管理的，从下表我们可以看出，这两个默认的帐户都不能下发策略。下面我们添加一个操作员（operator）帐户，为后面的下发策略做准备。



（1）以 admin 登录控制台，单击组织结构管理→角色和权限→用户管理，进入用户管理界面，显示内置的两个帐户，如图 3-18 所示。

图 3-18　用户管理

（2）单击“增加用户”菜单，弹出增加用户界面。输入用户名和密码，选择角色和管理范围（内置角色四个：管理员、操作员、安全官、审计员），最后单击“确定”按钮。如图 3-19 所示：

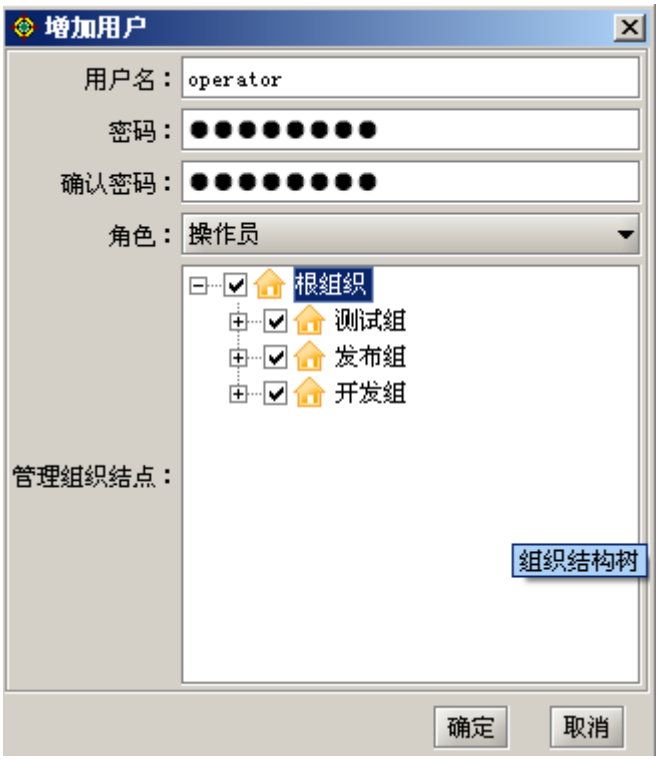


图 3-19　增加用户界面

（3）在用户列表中可以看到刚添加的用户“operator”，如图 3-20 所示。但此用户未经审核不能使用，下面进行用户审核。

图 3-20　用户列表

（4）以默认的 security 用户登录，进入用户管理界面，如图 3-21 所示。选择要审核的用户“operator”，单击右键菜单“审核通过”，此用户既被审核通过，可以使用。

图 3-21　用户管理

（5）用户也可单击右侧操作列表中的“审核状态”，在“审核状态”界面中，通过下拉框选择“审核通过”，单击“确定”按钮，如图 3-22 所示。新建的用户 operator 审核通过后，即可使用。

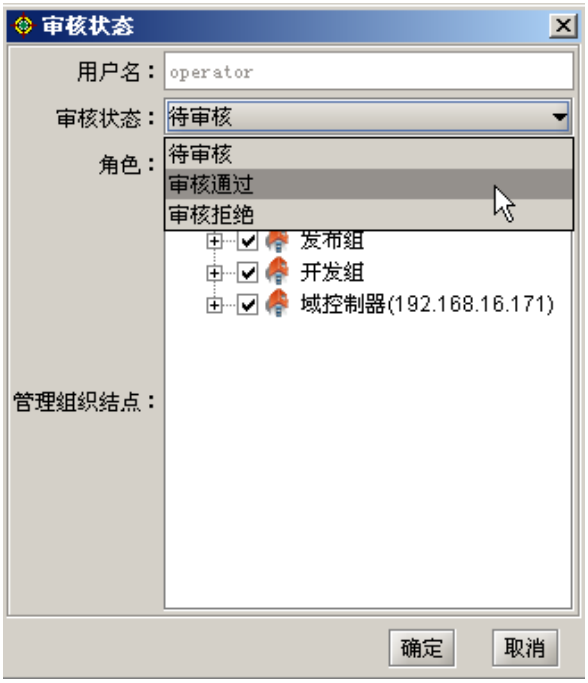


图 3-22　审核用户状态

（6）现在以 operator 用户身份登陆控制台，将能制定和下发策略。

3.2.3 向客户端下发策略

以操作员 operator 身份登录控制台，单击安全管理中心→失泄密防护策略→人员视图，进入失泄密策略编辑界面。下面我们举一个例子，制定一个存储介质控制策略向用户下发。

（1）在左边“人员视图”中选定一个用户，单击右边策略项中的“存储介质控制”→“可移动介质控制”，进入“可移动介质控制”策略编辑页面，如图 3-23 所示。

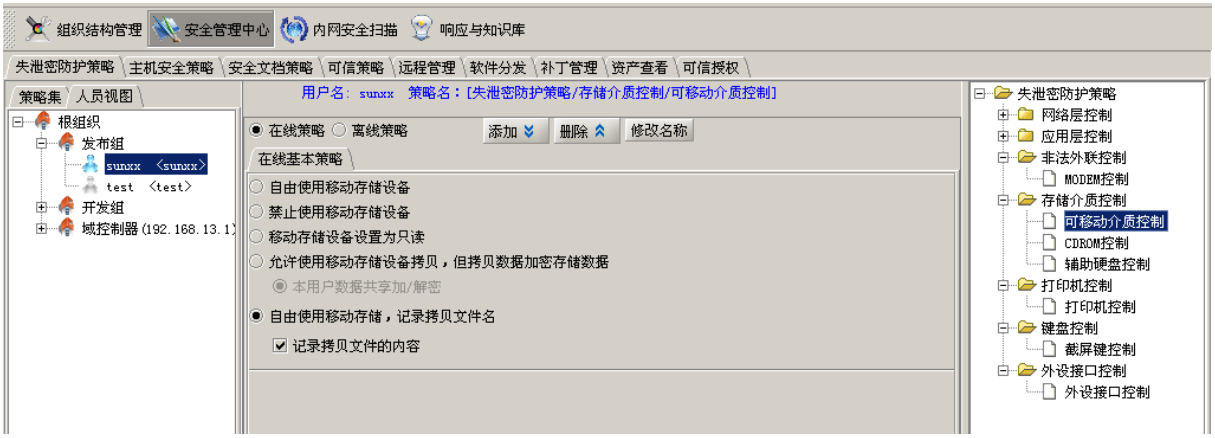


图 3-23　编辑可移动介质策略

选项说明：

自由使用移动存储设备：对客户端使用移动存储设备不做限制，可以任意使用；

禁止使用移动存储设备：不允许客户端使用移动存储设备；

移动存储设备设置为只读：只允许客户端使用移动存储设备进行读操作；

允许使用移动存储设备拷贝，但拷贝数据加密存储：允许客户端使用移动存储设备进行拷贝，但拷贝的数据都是加密。

自由使用移动存储，记录拷贝文件名：允许客户端使用移动存储设备，但记录拷贝文件名。如果同时选择下面选项，那么也记录拷贝文件的内容。

（2）我们选择“自由使用移动存储，记录拷贝文件名和文件内容”策略，点击下面的“应用到”按钮，将策略下发到客户端，下发成功后会弹出提示框，如图 3-24 所示。

图 3-24　应用策略成功提示框

（3）为了验证策略在客户端执行情形，我们在客户端往移动盘拷贝一个文件。然后，在控制台的统计审计分析中查看日志信息。

3.2.4 查看日志信息

从内置角色的分配我们知道，如果要查看日志信息，需要以审计员身份进入系统“统计审计分析”。下面介绍具体操作：

（1）在控制台新建一个审计员帐户 auditor（参考前面 operator 帐户的建立方法）。

（2）以 auditor 身份登录控制台，进入统计审计分析界面。在左边的树形结构中，按照日志类型一层一层往下找，你将看到移动存储器的记录带出日志，包括你前面在客户端往移动存储器拷贝的文件信息。单击右键菜单，还可以下载备份文件内容，如图 3-25 所示。

图 3-25　　移动存储器记录带出日志

3.3 菜单功能介绍

菜单栏包括文件、设置、工具和帮助四项。主要提供切换用户、修改密码、修改个人信息、同步域帐户、组织结构信息统计、客户端卸载口令管理和帮助等功能，下面一一介绍。

3.3.1 修改密码

前面我们讲到，用户第一次登录都是以系统默认的用户登录的。为了系统的安全，用户登录后请及时修改密码，或者根据自己需要，创建新的用户和密码。创建过程我们将在后面的组织结构管理中详述。

（1）在菜单栏中，单击“设置”→“修改密码”，或按“Ctrl+Alt-X”快捷键，进入修改密码界面，如图 3-26 所示。

图 3-26　修改密码界面

（2）输入新旧密码后，单击“确定”退出，下次登录时以新密码登录。

3.3.2 修改 KEY 密码

KEY 用户登录控制台后，在菜单的“设置”项中，可以看到“修改 KEY 密码”的选项。点击后，弹出用户的 KEY 密码修改界面，如图 3-27 所示。

用户在 KEY 密码修改界面中输入旧密码和新密码，在插入正确的 KEY 的情况下，将成功修改 KEY 密码。 如果 KEY 用户以普通方式登录，当前并没有插入正确的 KEY，则提示用户插入 KEY。

提示：使用 KEY 用户登录控制台前，首先要在用户管理中，将控制台用户与 KEY 关联起来，这样才能使用 KEY 用户登录。KEY 用户登录后，“修改 KEY 密码”菜单项才可用。利用此菜单可更改控制台 KEY 用户密码。参见控制台的启动和关联 KEY 章节。

图 3-27　修改 KEY 密码

3.3.3 切换用户

（1）在菜单栏中，单击“文件”→“切换用户”或者按“Ctrl+Alt-Q”快捷键，出现是否切换用户提示框，如图 3-28 所示。单击“确定”后，进入控制台登录界面。

图 3-28　切换用户提示框图

（2）在控制台登录对话框中，输入其它已审核通过的用户名和密码，单击“确定”后，将以新用户身份重新登录控制台，如图 3-29 所示。

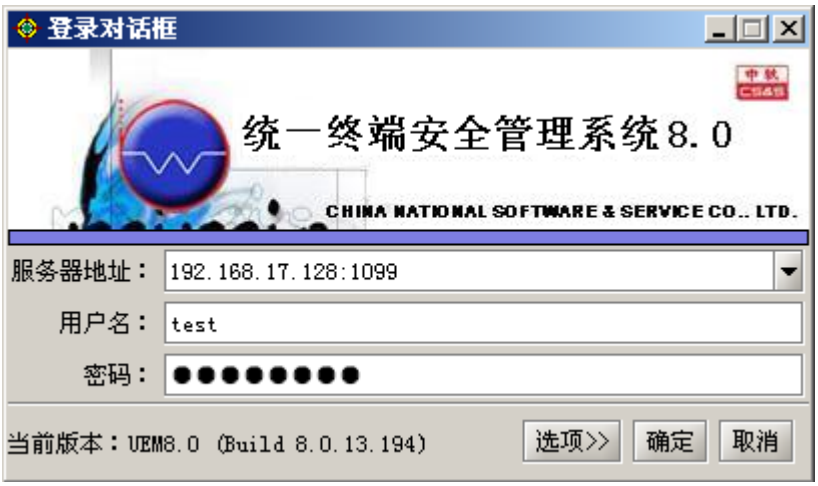


图 3-29　切换用户界面

3.3.4 修改个人信息

（1）在菜单栏中，单击“设置”→“修改个人信息”，或者按“Ctrl+Alt-U”快捷键，出现修改个人信息界面，如图 3-30 所示。

图 3-30　修改个人信息

（2）输入邮箱地址和手机号，测试通过后，根据知识库管理中的警报订阅向该邮箱发送邮件，或者向该手机发送短信，如图 3-31 所示。

图 3-31　测试邮件成功

提示：修改个人信息输入的邮箱和手机号，要和服务器端参数配置中（短信网关配置和 SMTP 邮箱配置）测试通过的邮箱地址和短信接收者号码相一致。该邮箱地址和手机号用于接收知识库管理中订阅的邮件警报和短信警报。

3.3.5 组织结构信息统计

单击控制台的“工具”→“组织结构信息统计”，或按“Ctrl+Alt-Z”快捷键进入组织结构信息统计界面，如图 3-32 所示。

当系统的组织结构非常复杂，非常庞大时，我们很难计算出该系统控制了多少个用户，多少个主机，以及多少在线，多少离线等，在这里我们就可看到组织结构中的人员和计算机情况。

图 3-32　　组织结构信息统计

3.3.6 同步域帐户

该系统可以导入域帐户，监控并同步域帐户，方便组织结构管理。

在菜单栏中，选择“设置”→“同步域帐户”，或按“Ctrl+Alt-T”快捷键，进入同步域帐户界面，如图 3-33 所示。

管理员在界面上输入域控制器地址、帐户、密码和域名之后，选择域帐户同步参数，然后点击“应用”按钮，控制台将给服务器下发应用域参数命令。

图 3-33　　同步域帐户

操作说明：

（1）“测试”按钮

管理员在界面上输入域控制器地址、账户、密码和域名之后，点击“测试”按钮。服务器对用户输入的域参数进行验证，将测试结果返回给控制台。

（2）“导入组织”按钮

管理员在界面上输入域控制器地址、账户、密码和域名之后，点击“导入组织”按钮。服务器接收到命令后，先检测域参数的有效性。如果无效，则给控制台返回导入失败的结果；如果有效，则从域控制器中读取组织结构，导入到 UEM 的 LDAP 数据库中。导入成功后，服务器给控制台返回导入结果，同时将域参数保存到配置文件中。控制台第二次打开同步域帐户窗口时，将自动从配置文件中读取域参数并显示，此时“域控制器地址”和“域名”栏将不可写。

（3）“导入全部”按钮

“导入全部”是从域控制器中读取组织结构和组织结构下的用户数据，将全部数据导入到 UEM 系统的 LDAP 数据库中，它和“导入组织”原理一样，不再详述。

（4）域帐户同步参数

监控并同步域帐户有两个选项：按需同步域帐户数据和实时同步所有数据。按需同步域帐户是指对于不在本系统中的域帐户，当用户注册时可以自动进行同步。实时同步所有数据是实时保持与域中帐户数据的一致性，需先手动导入域的全部数据。

提示：

1．服务器只能与一个 Windows 域控制器进行同步导入域帐户。当成功导入后，系统默认与 Windows 域控制器进行同步更新; 当用户取消“监控并同步域帐户”导入后，服务器不再监控 Windows 域控制器的变化。

2．从 Windows 域控制器导入的组织与用户，在控制台不能更改其属性，或者移动位置，这样将不能监控 Window 域控制器的变化。

3．当用户验证注册时，如果是 Windows 域帐户，这时密码验证采用 Windows 域帐户密码，而与控制台上该用户密码无关。

4．同步域帐户时，域控制器每个组织下用户超过 1000 个时，容易出错。

5．在已同步的域控制器中，大量频繁移动用户时，控制台将不断刷新，可能会影响工作。

3.3.7 客户端卸载口令管理

客户端卸载口令管理用于客户端本地卸载时，将产生的随机码发送给控制台管理人员，管理人员如果允许它本地卸载，就利用“客户端卸载口令管理”工具生成验证码传给客户端，这样客户端才能进行本地卸载。

单击控制台的“工具”→“客户端卸载口令管理”，或按“Ctrl+Alt-K”快捷键，进入卸载口令管理界面，如图 3-34 所示。输入客户端要求本地卸载时生成的随机码，单击“生成”按钮，即可得到验证码，然后将该验证码发给客户端。客户端输入该验证码后，即可自动卸载。

图 3-34　客户端卸载口令管理

3.3.8 灾难恢复动态口令管理

启用安全文档加密用户在卸载客户端后，机器内存有大量的加密文件，而解密的权限只有管理员拥有，普通用户无法自行解密。此时客户端用户可用动态口令认证模式启动灾难恢复工具，将产生的随机码发送给控制台管理人员，在管理员授权的情况下，运行灾难恢复工具，实现批量自解密。

单击控制台的“工具”→“灾难恢复动态口令管理”，或按“Ctrl+Alt-N”快捷键，进入灾难恢复动态口令管理界面，如图 3-35 所示。输入客户端启动灾难恢复工具时生成的随机码，单击“生成”按钮，即可得到验证码，然后将该验证码发给客户端。客户端输入该验证码后，即可运行灾难恢复工具。参见“灾难恢复工具的使用”章节。

图 3-35　灾难恢复动态口令管理

3.3.9 帮助

如果我们在操作过程中遇到什么困难，单击“帮助”菜单，或者“F1”进入系统帮助。

单击菜单栏“帮助”→“查看授权信息”，或“Ctrl+Alt-J”，可以查看已授权的功能模块。

单击菜单栏“帮助”→“关于”，或“Ctrl+Alt-A”，可以查看系统的**版本号**和版权信息。

3.4 退出

单击“文件”菜单下的“退出”（Ctrl-E），或者关闭控制台窗口，系统将弹出提示框，确定后即可退出控制台，如图 3-36 所示。

图 3-36　确定退出提示框

第四章　组织结构管理

用户登录安全管理系统控制台后，在正式使用控制台前，首先要建立自己的组织结构，设置用户角色及权限。这部分内容在前面快速入门中做了简单介绍，这一章我们按照菜单顺序做详细说明。

4.1 组织结构界面

以默认系统管理员 admin 登录，单击“组织结构管理”，进入组织结构管理界面，如图 4-1 所示。

图 4-1　组织结构界面

1：显示人员或计算机的组织结构树形列表。选中不同的节点，在子节点信息列表中显示不同的信息；选中的节点不同，右键菜单也不同。

2：地址栏，显示左侧选中节点的全路径信息。格式为：“当前选中节点的类型：当前选中节点的路径”。类型为“组织”、“人员”或“计算机”。路径中，每一个节点用“/”隔开。

3：显示子节点信息列表。信息列表支持鼠标单选或多选，用户可以根据自己需要选择可见列，各列之间可自由移动显示位置，并可按每列的升序或降序排列。

4：操作列表，显示各操作菜单项。在组织结构中选择的节点不同，显示的操作菜单项也不一样。

5：详细信息列表，显示选中节点的详细信息。可显示选中的组织、人员或计算机的详细信息，如果在子节点信息列表同时选择多行信息，这里只显示选中的对象数。

6：状态过滤栏，根据用户或计算机状态，过滤显示不同状态的用户或计算机。

7：图标示例栏，显示人员或计算机各种图标所代表的含义。

4.2 人员与计算机

该系统的人员管理是对组织结构中的用户进行操作，计算机管理是对组织结构中的计算机进行操作。不同的用户可以用同一台计算机，同一用户也可以用不同的计算机，用户和计算机不是一对一的关系，它们是可以分离的，也可以在不同的组织下。在实际使用时，可以通过组织结构中右建菜单—“关联主机”或“关联用户”，来实现用户和主机的关联。

4.2.1 人员管理

人员管理视图中，管理员选中组织结构树中的一个节点，根据选中的节点类型的不同，组织树右键菜单、子节点信息列表、操作列表和详细信息中，将分别显示不同的信息。选择组织节点、服务器级联节点和人员节点显示的内容都不一样，下面以人员节点为例说明。

单击选择人员组织结构树中的人员节点，界面如图 4-2 所示。

图 4-2　组织结构人员视图

组织树右键菜单所包含的菜单项为：刷新、搜索、迁移到、属性、重置密码、删除、恢复和“清除未注册”。其中，当且仅当被选中的人员为已删除的人员时，菜单项“恢复用户”才为可用状态，“删除”才为不可用状态。当且仅当被选中的人员为未注册人员时，菜单项“清除未注册”才为可用状态。

子节点信息列表中，显示该人员注册的所有计算机列表，列名为“计算机名”、“IP 地址”、“状态”、“操作系统”、“客户端版本”、“安全密级”，该表的显示列可以由管理员右键单击显示列表头自定义选择。子节点信息列表的条目可以被单击选中，支持单选或多选，根据选择情况的不同，操作列表和详细信息中，将分别显示不同的信息。

操作列表中，显示以下功能按钮：“属性”、“重置密码”，“恢复用户”，“更改所属群组”。其中，当该人员为已删除的人员时，“恢复用户”按钮可用，否则，“恢复用户”按钮不可用；“属性”中，显示该人员的详细信息列表，列表内容包括“用户名”、“真实名”、“性别”、“出生年月”、“职位”、“所属部门”、“电话”、“邮箱”、“描述”。

4.2.1.1　添加组织

（1）在组织结构树中选择组织节点，单击右键菜单，选择“添加组织”菜单项，如图 4-3 所示。或者在操作列表中，选择“添加组织”选项，出现添加组织界面。

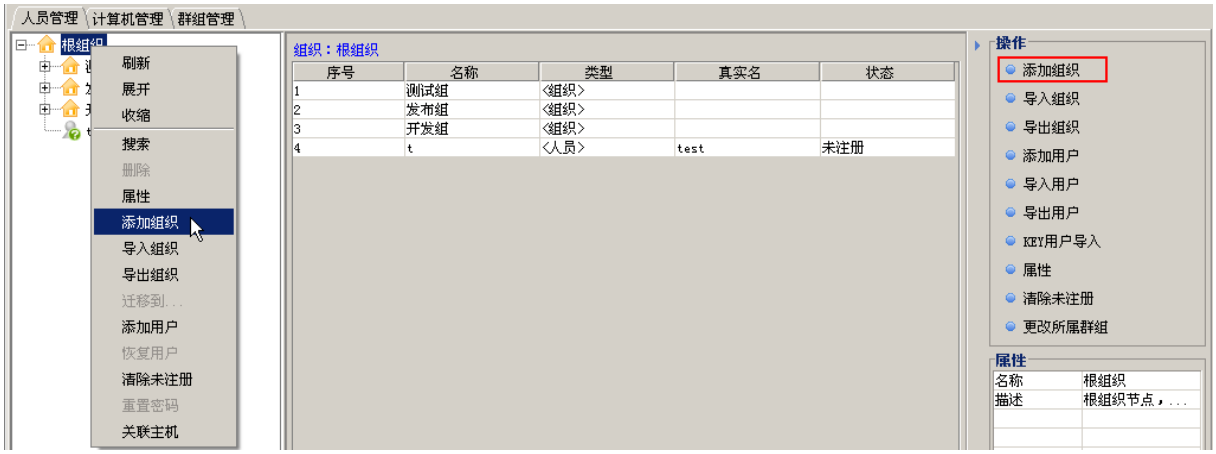


图 4-3　选择“添加组织”菜单

（2）输入组织结构名称和描述信息后，单击“确定”按钮，如图 4-4 所示。

图 4-4　添加组织节点

（3）组织结构视图区中显示刚添加的组织名称。用户可根据需要添加多个组织节点，建立自己的组织结构，如图 4-5 所示。

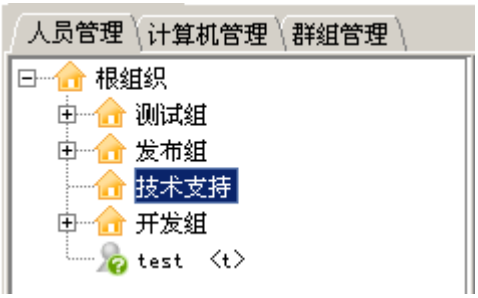


图 4-5　新建组织节点

4.2.1.2　迁移组织

（1）在组织结构中，选中要迁移的组织节点，例如：开发组。单击右键菜单，选择“迁移到...”菜单项，如图 4-6 所示。

图 4-6　选择迁移菜单项

（2）在弹出的“请选择部门”界面中，选择要迁移到的部门，例如：发布组，如图 4-7 所示。如果要同时迁移人员下的所有计算机，请勾选下面选项；否则，只迁移组织下的人员，不迁移人员下的计算机。最后，单击“确定”按钮。

图 4-7　请选择部门界面

（3）迁移成功后，弹出提示框。这时开发组的所有人员连同计算机，一起从开发组转移到发布组下面，如图 4-8 所示。

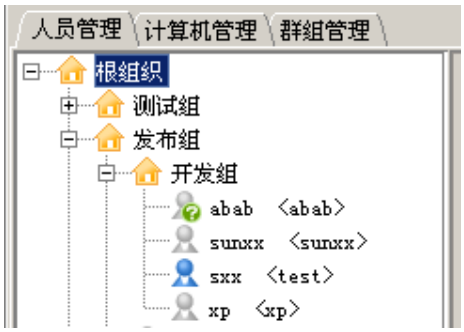


图 4-8　迁移后的组织节点

4.2.1.3　导出组织

（1）在组织结构树中，选择欲导出的组织节点，单击右键菜单“导出组织”；或者在操作列表中，单击“导出组织”选项，如图 4-9 所示。

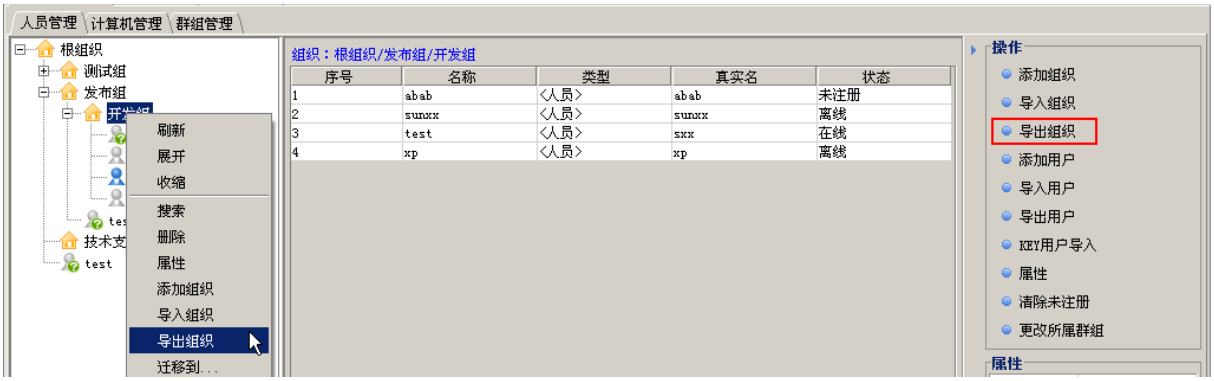


图 4-9　选择导出组织菜单

（2）系统将选中的组织节点导出，并保存成*.XML 文件，如图 4-10 所示。

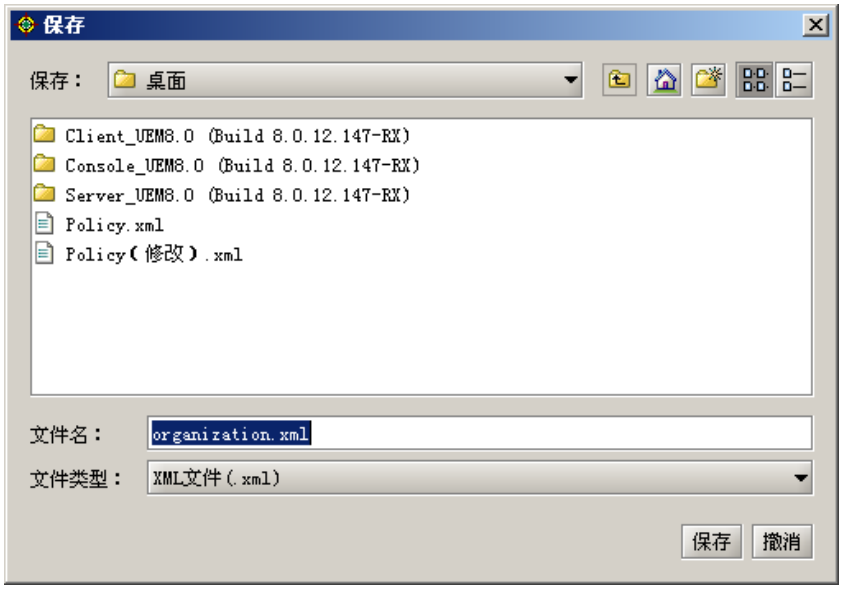


图 4-10　将导出组织保存为 xml 文件

提示：

1. 导出的*.XML 文件，可在“客户端二次打包→导入组织结构”时使用，方便用户在安装时自由选择所属的组织结构。

2. 导出的*.XML 文件，也可通过“导入组织”操作，导入到别的服务器或者同一服务器不同的节点下。再次导入到同一服务器时，需要将导出文件 “autogenguid”值 “false”改为“true”，否则导入不成功。

3. 导出组织操作只导出选定的组织结构,不导出组织下的用户。后面的导出用户操作，既可导出组织，也可导出组织下的用户。

4.2.1.4　导入组织

（1）在组织结构树中，选择欲导入的组织节点，单击右键菜单“导入组织”；或者在操作列表中，单击“导入组织”菜单，弹出导入组织文件选择框，如图 4-11 所示。

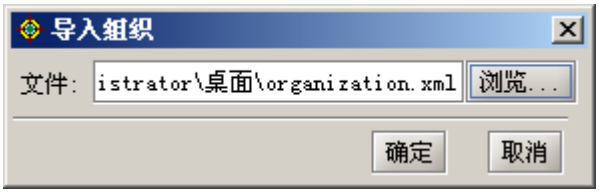


图 4-11　　导入组织界面

（2）选择欲导入的*.xml 文件，单击“确定”按钮，即可在选中的节点下导入新的组织结构。

提示：

同一节点下，不能有重名组织。如果欲导入的组织名称和选中组织下某一节点重名，则实际不进行导入操作。

4.2.1.5　添加用户

（1）在组织结构中，选择某组织节点，单击右键菜单“添加用户”，或者在操作列表中，单击“添加用户”菜单，出现添加用户界面，如图 4-12 所示。

输入用户名、真实名、性别、出生年月、用户密级和密码等相关信息后，单击“确定”按钮，组织结构中显示出新增加的用户。用户密级有四种：普通、秘密、机密、绝密，当用户访问密级文件时，受“密级文件访问控制策略”限制，详见 “密级文件策略”章节。

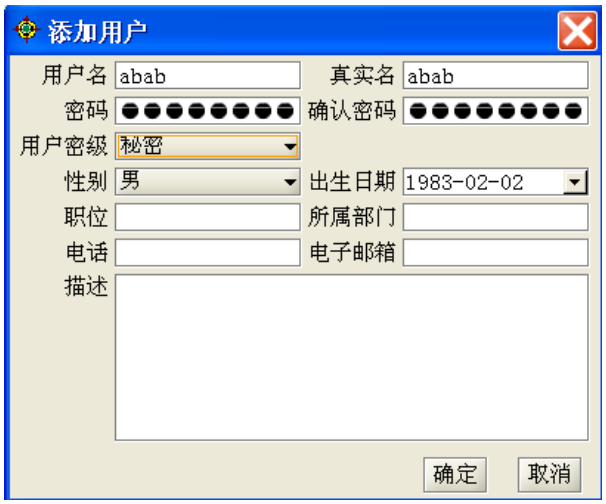


图 4-12　添加用户界面

（2）同样方法，根据需要添加多个新用户，并可通过右键菜单“迁移到...”改变人员所属的组织，如图 4-13 所示。

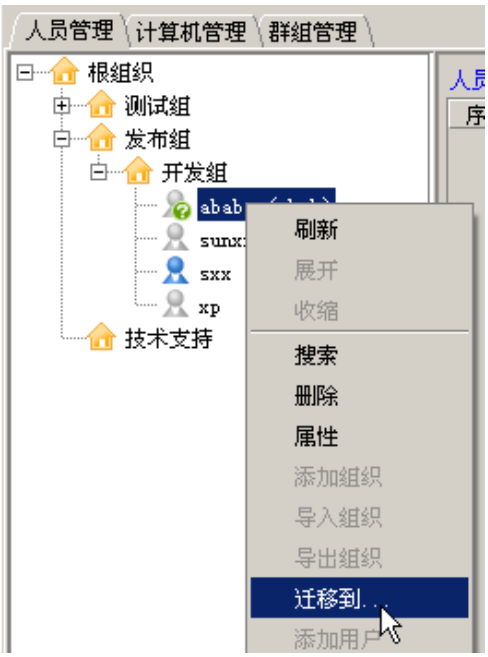


图 4-13　新增的用户

4.2.1.6　导入用户

为了方便批量建立用户操作，我们可以将用户信息保存成特定格式的*.xml、*.txt 或*.xls，然后通过“导入用户”菜单，导入到组织结构中选定的节点下面。其中 txt 文本的第一列为用户名，第二列为真实名，各列之间用“Tab”键隔开；*.xls 文本必须加上标头“用户名称”和“真实姓名”，“所属部门”可有可无，如图 4-14 所示。

图 4-14　导入文件格式

（1）在组织结构中，选择欲导入用户的组织节点，在操作列表中单击“导入用户”菜单，弹出导入用户界面，如图 4-15 所示。输入特定格式的用户文件（*.xml、*.txt 或*.xls），单击“确定”按钮。

图 4-15　导入用户文件选择框

（2）导入过程中，如果组织结构中有相同的用户名就不再导入。导入完成后，会弹出消息框，单击链接查看日志信息，如图 4-16 所示。

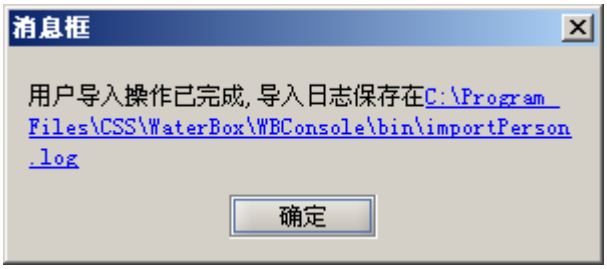


图 4-16　导入用户消息框

（3）导入成功后，可以在相应的组织节点中，看到刚导入的用户信息。导入用户的默认密码都是 1234567a.

4.2.1.7　导出用户

（1）在组织结构中，选择欲导出用户的组织节点，在操作列表中单击“导出用户”菜单，弹出导出用户界面，如图 4-17 所示。

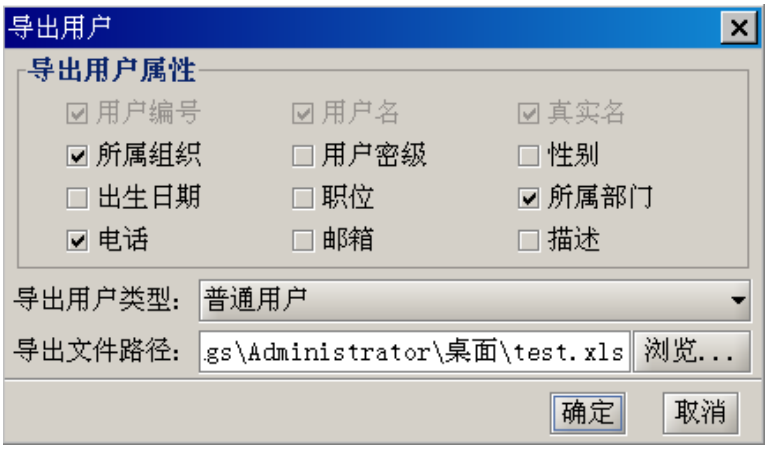


图 4-17　导出用户界面

（2）导出用户时，除默认的用户编号、用户名和真实名外，可以勾选“所属组织”、“用户密级”、“电话”、“邮箱”等其它属性。如果选择“所属组织”，也连同组织结构一并导出；如果不选“所属组织”，只将选定组织下的用户导出。

通过下拉框选择需要导出的用户类型，输入导出文件路径和文件名（*.xml 或*.xls），然后单击“确定”按钮。导出完成后，弹出提示框，如图 4-18 所示。

图 4-18　导出用户成功

4.2.1.8　导入 KEY 用户

如果客户端用户是 KEY 用户，可以在这里导入用户信息。导入成功后，系统就会默认该 KEY 用户为合法用户。

（1）确认系统已经安装了设备相关驱动，并将 KEY 接入了计算机。安装控制台时，就有是否安装 KEY 驱动选项。如果用户没有安装，可以单独再安装。

（2）在组织结构中，选择欲导入 KEY 用户的组织节点，单击操作列表“KEY 用户导入”菜单，弹出导入 KEY 用户界面，如图 4-19 所示。从下拉框中选择设备类型，输入设备 PIN 码，根据用户需要采用什么作为用户名，最后，单击“提取”按钮。

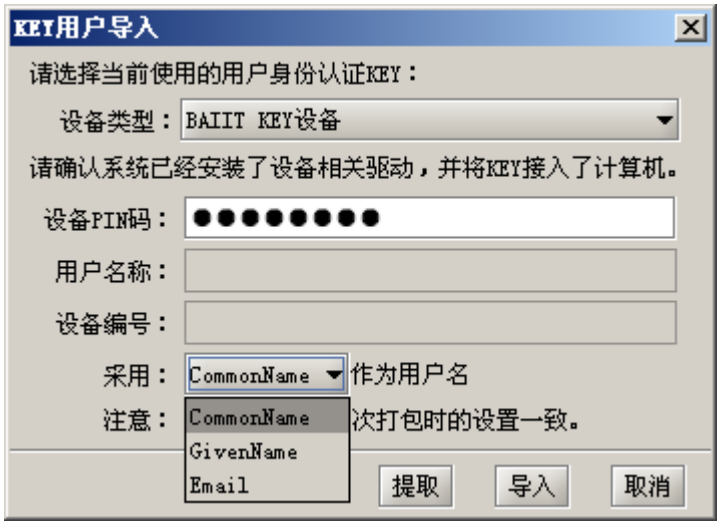


图 4-19　提取 KEY 用户信息

（3）系统会自动将 KEY 设备的“用户名称”和“设备编号”提取出来，如图 4-20 所示。单击“导入”按钮，即将 KEY 用户名称导入到选定的组织节点下。

提示：如果组织结构中存在相同的用户名，会提示导入失败。

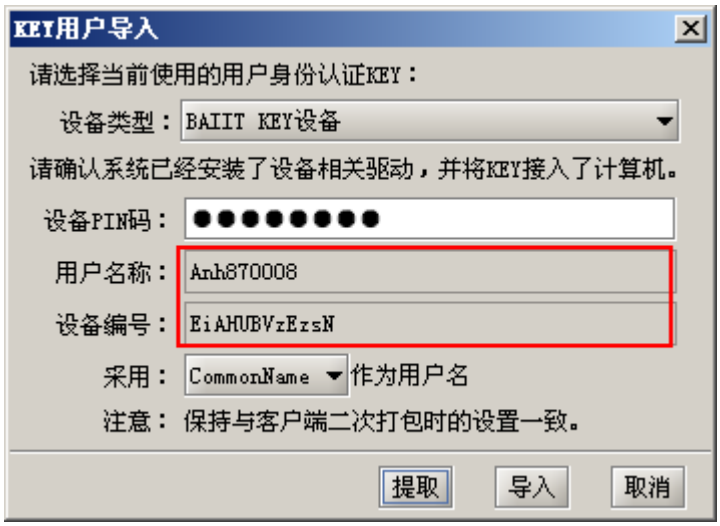


图 4-20　KEY 用户信息的导入

4.2.1.9　清除未注册用户

（1）选中组织结构中某节点，单击右键菜单“清除未注册”，或者从右侧的操作列表中单击“清除未注册”菜单，都可弹出确认框，如图 4-21 所示。确定后，即可将该节点下的所有未注册用户全部从 LDAP 库清除，并且不可恢复。

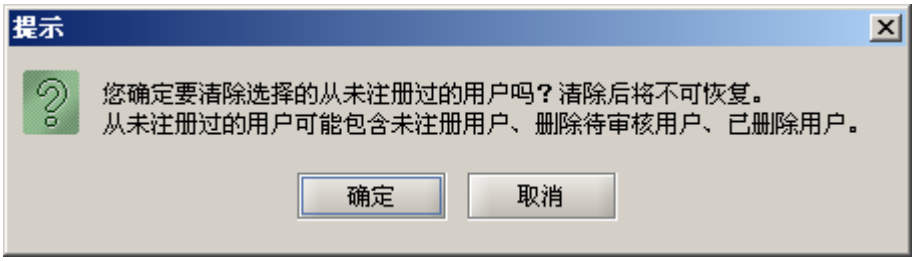


图 4-21　清除未注册用户确认

（2）如果在组织结构中选定某个未注册用户，单击右键菜单“清除未注册”，也可将该未注册用户单独从 LDAP 数据库清除。清除未注册用户和删除用户不同，删除后可以再恢复，清除后就不可。

提示：曾经注册过的用户,但已经取消注册的用户,当前显示也是未注册用户。这种未注册用户是无法使用“清除未注册用户”功能的，保留这样的用户是为审计日志。

4.2.1.10 更改所属群组

（1）在人员管理页面，选中组织或单个、多个人员，单击右侧操作列表中的“更改所属群组”菜单，如图 4-22 所示。

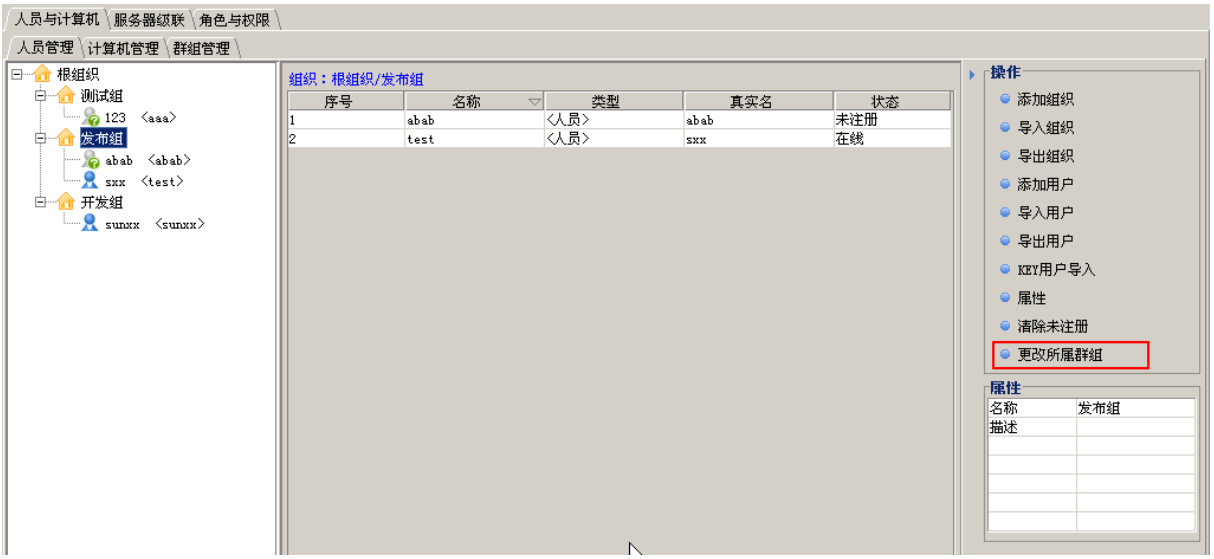


图 4-22　更改所属群组菜单项

（2）在弹出的更改所属群组界面中，单击下拉框，选择群组名称，如图 4-23 所示。如果勾选选项“同时修改每个人员下当前所有计算机的群组”，那么单击“确定”按钮后，选定的组织或人员将连同当前所有计算机一起隶属于某群组。

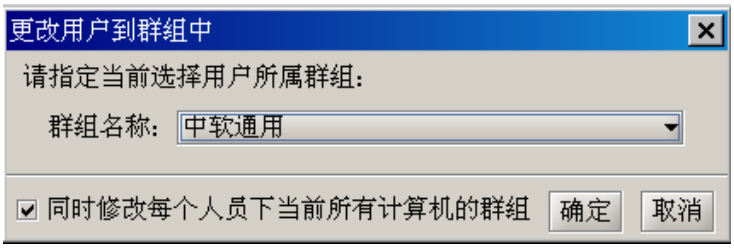


图 4-23　更改用户群组

4.2.1.11 删除用户

（1）在组织结构图中，选择要删除的未注册用户，单击鼠标右键，选择“删除”菜单项，出现删除确认框，如图 4-24 所示。

提示：带有客户端的用户不能被删除。如果在删除带有客户端的用户，首先应取消用户注册，使该用户变成未注册状态才可删除。

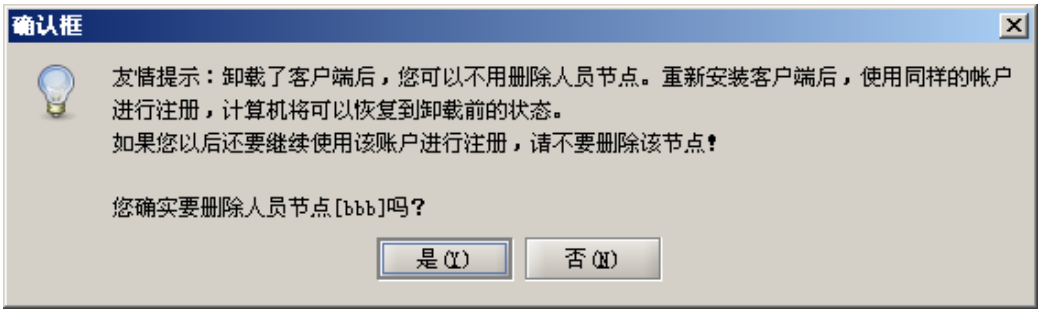


图 4-24　删除确认框图

（2）单击“是（Y）”，出现消息框，如图 4-25 所示。

图 4-25　删除消息框

（3）单击“确定”按钮，将用户临时删除。如果要彻底删除用户，需要在删除用户管理中，对用户进行审核，通过后即可彻底删除。详见删除用户管理部分。

4.2.1.12 恢复已删除用户

（1）在组织结构图中，选择已删除的用户，单击右键菜单“恢复用户”，或者在操作列表中选择“恢复用户”菜单项，出现恢复确认框，如图 4-26 所示。

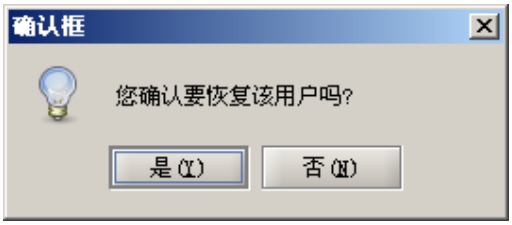


图 4-26　恢复用户确认

（2）确定后，即可将该用户恢复为未注册状态。

4.2.1.13 查看修改属性

（1）在组织结构中，选择某组织节点，单击右键菜单，选择“属性”菜单项；或者从右侧操作列表中，单击“属性”菜单，弹出组织信息框，如图 4-27 所示。这里可以修改组织名称和描述信息，修改完成后，单击“确定”退出，组织结构会自动刷新，显示修改后的组织名称。

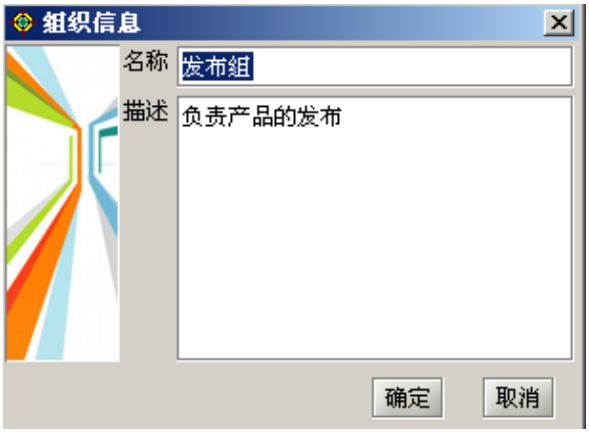


图 4-27　　查看、修改组织属性

（2）在组织结构中，选择某人员节点，单击右键菜单，选择“属性”菜单项；或者从右侧操作列表中，单击“属性”菜单，弹出用户信息框，如图 4-28 所示。在这里可以修改用户信息，但“用户名”和“密级”除外。修改完成后，单击“确定”保存退出，组织结构会自动刷新。

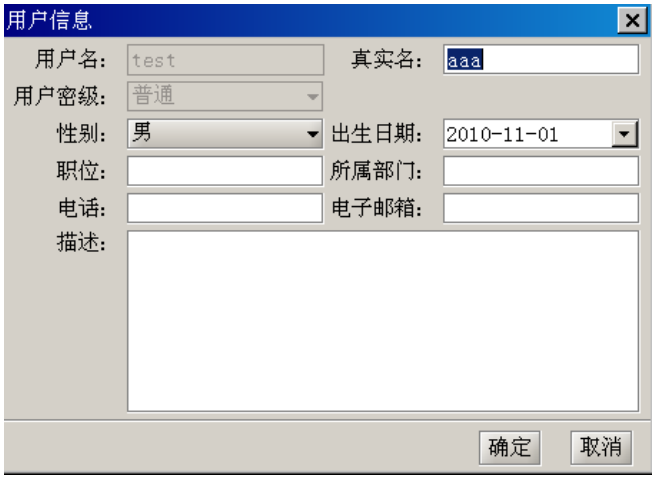


图 4-28　查看、修改人员属性

4.2.1.14 搜索

（1）在组织结构中选择组织节点，单击鼠标右键，选择“搜索”菜单项，或按“CTRL+F”组合键出现搜索框，如图 4-29 所示。从下拉框中选择检索对象“组织”，输入要搜索的组织名称，系统能够根据组织名称的模糊匹配，快速的定位到组织结构树中的某个组织上，或者给出匹配的组织列表。

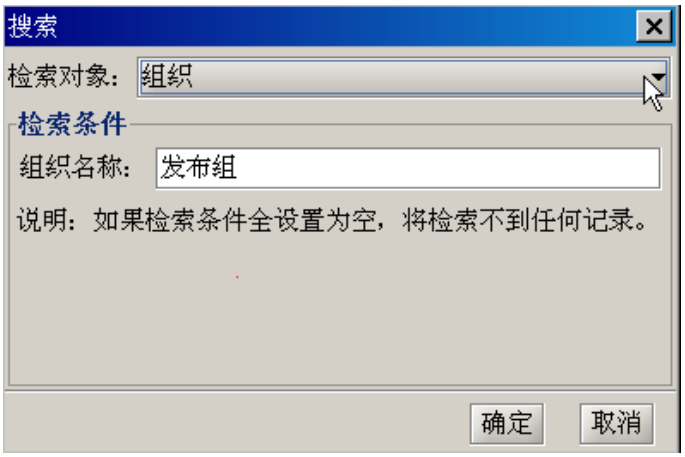


图 4-29　搜索组织

（2）如果“检索对象”设为用户，除了根据用户名和真实名查询用户外，还可以根据用户所使用的计算机名称，用户所使用的计算机 IP 地址来查找和定位到用户，如图 4-30 所示。

提示：

1. 查询条件支持模糊方式，例如查找用户：aaabbbccc，只需输入　ab 或 bc 就可查找。

2. 人员搜索对话框支持对 Enter、Esc 键的响应。按 Enter 键，则控制台执行人员检索；管理员按 Esc 键，控制台关闭搜索窗口。

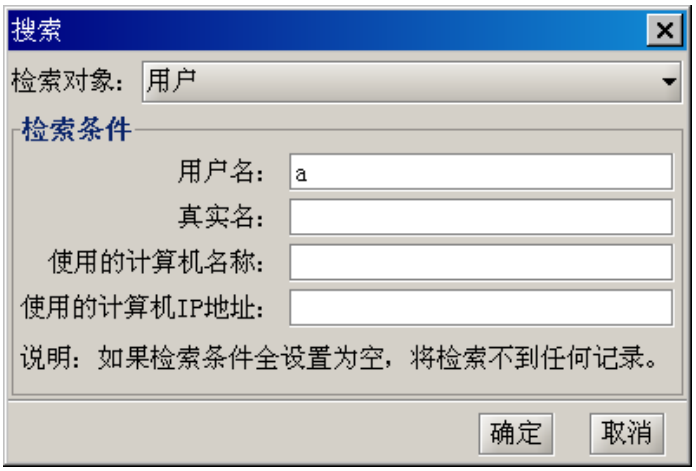


图 4-30　搜索用户

（3）若系统搜索到的只是单个用户，会在组织结构中将光标直接定位于该用户；如果搜索出的是多个符合条件的用户，会以列表的形式呈现。可双击列表某个的用户，光标将定位于组织结构中该用户，如图 4-31、4-32 所示。用户可以根据自己需要选择是否“定位后关闭窗口”，系统对此选项具有记忆功能，下次定位按此选项进行。

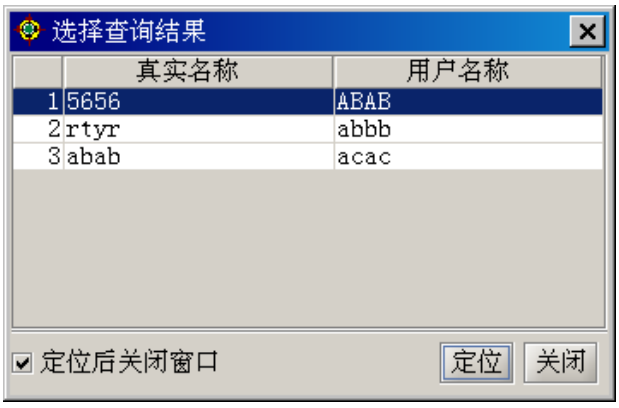


图 4-31　选择搜索出的人员

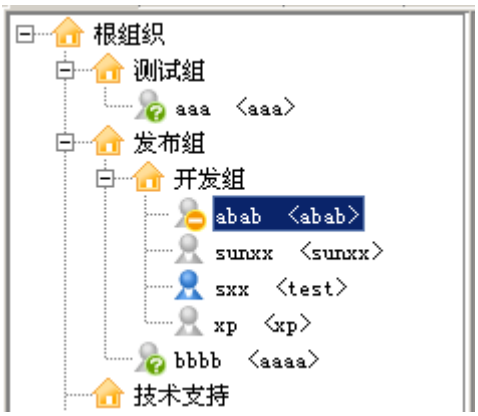


图 4-32　光标定位于搜索到人员

4.2.1.15 重置密码

在组织结构中，找到要更改密码的用户节点，单击鼠标右键，选择“重置密码”菜单项；或者在操作列表选择“重置密码”菜单，弹出设置密码对话框，如图 4-33 所示。输入“新密码”和“确认密码”，单击“确定”退出。

图 4-33　更改密码

提示：

（1）更改用户密码后，如果该用户启用网络认证功能，需要在该客户端重新输入新密码，确定后，才能恢复上网。参见客户端“网络身份认证”部分。

（2）重置密码对 key 用户无效。如果重置了 KEY 用户密码，重启客户端后，消息中心会弹出消息“更改客户端用户密码失败!”。这时，可以在客户端右键菜单中修改 PIN 码。修改成功后，重新登录系统，输入修改后的 PIN 码才能进入系统。

4.2.1.16 关联主机

（1）在组织结构中选择某人员节点，在中间的详情列表中，单击右键菜单“关联主机”，或者单击右侧的操作按扭“关联主机”，如图 4-34 所示。

图 4-34　选择“关联主机”菜单

（2）控制台自动跳转到计算机管理界面，并自动选中指定的计算机。新界面上，组织结构树展开到指定的计算机处，该计算机为选中状态，子节点信息列表、操作列表和详细信息列表也分别显示该计算机的信息，如图 4-35 所示。

图 4-35　计算机管理界面

4.2.1.17 单组织注册信息统计

（1）在组织结构中，选择某组织节点，单击右键菜单“单组织注册信息统计”，可以统计出当前组织下的注册信息，如图 4-36 所示。

图 4-36　单组织注册信息统计

（2）单击统计结果下方的“导出”按钮，可以将当前信息导出为*.xls、*.pdf、*.html 文件保存，如图 4-37 所示。

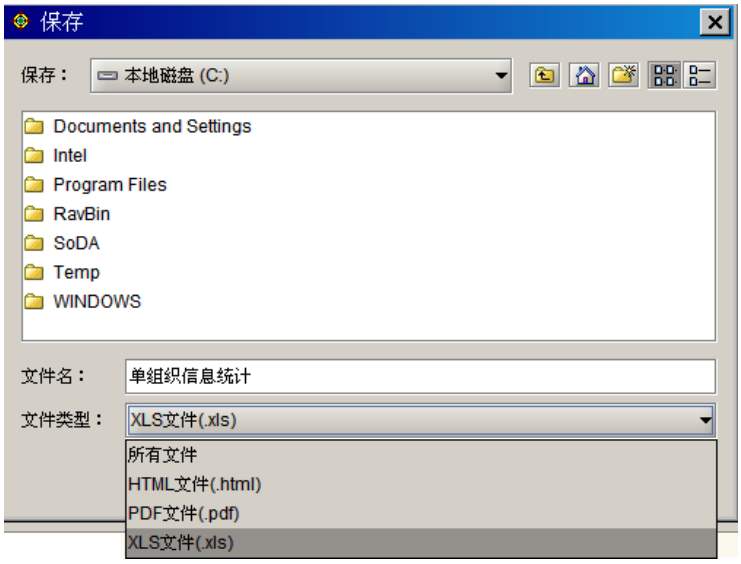


图 4-37　导出当前统计结果

4.2.1.18 多组织注册信息统计

（1）在组织结构中，选择某组织节点，单击右键菜单“多组织注册信息统计”，可以统计出当前组织及所有子组织下的注册信息，如图 4-38 所示。

图 4-38　多组织注册信息统计

（2）单击统计结果下方的“导出”按钮，可以将当前信息导出为*.xls、*.pdf、*.html 文件保存，如图 4-39 所示。

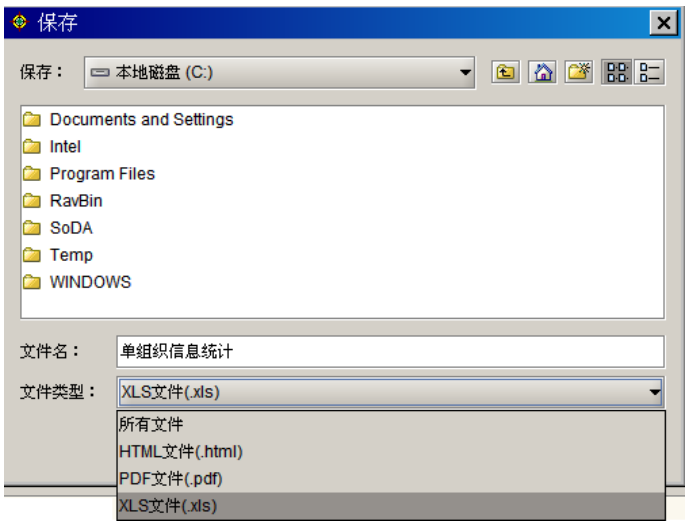


图 4-39　导出当前统计结果

4.2.2 计算机管理

计算机管理视图中，管理员选中组织结构树中的一个节点，根据选中的节点类型的不同，组织树右键菜单、子节点信息列表、操作列表和详细信息中，将分别显示不同的信息。单击选择计算机组织结构树中的组织节点、级联服务器节点和计算机节点显示内容不一样。

以单击选择计算机组织结构树中的组织节点时，如图 4-40 所示：

图 4-40　计算机管理组织节点视图

组织树右键菜单显示：刷新、展开、收缩、搜索、删除、添加组织、迁移到、属性等；

子节点信息列表显示：该组织下的计算机或子组织列表，默认显示列为“名称”、“类型”、“IP 地址”、“状态”、“操作系统”、“客户端版本”、“安全密级”。

子节点信息列表的显示列可以由管理员自定义。管理员鼠标右键点击列表的表头，弹出右键菜单“选择可见列”。点击此菜单后，弹出当前显示列的自定义窗口。在该窗口中，选择需要显示的列后，点击“确定”按钮，控制台按照选定的列显示子节点信息。

子节点信息列表支持通过表头拖拽来调整列的宽度。管理员可以通过表头拖拽，调整列的宽度。控制台将记录该列宽值。该值在关闭当前控制台之前将一直有效。

操作列表中，显示以下功能按钮：“添加组织”、“导入组织”、“导出组织”、“属性”。

详细信息中，显示该组织详细信息列表，列表内容包括“部门名称”和“部门描述”。

注意：计算机管理操作和人员管理操作有许多相似之处，我们不再一一详述。下面我们只讲针对计算机的特别操作。

4.2.2.1 查看计算机属性

（1）在计算机管理视图中，选择某计算机，点击“属性”菜单，或者在人员管理视图中，选择某人员，双击详情区计算机列表条目，都可出现该计算机信息列表框，如图 4-41 所示。实际上，在计算机管理视图中，选中某计算机，在右边的属性框中就可看到该计算机的属性。

图 4-41　　计算机属性列表

（2）计算机的属性包括：标识号、IP 地址、操作系统、MAC 地址、机器类型、计算机密级、购入日期等，大多数信息只能查看不能更改，只有机器类型可以更改。

4.2.2.2 更改计算机密级

（1）在计算机管理视图中，选择要更改密级的计算机，可以单选，也可多选，点击“更改计算机密级”菜单，如图 4-42 所示。

图 4-42　选择计算机更改密级

（2）在弹出的“更改计算机密级”界面中，选择新的安全密级，如图 4-43 所示。确定后，选中的计算机将更新密级。

图 4-43　更改计算机密级

4.2.2.3 更改购入日期

（1）在计算机管理视图中，在左侧选择一个组织，在中间的详情列表中，选择一个或多个组织或计算机的组合，单击右侧的“更改购入日期”菜单，如图 4-44 所示。

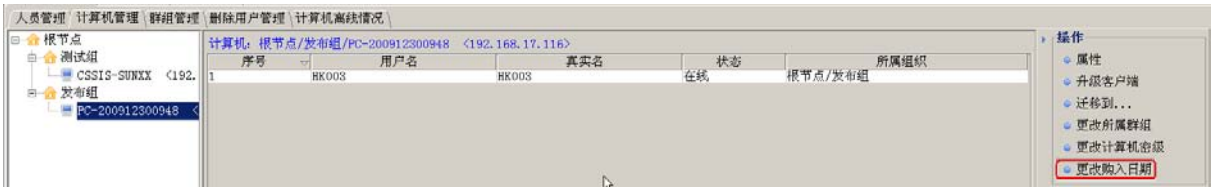


图 4-44　选择计算机更改购入日期

（2）在弹出的“更改计算机购入日期”界面中，选择新的购入日期，如图 4-45 所示。确定后，选择的组织下所有的计算机以及选择的计算机的购入时间都将被成功修改。

图 4-45　更改计算机购入日期

（3）在计算机管理视图中，选中某组织节点，鼠标右键点击计算机详情列表区的表头，在弹出的右键菜单中选择“选择可见列”，弹出可见列选择界面，如图 4-46 所示。默认情况下，“购入日期”为可选列，将其加入到“可见列”中，计算机的详情列表中就会显示“购入日期”字段。

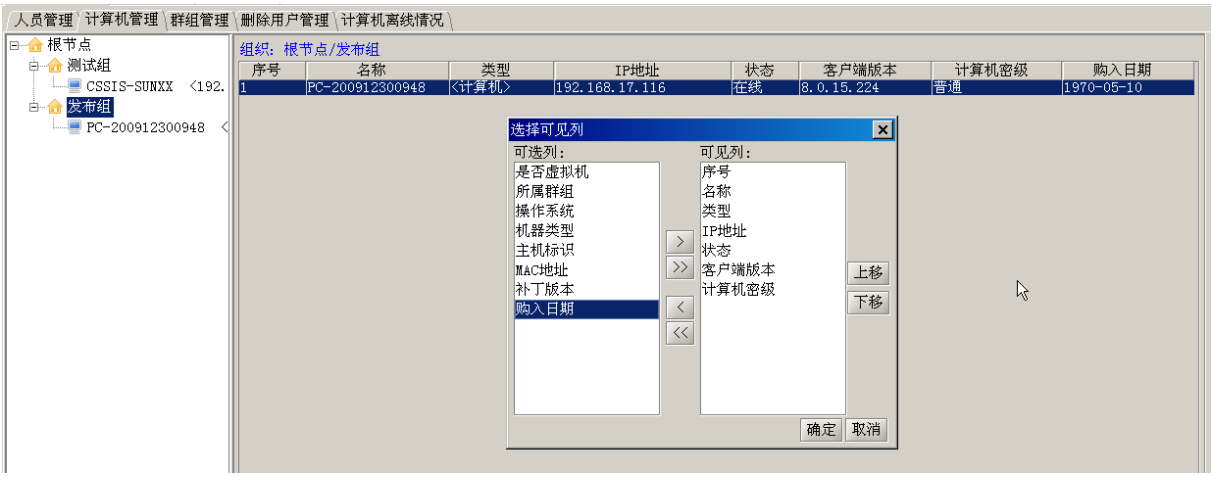


图 4-46　选择显示计算机购入日期列表项

4.2.2.4 升级客户端

升级客户端时，需要配置服务器端参数。具体步骤如下：

（1）单击“系统参数设置”→“客户端升级设置”，进入参数设置界面，如图 4-47 所示。点击“浏览”按钮，输入升级包位置，然后单击“上传”按钮，将升级包上传至服务器。升级包状态栏中显示是否有升级包，以及升级包的版本号。最后，点击“应用”按钮。

提示：这里不启用客户端自动升级模式，采用控制台下发命令方式，给指定的计算机进行升级。

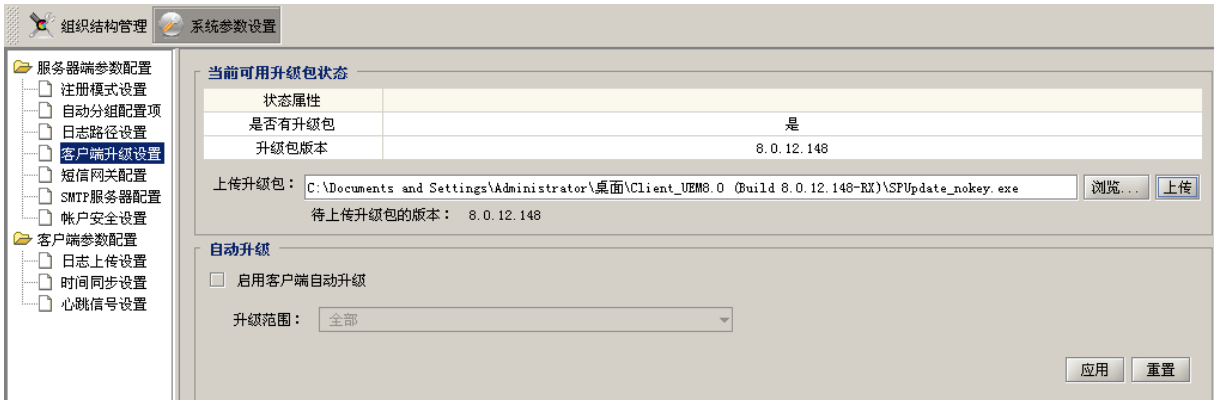


图 4-47　客户端升级设置

（2）单击“组织结构管理”→“计算机管理”，进入计算机管理界面。选择要升级的计算机，可以单选，也可以多选，最后点击“升级客户端”菜单，如图 4-48 所示。

图 4-48　客户端升级

（3）系统弹出提示框，询问是否升级所选中的客户端，以及版本相同时是否强制升级，如图 4-49 所示。单击“确定”后，选中的客户端自动进行升级操作。

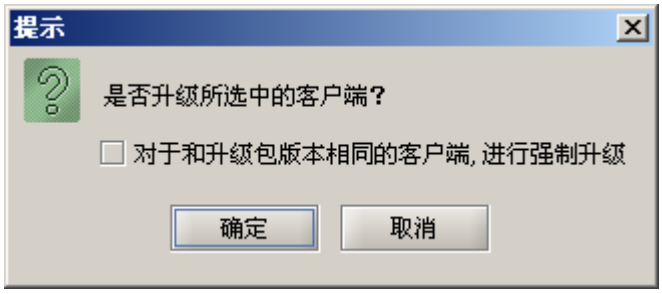


图 4-49　客户端升级确认框

4.2.2.5 取消注册

（1）在计算机管理视图中，选择某计算机下一个用户（在线或不在线），也可在人员管理视图中，选择某人员节点下的一个计算机，单击右侧操作列表中“取消注册”菜单，如图 4-50 所示。

图 4-50　选择取消注册对象

（2）客户端收到命令后，自动取消该用户注册，其它用户不受影响。如果该用户是本计算机的最后一个用户，那么在取消最后一个用户注册时，弹出提示框“您确定要卸载该用户注册的客户端吗？”，让用户选择是否卸载客户端。

4.2.2.6 客户端卸载

如果在一个计算机中注册了好多客户端用户，那么一个一个取消用户注册就显得不方便。这时，我们可以在组织结构管理中，找到计算机管理视图，选中多个用户的计算机，单击右键菜单“卸载客户端”，如图 4-51 所示。客户端收到该命令后，会自动卸载，同时取消本机上注册的所有用户。

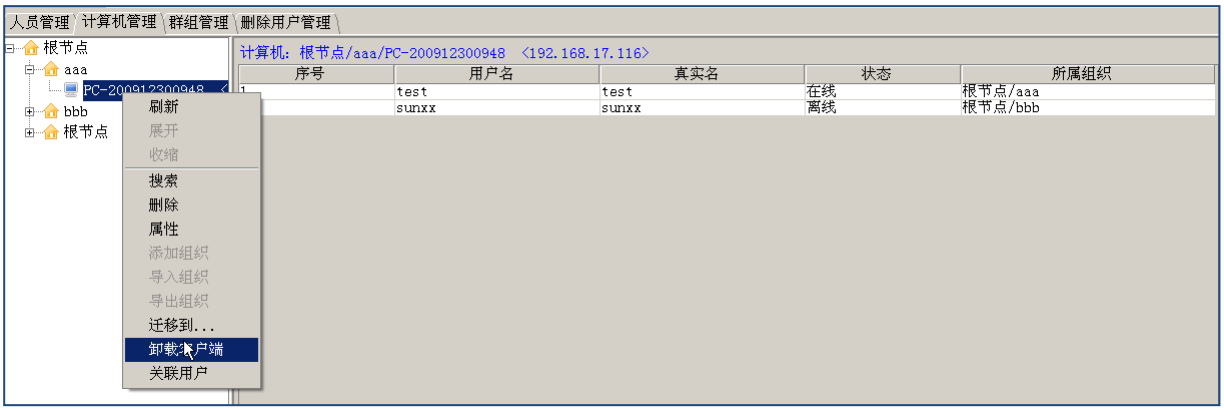


图 4-51　卸载客户端

4.2.2.7 清除未注册主机

客户卸载后，计算机显示未注册状态。

在组织结构中选择某个未注册的主机，单击右键菜单“清除未注册主机”，可将选中未注册主机清除。如果在组织结构中，选中某组织节点，单击右键菜单“清除未注册主机”，或者单击右侧操作区“清除未注册”命令项，系统将批量清除该组织下所有未注册的主机，如图 4-52 所示。

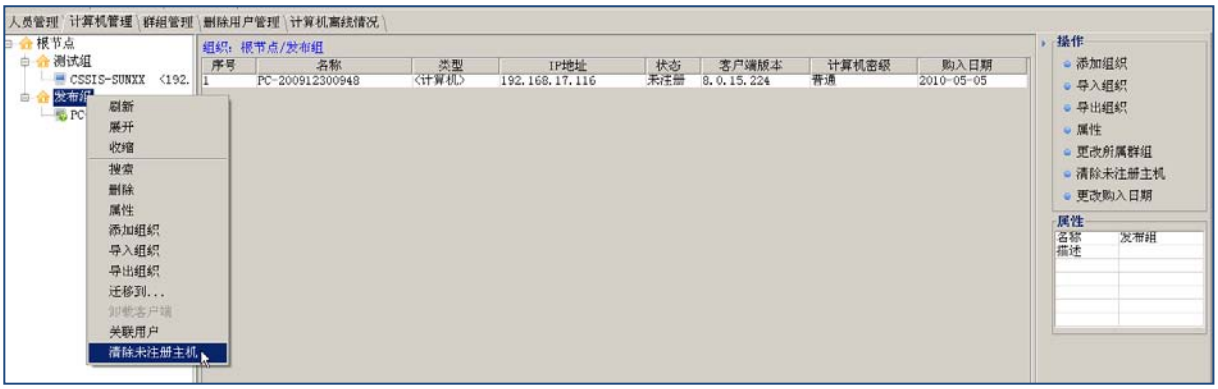


图 4-52　选择清除未注册的主机

清除未注册的主机时，控制台给出提示信息，如图 4-53 所示。确认后，执行清除操作。

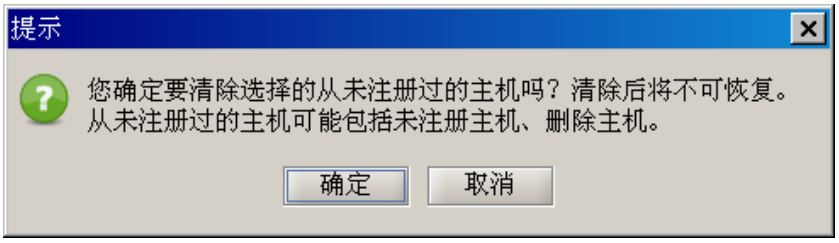


图 4-53　确认清除未注册主机提示框

4.2.2.8 关联用户

（1）在计算机管理视图中选择某计算机，在中间的详情列表中，单击右键菜单“关联用户”，或者单击右侧的操作按扭“关联用户”，系统自动切换到人员管理视图，并定位于该用户，如图 4-54 所示。也可能该计算机下面有多个用户，需选择要定位的用户。

图 4-54　切换到人员管理

（2）控制台自动跳转到人员管理界面，并自动选中指定的用户。新界面上，组织结构树展开到指定的用户处，该用户为选中状态，子节点信息列表、操作列表和详细信息列表也分别显示该用户的信息，如图 4-55 所示。

图 4-55　人员管理视图

提示：计算机视图和人员视图可以相互切换，用户在实际操作中要灵活运用。

4.2.3 群组管理

群组是对人员和计算机的逻辑分组。创建群组后，将人员或计算机添加进群组时，该人员或计算机将自动应用该群组对应的策略（包括失泄密防护策略、主机安全策略、安全文档策略、可信策略和密级文件策略）。这样，大大方便了管理人员对策略的下发和管理。参见 5.4 群组策略。

群组管理主界面，如图 4-56 所示：

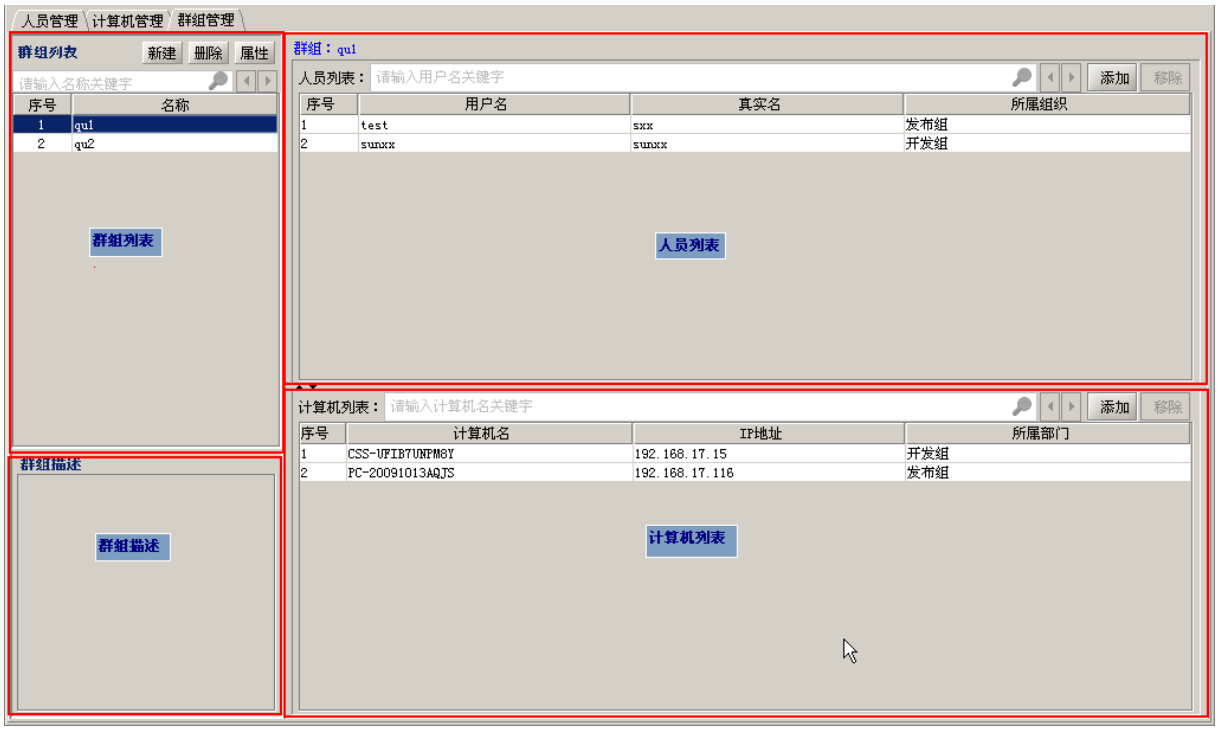


图 4-56　群组管理界面

群组列表显示当前存在的所有群组，支持根据群组名称的搜索。在群组列表区点击鼠标右键，显示“刷新、新建、删除、属性”四项右键菜单。点击列表中某个群组，左侧下方显示该群组的描述信息，右侧显示该群组下的人员列表和计算机列表。

群组描述显示某选定群组的详细描述信息。

人员列表显示“用户名”、“真实名”和“所属部门”三项。支持点击表头的排序功能，支持用户名关键字搜索。

计算机列表显示“计算机名”、“IP 地址”、“所属部门”三项，支持点击表头的排序功能，支持计算机名关键字搜索。

4.2.3.1　添加群组

（1）在群组管理视图中，单击群组列表区的“新建”按钮；或者在群组列表上点击鼠标右键菜单，选择“新建”菜单项，都将弹出群组新建窗口。输入群组名称和描述信息，如图 4-57 所示。

提示：

① 群组名称只支持字母、数字、下划线和中文，名称不能超过 30 个字符

② 群组的描述不能超过 100 个字符

③ 群组的个数不能超过 50 个。当群组数目已经达到 50 个时，不能再添加新的群组。

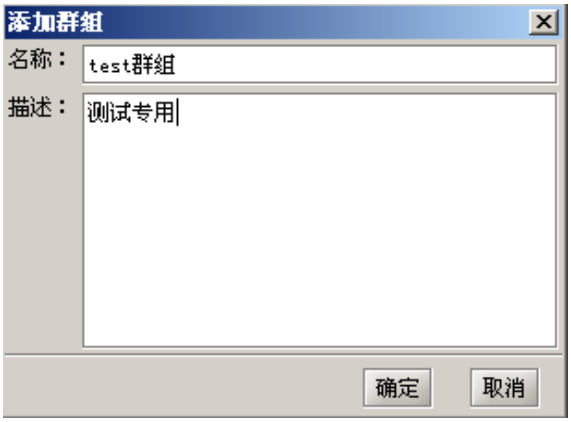


图 4-57　新建群组界面

（2）单击上图“确定”按扭后，在群组列表视图中，将能看到新建的群组“test 群组”，如图 4-58 所示。

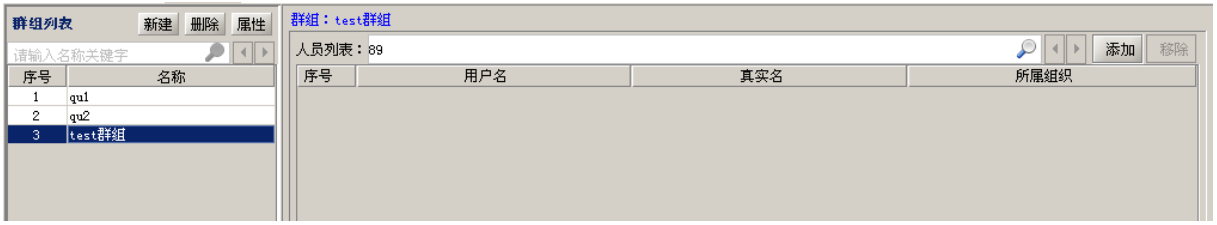


图 4-58　群组列表显示新建群组

（3）用户根据自己的需要，添加多个群组，如：qu1\qu2\qu3 等。

4.2.3.2　删除群组

（1）在群组列表中，选择欲删除的某个群组，单击“删除”按钮，或者单击鼠标右键，选择右键菜单“删除”，如图 4-59 所示。

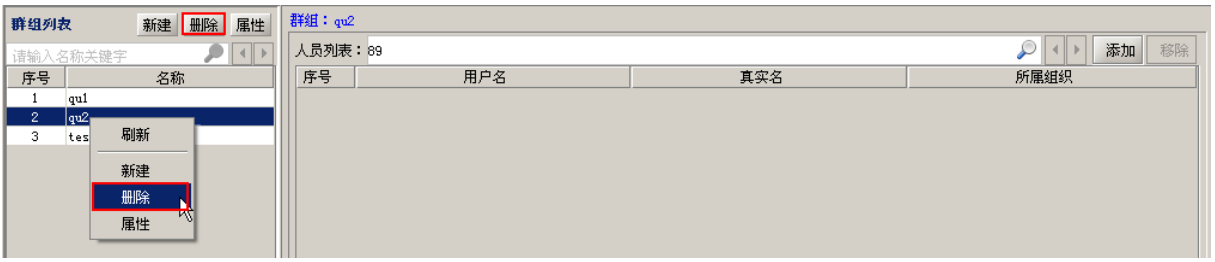


图 4-59　删除群组选项

（2）在弹出删除群组提示框，如图 4-60 所示。单击“是（Y）”按钮，既可将选定的群组删除，同时群组列表中也不再显示。

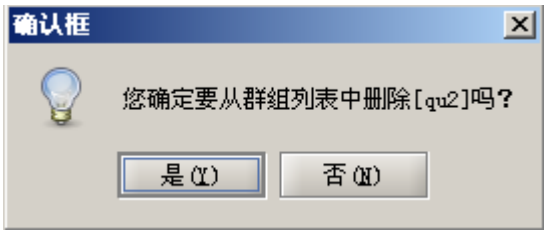


图 4-60　删除群组确认框

4.2.3.3　修改群组属性

（1）在群组列表中，选择某个群组，单击“属性”按钮，或者单击群组列表鼠标右键，选择右键菜单“属性”，都将弹出“修改属性”对话框，如图 4-61、4-62 所示。

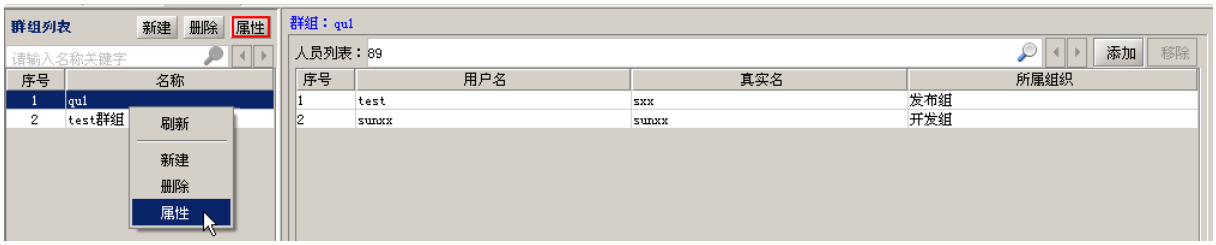


图 4-61　修改群组属性选项

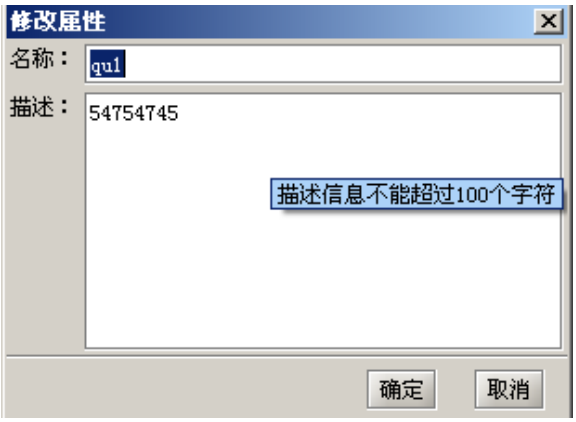


图 4-62　修改群组属性对话框

（2）在修改群组属性对话框中，输入新的群组名称和描述信息，单击“确定”按钮后，该群组将显示新的属性。

提示：

① 群组名称只支持字母、数字、下划线和中文，名称不能超过 30 个字符

② 群组的描述不能超过 100 个字符

4.2.3.4　添加群组人员

（1）在群组列表中，选择某个群组，单击人员列表区的“添加”按钮；或者单击人员列表区鼠标右键，选择右键菜单“添加”，如图 4-63 所示。都将弹出“添加人员到群组”界面。

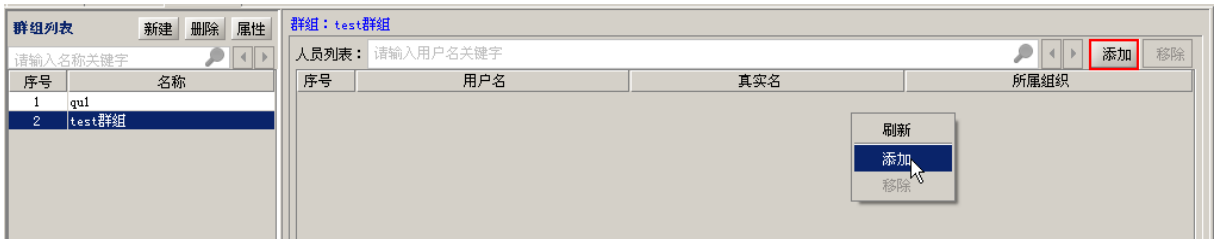


图 4-63　添加人员到群组选项

（2）在弹出的“添加人员到群组”界面中，选择一个或多个人员，单击“确定”按钮，添加到选定的群组中，如图 4-64 所示。

每个人员只能属于一个群组，如果指定的人员已经属于别的群组，将被强制拖动到本群组中。如果勾选了“同时将指定人员下的所有计算机添加到该群组中”，则对应的计算机也将被强制拖动到该群组中。

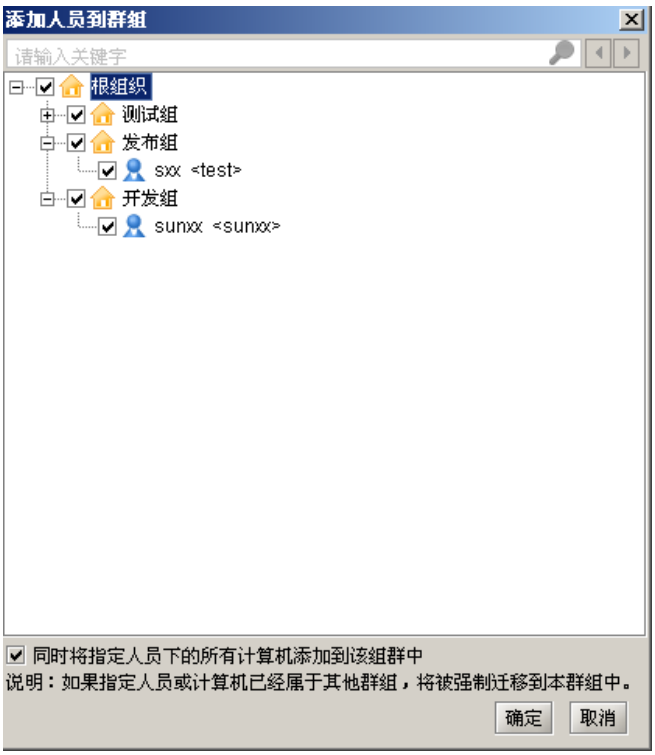


图 4-64　选择人员添加到群组

（3）返回到群组管理页面，在人员列表中将看到刚添加的人员，如图 4-65 所示。

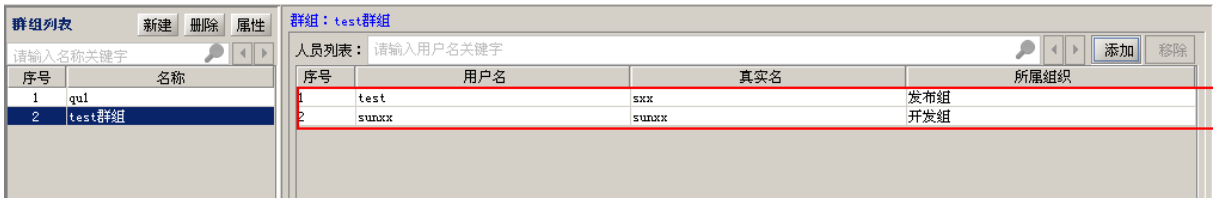


图 4-65　添加的群组人员

4.2.3.5　删除群组人员

（1）在群组的人员列表中，选择一个或多个人员（多个人员使用 SHIFT/CTRL 键+鼠标左键单击选中），然后单击人员列表区中“移除”按钮，或者单击鼠标右键菜单“移除”，如图 4-66 所示。

图 4-66　移除人员选项

（2）在弹出的移除人员确认框中，如图 4-67 所示。单击“确定”按扭后，既可将选定的人员从群组中删除。如果要同时移除选定人员所有注册的计算机，必须勾选选项“同时移除选中人员下所有注册的计算机”，这样单击“确定”按钮后，才能连同所注册的计算机，一起从群组中删除。

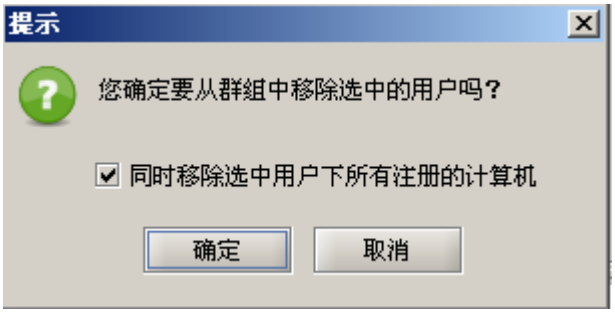


图 4-67　移除人员确认框

4.2.3.6　搜索群组人员

在人员列表搜索框中，输入人员名称（全称或者部分名称，支持模糊查询），单击后面的放大镜图标，开始搜索符合条件的人员，并将符合条件的人员显示出来，如图 4-68 所示。

图 4-68　搜索群组人员

提示：

① 人员搜索支持模糊查询。例如：输入“t”、“te”、”tes”都可搜索出人员“test”，或者与之相关的人员。

② 输入群组名称关键字，可搜索出相关的群组；输入计算机名称关键字，可搜索出相关的计算机。他们的操作方法和人员搜索方法一样，不在叙述。

4.2.3.7　添加群组计算机

（1）在群组列表中，选择某个群组，单击计算机列表区的“添加”按钮；或者单击计算机列表区鼠标右键，选择右键菜单“添加”，如图 4-69 所示。

图 4-69　添加人员到群组选项

（2）在弹出的“添加计算机到群组”界面中，选择一个或多个计算机，单击“确定”按钮，添加到选定的群组中，如图 4-70 所示。

每个计算机只能属于一个群组，如果指定的计算机已经属于别的群组，将被强制拖动到本群组中。如果勾选了“同时将指定计算机下的所有人员添加到该群组中”，则对应的人员也将被强制拖动到该群组中。

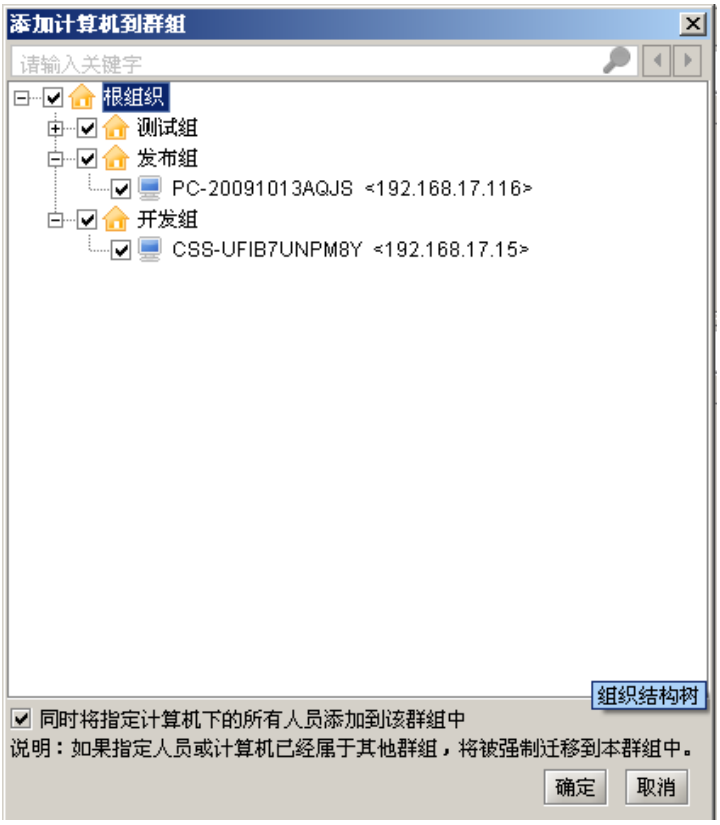


图 4-70　选择计算机添加到群组

（3）返回到群组管理页面，在计算机列表中，将看到刚添加的计算机，如图 4-71 所示。

图 4-71　群组中新增的计算机

4.2.3.8　删除群组中计算机

（1）在群组的计算机列表中，选择一个或多个计算机（多个人员使用 SHIFT/CTRL 键+鼠标左键单击选中），然后单击计算机列表区中“移除”按钮，或者单击鼠标右键菜单“移除”，如图 4-72 所示。

图 4-72　移除计算机选项

（2）在弹出的移除计算机确认框中，如图 4-73 所示。单击“确定”按扭后，既可将选定的计算机从群组中删除。如果要同时移除选定计算机下所有注册的人员，必须勾选选项“同时移除选中计算机下所有注册的人员”，这样单击“确定”按钮后，才能连同所注册的人员，一起从群组中删除。

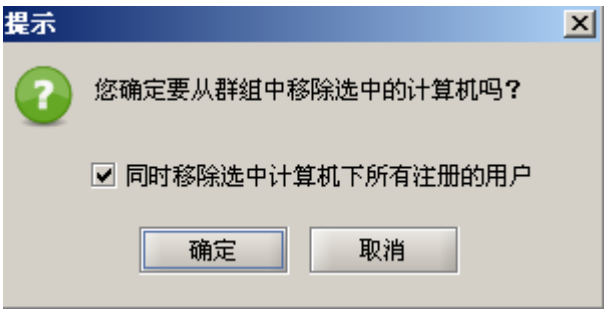


图 4-73　移除计算机确认框

4.2.4 删除用户管理

（1）在人员管理的组织结构图中，选择要删除的未注册用户，单击右键菜单“删除”，系统弹出提示框，确定后，可以将该用户临时删除，如图 4-74 所示。用户临时删除后,在组织结构中显示图标为 。

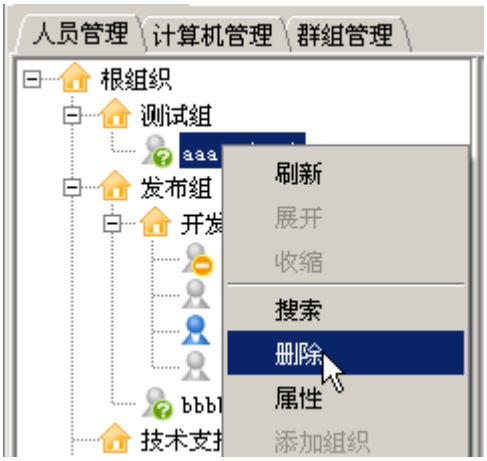


图 4-74　删除用户

（2）以有审核权限的管理员登录控制台（默认是 security 用户）。在删除用户管理界面中，可以看到刚删除的用户，如图 4-75 所示。

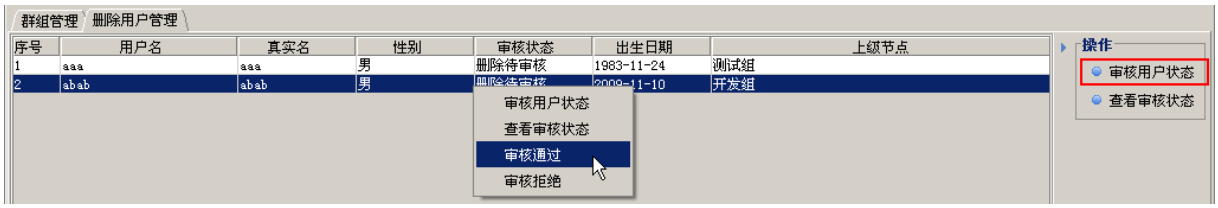


图 4-75　被临时删除的用户

（3）单击右键菜单“审核通过”，或者单击“审核用户状态”，进入用户信息界面，选择审核通过，如图 4-76 所示。审核通过后，该用户在组织结构中显示为 。如果选择审核拒绝，该用户恢复到原来状态。

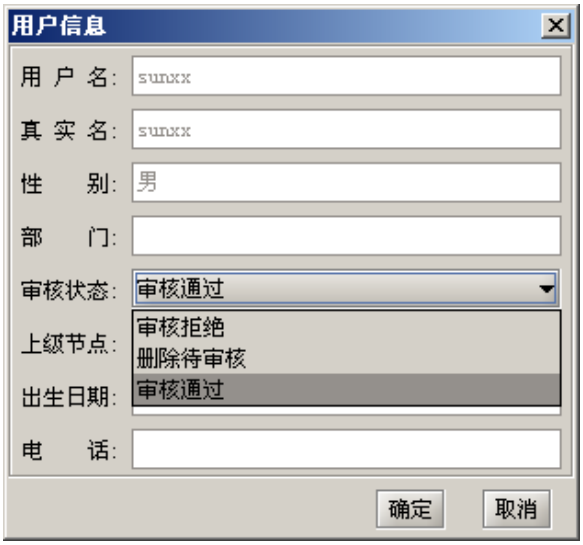


图 4-76　审核删除的用户

（4）再以管理员用户（默认 admin）登录控制台，单击组织结构树左下角的下拉框，选择显示用户的种类，查看已删除的用户，如图 4-77 所示。如果选择的是普通用户，那么被删除的用户将被过滤掉，在组织结构树上不显示。

图 4-77　显示用户种类选择

4.2.5 计算机离线情况

（1）在人员与计算机视图中，单击“计算机离线情况”标签页（受权限控制），进入计算机离线情况查询界面。输入查询条件：最近未上线时间（常用时间和自定义时间）、计算机名、起始计算机 IP、截止计算机 IP 和计算机所属组织名，单击“查询”按钮，展示当前所有客户端最后一次上线时间的统计列表，如图 4-78 所示。

提示：列表中展示的是当前存在的客户端最后上线时间，已正常卸载的客户端不展示。

图 4-78　显示客户端最后一次上线时间

（2）在未上线的客户端详情列表中，选择一行或多行信息，单击“强制删除”按钮，或者右键菜单“强制删除”，可以强制删除指定客户端的相关数据，如图 4-79 所示。

强制删除一般用于清理已实施本地卸载或客户端代理程序已被破坏的计算机，执行该操作将直接删除系统中指定计算机上所有的用户注册信息以及计算机属性，但不会卸载指定计算机上的客户端代理程序。

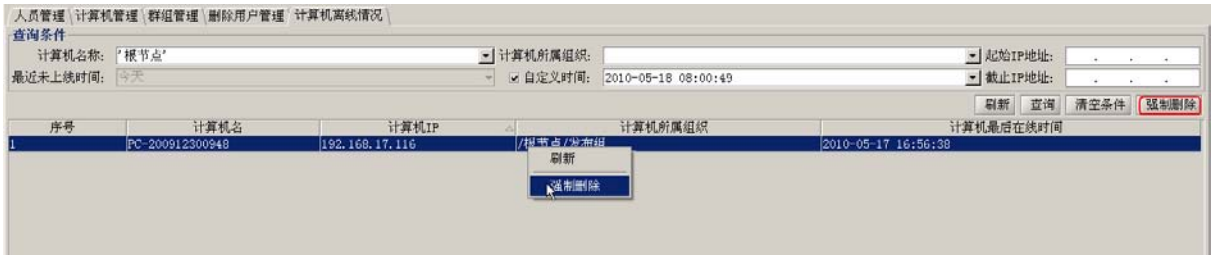


图 4-79　强制删除长时间未上次的客户端

4.2.6 客户端健康检查情况

客户端每次重启时，都要对自己的健康情况做检查，如果发现自身文件被破坏，尝试自动修复，并将检查结果上传服务器，通过控制台“客户端健康检查情况”展示。

在人员与计算机视图中，单击“客户端健康检查情况”标签页，输入查询条件，单击“查询”按钮，展示客户端健康检查情况及修复结果，如图 4-80 所示。

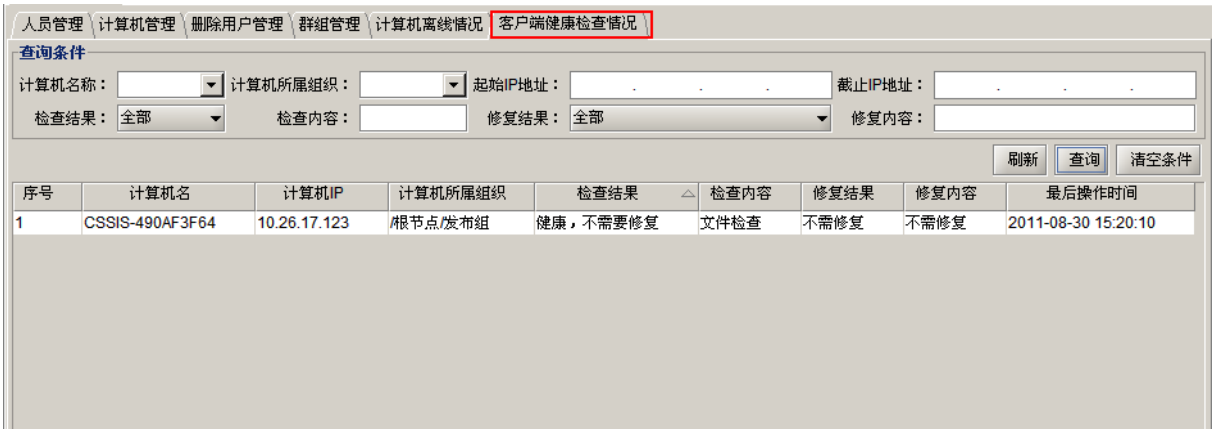


图 4-80　客户端健康检查情况

4.3 角色与权限

在组织结构管理中，单击“角色与权限”选项卡，进入“角色管理”和“用户管理”界面。用户根据自己的需要设置相应角色和权限，实现分级分权管理。

4.3.1 角色管理

角色管理是设置、修改、删除、审核及查看角色的具体权限。系统内置的角色有四个：管理员、安全官、审计员、操作员。单击“角色与权限”→“角色管理”，进入角色管理界面，在角色列表中可以查看他们的具体权限，如图 4-81 所示。

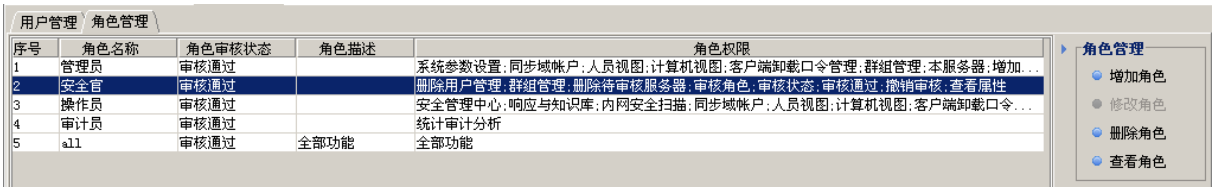


图 4-81　角色和权限管理界面

例如：系统内置的安全官主要负责删除用户管理、审核角色、审核用户状态和解除用户锁定工作，如果用户对此规定不满意，完全可以自己添加一个安全官角色，重新规定他的权限。

4.3.1.1 增加角色

（1）在“角色管理”中，单击“增加角色”选项，进入“增加角色”界面。输入角色名称、角色描述，并勾选角色权限，最后单击“确定”按钮，如图 4-82 所示。

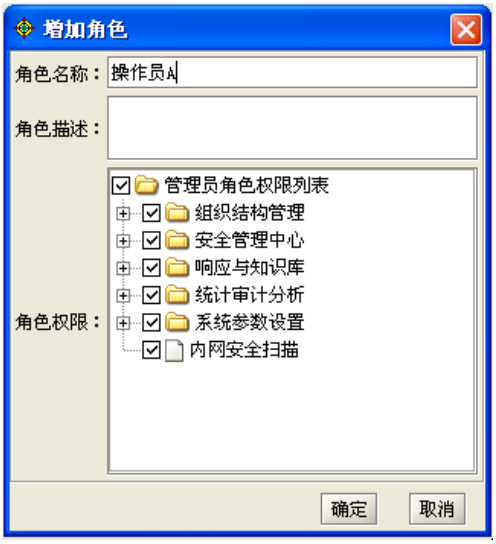


图 4-82　增加角色

（2）在角色列表中，可以看到刚添加的角色，如图 4-83 所示。

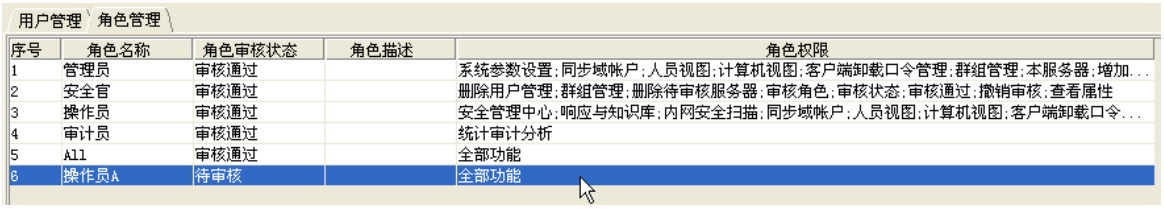


图 4-83　用户角色列表

提示：新建的角色要经过审核，未审核的角色不起作用。

4.3.1.2 修改角色

在角色列表中选择要修改的角色，单击鼠标右键菜单的“修改角色”，或者单击角色管理中“修改角色”，都可进入修改角色界面。修改角色描述，重新勾选角色权限，最后，单击“确定”按钮即可，如图 4-84、4-85 所示。

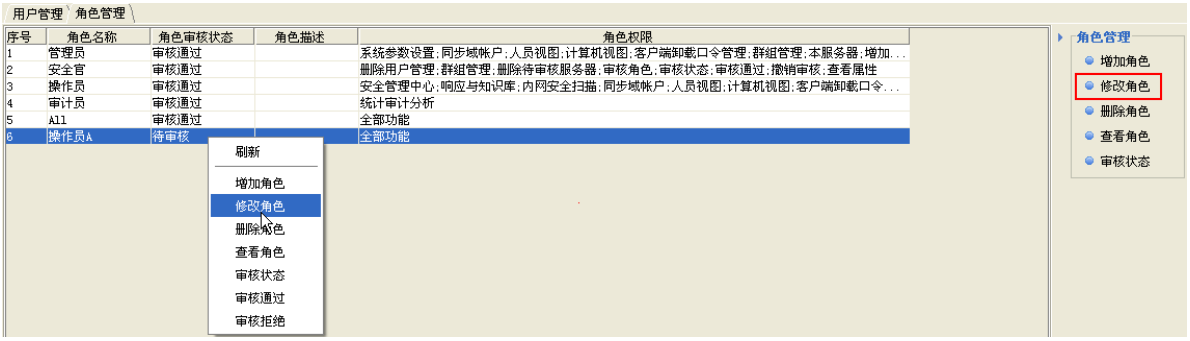


图 4-84　修改角色

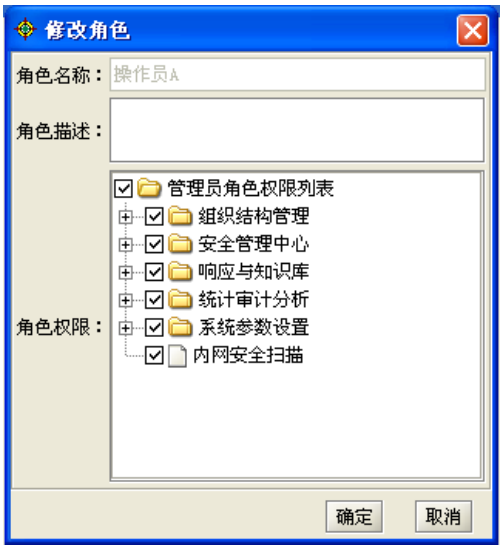


图 4-85　选择角色修改

修改角色完成后，该角色的审核状态更改为“待审核”，同时该角色下的所有管理员的审核状态也更改为“待审核”。如需使用该角色和该角色下的管理员，需要有审核权限的管理员进行审核。

审核通过后即可使用新角色；如果审核被拒绝，那么该角色的权限恢复至审核前状态，该角色下的管理员也恢复至角色审核前状态。

提示：不能修改内置角色。修改日志可以在“统计审计分析→日志信息统计→控制台操作日志”中查看

4.3.1.3 删除角色

在角色列表中，选择要删除的角色，单击鼠标右键菜单的“删除角色”，或者单击角色管理中“删除角色”，都可执行“删除”操作。

如果要删除系统内置的角色，或者要删除的角色正被用户使用，系统将弹出提示框，如图 4-86、4-87 所示。

图 4-86　删除内置角色消息框

图 4-87　删除正在使用角色消息

4.3.1.4 查看角色

在角色列表中，选择要查看的角色，单击鼠标右键，选择“查看角色”菜单项（或者单击操作列表中“查看角色”），可以查看角色属性，但不能修改，如图 4-88 所示。

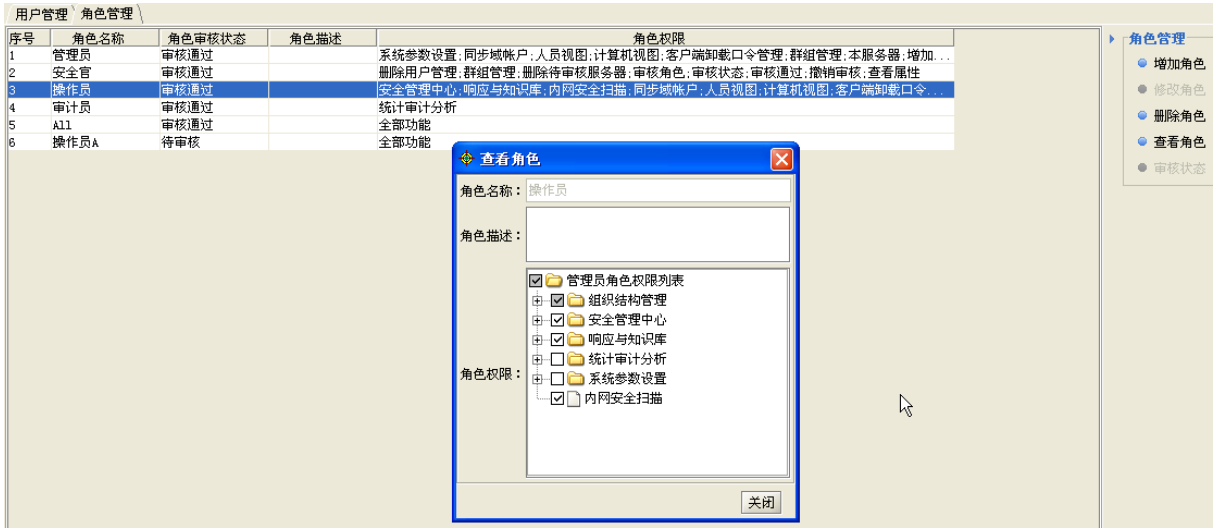


图 4-88　查看角色属性

4.3.1.5 审核角色

（1）以有审核权限的用户登录控制台（默认 security），在角色列表中选择未审核的角色，单击右侧操作列表中的“审核状态”，如图 4-89 所示。也可单击鼠标右键菜单的“审核通过”或“审核拒绝”，直接进行审批，如图 4-90 所示。

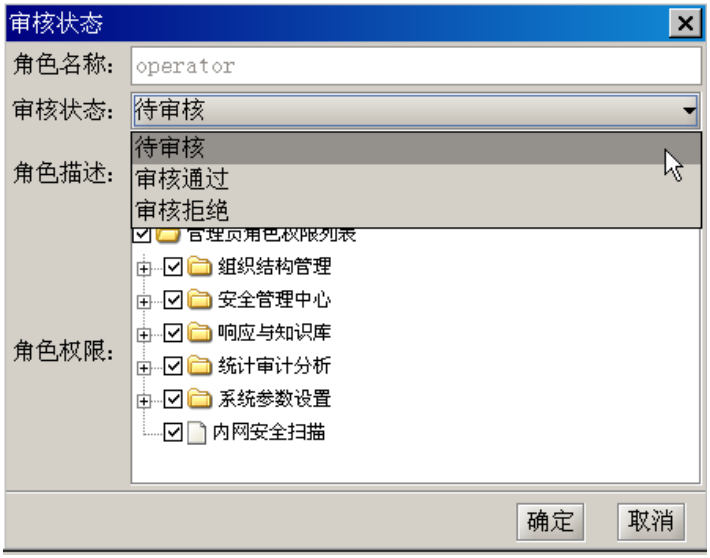


图 4-89　审核角色状态

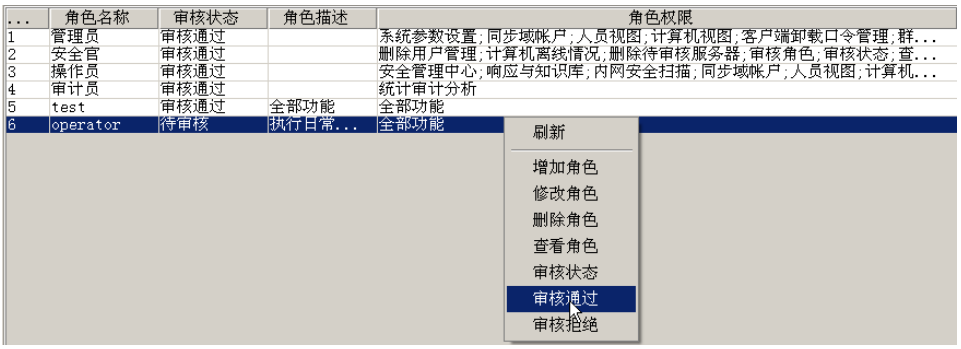


图 4-90　审核角色状态

（2）审核通过后，在角色列表的用户审核状态中，可看到审核通过，如图 4-91 所示。审核通过后的角色可以正常使用。

用户管理　角色管理

...	角色名称	审核状态	角色描述	角色权限
1	管理员	审核通过		系统参数设置;同步域帐户;人员视图;计算机视图;客户端卸载口令管理;群...
2	安全官	审核通过		删除用户管理;计算机离线情况;删除待审核服务器;审核角色;审核状态;查...
3	操作员	审核通过		安全管理中心;响应与知识库;内网安全扫描;同步域帐户;人员视图;计算机...
4	审计员	审核通过		统计审计分析
5	test	审核通过	全部功能	全部功能
6	operator	审核通过	执行日常...	全部功能

图 4-91　角色列表视图

4.3.1.6 导出角色

在角色列表中，单击右键菜单“导出角色”，或者单击右侧操作列表中的“导出角色”，可以将当前整个角色列表导出，保存为*.xls、*. pdf、*.html 文件，如图 4-92 所示。

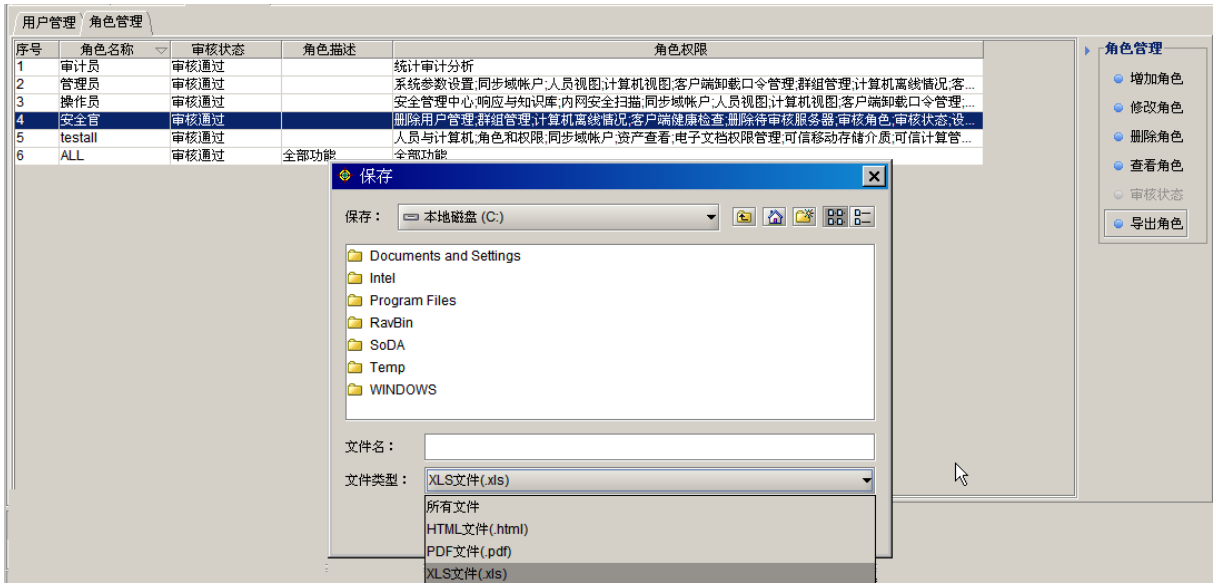


图 4-92　导出角色

4.3.2 用户管理

用户管理是针对管理员用户的操作，包括增加用户、修改用户、删除用户、修改密码、查看用户、解除锁定、审核用户状态等。

4.3.2.1 增加用户

（1）以管理员用户(默认 admin)登录，单击“组织结构管理”→“角色与权限”→“用户管理”，进入用户管理界面，如图 4-93 所示。

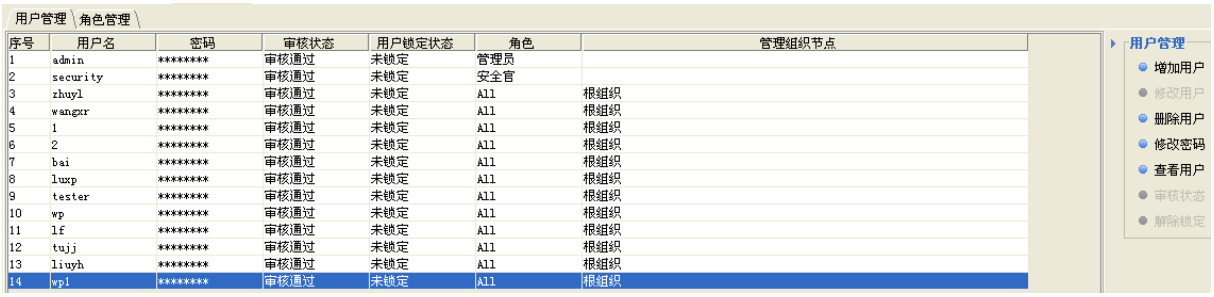


图 4-93　用户管理界面

（2）在“用户管理”页面中，单击右侧操作列表“增加用户”菜单项，进入“增加用户”界面，如图 4-94 所示。输入帐户名、密码，在下拉框中选择角色，并勾选管理组织节点，最后单击“确定”按钮。

提示：（1）以 admin 用户登录，能够看到所有用户；以其它用户身份登录只能看到它管理范围内的下级用户；（2）用户可以根据需要添加多个用户，用户需审核通过才能正常使用。

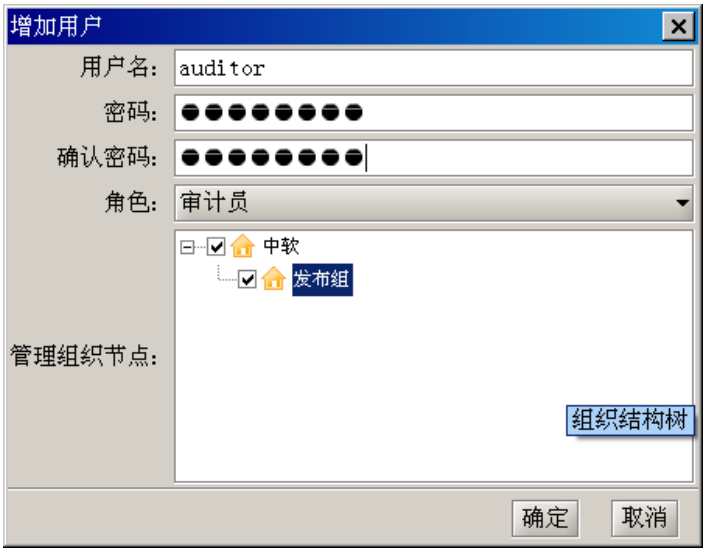


图 4-94　增加新用户

（3）在用户列表视图中，可以看到刚添加的用户，如图 4-95 所示。新增的用户没有经过审核不能使用，但可以修改。

...	用户名	审核状态	是否锁定	角色	关联KEY	登录验...	管理组织节点
1	admin	审核通过	未锁定	管理员		任意	
2	security	审核通过	未锁定	安全官		任意	
3	test	审核通过	未锁定	test		任意	中软
4	auditor	待审核	未锁定	审计员		任意	中软

图 4-95　用户列表显示增加用户

4.3.2.2 修改用户

在用户列表中选择要修改的用户，单击鼠标右键，选择“修改用户”菜单项，或者单击右侧操作列表中“用户管理”菜单，都可以进入修改用户界面。重新选择角色，勾选管理范围后，单击“确定”退出，如图 4-96、4-97 所示。

修改用户完成后，该管理员的审核状态更改为“未审核”。如需使用该用户，需要对该用户进行审核。审核通过后，该用户可使用；如果审核被拒绝，用户恢复至原来的状态。

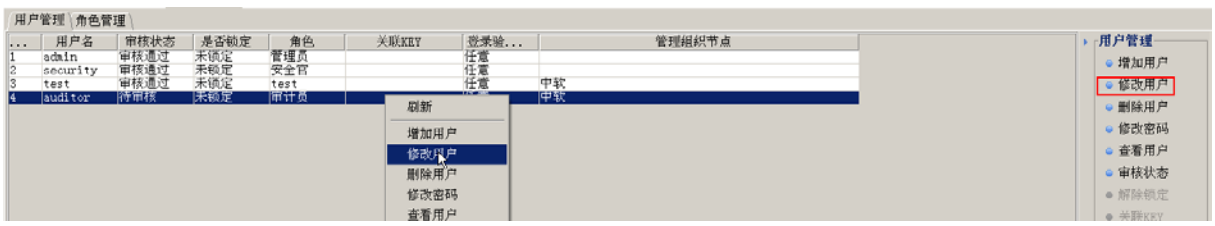


图 4-96　选择修改用户

提示：不能修改内置用户。修改日志可以在“统计审计分析→日志信息统计→控制台操作日志”中查看。

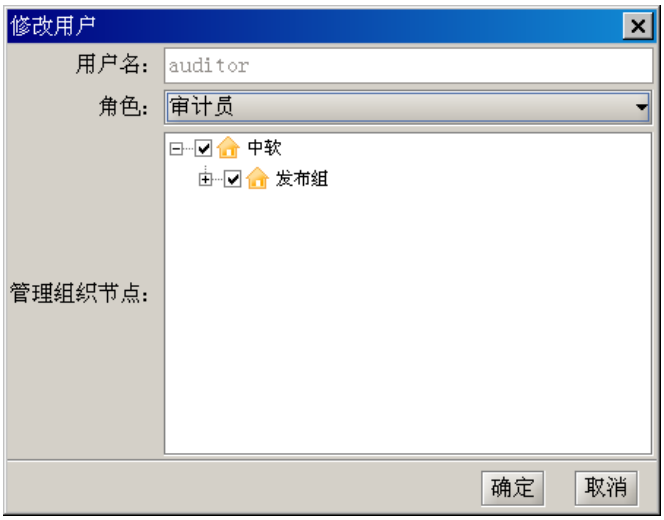


图 4-97　修改用户界面

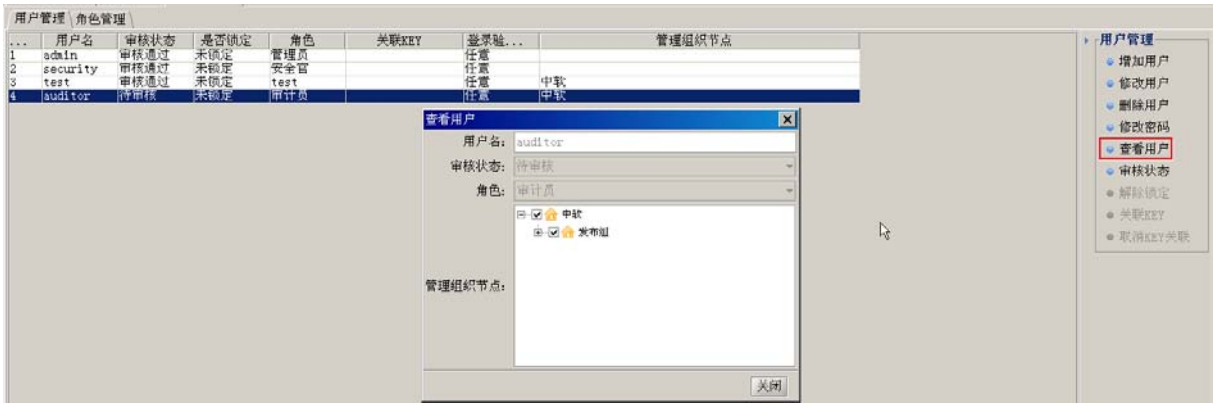
4.3.2.3 删除用户

在用户列表中，选择要删除的用户，单击鼠标右键菜单的“删除用户”，或者单击右侧操作列表中“删除用户”菜单，都可执行“删除”操作。但系统内置帐号不能删除，例如：security 和 admin.

4.3.2.4 查看用户

在用户列表中，选择要查看的用户，双击鼠标或者单击用户管理中“查看用户”，都可进行用户的查看，如图 4-98 所示。

提示：这里只能进行用户查看，不能进行修改。



4-98　查看用户

4.3.2.5 重置密码

如果某个管理员忘记了密码，再也无法找回密码，这时，其它具有重置密码功能的管理员可以登录控制台，将忘记密码的管理员重置密码。重置过程不需要输入原密码，只需要输入新密码，被重置密码的管理员重新登录后，可以通过修改密码功能，重新设置自己的密码。

在用户列表中，选择要重置密码的用户，单击鼠标右键菜单的“重置密码”，或者单击右侧操作列表中“重置密码”菜单，进入重置密码界面。输入新密码和确认密码后，单击“确定”按钮既可完成，如图 4-99 所示。

提示：可重置内置管理员密码，密码长度至少 8 位以上，不能超过 50 位，由字母、数字或符号组合而成。

图 4-99　修改密码

4.3.2.6 审核用户状态

新建用户需经审核才可使用，下面是审核过程。

（1）以有审核权限的管理员用户登录控制台（系统默认为 security 用户），在用户列表中，选择未审核的用户，单击右键菜单“审核通过”，如图 4-100。也可单击右侧操作列表中“审核状态”，从下拉框选择“审核通过”或“审核拒绝”。

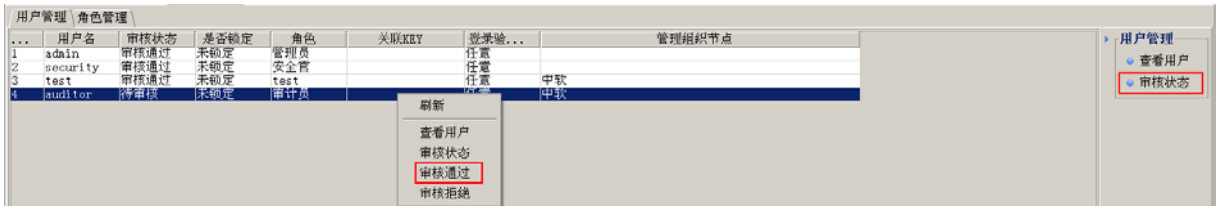
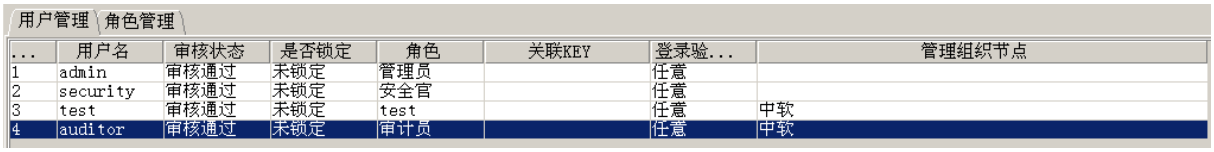


图 4-100　审核用户状态

（2）审核通过后，在用户列表的“审核状态”栏中，看到“审核通过”字样，如图 4-101 所示。审核通过后的用户可以正常使用。



...	用户名	审核状态	是否锁定	角色	关联KEY	登录验...	管理组织节点
1	admin	审核通过	未锁定	管理员		任意	
2	security	审核通过	未锁定	安全官		任意	
3	test	审核通过	未锁定	test		任意	中软
4	auditor	审核通过	未锁定	审计员		任意	中软

图 4-101　审核用户通过

4.3.2.7 关联 KEY

（1）将 KEY 插入到控制台上。在用户列表中，选择已审核通过的用户，单击右键菜单“关联 KEY”，或者单击右侧列表中的“关联 KEY”命令项，出现设置 KEY 用户界面，如图 4-102 所示。

选择设备类型，都能将该控制台的用户与某个 Key 关联起来。如果本用户已经关联了另外一个 key，则可以将其关联关系修改到新的 key 上。

图 4-102　关联 KEY 用户

（2）在“设置 KEY 用户”界面中，选择设备类型，单击“刷新”按钮，出现 KEY 列表和 KEY 序列号，如图 4-103 所示。设置该关联关系时，还可以设置该用户的登录方式，可以是普通方式和 KEY 都能登录，也可以是“只能通过 KEY 身份验证登陆”。只允许使用 key 登录的话，这种用户不能使用 web 控制台。

参见控制台登录章节

图 4-103　设置 KEY 用户

（3）最后，单击“确定”按钮，将该控制台的用户与 KEY 关联起来。如果本用户已经关联了另外一个 KEY，则可以将其关联关系修改到新的 KEY 上。

4.3.2.8 取消 KEY 关联

在用户列表中，选择已建立 KEY 关联的用户，单击右键菜单“取消 KEY 关联”，或者单击右侧列表中的“取消 KEY 关联”命令项，出现确认提示框。确定后即可取消该用户和 KEY 的关联关系，如图 4-104、4-105 所示。

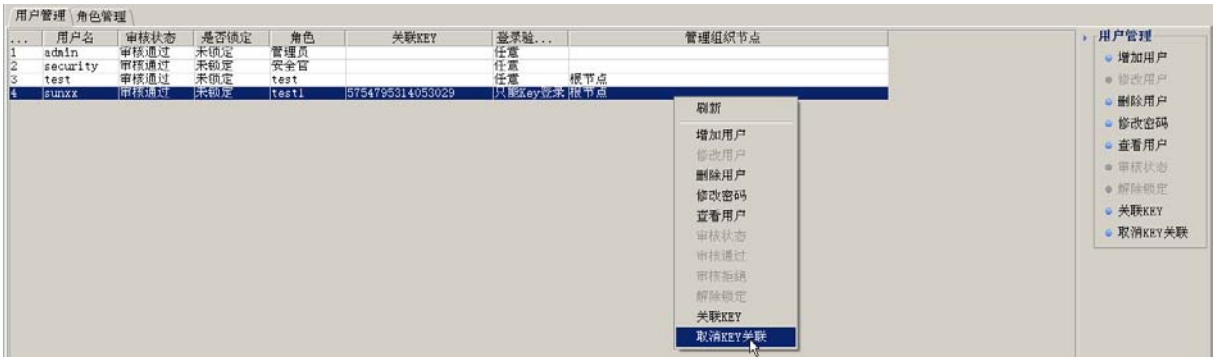


图 4-104　选择用户取消 KEY 关联

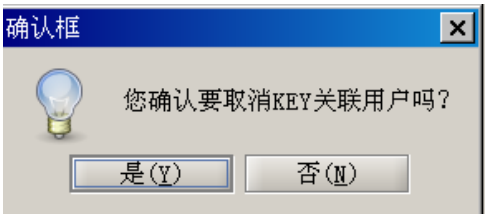


图 4-105　取消 KEY 关联确认框

4.3.2.9 解除锁定

登录控制台时，若用户尝试的密码次数超过了系统规定的最大次数，该用户将被锁定。这时可以管理员角色的用户（默认 admin）登录控制台，在用户列表中选定被锁定的用户，单击右键菜单“解除锁定”，或者从右则操作列表选中“解除锁定”菜单，都解除被锁定的帐户，如图 4-106 所示。

参见帐户安全设置和控制台使用控制章节

图 4-106　解除锁定的帐号

4.3.2.10　导出用户

在用户列表中，单击右键菜单“导出用户”，或者单击右侧操作列表中的“导出用户”，可以将当前整个用户列表导出，保存为*.xls、*. pdf、*.html 文件，如图 4-107 所示。

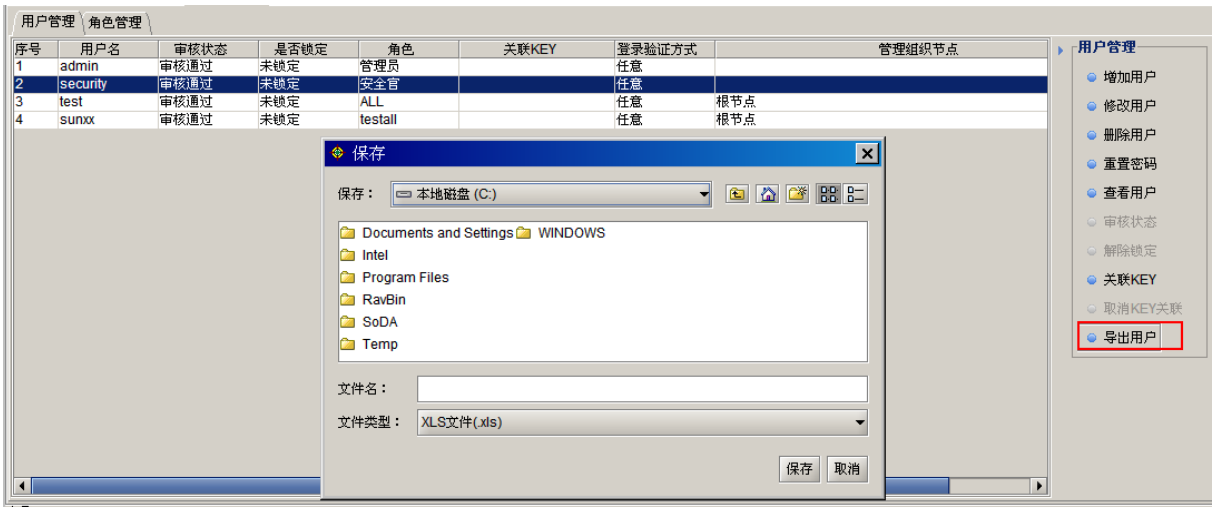


图 4-107　导出用户

4.3.3　举例说明

为了帮助用户更好的理解“角色与权限”这部分内容，下面举例说明如何建立一个最高权限的用户。

◆ **增加角色**

1. 以默认的 admin 用户登录，进入角色管理界面，如图 4-108 所示。

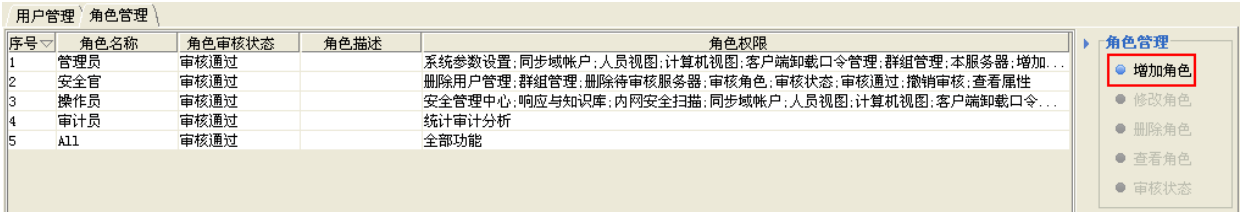


图 4-108　角色管理

2. 单击“增加角色”，进入“增加角色”界面。添加一个名称为“超级用户”，具有全部角色权限的用户，如图 4-109 所示。

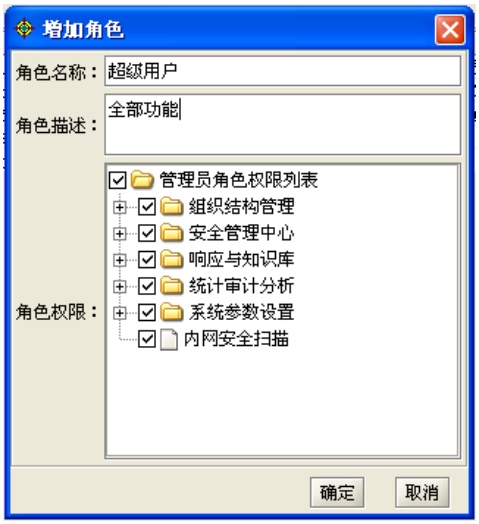


图 4-109　增加角色

3. 在角色列表中可以看到刚添加的角色“超级用户”，如图 4-110 所示。但此角色未经审核不能使用，后面进行角色审核。

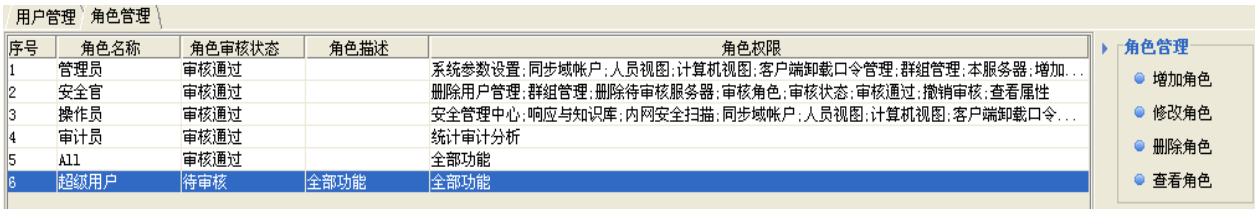


图 4-110　角色列表

◆ 审核状态

1. 以默认的 security 用户登录，进入角色管理界面，如图 4-111 所示。

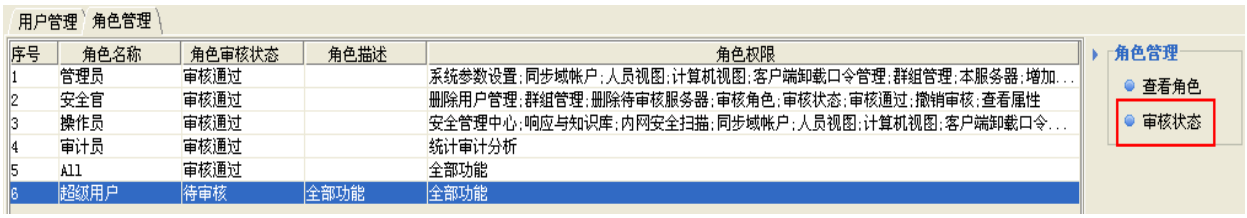


图 4-111　角色管理

2．选择未审核的角色“超级用户”，单击“审核角色”，进入“审核状态”界面，如图 4-112 所示。单击“审核状态”右面的下拉框，选择“审核通过”，然后“确定”即可。经过审核的角色，在角色列表中显示为“审核通过”，用户可以查看。

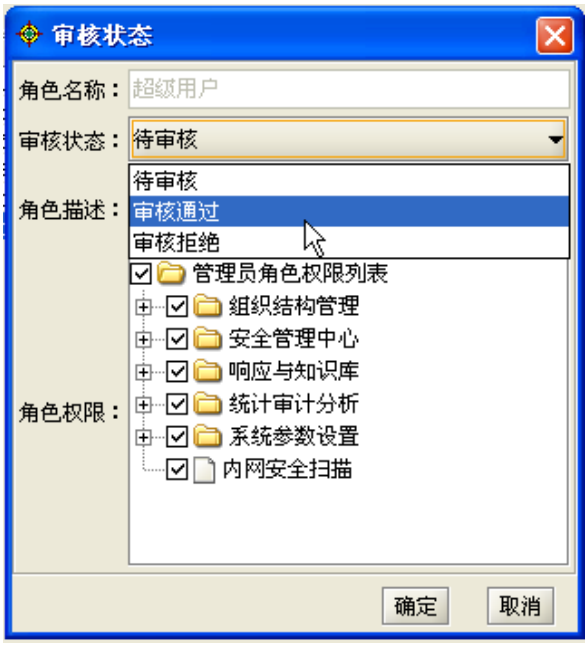


图 4-112　审核角色

◆ **增加用户**

1．以默认的 admin 用户登录，进入用户管理界面，如图 4-113 所示。

图 4-113　用户管理

2．单击“增加用户”，进入“增加用户”界面。添加一个“测试”用户，选择前面建立的角色“超级用户”，管理所有组织节点，如图 4-114 所示。

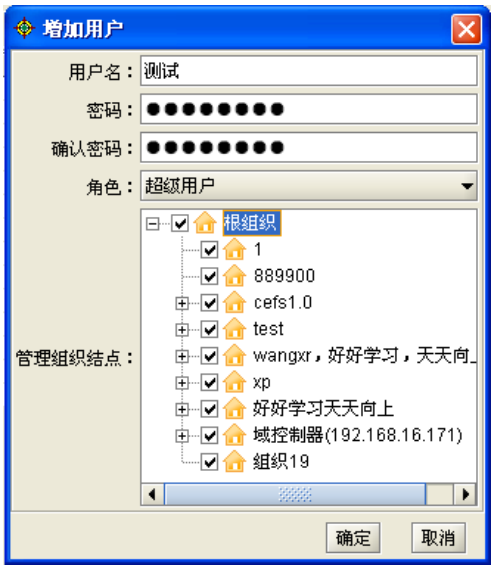


图 4-114　增加用户

3. 在用户列表中可以看到刚添加的用户“测试”，如图 4-115 所示。但此用户未经审核不能使用，下面进行用户审核。

序号	用户名	密码	审核状态	用户锁定状态	角色	管理组织节点
1	admin	********	审核通过	未锁定	管理员	
2	security	********	审核通过	未锁定	安全官	
3	zhuyl	********	审核通过	未锁定	All	根组织
4	wangxr	********	审核通过	未锁定	All	根组织
5	1	********	审核通过	未锁定	All	根组织
6	2	********	审核通过	未锁定	All	根组织
7	bai	********	审核通过	未锁定	All	根组织
8	luxp	********	审核通过	未锁定	All	根组织
9	tester	********	审核通过	未锁定	All	根组织
10	wp	********	审核通过	未锁定	All	根组织
11	lf	********	审核通过	未锁定	All	根组织
12	tujj	********	审核通过	未锁定	All	根组织
13	liuyh	********	审核通过	未锁定	All	根组织
14	wp1	********	审核通过	未锁定	All	根组织
15	测试	********	待审核	未锁定	超级用户	根组织

图 4-115　用户列表

◆　**审核用户**

1．以默认的 security 用户登录，进入用户管理界面，如图 4-116 所示。选择要审核的用户“测试”，点击“审核状态”。

序号	用户名	密码	审核状态	用户锁定状态	角色	管理组织节点
1	admin	********	审核通过	未锁定	管理员	
2	security	********	审核通过	未锁定	安全官	
3	zhuyl	********	审核通过	未锁定	All	根组织
4	wangxr	********	审核通过	未锁定	All	根组织
5	1	********	审核通过	未锁定	All	根组织
6	2	********	审核通过	未锁定	All	根组织
7	bai	********	审核通过	未锁定	All	根组织
8	luxp	********	审核通过	未锁定	All	根组织
9	tester	********	审核通过	未锁定	All	根组织
10	wp	********	审核通过	未锁定	All	根组织
11	lf	********	审核通过	未锁定	All	根组织
12	tujj	********	审核通过	未锁定	All	根组织
13	liuyh	********	审核通过	未锁定	All	根组织
14	wp1	********	审核通过	未锁定	All	根组织
15	测试	********	待审核	未锁定	超级用户	根组织

图 4-116　　用户管理

2．在“审核状态”界面中，通过下拉框选择审核通过。然后，点击“确定”按钮，如图 4-117 所示。新建的用户“测试”审核通过后，即可使用。

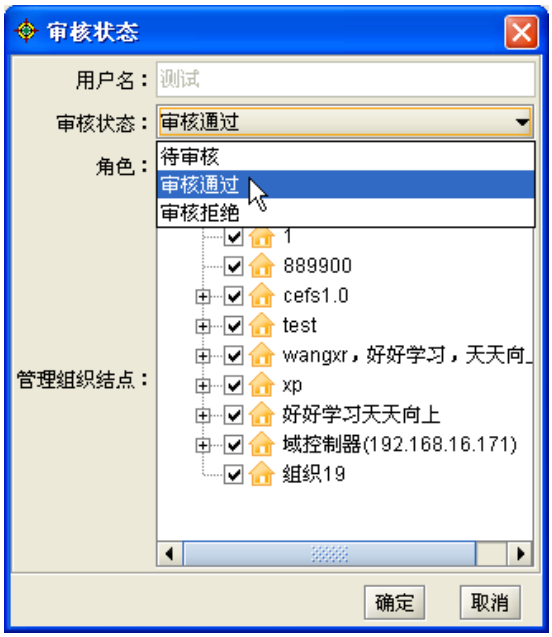


图 4-117　审核用户状态

3．以“测试”用户身份登陆，将看到控制台的全部功能，并能管理全域下的所有组织节点。

注意：本手册为叙述方便，大部分截图是在最高权限用户下截图的，可能与用户的实际界面有所不同。

第五章　安全管理中心

安全管理中心是控制台工作核心，对组织结构进行有效的管理和控制。包括：失泄密防护策略、主机安全策略、安全文档策略、可信策略、远程管理、软件分发、补丁管理、资产查看、可信授权，不同的授权功能模块也可能有所不同。

5.1 界面介绍

我们以操作员用户登录中软统一终端安全管理系统 8.0 控制台，进入安全管理中心，显示界面如图 5-1 所示。控制台采用单文档-多视图结构设计，大体由六部分组成：

1. 菜单栏　**2.** 工具条　**3.** 组织结构　**4.** 信息显示窗　**5.** 策略树　6. 系统状态区

注意：不同的用户登陆控制台界面会有所差异，具体的用户界面取决于您所购买的产品授权许可证和当前用户权限范围。

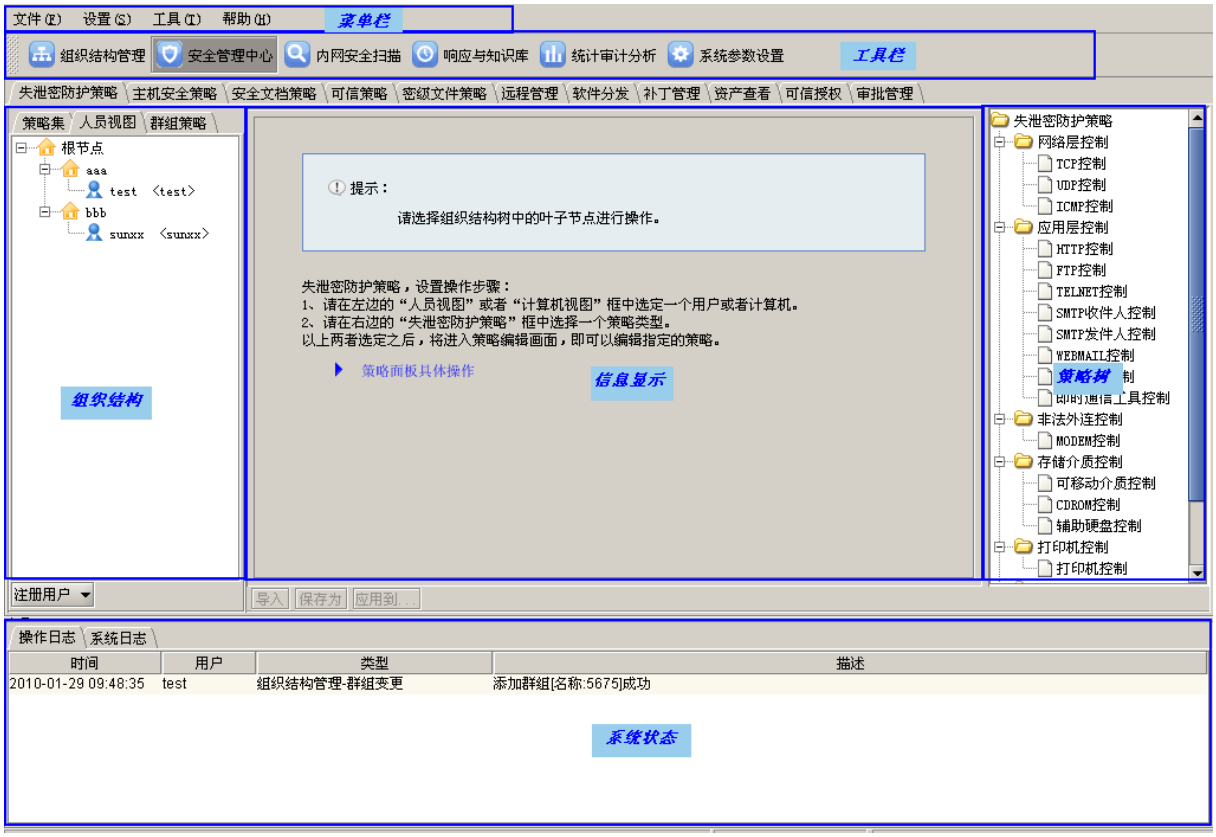


图 5-1　控制台操作界面

- **菜单栏**：包括文件、设置、工具和帮助四项。主要提供切换用户、修改密码、同步域帐户、修改个人信息、组织结构信息统计、客户端卸载口令管理、帮助和查看授权信息等功能。
- **工具条**：包括组织结构管理、安全管理中心、内网安全扫描、响应与知识库、统计审计分析和系统参数设置。用户选择不同的工具条，显示的界面会有所不同。
- **组织结构**：显示控制台现有的组织结构和策略集。通过下方的过滤按钮，可以查看注册用户、在线用户和离线用户以及注册主机、在线主机和离线主机等信息。
- **信息显示窗**：提示操作信息，显示所选人员或计算机的具体策略。
- **策略树**：显示失泄密防护策略、主机安全策略、可信策略、远程管理、资产查看的具体项。通过各项策略的制定和下发，对客户端实施全方位控制和管理。
- **系统状态区**：显示控制台操作日志和系统日志。点击“操作日志”左上方的上、下小箭头  可以展开或伸缩系统状态区。

5.2 策略定义

中软统一终端安全管理系统 8.0 通过策略设置实现对终端用户的行为管理和失泄密防护。该系统的策略指客户端控制规则的集合。策略的修改、添加、删除、应用都由控制台实施，通过服务器下发至客户端。客户端在该策略的有效时间段内依据策略执行安全控制。形象地说，策略就是服务器下达给客户端的控制指令集，控制台可以制订一些策略并使之在客户端起作用。安全管理系统策略分**默认策略**、**在线策略**和**离线策略**三种：

默认策略是针对新注册的计算机或者用户，在管理员没有给其特别设置策略的情况下，由系统默认执行的一套策略。该策略在计算机或用户第一次上线时，由客户端从服务器获取并执行。

在线策略是客户端主机和服务器通讯正常情况下运行的有效策略集，它通过控制台配置、修改下发。在线策略可分为两类：基本策略和时间段策略。主机在线的情况下，默认会执行基本策略；如果管理员设定了时间段策略，则在生效的时间段内优先执行时间段策略。基本策略是管理员必须配置的策略，时间段策略依据需求，可以配置也可以不配置。

离线策略是客户端的备用策略，由控制台配置并下发，正常情况下不会生效。当客户端一旦与服务器之间的网络通讯断开了，则立即启用离线策略。通常离线策略相当严格，以保护客户端主机的安全。

5.3 策略集

为方便策略的应用，增加以策略为对象的策略编辑和应用模式，即策略集，并将所有设置好的策略集放置在策略集列表中统一管理。管理员可以针对不同的用户身份，设置不同的策略集，也可以针对不同的部门设定不同的策略集。

在控制台中的“失泄密防护策略”、“主机安全策略”、“安全文档策略”及“可信策略”策略集中，均增加相应策略集的管理，包括策略集的增加、删除、修改、导入、导出、应用等。

5.3.1 策略集界面

以操作员（operator）身份登录控制台，单击“安全管理中心”→“失泄密防护策略”（或者主机安全策略、安全文档策略或可信策略）→“策略集”，进入策略集界面，如图 5-2 所示。

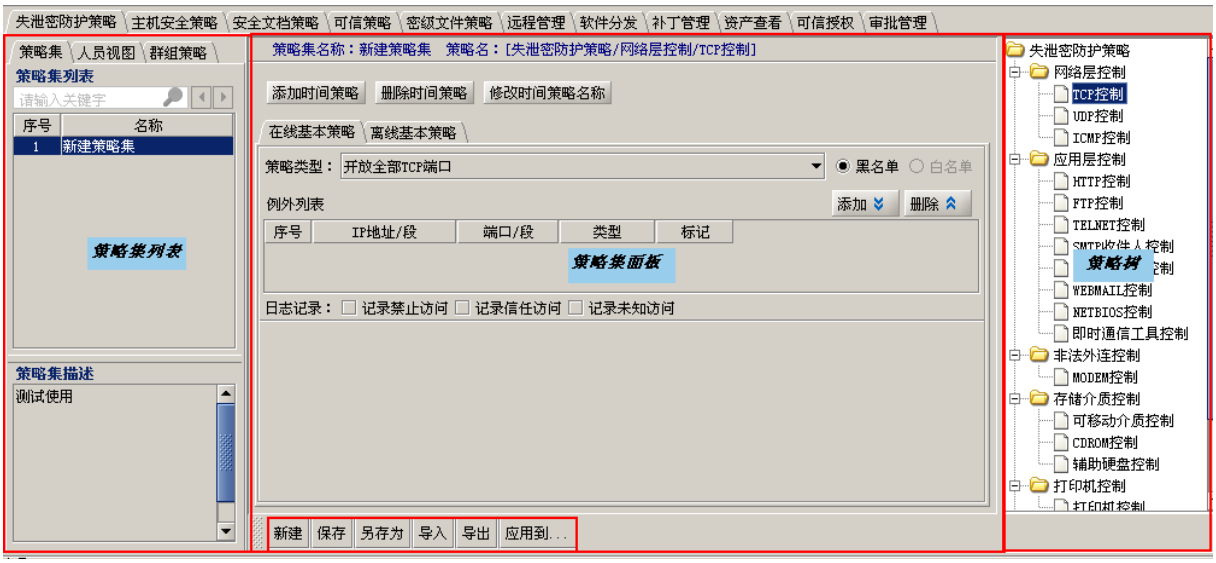


图 5-2　策略集界面

说明：

（1）左侧为系统现有策略集，以列表形式显示。

（2）中心为策略集面板，显示每项策略的具体内容。下方为策略集操作工具栏，包括“新建”、“保存”、“另存为”、“导出”、“导入”、“应用到...”按钮。

（3）右侧为策略树，显示具体策略项。

5.3.2 策略集使用方法

5.3.2.1 新建策略集

（1）在策略集界面上，单击策略集列表右键菜单，选择“新建”菜单项；或者单击工具栏“新建”按钮，都可进入新建策略集界面，如图 5-3 所示。

图 5-3　选择“新建”策略集

（2）在“新建策略集”界面中，输入策略集名称和描述信息，单击“确定”按钮，即可将新建策略集添加到策略集列表中，如图 5-4 所示。

图 5-4　新建策略集

（3）在策略集列表中，选中“新建策略集”，在右侧的策略树中选择策略项，在策略集面板中制定具体的策略。例如：我们选择 HTTP 控制策略项，添加禁止访问的黑名单，如图 5-5 所示。

提示：具体策略项的使用，后面有详细讲解，这里只做大致介绍。

图 5-5　编辑策略集内容

（4）设置好各个策略项后，单击工具栏“保存”按钮，或单击策略集右键菜单“保存”，都可将“新建策略集”保存，并弹出提示框，如图 5-6 所示。

图 5-6　保存策略集

5.3.2.2 修改策略集

（1）在策略集界面上，单击策略集列表右键菜单，选择“属性”菜单项。在属性框中，修改策略集名称和描述信息，例如：把“新建策略集”改为“测试策略集”，最后单击“确定”按钮，如图 5-7 所示。属性修改完成后，在策略集列表中显示更改后的名称。

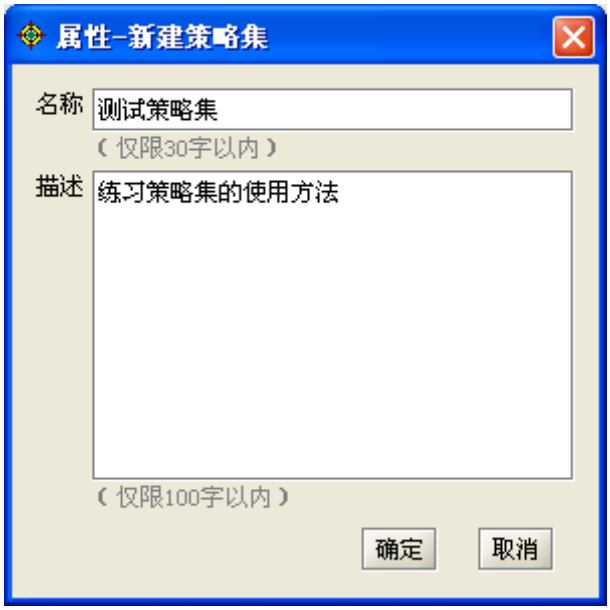


图 5-7　修改策略集属性

（2）在策略集列表中，选中“测试策略集”，然后选择右侧的策略项，重新进入编辑界面，在这里可以任意修改每个策略项内容，如图 5-8 所示。修改后的策略项，会以红色显亮表示。修改完成后，一定记住保存。如果没有保存，切换策略时会有提示。

图 5-8　修改策略集内容

5.3.2.3 应用策略集

在策略集列表中，选中已编辑好的策略集，单击工具栏中的“应用到...”按钮，弹出应用策略界面，如图 5-9 所示。

在左侧勾选要应用的策略项，支持部分策略下发；在右侧选择策略应用范围，具体到某个组织下的某个用户。最后，单击“确定”按钮，下发应用策略的命令。在控制台产生操作日志，记录应用的策略项及策略应用范围。

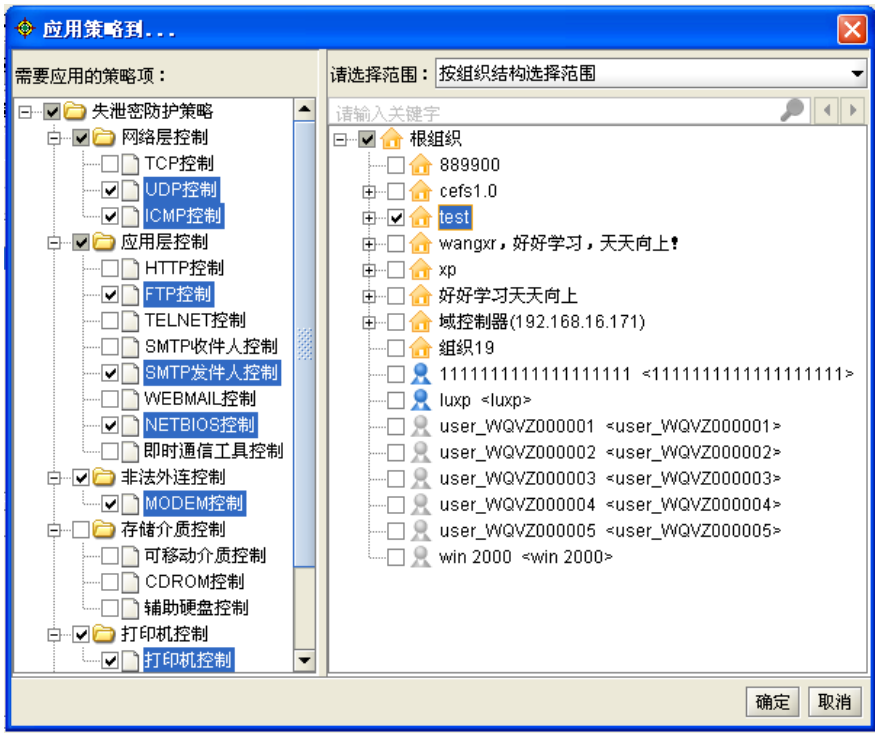


图 5-9　应用策略集

5.3.2.4 复制策略集

在策略集列表中，选中已编辑好的策略集，单击右键菜单“另存为”，或者单击工具栏中的“另存为”按钮，弹出另存策略界面，如图 5-10 所示。输入新的策略名称，单击“确定”退出。

利用这种方法，我们可以将现在策略集复制保存一份，然后在此基本上更改为新的策略集。

图 5-10　复制策略集

5.3.2.5 导出策略集

在策略集列表中选择某策略集，单击右键菜单“导出”，或者单击工具栏中的“导出”按钮，弹出导出策略界面，如图 5-11 所示。选择导出路径，输入文件名，单击“保存”按钮，即将选中的策略集以文件格式保存起来。

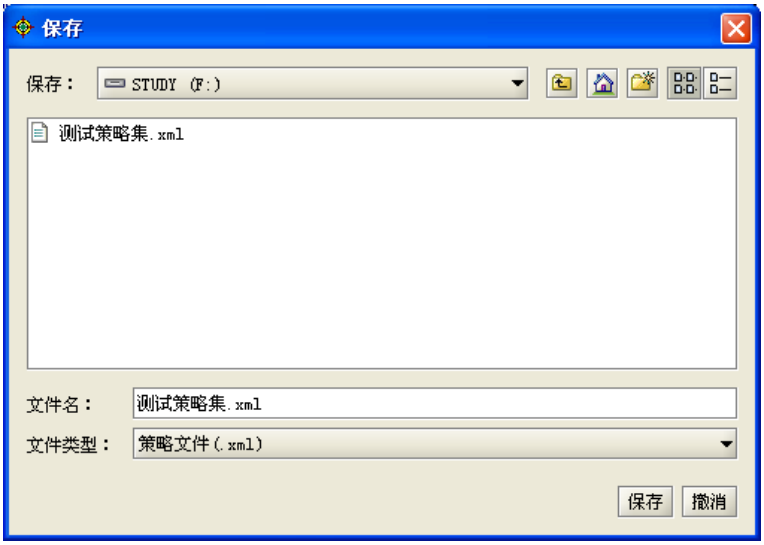


图 5-11　导出策略集

5.3.2.6 导入策略集

在策略集列表中选择某策略集，单击右键菜单“导入”，或者单击工具栏中的“导入”按钮，弹出导入策略界面，如图 5-12 所示。选择一个准备导入的 XML 文件，单击“打开”按钮。控制台会判断 XML 文件的合法性，并给出相应的提示，如果格式不对，会提示导入失败。导入成功后，更新选定的策略集内容。

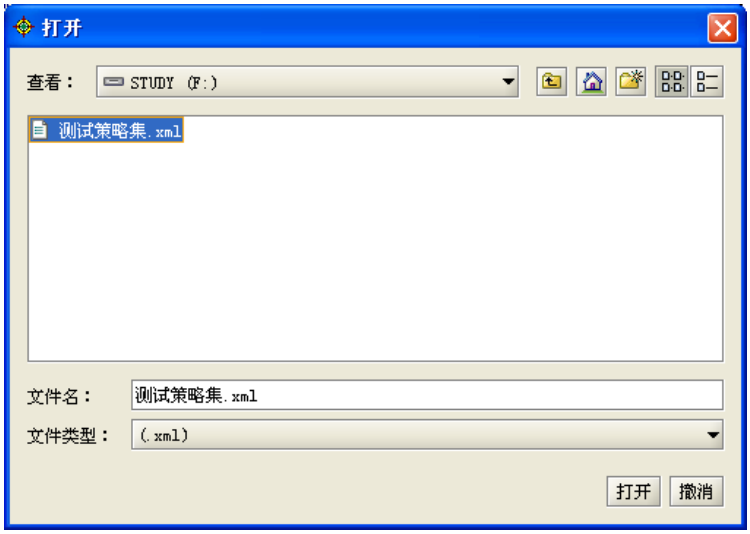


图 5-12　导入策略集

5.3.2.7 删除策略集

在策略集列表中选择某策略集，单击右键菜单“删除”，弹出删除确认框，如图 5-13 所示。确定后，既可将策略集删除。如果此策略集已应用下发，删除后不影响客户端策略。

图 5-13　删除策略集

5.4 群组策略

为了便于系统管理员制定和下发策略，我们将一些不同类型的人员和计算机归属于不同的群组，对不同的群组有针对性的制定下发不同的策略，大大提高管理效率。

在 4.2.3 群组管理中，我们已经学会了创建群组，向群组中添加人员和计算机。这节我们主要讲述群组策略的制定和下发，以及群组策略的导出和导入。

5.4.1　群组策略界面

以操作员（operator）身份登录控制台，单击“安全管理中心”→“失泄密防护策略”（或者主机安全策略、安全文档策略或可信策略）→“群组策略”，进入群组策略界面，如图 5-14 所示。

图 5-14　群组策略界面

说明：

（1）**群组列表**显示群组管理中创建的所有群组，在这里不能新建群组。

（2）**群组描述**显示选定群组的详细信息。这些详细信息也是在创建群组过程中添加的，在这里只展示，不能修改。

（3）**群组策略面板**显示每项策略的具体内容。在这里进行具体策略的制定和下发，也可通过下方“导入”、“保存”按钮，进行策略的导入和导出。

（4）**策略树**显示具体策略项。在不同的策略中（失泄密防护策略、主机安全策略、安全文档策略和可信策略），策略树显示的内容也不同。

5.4.2　群组策略使用方法

5.4.2.1　编辑群组策略

（1）在群组策略界面中，左侧群组列表中选择某群组，右侧策略树中选择某策略项，中间的群组策略面板编辑具体的策略。例如：我们选择“test 群组”，编辑键盘控制策略项，设置禁止用户使用载屏键策略，如图 5-15 所示。

图 5-15　编辑群组策略——键盘控制

（2）再举个例子，我们编辑打印机控制策略，设置“允许群组中的人员使用打印机，但记录打印文件名称和内容”策略，如图 5-16 所示。

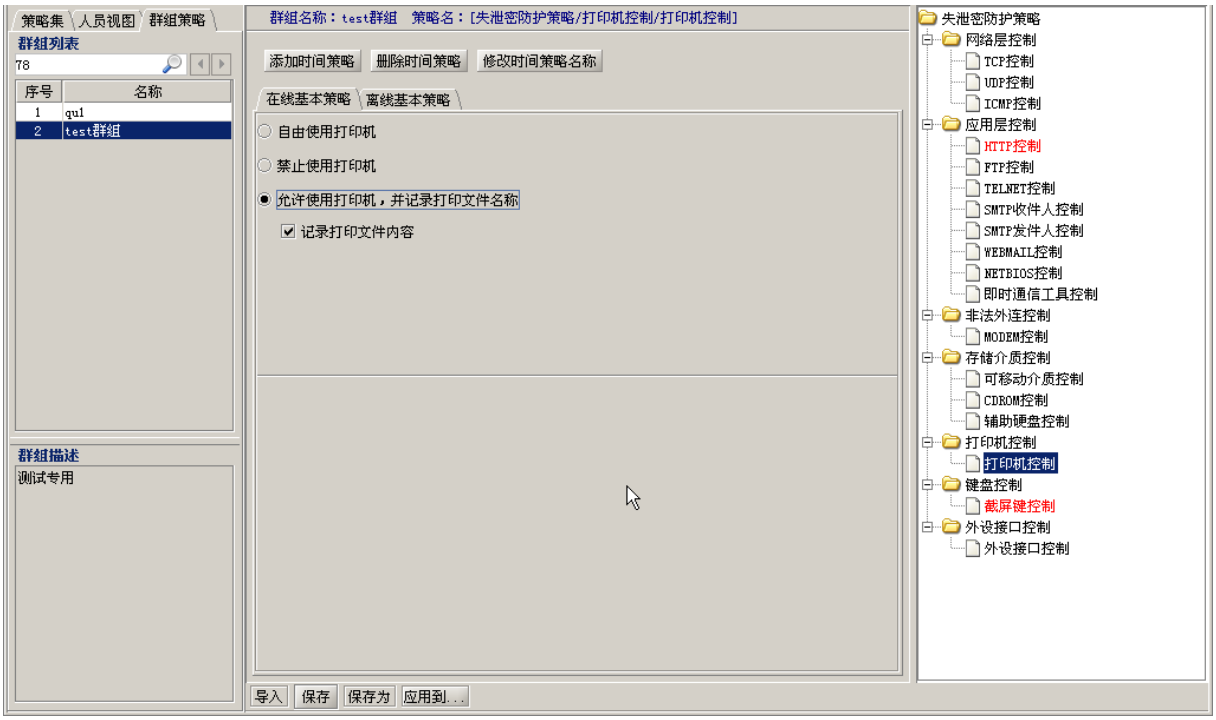


图 5-16　编辑群组策略——打印机控制

（3）参照上面的操作方法，设置好各个策略项后，最后单击下方的“保存”按钮，将编辑好的群组策略保存，系统会弹出成功保存提示框，如图 5-17 所示。

图 5-17　成功保存群组策略

5.4.2.2　应用群组策略

（1）在群组策略列表中，选中已编辑好的群组策略（例如：我们上面编辑好“test 群组”），单击群组策略下面的“应用到...”按钮，弹出应用策略界面，如图 5-18 所示。

在左侧勾选要应用的策略项，支持部分策略下发；在右侧选择策略应用范围，可以按群组选择范围，也可以按组织结构选择范围。例如：我们将上面编辑的打印机控制策略和键盘控制策略，下发给“test 群组”人员。最后，单击“确定”按钮，下发应用策略的命令。

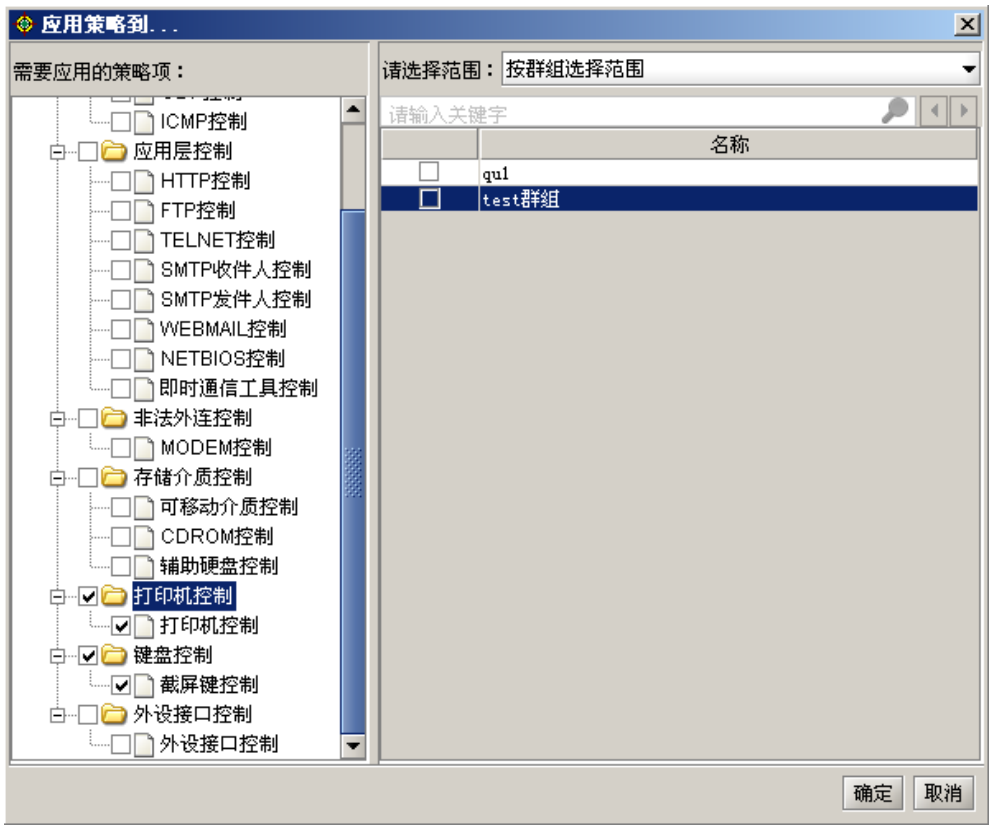


图 5-18　应用群组策略

（2）策略应用成功后，系统会弹出成功提示框，如图 5-19 所示。

图 5-19　应用群组策略成功

（3）在客户端验证以下策略执行情况。隶属于“TEST 群组”的用户，在客户端使用截屏键时，将弹出禁止使用提示框，如图 5-20 所示。同时，使用打印机打印文件时，都将记录打印文件名称和文件内容，可以在控制台的“统计审计分析→客户端监控日志→失泄密防护→打印机”中查看。

图 5-20　应用策略集

注意：

1. 制定一个群组策略后，将一个人员或计算机从其他群组迁移到这个群组后，他们会自动应用这个群组的策略。

2. 将一个群组中的人员或计算机单独下发策略后，他会应用后来下发的策略，不再使用原来的群组策略。

5.4.2.3　导出群组策略

（1）在群组策略列表中，选择编辑好的群组策略，单击下方的“保存为”按钮，可以将群组策略保存为“文件”、“默认策略”、“策略集”三种形式，如图 5-21 所示。

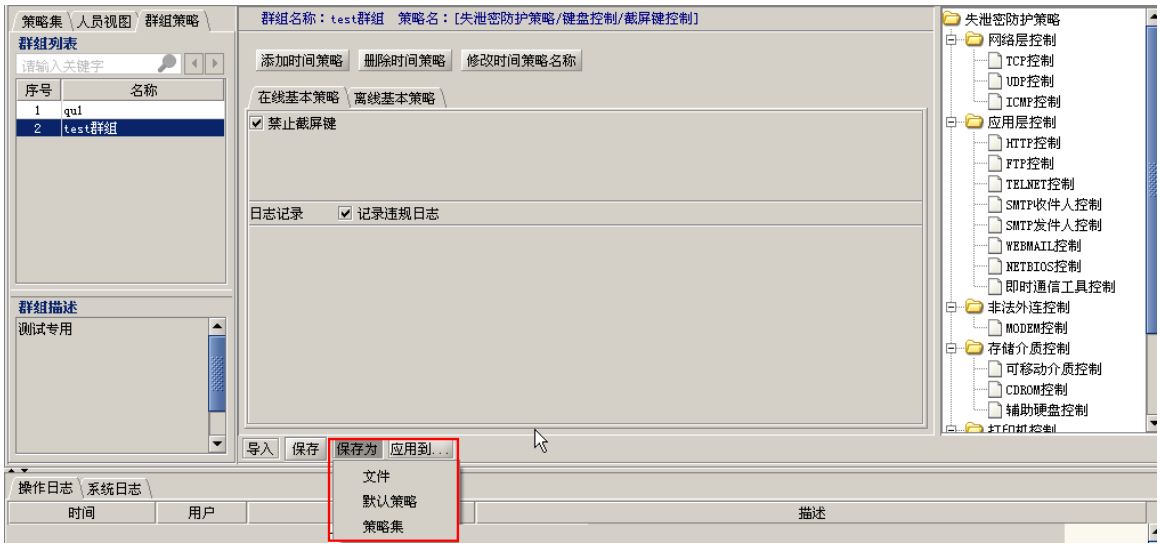


图 5-21　导出群组策略

（2）如果我们要保存为文件形式，就要选择导出路径，输入文件名，单击“保存”按钮，既可保存，如图 5-22 所示。保存的群组策略文件，需要时可通过导入按钮重新导入。

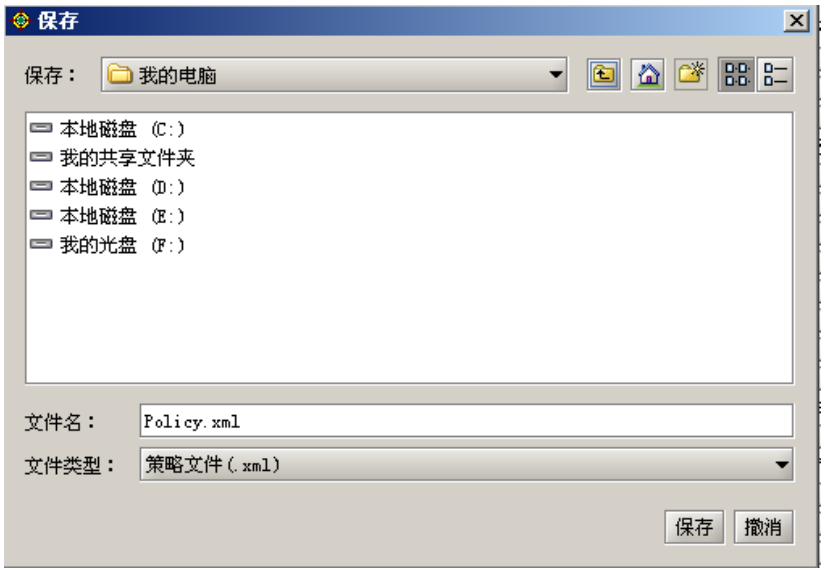


图 5-22　保存群组策略

5.4.2.4　导入群组策略

（1）在群组策略列表中，选择某群组策略，单击下方的“导入”按钮，可从“文件”、“默认策略”、“策略集”三种方式导入群组策略，如图 5-23 所示。

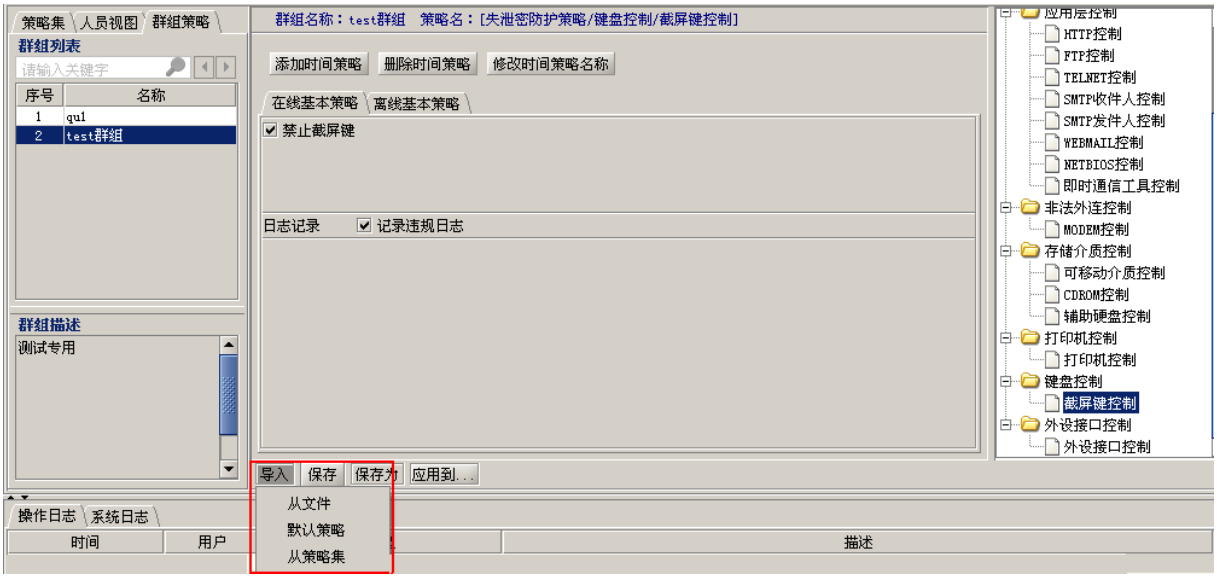


图 5-23　导入群组策略

（2）如果要导入策略集，就要从策略集列表中选择欲导入的策略集，如图 5-24 所示。导入成功后，更新选中的群组策略内容。

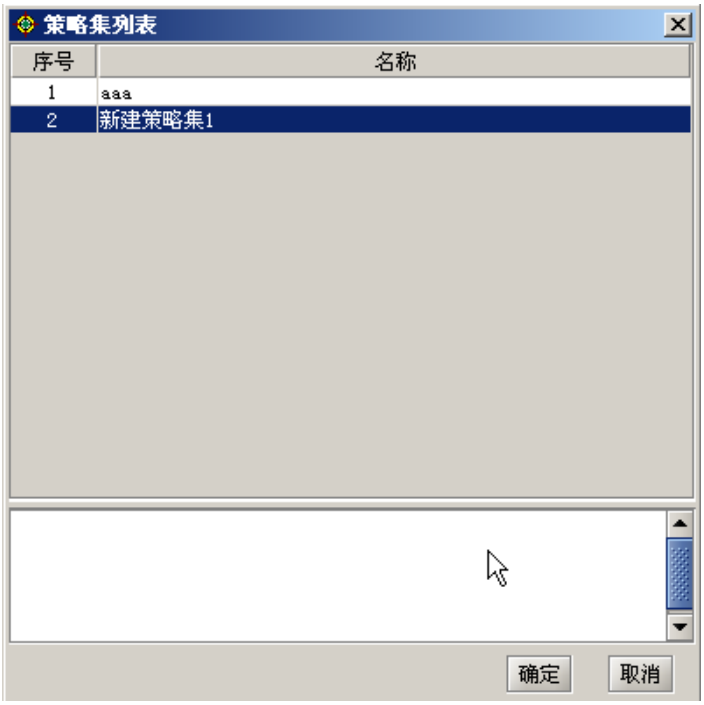


图 5-24　导入策略集

5.5 失泄密防护策略

失泄密防护是中软统一终端安全管理系统 8.0 的主要功能之一，它能对客户端进行全方位的控制，包括网络、外设、接口等的访问控制。其中网络控制主要是对网络层和应用层的访问控制；外设控制主要是对打印机、光驱、移动硬盘等的访问控制；接口控制主要是对 USB 接口、串口、并口、红外线设备接口等的访问控制。

启动控制台后，进入安全管理中心，单击“失泄密防护策略”标签项，进入失泄密策略编辑界面，如图 5-25 所示。在左边的“人员视图”框中选择一个用户，注意一次只能选择一个用户；在右边的“失泄密防护策略”中选择一个策略类型，注意一次只能选择一个策略类型。待用户和策略类型选定之后，就进入策略编辑画面，下面详细介绍失泄密防护策略的应用。

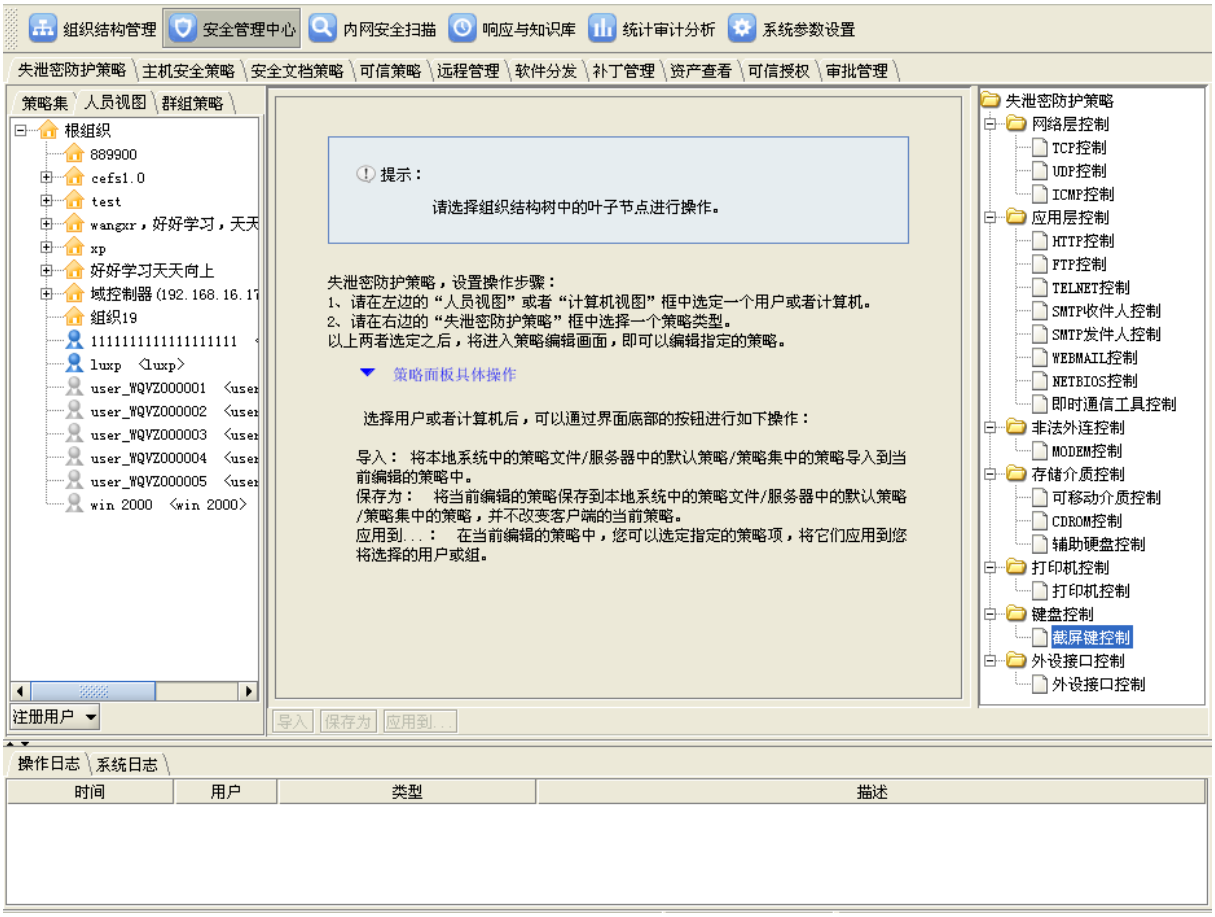


图 5-25　用户策略设置界面

5.5.1　网络层控制

5.5.1.1　TCP 控制

（1）在左边“人员视图”中选定一个用户，单击“网络层控制”→“TCP 控制”，进入 TCP 控制策略编辑页面。首先学会编辑在线基本策略（默认策略），在策略类型下拉框中选择“开放全部 TCP 端口”，可以根据需要单击“添加”按钮，在控制列表中添加黑名单，同时选择日志记录项，如图 5-26 所示。

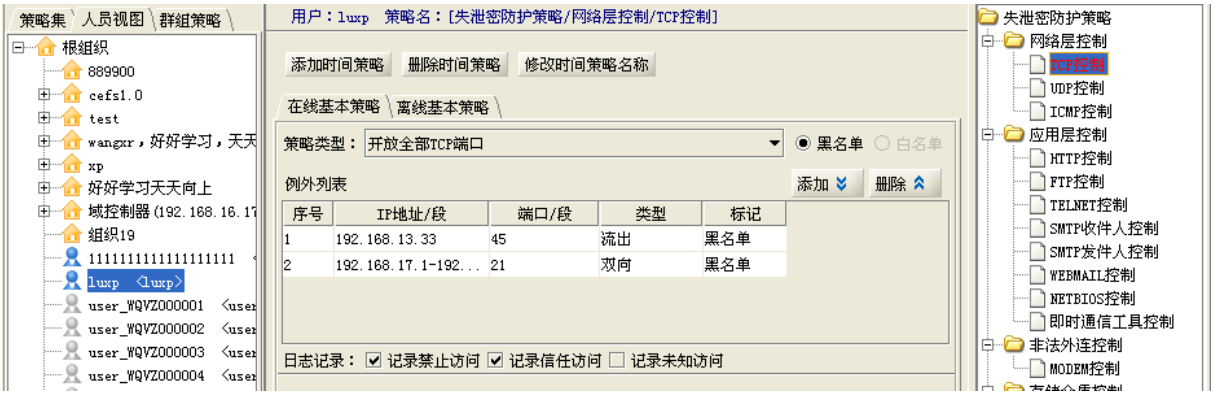


图 5-26　编辑 TCP 在线基本策略

（2）策略编辑完成后，单击下方“应用到…”按钮，弹出应用策略界面，如图 5-27 所示。从左侧勾选要下发的策略项，从右侧勾选用户，单击确定按钮，将策略下发给选定的用户。

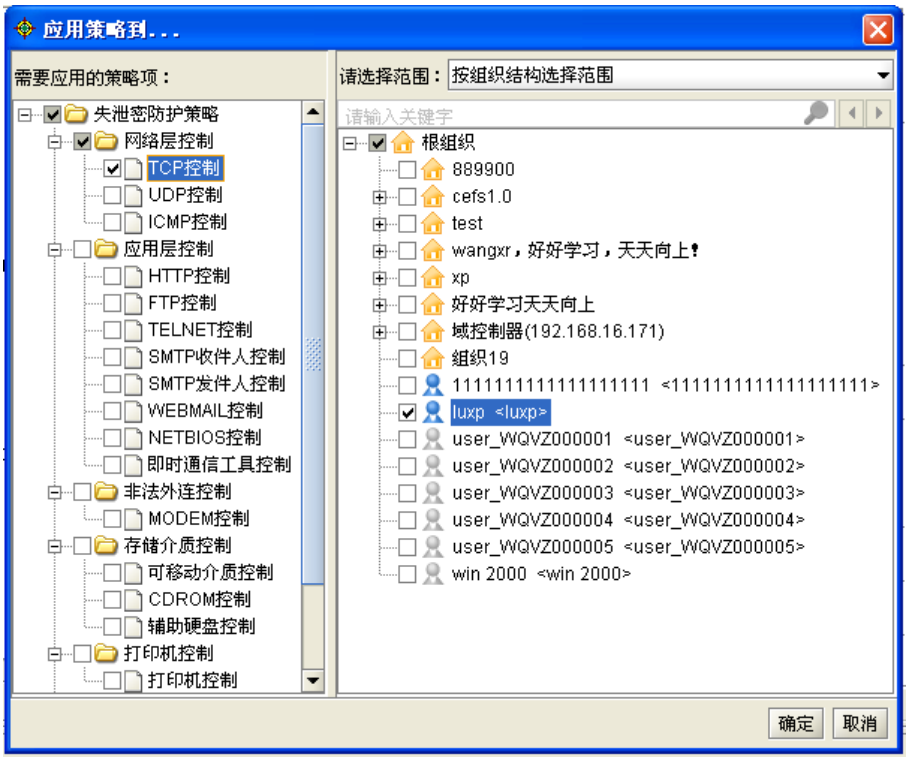


图 5-27　下发 TCP 策略

（3）策略下发成功后，出现成功提示框，如图 5-28 所示。同时，在下面的系统日志框中能够看到相关信息。

客户端收到策略后，**禁止**和黑名单中用户进行 TCP 连接。有违规行为将产生报警信息，可以在“响应与知识库”→“警报处理”中查看。如果客户端有信任访问和未知访问行为，将产生日志记录，可以在统计审计分析的失泄密防护日志中查看。另外，请用户注意，如果已经和黑名单建立连接，再下发禁止策略就不起作用了。

图 5-28　应用策略成功

5.5.1.2　UDP 控制

（1）在左边“人员视图”中选定一个用户，单击“网络层控制”→“UDP 控制”，进入 UDP 控制策略编辑页面。在策略类型下拉框中选择“关闭全部 UDP 端口”，可以根据需要单击“添加”按钮，在控制列表中添加白名单，同时选择日志记录项，如图 5-29 所示。

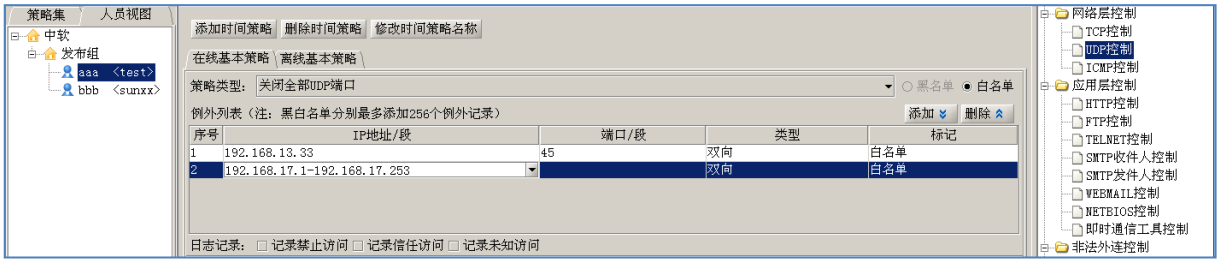


图 5-29　编辑 UDP 在线基本策略

（2）策略编辑完成后，单击“应用到…”按钮，将策略下发给选定的用户。策略下发成功后，出现成功提示框，如图 5-30 所示。同时，下面的系统日志框中能够看到相关信息。客户收到策略后，**只允许**和白名单中用户进行 UDP 连接。

提示：TCP 和 UDP 的日志量很大，建议一般不要开启，影响机器性能。

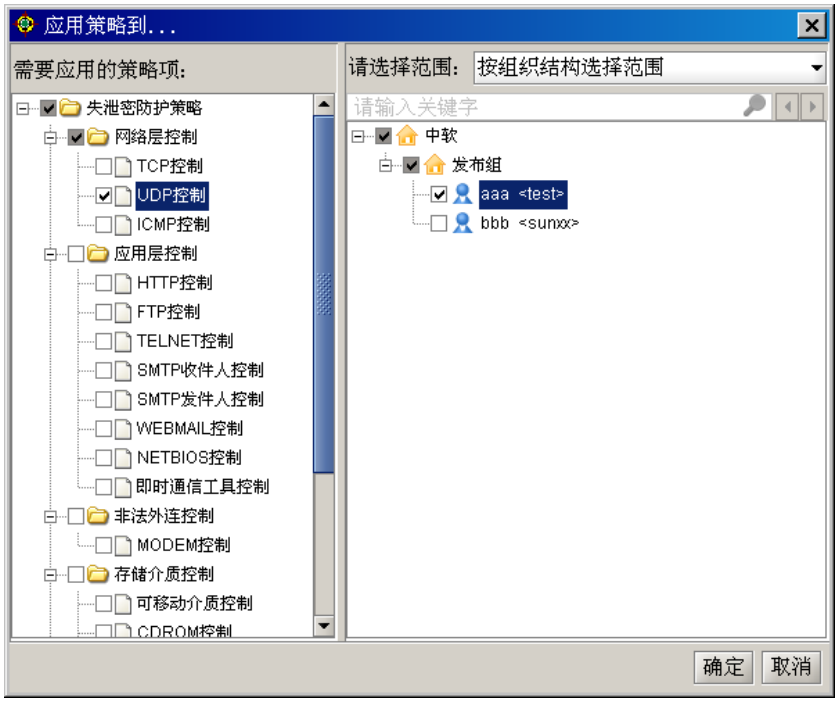


图 5-30　下发 UDP 策略

5.5.1.3　ICMP 控制

（1）在左边“人员视图”中选定一个用户，单击“网络层控制”→“ICMP 控制”，进入 ICMP 控制策略编辑页面，如图 5-31 所示。

图 5-31　编辑 ICMP 在线基本策略

提示：

（1）此项策略暂不支持 Windows Vista，不记录日志信息。

（2）禁止 ping 入：禁止别的主机 ping 应用该策略的用户；禁止 ping 出：禁止应用该策略的用户 ping 别的主机。

（3）禁止 ping，但不禁止 TCP 连接。

（2）如果选择“禁止 ping 出”，单击“应用到…”按钮，将策略下发给选定的用户。用户收到策略后，禁止 ping 别人的主机。

5.5.2　应用层控制

5.5.2.1　HTTP 控制

（1）在左边“人员视图”中选定一个用户，单击“应用层控制”→“HTTP 控制”，进入 HTTP 控制策略编辑页面。下面我们学习一下添加时间策略：

单击**上面的**“添加时间策略”按钮，添加“时间策略 1”。在“策略类型”下拉框中，选择“开放 HTTP 访问网络”，根据需要在黑名单列表中，添加黑名单，选择日志记录项，如图 5-32 所示。

图 5-32　添加时间策略 1

（2）单击日期后面的下拉框，设置策略的有效日期，例如设置“时间策略 1”在 2009/11/27~2010/11/27 这段时间内有效，如图 5-33 所示。勾选星期前面的复选框☑，可以设置策略的具体作用周期。

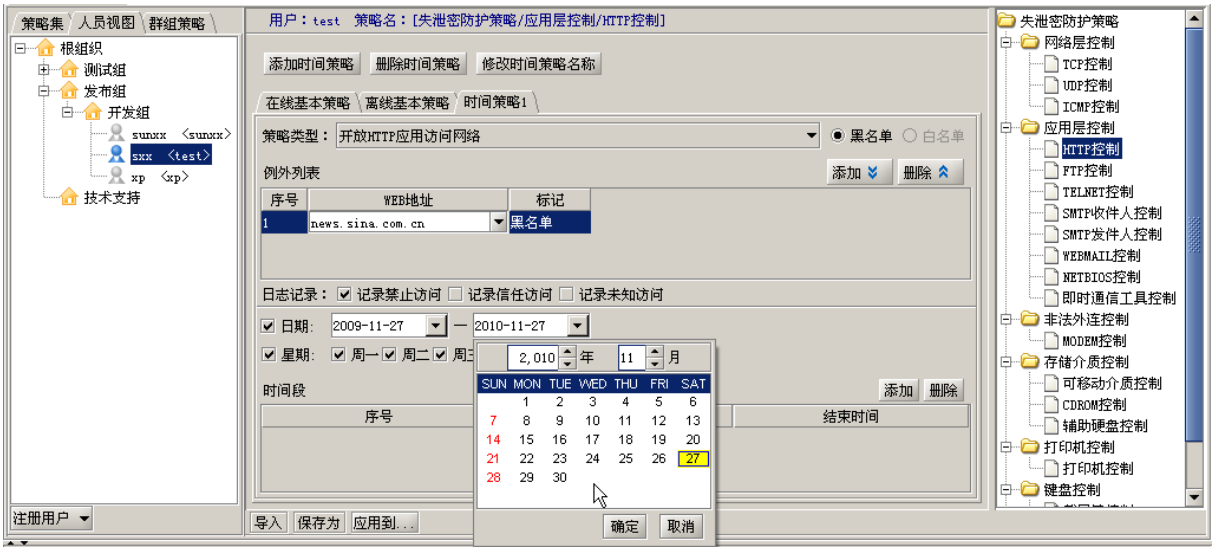


图 5-33　时间策略 1—设置有效日期

（3）策略的设置非常灵活，日期设置好以后，还可以设置具体的作用时间，把策略细化到分秒。单击“添加”按钮，设置有效时间段，如图 5-34 所示。

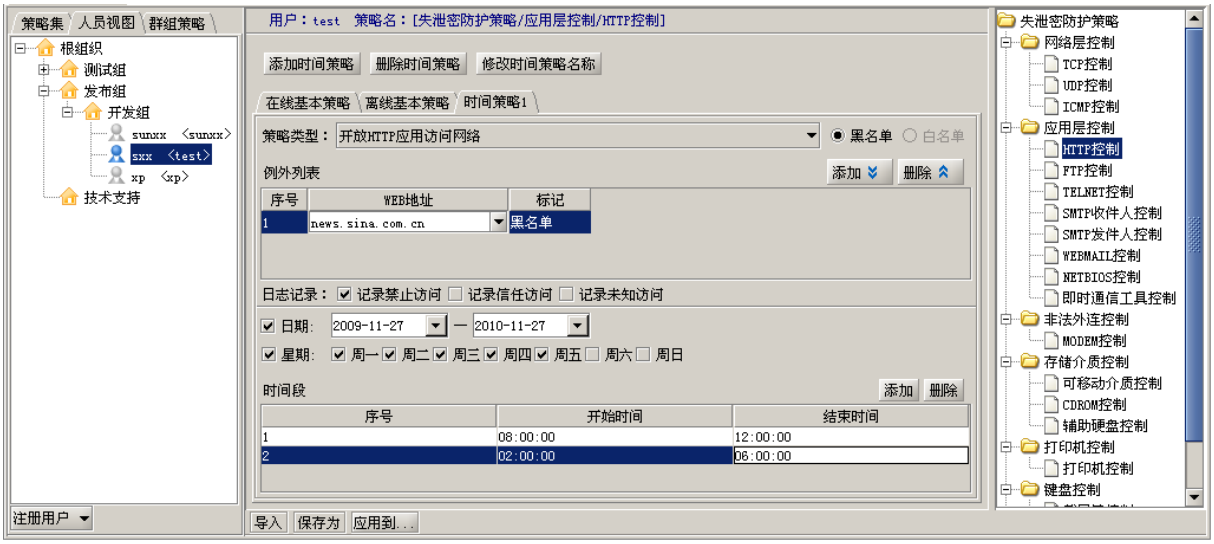


图 5-34　时间策略 1—设置有效时间段

（4）根据需要参照“时间策略 1”，设置“时间策略 2”、“时间策略 3”、“时间策略 4”…… 。单击“修改名称”，可以将策略改名，如图 5-35 所示。

图 5-35　更新策略名称

提示：时间策略的时间段不能重叠、交叉。

（5）时间策略编辑好以后，单击“应用到...”按钮，将策略下发给选定的用户。如果各子策略时间重叠，系统会自动判断，并出现错误提示框，如图 5-36 所示。重新调整好以后，会出现成功应用提示框。

图 5-36　时间重叠提示框

（6）客户端收到策略后，在规定的日期、时间段内执行相应的策略，并记录日志信息。如果有违规操作，将产生警报信息（参见告警信息和统计审计分析→失泄密防护日志→HTTP 控制）。

5.5.2.2　FTP 控制

（1）在左边“人员视图”中选定一个用户，单击“应用层控制”→“FTP 控制”，进入 FTP 控制策略编辑页面。编辑一个工作时间策略，单击**上面的**“添加”按钮，添加“时间策略 1”，通过”修改名称”按钮，更名为“工作时间策略”，如图 5-37 所示。

图 5-37　添加工作时间策略

（2）添加黑名单，选择工作日（星期一～星期五），设置工作时间（09:00:00～12:00:00；14:00:00～17:30:00），如果不选择日期，默认日期不加限制，如图 5-38 所示。根据用户需要选择记录日志类型。

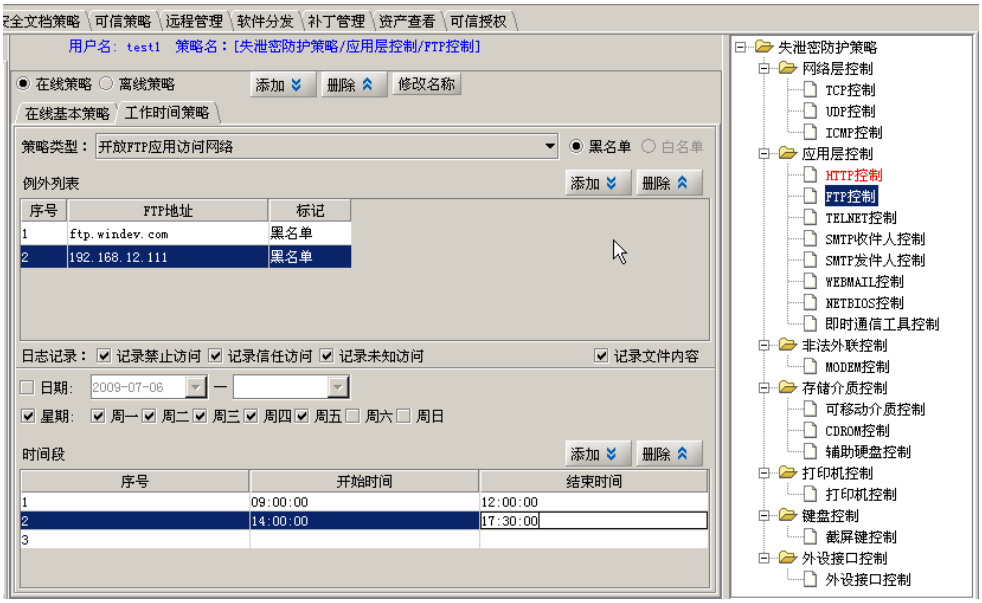


图 5-38　编辑 FTP 工作时间策略

（3）策略编辑完成后，将策略成功下发给选定的用户。客户端收到策略后，在**工作时间内禁止**和黑名单中用户进行 FTP 连接，并根据记录选项记录日志内容，可以在统计审计分析→客户端监控日志→失泄密防护→FTP 查看。

如果下发的策略中记置“记录文件内容”，那么通过 FTP 成功访问后，日志记录中将有备份文件，单击右键菜单可以下载。

5.5.2.3　TELENT 控制

（1）在左边“人员视图”中选定一个用户，单击“应用层控制”→“TELNET 控制”，进入“TELNET 控制策略”编辑页面。添加“时间策略 1”，在“策略类型”下拉框中选择“禁止 TELNET 访问网络”，根据需要添加“白名单”，并设置策略的有效期（2009/07/06~2009/12/06），如图 5-39 所示。

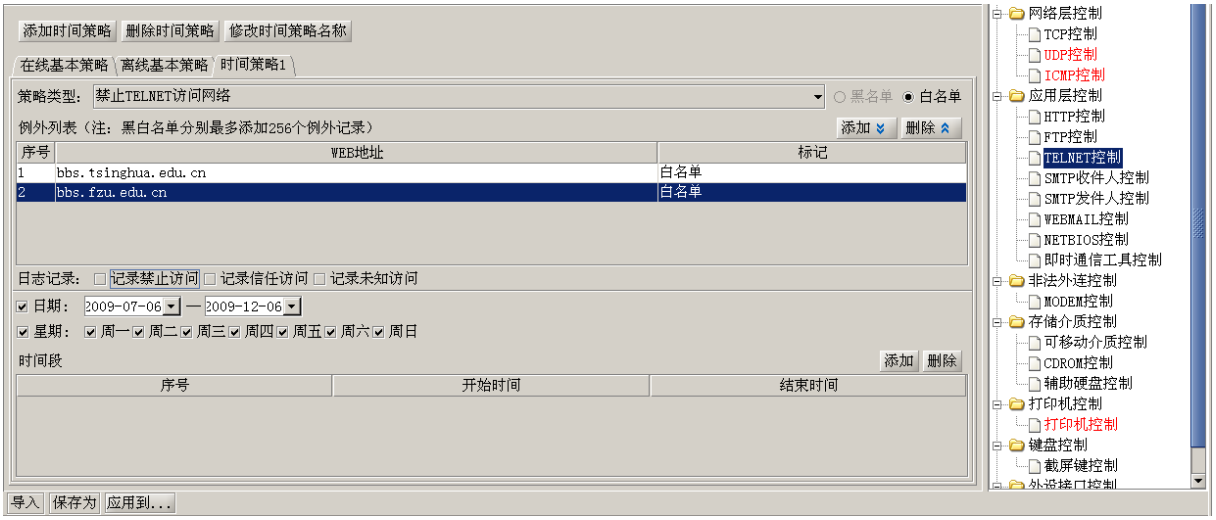


图 5-39　编辑 TELNET 时间策略

（2）策略编辑完成后，单击“应用到…”按钮，将策略下发给选定组织或用户，如图 5-40 所示。

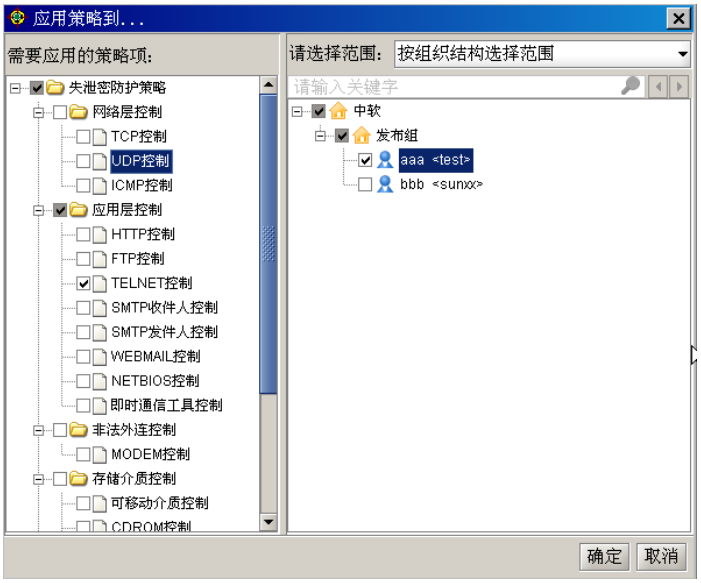


图 5-40　应用策略到组织或用户

（3）客户端收到策略后，**在规定的日期内只允许 TELNET 远程访问白名单中的地址**。可以根据记录选项记录访问日志，在统计审计分析→失泄密防护日志中能够查看。

5.5.2.4　SMTP 收件人控制

（1）在左边“人员视图”中选定一个用户，单击“应用层控制”→“SMTP 收件人控制”，进入“SMTP 收件人控制”策略编辑页面。在“策略类型”下拉框中选择“自由发送 SMTP 邮件”，根据需要添加“黑名单”，勾选邮件附件中包含特定字符时，禁止发送邮件，如图 5-41 所示。

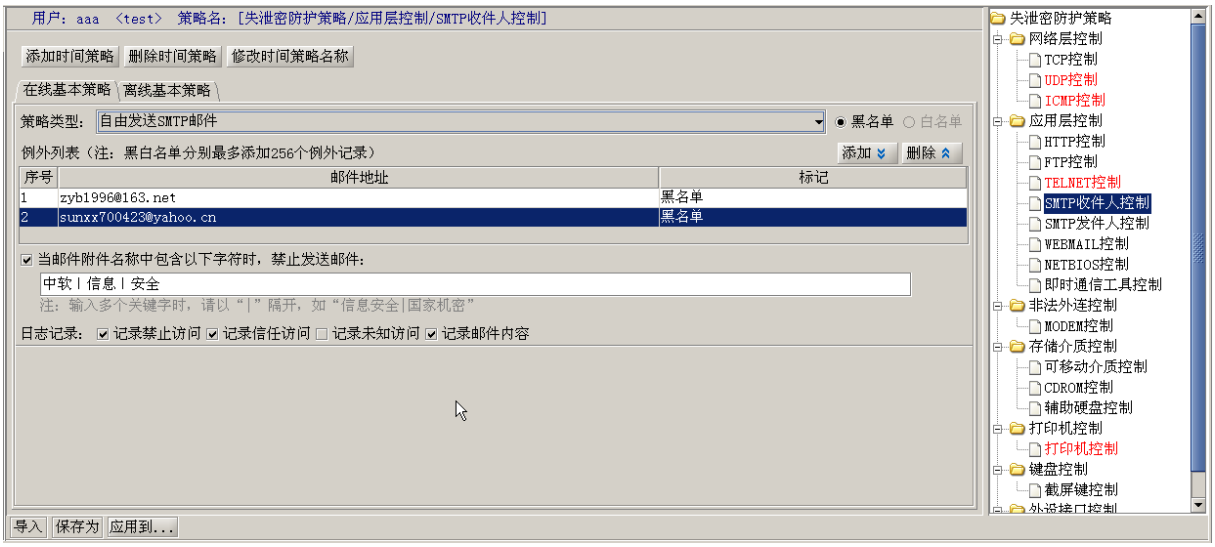


图 5-41　编辑 STMP 收件人控制策略

（2）策略编辑完成后，可以单击“保存为”按钮，将当前编辑的策略保存为本地系统中的策略文件（*.XML），如图 5-42 所示。也可保存为服务器中的默认策略，或者策略集中的策略，这些都不改变客户端的当前策略。

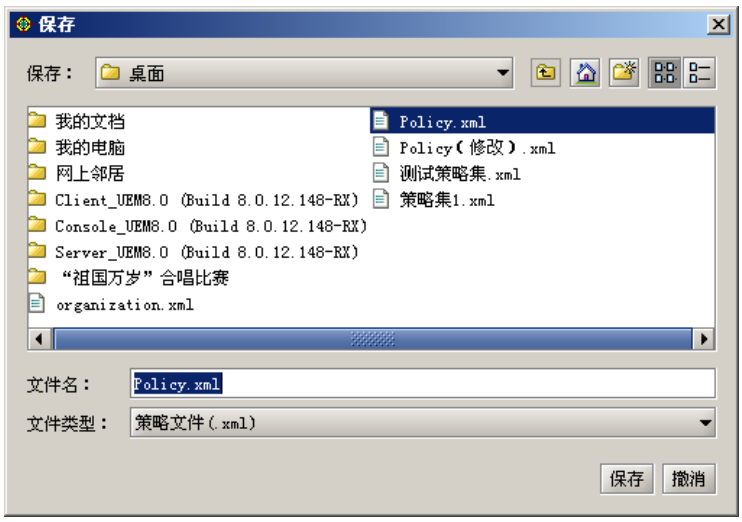


图 5-42　保存策略文件

（3）单击“应用到…”按钮，将此策略下发指定的客户端。禁止客户端通过 OUTLOOK 或者 FOXMAIL，向黑名单中的邮件地址发送邮件，并有相应的日志记录和告警记录。如果发送的邮件附件中含有特定字符，也禁止发送。

5.5.2.5　SMTP 发件人控制

（1）在左边“人员视图”中选定一个用户，单击“应用层控制”→“SMTP 发件人控制”，进入“SMTP 发件人控制”策略编辑页面。在“策略类型”下拉框中选择“禁止发送 SMTP 邮件”，根据需要添加“白名单”，如图 5-43 所示。

提示：如果不想手动编辑策略，也可单击下方的“导入”按钮，将保存的策略文件、默认策略或策略集导入到当前编辑的策略中，省去重新编辑的麻烦。

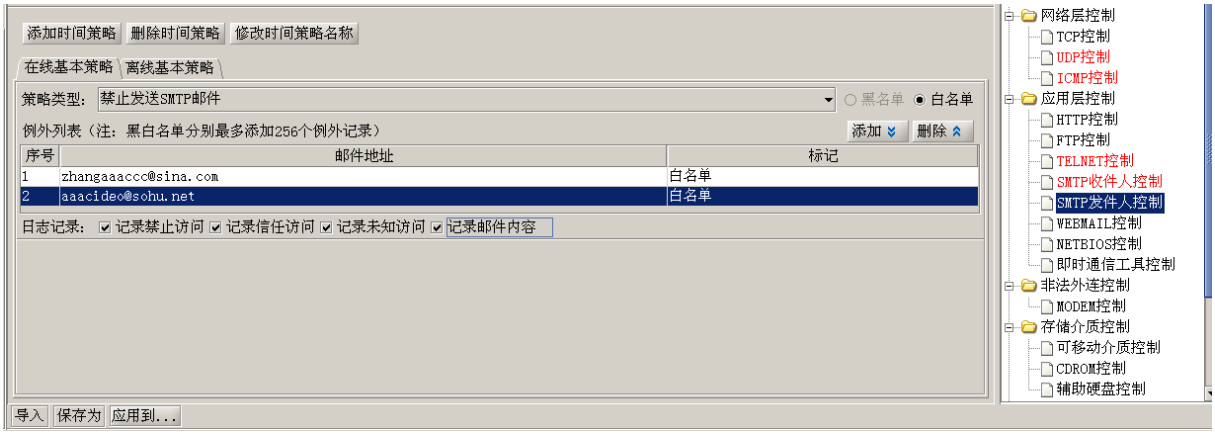


图 5-43　编辑 STMP 发件人控制策略

（2）此策略下发后，客户端只能使用白名单中的邮箱地址，以 OUTLOOK 或者 FOXMAIL 的方式发送邮件。

5.5.2.6　WEBMALL 控制

（1）在左边“人员视图”中选定一个用户，单击“应用层控制”→“WEBMAIL 控制”，进入“WEBMAIL 控制”策略编辑页面。添加“时间策略 1”，在“策略类型”下拉框中选择“开发 WEB 邮件/BBS 发送”，根据需要添加“黑名单”，并设置策略的日期，如图 5-44 所示。

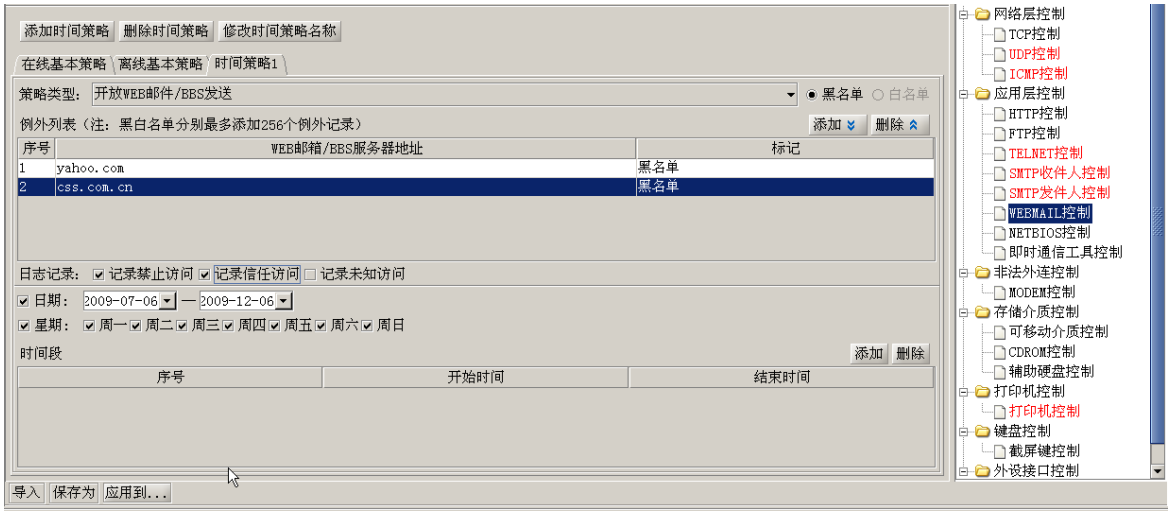


图 5-44　编辑 WEBMAIL 控制策略

（2）策略编辑完成后，可以单击“保存为默认”按钮，将策略保存成默认策略，如图 5-45 所示。

图 5-45　保存为默认策略

（3）此策略下发成功后，客户端在规定的日期和时间段内，禁止使用黑名单中的邮箱服务器发送 WEB 邮件/BBS，并有相应的日志记录。WEBMAIL 控制可禁止需要输入用户名、密码登录的地方，例如：登陆网站的邮箱、BBS 等。

5.5.2.7　NETBIOS 控制

（1）在左边“人员视图” 中选定一个用户，单击“应用层控制”→“NETBIOS 控制”，进入“NETBIOS 控制”策略编辑页面。在“策略类型”下拉框中选择“自由通过 NETBIOS 访问网络”，根据需要添加“黑名单”，设置记录日志类型，如图 5-46 所示。记录信任的访问时，可设置记录的文件操作类型，或者只记录指定后缀的文件操作。

类型选项的含义：

双向：禁止应用策略的客户端访问设置的 IP，也禁止设置的 IP 访问应用策略的客户端。

流出：禁止应用策略的客户端访问黑名单中的 IP 地址。

流入：禁止黑名单中的 IP 地址访问应用策略的客户端。

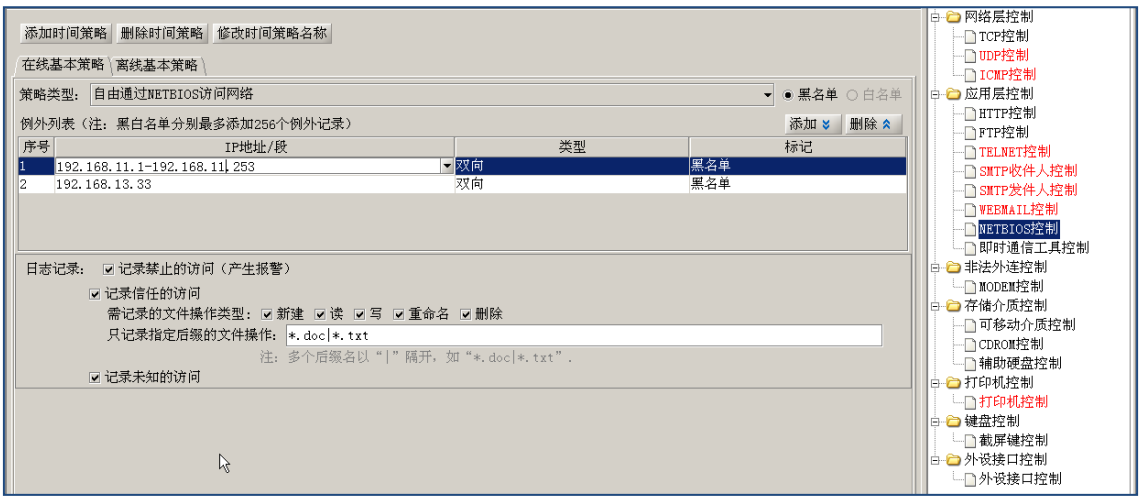


图 5-46　编辑 NETBIOS 控制策略

（2）策略下发成功后，禁止客户端通过 NETBIOS 访问黑名单中的地址，如图 5-47 所示。记录的禁止访问可在报警信息里查看；记录信任访问时，可记录指定后缀的文件操作类型，在统计审计分析中查看。

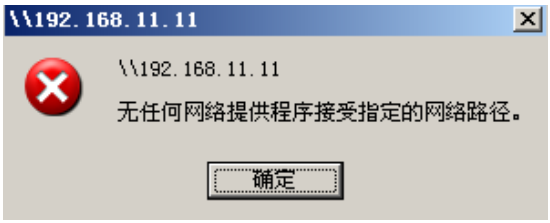


图 5-47　禁止通过 NETBIOS 访问

5.5.2.8　即时通信工具控制

（1）在左边“人员视图”中选定一个用户，单击“应用层控制”→“即时通信工具控制”，进入“即时通信工具控制”策略编辑页面，选择控制方式和日志记录类型，如图 5-48 所示。其中“自由使用即时通信工具”控制方式，提供发送文件名称的过滤功能，可以在下方的文本框中输入多个受控制的敏感关键字，当发送文件时，按照设置的关键字对发送文件进行控制，并给予相应提示信息。

图 5-48　即时通信工具控制策略

（2）策略下发成功后，客户端按照此策略进行。

提示：在只禁止发送文件的情况下，装有客户端的机器不能通过msn给对方发送文件，但是对方发送的文件是能够接收的。在禁止聊天和发送文件的策略时，那么双方的发送文件行为都是阻止的。

5.5.3　非法外联控制

（1）在左边“人员视图”中选定一个用户，单击“非法外联控制”→“MODEM 控制”，进入“MODEM 控制”策略编辑页面。在“策略类型”下拉框中选择“禁止拨号上网”，根据需要添加白名单，并选择日志记录项，如图 5-49 所示。

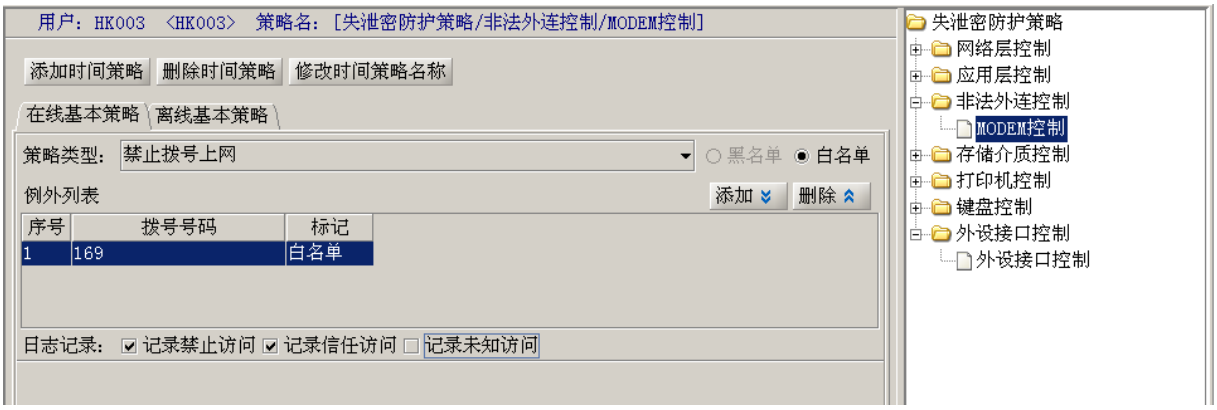


图 5-49　编辑 MODEM 控制策略

（2）策略编辑成功后，单击“应用”按钮，将策略下发给选定的用户。客户端收到策略后，只允许通过“169”拨号上网，并产生相应的日志记录，参看“统计审计分析→客户端监控日志→失泄密防护→非法外连”。

5.5.4　存储介质控制

5.5.4.1　可移动介质控制

（1）在左边“人员视图”中选定一个用户，单击“存储介质控制”→“可移动介质控制”，进入“可移动介质控制”策略编辑页面，如图 5-50 所示。

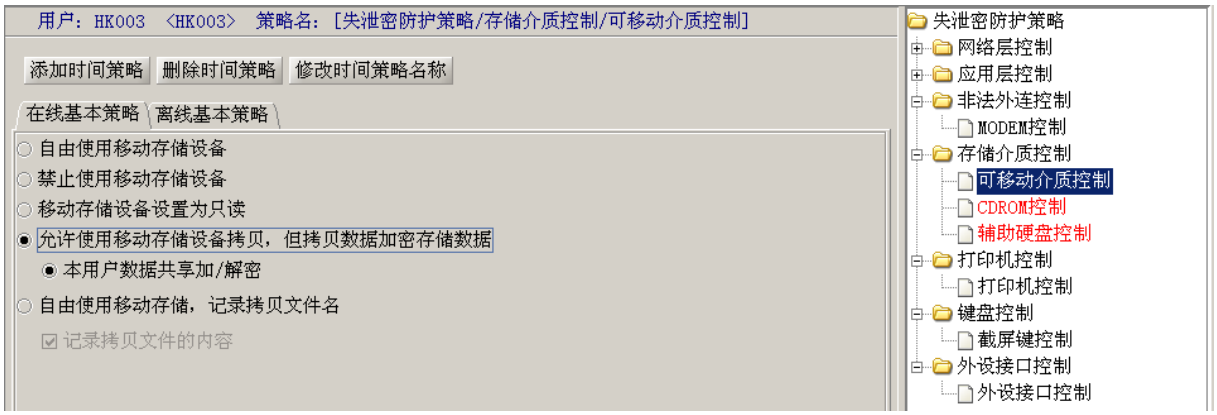


图 5-50　编辑可移动介质策略

（2）选择“允许使用移动存储设备拷贝，但拷贝数据加密存储”策略，将此策略下发后，客户端往移动存储器上拷贝数据时都会被加密，可以在“统计审计分析→客户端监控日志→失泄密防护→媒体介质→移动存储器→加密带出”查看。

如果选择“自由使用移动存储，记录拷贝文件名和文件内容”策略，那么客户端往移动存储器上拷贝数据时不加密，但记录文件名和文件内容，可以在“统计审计分析→客户端监控日志→失泄密防护→媒体介质→移动存储器→记录带出”查看，点击右键可以下载备份文件。

5.5.4.2　CDROM 控制

（1）在左边“人员视图”中选定一个用户，单击“存储介质控制”→“CDROM 控制”，进入“CDROM 控制”策略编辑页面。编辑“离线策略”，通常离线策略的制定比较严格，我们选择“禁止使用刻录机/CDROM 存储设备”，如图 5-51 所示。

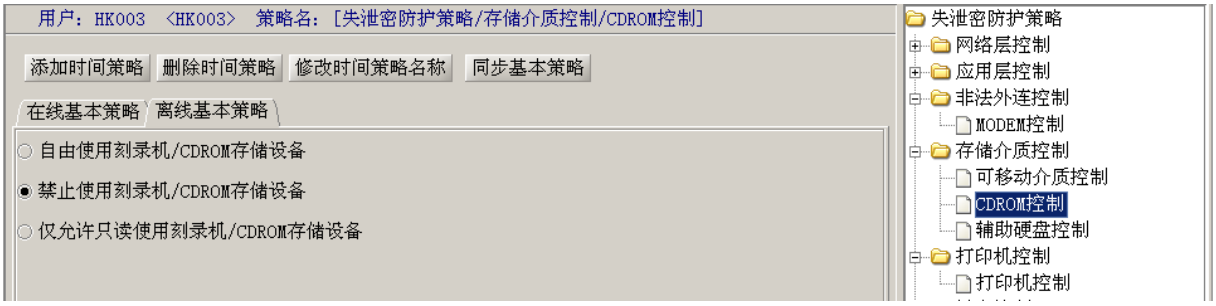


图 5-51　编辑 CDROM 离线策略

（2）策略编辑成功后，单击“应用”按钮，将策略下发给选定的用户。客户端收到策略后，如果和服务器通讯中断，也就是说离线了，则禁止使用刻录机/CDROM 存储设备。

离线策略和在线策略的编辑方法一样，内容也非常相似。为提高编辑策略效率，可采用“同步基本策略”功能，将编辑好的在线策略导入到离线策略中，方便用户使用。

5.5.4.3　辅助硬盘控制

（1）在左边“人员视图”中选定一个用户，单击“存储介质控制”→“辅助硬盘控制”，进入“辅助硬盘控制”策略编辑页面。编辑“离线策略”，选择“禁止使用辅助硬盘”，如图 5-52 所示。

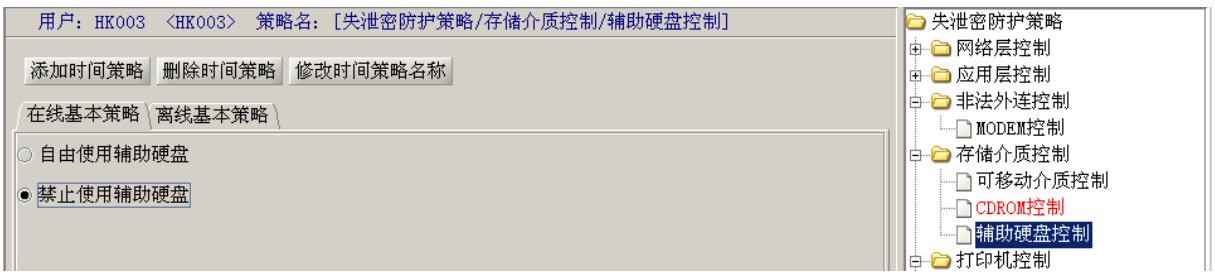


图 5-52　编辑辅助硬盘离线策略

（2）策略编辑成功后，单击“应用”按钮，将策略下发给选定的用户。客户端收到策略后，如果和服务器通讯中断，也就是说离线了，则禁止使用辅助硬盘。

5.5.5　打印机控制

（1）在左边“人员视图”中选定一个用户，单击“打印机控制”，进入策略编辑页面。可以选择使用打印机，并记录打印文件名称和内容，如图 5-53 所示。

这里可以设置允许使用的打印机名称、类型，以及允许打印的进程名。

在“打印机名称”框中，输入具体的打印机名称，或者某种系列的打印机，指定客户端只能用此设置的打印机打印文件。打印机名称的输入支持通配符*和？，多个打印机用“,”分隔；在“进程名”输入框中，输入客户端能使用打印机打印文件的应用程序进程，进程名的输入支持通配符*和？，多个进程名用“|”分隔。最后，在“仅限使用以下类型的打印机”下面，勾选“真实打印机”或“虚拟打印机”，不勾选表示不受限制。

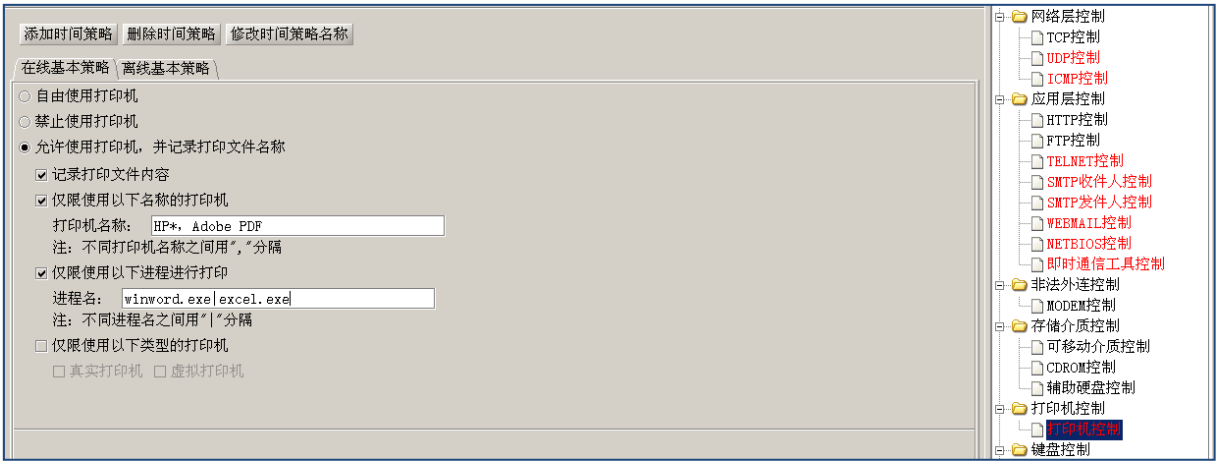


图 5-53　编辑打印机控制策略

（2）此策略下发成功后，允许客户端使用设置的进程和打印机打印文件，并记录打印文件名称和内容。用户可以在“统计审计分析→失泄密防护→打印机”查看日志信息，单击右键菜单也可下载备份的文件。

5.5.6　键盘控制

（1）在左边“人员视图”中选定一个用户，单击“键盘控制”→“截屏键控制”，进入策略编辑页面，如图 5-54 所示。

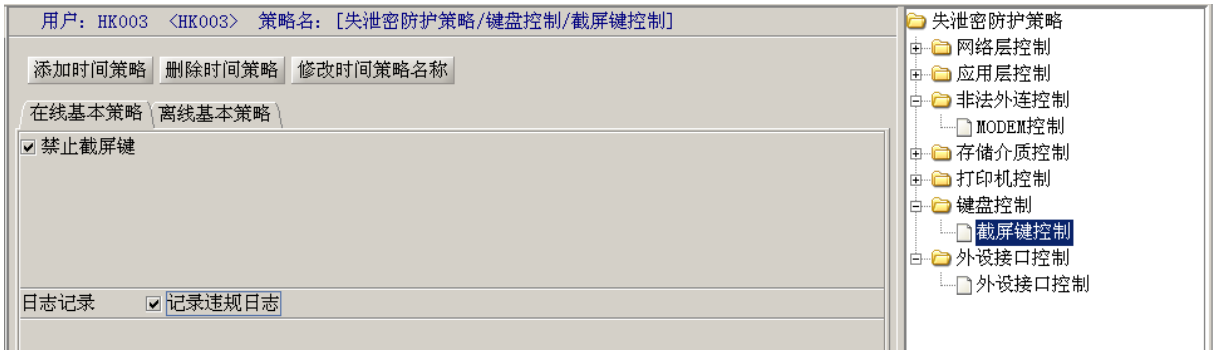


图 5-54　编辑截屏键控制策略

（2）选择“禁止截屏键”，将此策略下发成功后，客户端如果尝试使用截屏键，就会产生告警信息。

5.5.7　外设接口控制

（1）在左边“人员视图”中选定一个用户，单击“外设接口控制”，进入策略编辑页面，如图5-55所示。上半部分对USB接口设备进行细化分类，可以设置禁用所有USB设备、启用所有USB设备，也可以添加USB设备类型，对相应设备的启用状态进行设置。下半部分为其他接口的控制，勾选表示启用接口，不勾选表示不启用接口。

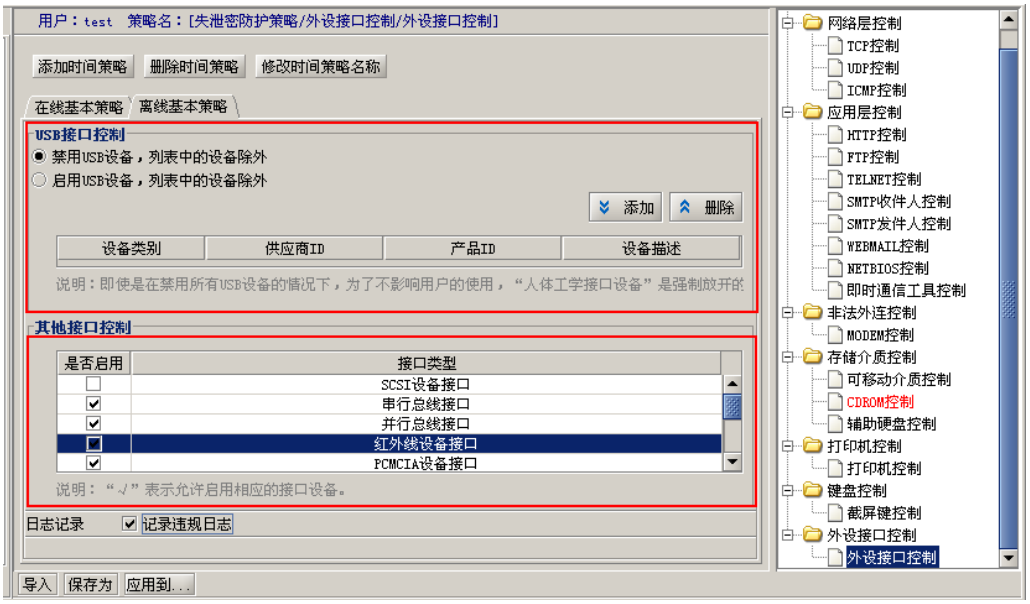


图5-55　离线策略——外投接口控制

（2）我们编辑离线基本策略，选择“禁用USB设备，列表中的设备除外”。单击“添加”按钮，弹出“添加例外USB设备”界面，如图5-56所示。从下拉框中选择例外USB设备，添加到例外列表中。根据用户需要，可以添加一个或多个。

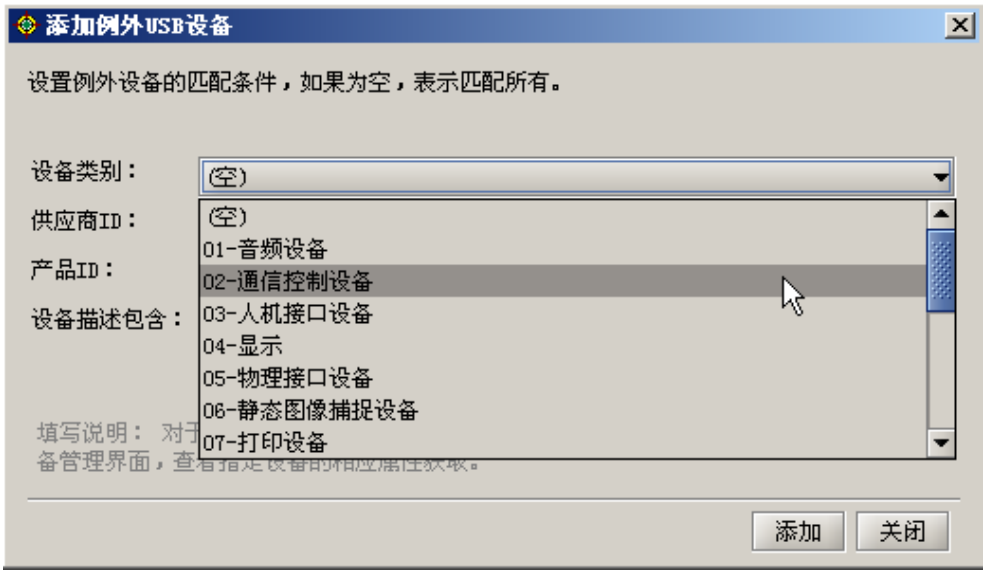


图5-56　添加例外USB设备

提示：对于 USB 设备的类别、供应商 ID、产品 ID 以及设备描述，可以通过操作系统的设备管理界面，查看指定设备的相应属性获取。当“设备类别”选择“(空)”，但是供应商 ID 或者产品 ID 不为空，则表示匹配所有符合供应商 ID 或者符合所有产品 ID 的设备；当选择了某个设备类别，但是供应商 ID 或者产品 ID 为空，则表示匹配所有该类别的设备，不区分供应商和产品。

设备类型和常用设备之间的对应关系如下表。

设 备 类 型	常 用 设 备
01-音频设备	扬声器、声卡
02-通信控制设备	网卡、调制解调器、串口、智能手机
03-人机接口设备	鼠标、键盘
05-物理接口设备	力回馈式游戏操纵杆
06-静态图像捕捉设备	网络照相机、扫描仪
07-打印设备	打印机
08-大容量存储设备	移动硬盘，闪存盘，MMC、SD、CF卡读卡器，数码相机，数字音频播放器等
09-集线器	USB集线器
0A-通信数据设备	调制解调器、双绞线网卡、ISDN、传真等
0B-智能卡	读卡器
0D-内容安全设备	
0E-USB视频设备	摄像头、电视卡的动态图像捕捉设备等
0F-个人保健设备	
DC-诊断设备	
E0-无线控制器	蓝牙适配器、WiFi适配器
EF-杂项	微软的ActiveSync设备
FE-特定于应用程序的设备	红外线数据桥接器
FF-特定于供应商的设备	定制设备

（3）策略下发成功后，客户端在离线情况下，不能启用 USB 接口设备和没有勾选的其他接口设备，例外列表中 USB 设备除外。如果尝试使用，就会产生告警信息。客户端离线日志暂时保留在客户端，等客户端上线后再上传到服务器。

5.6 主机安全策略

5.6.1 资产信息管理

资产信息管理对终端主机上的软硬件资产的安装、使用情况进行跟踪，规范终端用户的软硬件的安装行为，功能如下：

- 对软件资源和硬件资源能够提供及时的快照，并形成相应的资产列表；
- 自动发现、收集和跟踪终端主机上的软硬件资产的详细清单，即时提供企业软硬件资产的分类汇总报告；
- 根据配置“软硬件黑白名单”，发现非授权的软硬件时告警；支持自定义的硬件黑名单配置。
- 对软硬件资产的非授权变更根据策略进行告警。

5.6.1.1 软件管理策略

1. 在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“资产信息管理”中的“软件管理策略”，进入软件管理策略界面。“系统内软件列表”区默认显示组织结构中全部主机安装的软件类型、软件名称和数量等，支持按软件类型和软件名称排序，如图 5-57 所示。如果为“自由使用”状态，则表示应用此软件策略的组织或主机可以不受限制，任意安装、使用软件。

图 5-57　系统内软件列表

2. 点选“黑名单”，在“系统内软件列表”中选择禁止的软件，单击“添加”，加入软件策略黑名单列表中，如图 5-58 所示。如果点选 “本机列表”选择框，“系统内软件列表”只显示本机安装的软件类型、软件名称和数量等。然后将编辑好的软件策略下发到组织或主机，收到策略的客户端若有黑名单中的软件时，系统将产生报警信息，但不阻止违规软件的运行。报警方式可设置为邮件报警、短信报警和声音报警，具体参见知识库管理章节。

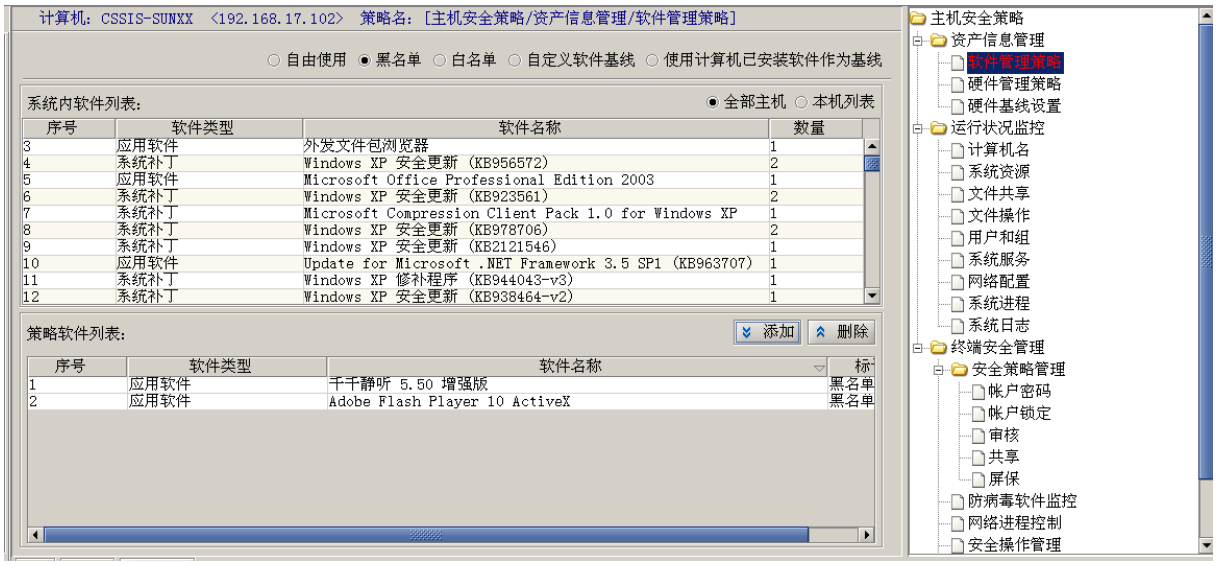


图 5-58　　软件管理策略-黑名单

3. 点选“白名单”，在“系统软件列表”中选择允许的软件，点击“添加”，加入软件策略白名单列表中，如图 5-59 所示。将软件策略应用下发到组织或计算机，收到策略的客户端若存在白名单规定以外的软件时，系统将产生报警信息，但不阻止违规软件的运行。

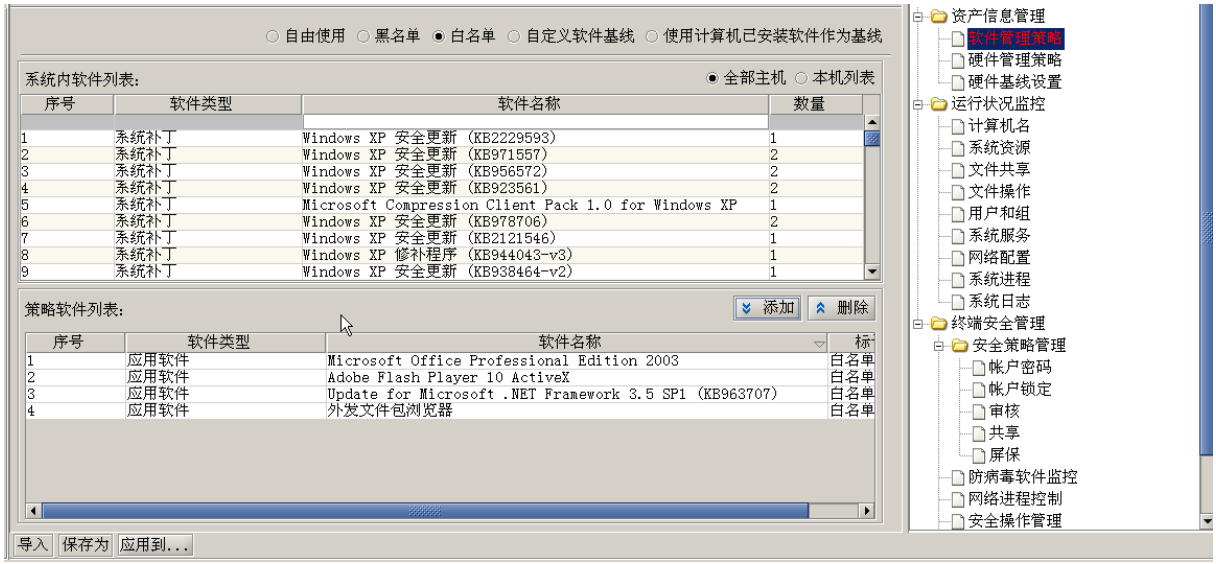


图 5-59　　软件管理策略-白名单

4. 点选“自定义软件基线”，在“系统内策略软件列表”中选择允许的软件基线，单击“添加”按钮，加入到下面的软件策略列表中，如图 5-60 所示。当此软件策略应用下发到组织或计算机后，收到策略的客户端若和基线规定的软件不一致时，将产生报警信息，同样不阻止违规软件的运行。

图 5-60　　软件管理策略-自定义软件基线

5. 点选“使用计算机已安装软件作为基线”，如图 5-61 所示。将此软件策略应用下发到计算机后，收到策略的客户端将以当前本机已安装的软件作为基线来监控软件变化情况，如果出现软件安装或卸载的操作时，将产生报警信息，但不阻止违规软件运行。与此同时，将重新设置客户端基线，所设置的基线将与最新的已安装软件保持一致。

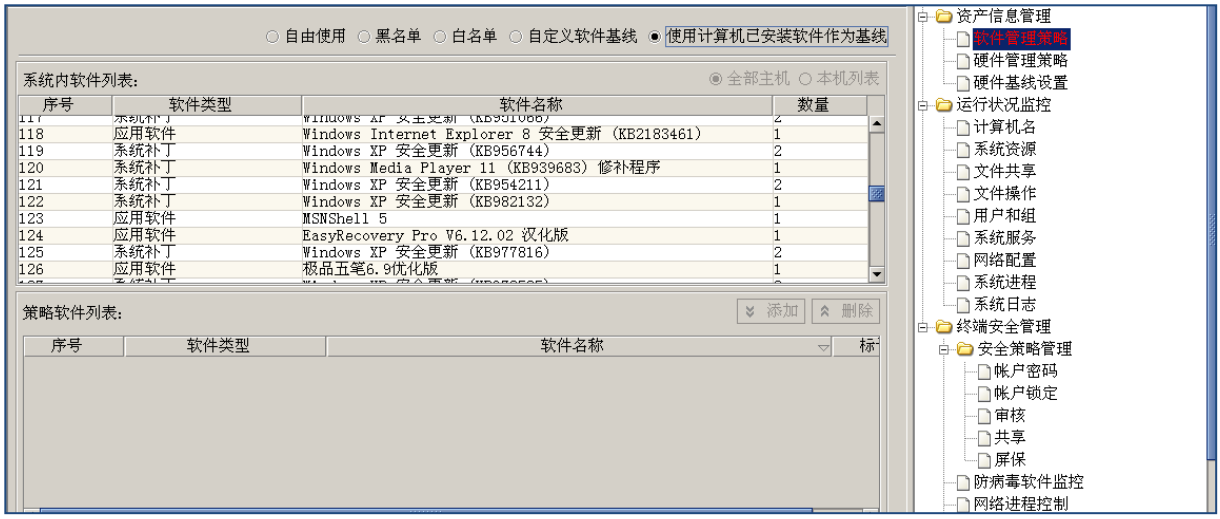


图 5-61　　使用计算机已安装软件作为基线

5.6.1.2 硬件管理策略

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“主机安全策略”→“资产信息管理”→“硬件管理策略”，进入硬件管理策略界面，如图 5-62 所示。

点选“自由使用”，策略应用下发给客户端，客户端不受限制，任意使用“可控制硬件列表”中硬件，如调制解调器、无线网卡、无线上网卡、打印机、采集卡等。

点选“设置非法硬件”，在“可控硬件列表”中选择硬件，单击“添加”，加入到“非法硬件列表”中。策略应用下发成功后，客户端如果使用“非法硬件列表”中硬件时，系统将报警。

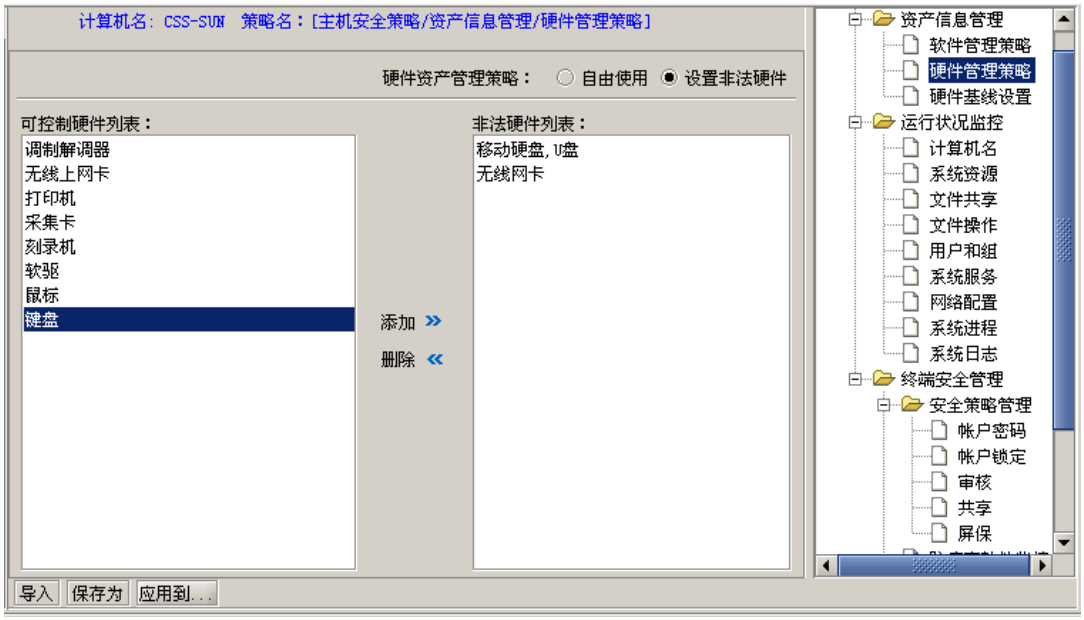


图 5-62　硬件管理策略

5.6.1.3 硬件基线设置

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧的“主机安全策略”→“资产信息管理”→“硬件基线设置”，进入硬件基线设置界面，如图 5-63 所示。

默认选中“使用计算机自身的配置作为基线”，此时“载入主机配置”按钮不可用，下方的设置面板不可编辑。下发此策略后，客户端将以自身计算机硬件的配置信息作为基线。

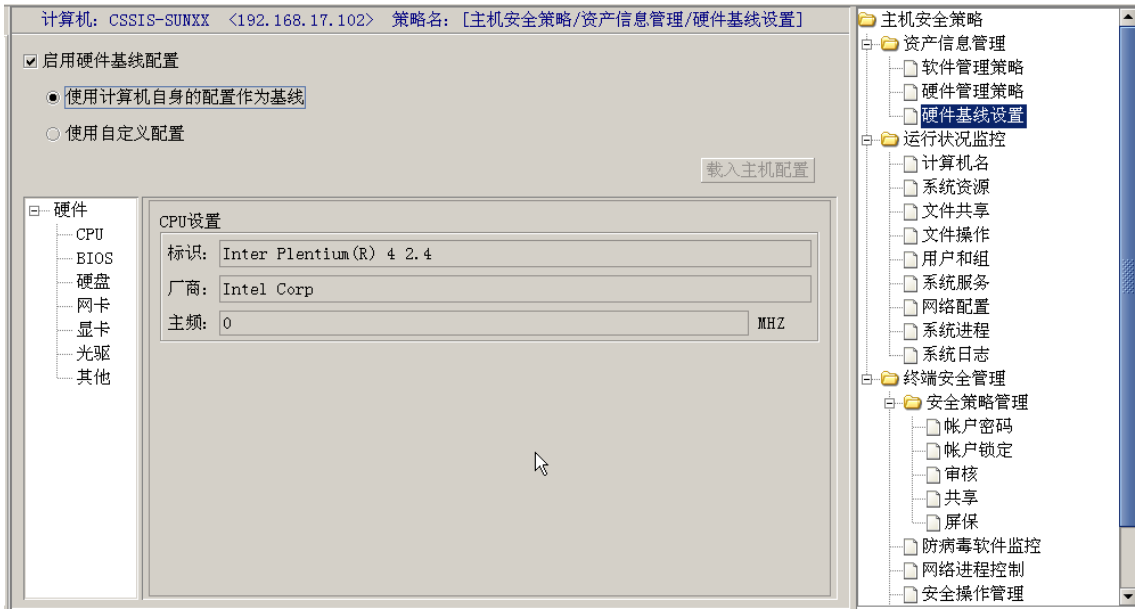


图 5-63　默认硬件基线配置

如果选择“使用自定义配置”，下方的基线设置面板可编辑，如图 5-64 所示。可以将计算机的配置载入配置表中，也可在此基础上进行随意编辑，下发策略后，客户端只能使用基线设置中所规定的硬件，否则系统将报警。

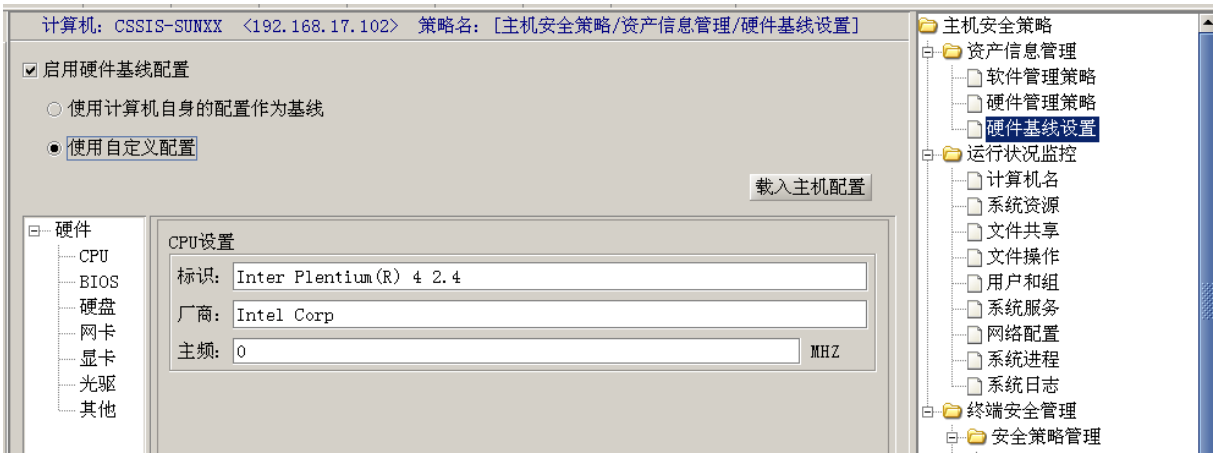


图 5-64　自定义配置硬件基线

提示：在使用自定义配置时，若对策略集或者群组进行策略编辑，则“载入主机配置”按钮不可用。

5.6.2 运行状况监控

运行状况监控能及时报告客户端的运行情况和资源使用情况，为管理员的远程监控提供帮助，该功能模块包括两个方面：一方面是远程监测，实时监测针对不同客户端所定义的阀值，如果超过阀值则系统产生报警日志；另一方面是远程监控，监测用户行为，当发现有违规行为产生时，及时纠正用户行为，并产生违规报警日志。

5.6.2.1 计算机名

在安全管理中心中，用鼠标单击“主机安全策略”→“运行状况监控”→“计算机名”，进入计算机名监控界面，如图 5-65 所示。选择“计算机名监控”中的“禁止修改计算机名称”，策略下发成功后，客户端不能修改计算机名称，该项被灰掉。 如果客户端是 Vista 系统，从表面上看用户仍然可以修改计算机名称,实际上修改无效，系统会监控到并修改回来。

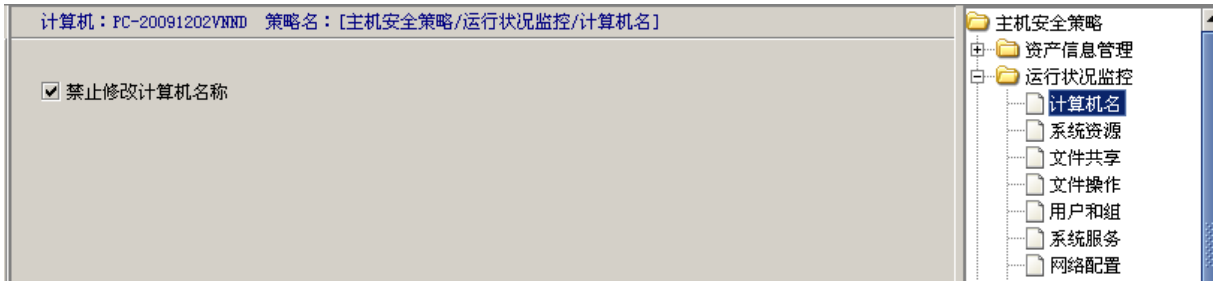


图 5-65　计算机名监控

5.6.2.2 系统资源

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“运行监控设置”下的“系统资源”，进入“系统资源监控”设置，如图 5-66 所示。根据用户需要，设置监测系统资源的具体参数，CPU（64%～100%）、内存（1%～100%）、硬盘分区（1MB～10230MB）。

单击下面列表项的箭头，在下拉框中显示监测网络流量的具体设置：包括网络实时流量（流入、流出、总体）和总体流量（流入、流出、总体）。用户可以设置当网络流量超过阀值时采取的方式：报警或者自动断开网络。

这里的断网定义为切断对外的网络连接，内部客户端与服务器的网络连接依然保持。超过阈值时，可设置自动断开网络，并在客户端给出相应提示。如果因为实时流量超出而断网，可以设置断网后自动恢复网络连接的时间和断网时的提示信息。如果因为总流量超出而断网，需重启计算机才能恢复网络连接。可以设置断网时的提示信息。

图 5-66　系统资源监控

提示：当网络流量超过阈值时，正在链接中连接断不开。

5.6.2.3 文件共享

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“运行状况监控”下的“文件共享”，进入“文件共享”设置，如图 5-67 所示。如果选择“监测共享文件夹的添加、删除变化”，策略下发成功后，客户端添加、删除共享文件夹时，系统都将记录日志并报警。

图 5-67　文件共享监控

5.6.2.4 文件操作

（1）在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“运行监控设置”下的“文件操作”，进入文件操作监控设置界面，如图 5-68 所示。若单击“重命名文件操作监控”标签页，选择“检测重命名文件操作并记录日志”，单击“增加”按钮，可以添加要监测的文件。

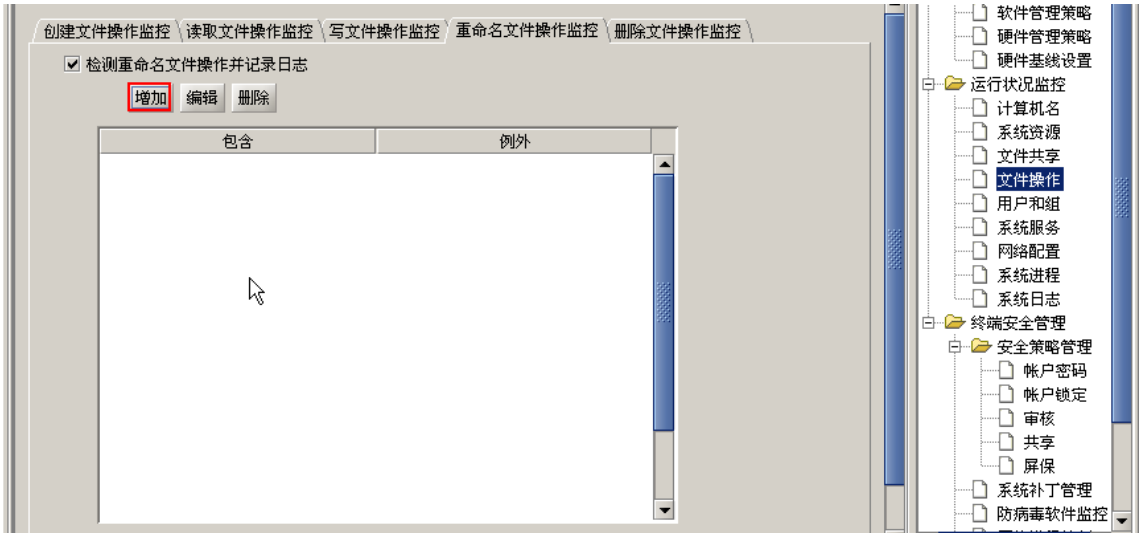


图 5-68　重命名文件操作监控

（2）在“添加检测文件”界面中，选择盘符，输入路径和文件名，单击“确定”即可。也可以单击“添加”按钮，在例外列表中输入例外文件名，如图 5-69 所示。

提示：路径的前面不输入盘符，开始和结束不能为“/”；文件名支持通配符。

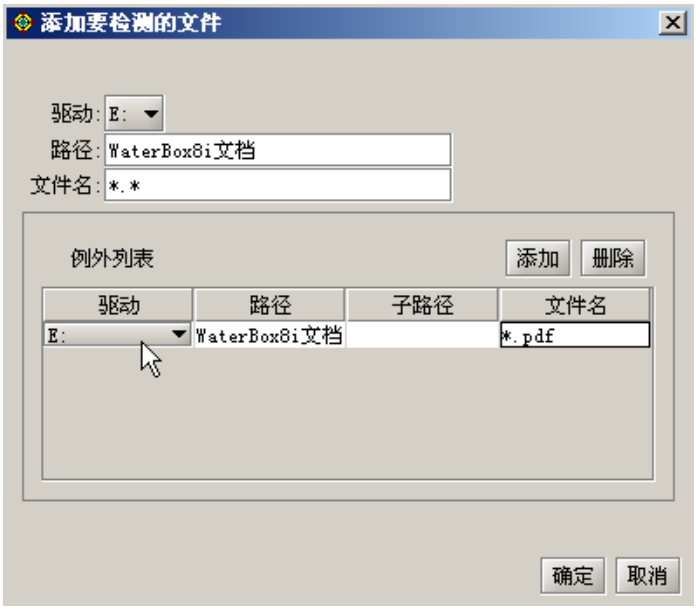


图 5-69　添加监测文件

（3）添加检测文件完成后，返回上一界面，可以看到刚添加的检测文件，如图 5-70 所示。策略下发成功后，客户端重命名设置范围内的文件时，系统将记录日志。

图 5-70　查看添加的监测文件

提示：创建文件、读取文件、写文件、删除文件的操作监控设置和重命名文件的操作监控设置类似，这里不再叙述。只是文件操作监控的日志量很大，一般不要开启，影响机器性能。另外，文件操作日志记录项可能会有重复现象。对于安全文件删除操作，系统不记录日志信息。

5.6.2.5 用户和组

在左侧的计算机视图中选定计算机，用鼠标单击右侧选择“运行监控设置”下的“用户和组”，进入“用户和组操作监测”设置界面，如图 5-71 所示。如果勾选监测用户和组的添加、删除和属性变化，策略下发成功后，客户端用户和组的添加、删除、属性变化都将记录日志，并报警。

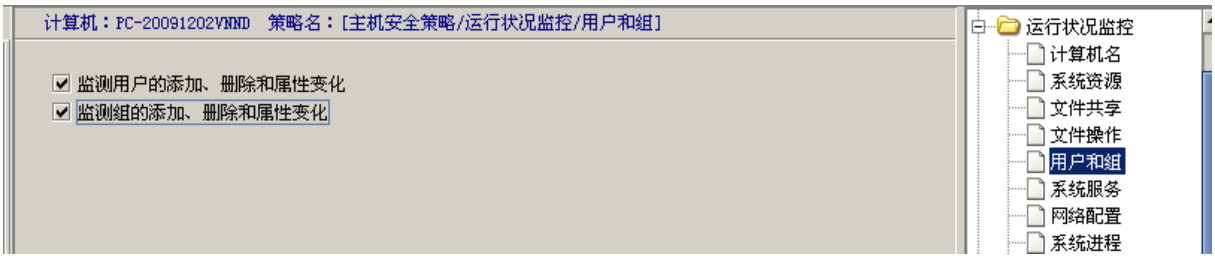


图 5-71　用户和组操作监测设置

5.6.2.6 系统服务

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“运行监控设置”下的“系统服务”，进入系统服务监控设置界面，如图 5-72 所示。

在这里可以通过“手动添加服务”和“获取当前计算机的所有服务”两种方式，来指定需要控制的服务，并将服务添加至“被控制服务列表”中。策略下发成功后，被检测的客户端，系统服务的启动和停止，都将记录日志，并报警。

图 5-72　系统服务监控设置

选项说明：

（1）勾选或取消“监测系统服务变化情况”复选框，设置监控系统服务的启动与停止。

（2）勾选或取消“监测所有服务的变化情况，并记录日志”复选框，设置是否监测所有服务的变化情况。当某服务发生变化时，将默认记录日志

（3）勾选或取消“控制服务运行”复选框，设置是否通过黑白名单的方式，对“被控制服务列表”中的服务进行控制。

勾选“只禁止被控制服务列表”中的服务，表示“被控制服务列表”中的所有服务，将被列为黑名单。当该策略下发给客户端时，客户端无法启动“被控制服务列表”中列出的服务。

勾选“只开放被控制服务列表”中的服务，表示“被控制服务列表”中的所有服务，将被列为

白名单。当该策略下发给客户端时，客户端只能运行“被控制服务列表”中列出的服务。如果“被控制服务列表”中没有添加任何记录，在应用策略时会给出提示，这样防止用户没有开放任何服务而导致主机无法启动的后果。

（4）获取服务的方式

点击“获取该计算机当前的所有服务”按钮，自动获取计算机当前的所有启动和未启动的服务。如果计算机在线，则将获取到得所有服务直接添加至“可选服务列表”中；如果该计算机不在线，则弹出提示框“计算机不在线”。

点击“手动添加服务”按钮，则弹出“手动添加服务”对话框。在“服务名”文本框中，输入计算机管理中服务名称；在“显示名称”文本框中，输入计算机管理中服务的显示名称。

（5）“添加”和“删除”按钮

从左侧“可选服务列表”中，选择一个或者多个服务，单击“添加”按钮，将选择的服务添加至“被控制服务列表”中；从右侧“被控制服务列表”中，选择一个或者多个服务，单击“删除”按钮，将选择的服务从“被控制服务列表”中删除，并默认追加在“可选服务列表”中。

5.6.2.7 网络配置

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“运行监控设置”下的“网络配置”，进入“网络配置监控”设置界面，如图 5-73 所示。

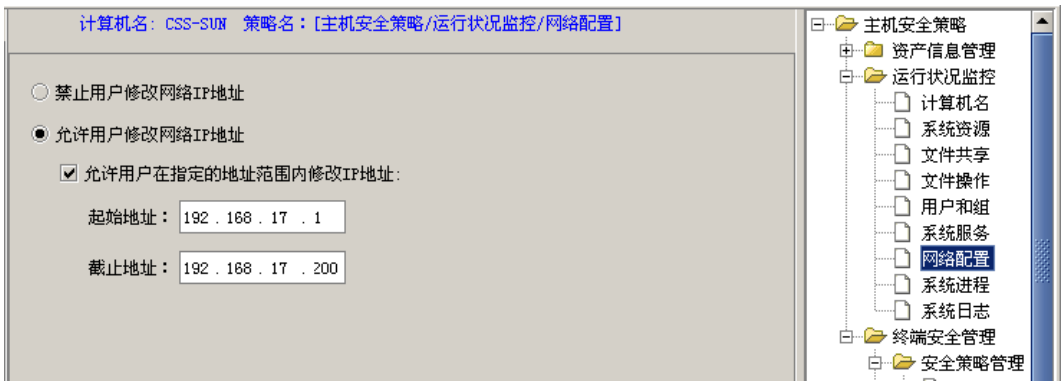


图 5-73　网络配置

点选“禁止用户修改网络 IP 地址”前的复选框，策略下发成功后，客户端不能修改 IP 地址。如果客户端尝试修改 IP 地址，控制台将会看到有报警。如果客户端是 Vista 系统，从表面上看用户仍然可以修改网络 IP 地址,实际上修改无效，系统会监控到并修改回来。

点选“允许用户修改网络 IP 地址”，不勾选“允许用户在指定的地址范围内修改 IP 地址”，则表示允许用户自由修改 IP 地址；

点选“允许用户修改网络 IP 地址”，同时勾选“允许用户修改网络 IP 地址”，需要用户在“起始地址”和“截止地址”输入框中输入 IP 地址，限制客户端更改 IP 地址范围，实现 IP 地址与 MAC 地址的绑定功能。

5.6.2.8 系统日志

选择“运行状况监控”下的“系统日志”，进入“系统日志”设置界面，如图 5-74 所示。选择“上传系统日志”，设置上传时间间隔，也可将上传后删除本地系统日志。策略下发成功后，被检测的客户机主机将执行此策略，按设置的时间上传操作系统日志。

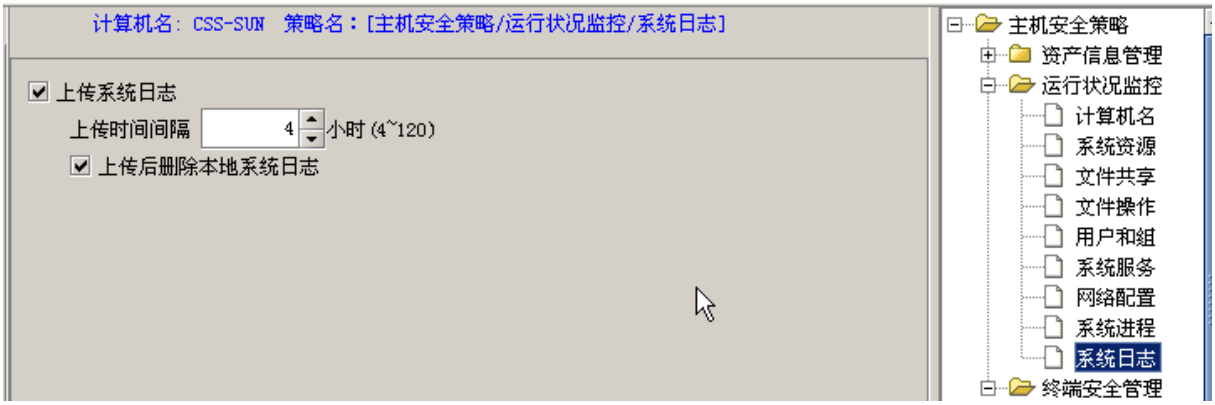


图 5-74　系统日志监控

5.6.3　终端安全管理

终端安全管理集中实现 Windows 安全策略配置和分发，及时清理系统在处理敏感信息所遗留的临时文件，提供安全删除临时文件策略配置。对主机的网络服务和网络连接进行管理，控制非授权或禁止的网络服务和网络连接，实现黑客和病毒“进不来、出不去”。监视防病毒软件的安装、运行、病毒库升级情况，对不符合安全策略的状态进行报警。检查终端补丁状态并自动升级系统补丁，系统补丁包括：主流 Windows 操作系统补丁、Windows 办公软件补丁等。

5.6.3.1 安全策略管理

- **帐户密码**

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“主机安全策略”→“终端安全管理”→“安全策略管理”，进入安全策略设置界面。在帐户密码设置中，点选“配置账户密码策略”，设置密码最小长度（0~14 个字符）、最短存留期（0~80 天）和最长存留期（0~999 天），然后选择“实施监控策略变化”和“系统报警”，如图 5-75 所示。策略下发成功后，客户端密码设置与下发的策略一致；当系统发现客户端密码设置与下发策略不一致时，产生报警。

注意：密码长度验证策略，对安装该系统之前就存在的帐户无效，只能对新建帐户或者下发策略后修改的密码帐户生效。

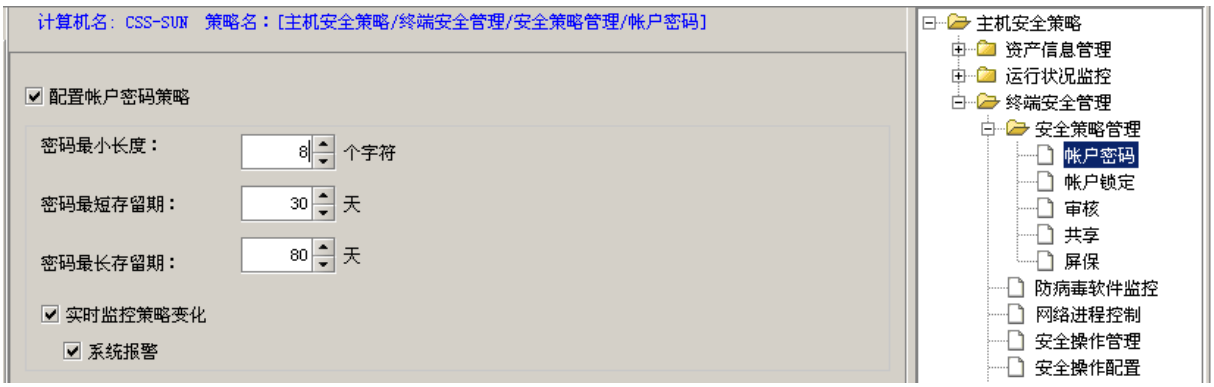


图 5-75　系统安全策略——帐户密码

◆ **帐户锁定**

选择 “安全策略管理”下的“帐户锁定”，进入“帐户锁定”设置界面，如图 5-76 所示。点选“配置帐户锁定策略”复选框，输入锁定阀值（0~999 次）、锁定时间（0~99999 分）、计数器复位时间（0~99999 分），然后选择“实时监控策略变化”和“生成日志报警”。策略下发成功后，如果系统发现客户端帐户锁定设置与下发策略不一致时，产生报警。

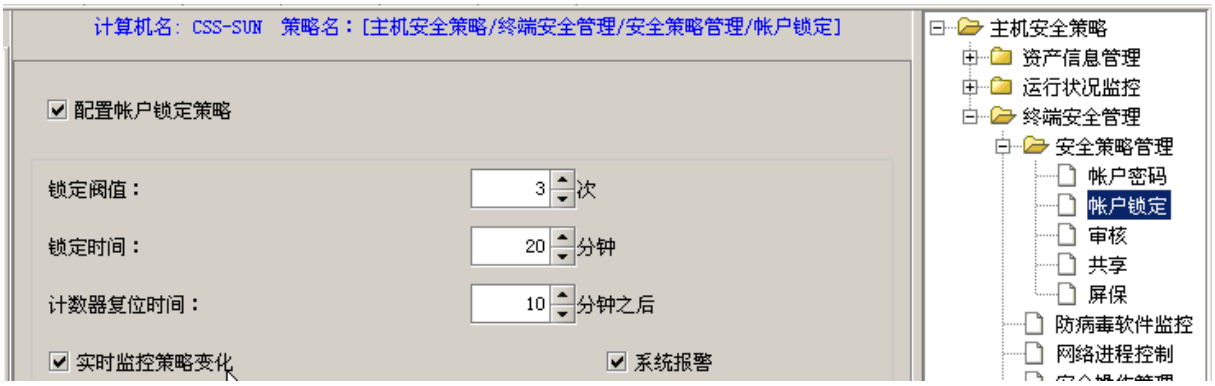


图 5-76　系统安全策略——帐户锁定

◆ **审核**

选择“安全策略管理”下的“审核”，进入“审核”设置界面，如图 5-77 所示。点选“配置审核策略”复选框，选择审核策略项，如登录事件、帐户管理、目录服务访问等，然后勾选“成功”或“失败”审核操作项，最后选择“实时监控策略变化”和“系统报警”。策略下发成功后，若系统发现客户端审核项设置与下发策略不一致时，产生报警。

提示：安全策略的帐户密码、帐户锁定和审核项，可以在客户端的“控制面板”→“管理工具”→“本地安全策略”中找到对应项，并查看策略的执行情况。

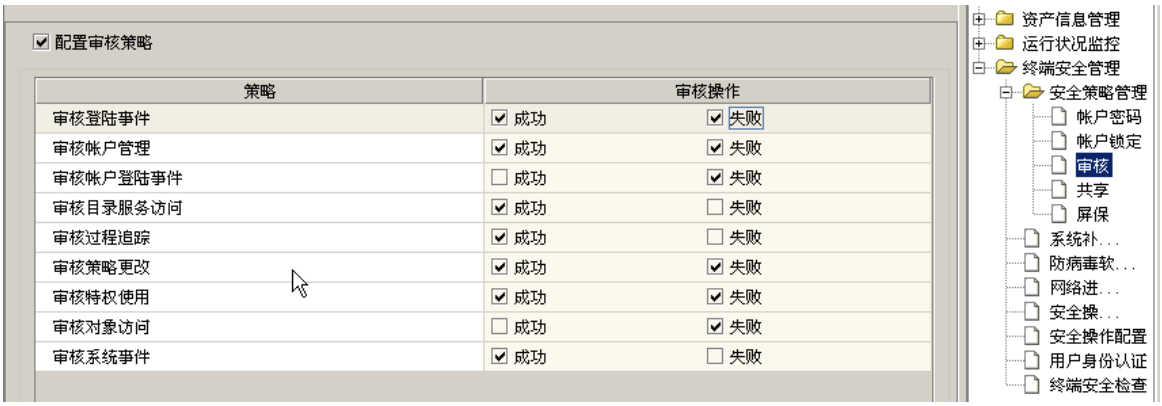


图 5-77　系统安全策略——审核

◆ 共享

选择 “安全策略管理”下的“共享”，进入“共享”设置界面，如图 5-78 所示。点选“配置共享策略”复选框，选择“远程管理共享”、“默认共享”、“远程 IPC”或“普通共享”，其中“远程 IPC”为必选项。也可以选择“实时监控策略变化”和“系统报警”。策略下发成功后，若系统发现客户端共享设置与下发策略要求不一致时，产生报警。

提示：用户可以在客户端的“控制面板”→“管理工具”→“计算机管理”中找到对应项查看。

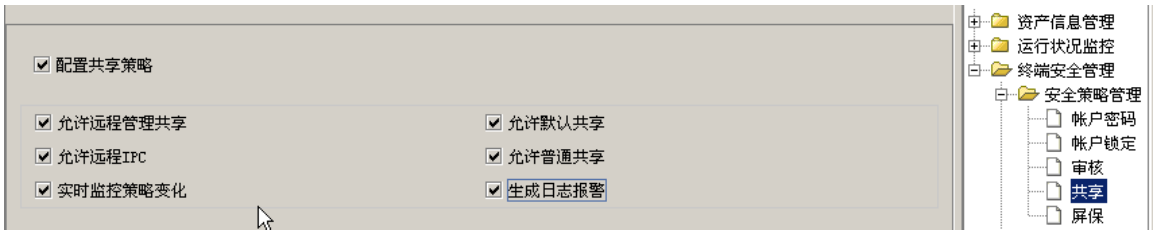


图 5-78　系统安全策略——共享

◆ 屏保

选择 “安全策略管理”下的“屏保”，进入“屏保”设置界面，如图 5-79 所示。

勾选“配置屏保策略”复选框，输入等待时间，选择“恢复时使用密码保护”，将策略应用下发，收到策略的客户端执行控制台下发的屏保策略。用户可以在客户端桌面，点击鼠标右键，选择“属性”菜单，查看屏幕保护程序，这样验证客户端是否与控制台下发的屏保策略一致。

勾选“配置密码保护屏幕保护程序策略”复选框，选择“未设置”、“已启用”或“已禁用”，将策略应用下发，收到策略的客户端执行控制台下发的密码保护策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→控制面板→显示→密码保护屏幕保护程序”找到对应项，可以验证与控制台下发的策略是否一致。

图 5-79　系统安全策略——屏保

勾选“配置屏幕保护程序策略”复选框，选择“未设置”、“已启用”或“已禁用”，将策略应用下发，收到策略的客户端执行控制台下发的屏幕保护程序策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→控制面板→显示→屏幕保护程序”找到对应项，验证与控制台下发的策略是否一致。

勾选“配置可执行的屏幕保护程序名称”复选框，选择“未设置”，“已禁用”，或“已启用”，以及可执行的屏幕保护程序名称，将策略应用下发，收到策略的客户端执行控制台下发的屏幕保护程序策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→控制面板→显示→可执行的屏幕保护程序名称”找到对应项，可以验证与控制台下发的策略是否一致。

如果下发屏保策略时，勾选了“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的屏保策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改屏保策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的屏保策略。

◆ 自动播放

选择 “安全策略管理”下的“自动播放”，进入用户或计算机自动播放策略设置界面，如图 5-80 所示。

勾选“配置用户自动播放策略”复选框，选择驱动器类型和自动播放状态，将策略应用下发，收到策略的客户端执行控制台下发的自动播放策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→系统→关闭自动播放”找到对应项，验证与控制台下发的策略是否一致。

图 5-80　系统安全策略——自动播放

勾选“配置计算机自动播放策略”复选框，选择驱动器类型和自动播放状态，将策略应用下发，收到策略的客户端执行控制台下发的自动播放策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“计算机配置→管理模板→系统→关闭自动播放”找到对应项，可以验证与控制台下发的策略是否一致。

如果下发“自动播放”策略时，勾选了“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的自动播放策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改自动播簇策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的自动播放策略。

◆ 脱机文件

选择 “安全策略管理”下的“脱机文件”，进入登录或注销时同步脱机文件策略设置界面，如图 5-81 所示。

勾选“配置登录时同步脱机文件策略”复选框，选择当前同步状态（未设置、已启用、已禁用），将策略应用下发，收到策略的客户端执行控制台下发的脱机文件策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“计算机配置→管理模板→网络→脱机文件→在登录时同步所有脱机文件”中找到对应项，验证与控制台下发的策略是否一致。

勾选“配置注销时同步脱机文件策略”复选框，选择当前同步状态（未设置、已启用、已禁用），将策略应用下发，收到策略的客户端执行控制台下发的脱机文件策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“计算机配置→管理模板→网络→脱机文件→注销时同步所有脱机文件”找

到对应项，可以验证与控制台下发的策略是否一致。

图 5-81　系统安全策略——脱机文件

如果下发“脱机文件”策略时，勾选了“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的脱机文件策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改脱机文件策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的脱机文件策略。

◆ **WIN 组件**

选择 “安全策略管理”下的“WIN 组件”，进入 WIN 组件策略设置界面。

（1）在“登录脚本”标签页，勾选“配置登录脚本策略”复选框，单击“增加脚本”按钮，添加脚本文件，如图 5-82 所示。将策略应用下发，收到策略的客户端执行控制台下发的登录脚本策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→Windows 设置→脚本→登录”找到对应项，可以验证与控制台下发的策略是否一致。

如果下发“登录脚本”策略时，勾选了下面的“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的登录脚本策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改登录脚本策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的登录脚本策略。

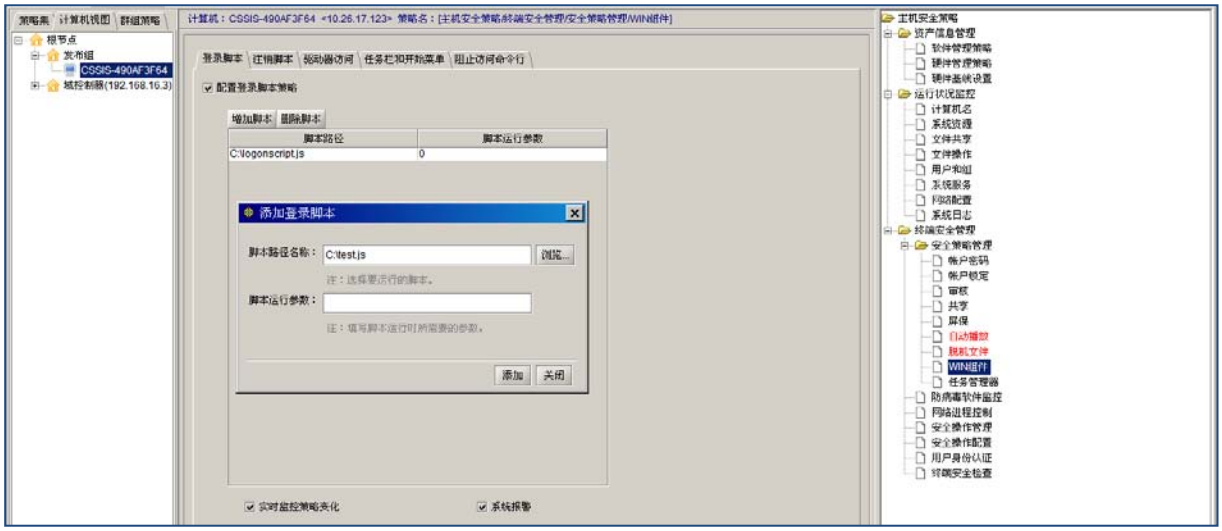


图 5-82　WIN 组件——登录脚本

（2）在“注销脚本”标签页，勾选“配置注销脚本策略”复选框，单击“增加脚本”按钮，添加脚本文件，如图 5-83 所示。将策略应用下发，收到策略的客户端执行控制台下发的注销脚本策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→Windows 设置→脚本→注销”找到对应项，验证与控制台下发的策略是否一致。

如果下发“注销脚本”策略时，勾选了下面的“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的注销脚本策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改注销脚本策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的注销脚本策略。

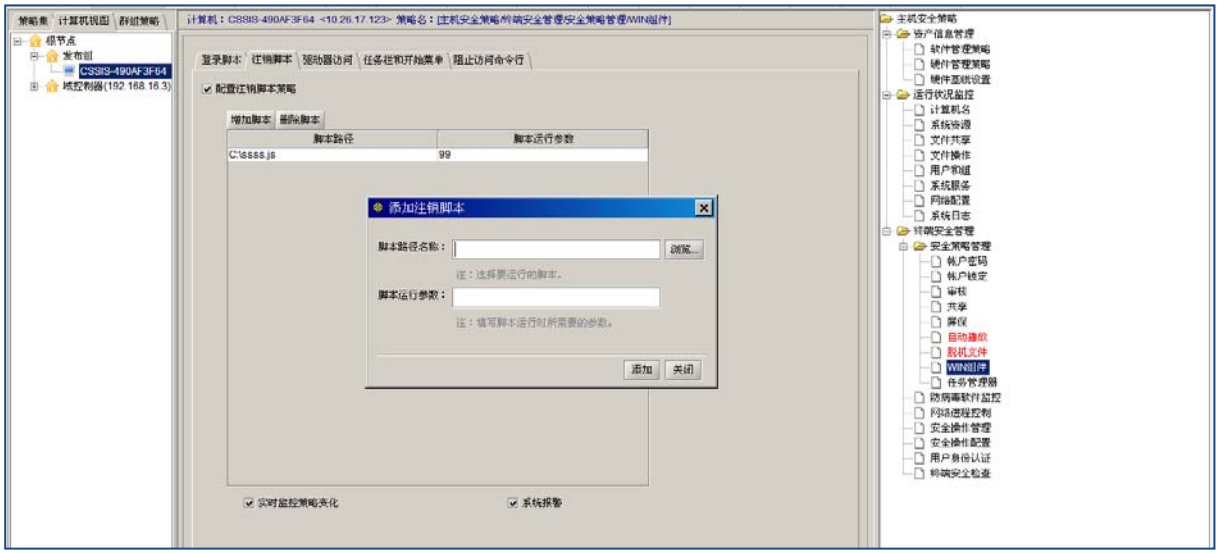


图 5-83　WIN 组件——注销脚本

（3）在“驱动器访问”标签页，勾选“配置隐藏驱动器策略”复选框，选择当前驱动器状态（未设置、已启用、已禁用），如果选择已启用，从选择框中选择限制的驱动器类型，如图 5-84 所示。将策略应用下发，收到策略的客户端执行控制台下发的隐藏驱动器策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→Windows 组件→Windows 资源管理器→隐藏‘我的电脑’中的这些指定的驱动器”找到对应项，验证与控制台下发的策略是否一致。

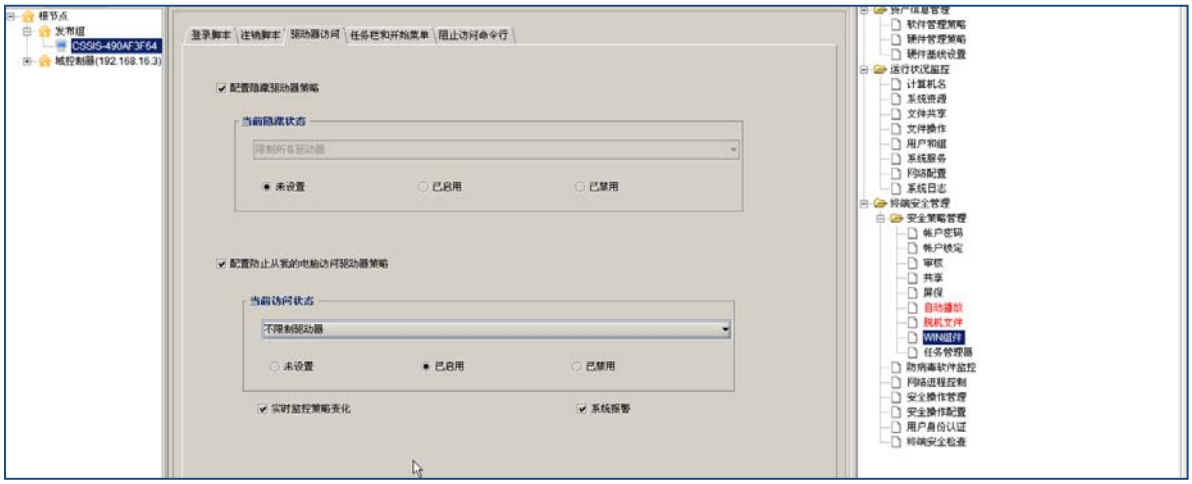


图 5-84　WIN 组件——驱动器访问

同理，勾选“配置防止从我的电脑防问驱动器策略”复选框，选择当前驱动器状态（未设置、已启用、已禁用），如果选择已启用，从选择框中选择限制的驱动器类型。将策略应用下发，收到策略的客户端执行控制台下发的防止从我的电脑防问驱动器策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→Windows 组件→Windows 资源管理器→防止从我的电脑防问驱动器”找到对应项，验证与控制台下发的策略是否一致。

如果下发“驱动器访问”策略时，勾选了下面的“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的驱动器访问策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改驱动器访问策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的驱动器访问策略。

（4）在“任务栏和开始菜单”标签页，勾选“配置删除运行策略”复选框，选择当前删除运行状态（未设置、已启用、已禁用），如图 5-85 所示。将策略应用下发，收到策略的客户端执行控制台下发的删除运行策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→Windows 组件→任务栏和开始菜单→从开始菜单中删除运行菜单”找到对应项，验证与控制台下发的策略是否一致。

同理，勾选“配置添加注销策略”复选框，选择当前添加状态（未设置、已启用、已禁用），。将策略应用下发，收到策略的客户端执行控制台下发的添加注销策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→Windows 组件→任务栏和开始菜单→将注销添加到

开始菜单”找到对应项，验证与控制台下发的策略是否一致。

如果下发“任务栏和开始菜单”策略时，勾选了下面的“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的“任务栏和开始菜单”策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改“任务栏和开始菜单”策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的“任务栏和开始菜单”策略。

图 5-85　WIN 组件——任务栏和开始菜单

（5）在“阻止访问命令行”标签页，勾选“配置阻止访问命令行策略”复选框，选择当前阻止状态（未设置、已启用、已禁用），如图 5-86 所示。将策略应用下发，收到策略的客户端执行控制台下发的阻止访问命令行策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→系统→阻止访问命令提示符”找到对应项，验证与控制台下发的策略是否一致。

如果下发“阻止访问命令行”策略时，勾选了下面的“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的“任务栏和开始菜单”策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改“阻止访问命令行”策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的“阻止访问命令行”策略。

图 5-86　WIN 组件——阻止访问命令行策略

◆ 任务管理器

选择 “安全策略管理”下的“任务管理器”，进入任务管理器策略设置界面，如图 5-87 所示。

勾选“配置任务管理器策略”复选框，选择当前同步状态（未设置、已启用、已禁用），将策略应用下发，收到策略的客户端执行控制台下发的任务管理器策略。在客户端运行 gpedit.msc 打开组策略编辑器，点击“用户配置→管理模板→系统→Ctrl+Alt+Del 选项→删除任务管理器”找到对应项，验证与控制台下发的策略是否一致。

如果下发“任务管理器”策略时，勾选了下面的“实时监控策略变化”和“系统报警”，那么策略下发成功后，客户端不能更改自己的“任务管理器”策略，必须和控制台下发的策略一致。即使客户端尝试进行了更改，系统也会实时监测到策略的变化，并改回到控制台下发的策略状态。同时，客户端试图更改“任务管理器”策略的行为，系统会产生报警信息，用户可以在控制台报警信息列表中查看。当然，如果控制台在下发策略时，没有勾选“实时监控策略变化”，那么，客户端是可以更改自己的“任务管理器”策略。

图 5-87　系统安全策略——任务管理器

◆ **关于 Windows 组策略管理器的使用**

在“开始”→“运行”中输入“gpedit.msc”打开组策略管理器，如图 5-88 所示。选择左侧的配置类型，可以在右侧的界面中，查看所包含的策略项。

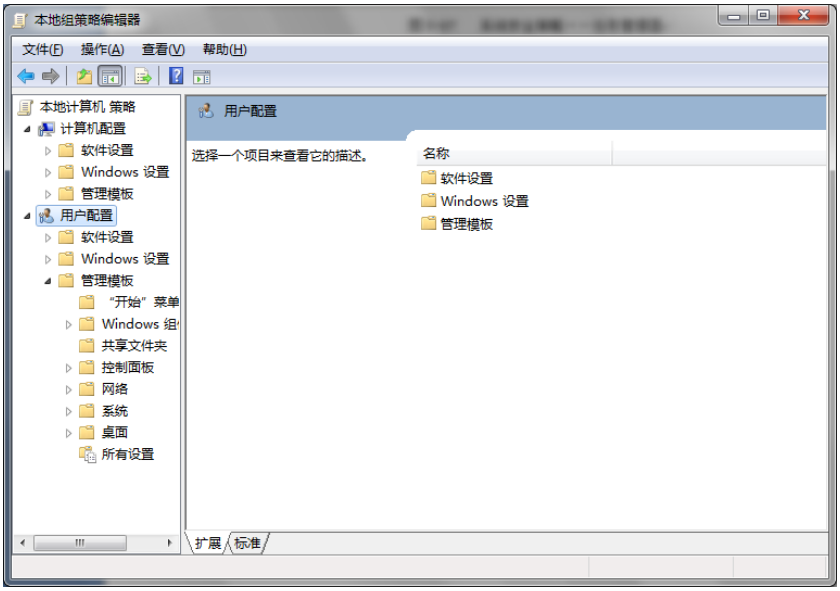


图 5-88　Windows 组策略管理器

从右侧视图界面打开策略项可以看到具体策略的内容，以及配置选择，如图 5-89 所示。例如：“删除任务管理器”策略，通过改变启用状态，决定是否使用策略功能。

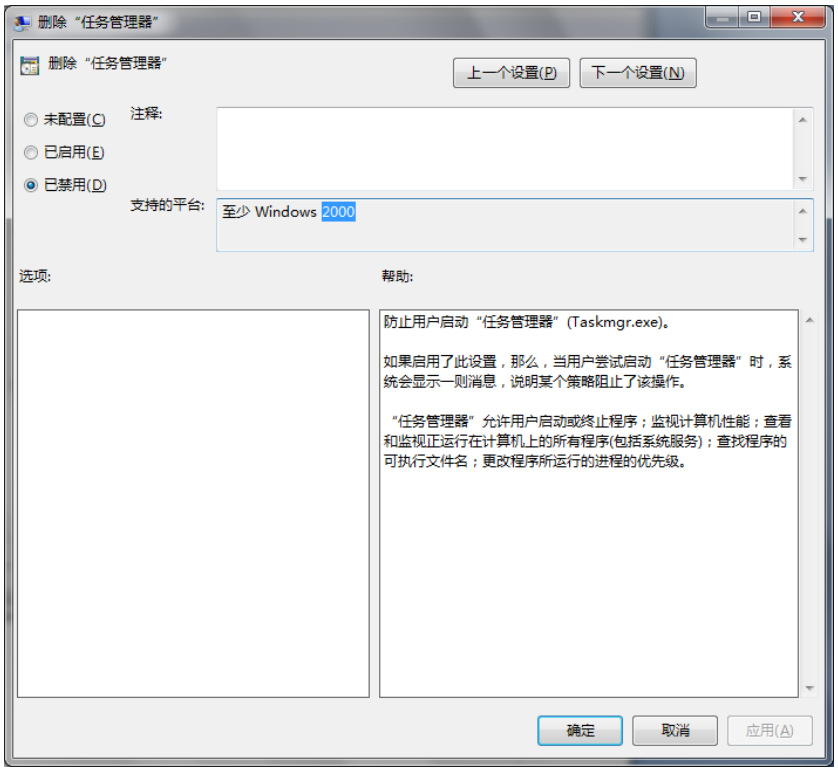


图 5-89　“删除任务管理器”策略

5.6.3.2　防病毒软件监控

在安全管理中心中，在左侧的计算机视图中选定计算机，用鼠标单击右侧“终端安全管理”中的“防病毒软件监控”，进入防病毒软件监控设置界面，如图 5-90 所示。可以设置常用防病毒软件过期（也就是病毒库过期）几天报警，然后将策略应用到指定的组织或计算机。

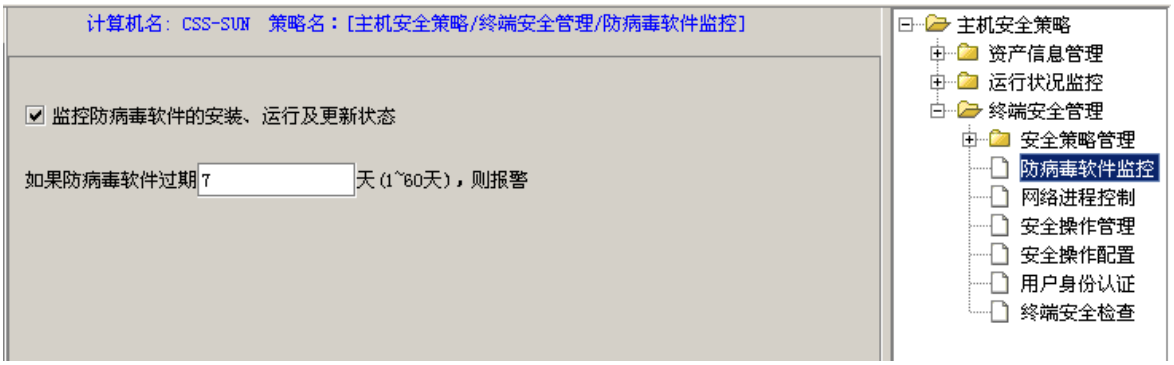


图 5-90　设置病毒软件监控策略

5.6.3.3　网络进程控制

1．在安全管理中心中，用鼠标单击 “主机安全策略”→“终端安全管理”→“网络进程控制”，进入网络进程控制界面。在“网络进程控制”选项卡中，可以在下拉框中选择“放开所有进程连接网络”，在“进程名”后面空白框中输入进程名，然后单击“添加”加入黑名单列表中，用户根据需要选择“监测所有网络进程的变化情况，并记录日志”，如图 5-91 所示。客户端收到策略后，禁止黑名单中的进程。

图 5-91　网络进程控制

2. 在“网络服务控制”选项卡中，可以在下拉框中选择“禁止所有进程开启网络监听”，在“进程名”和“端口号”后面空白框中输入进程名和端口号，然后单击“添加”加入白名单列表中，用户根据需要选择“监测所有网络服务的变化情况，并记录日志”，如图 5-92 所示。客户端收到策略后，只放开白名单中的服务进程。

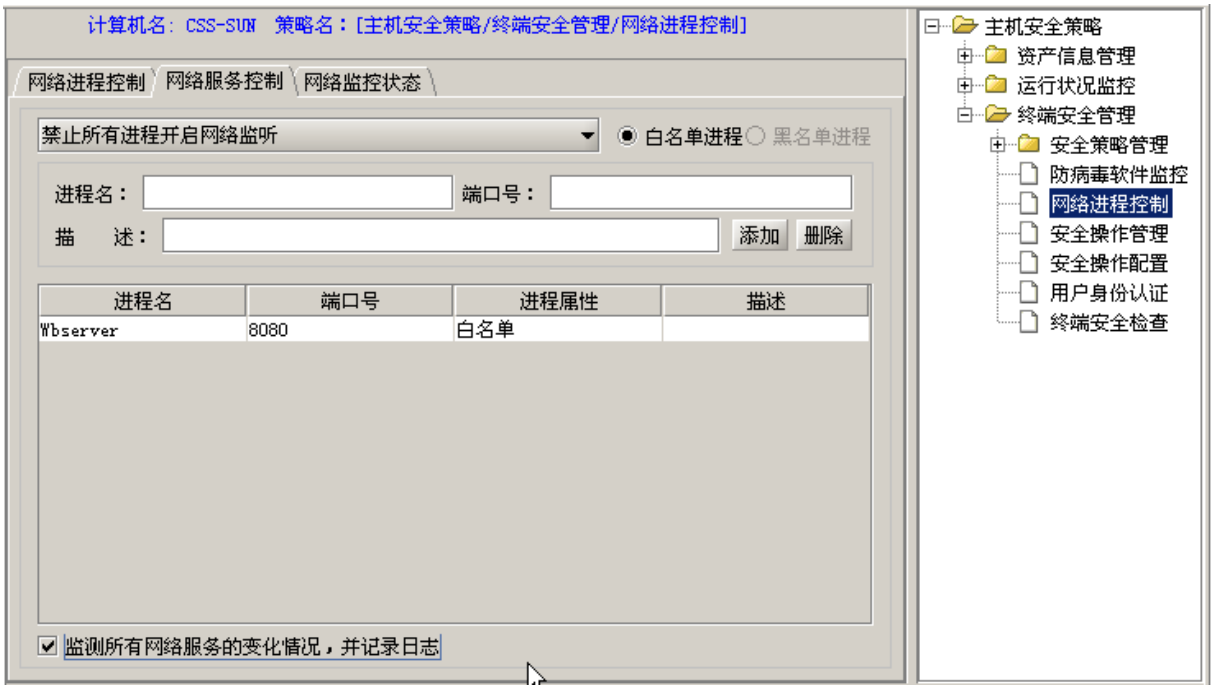


图 5-92　网络服务控制

提示：

(1) 并列的端口号中间用逗号隔开(80,81,83),连续的端口号用“-”隔开(80-88).

(2) 如果设置有条件访问网络进程，同时下发黑名单和白名单控制策略，对黑白名单以外的进程允许访问，按白名单处理。

3. 在“网络监控状态”选项卡中，可以根据用户需要设置最大连接数和最大并发连接数，以及超过最大连接是否报警，如图 5-93 所示。客户端收到策略后，超过设定的最大连接数或并发连接数时将报警。

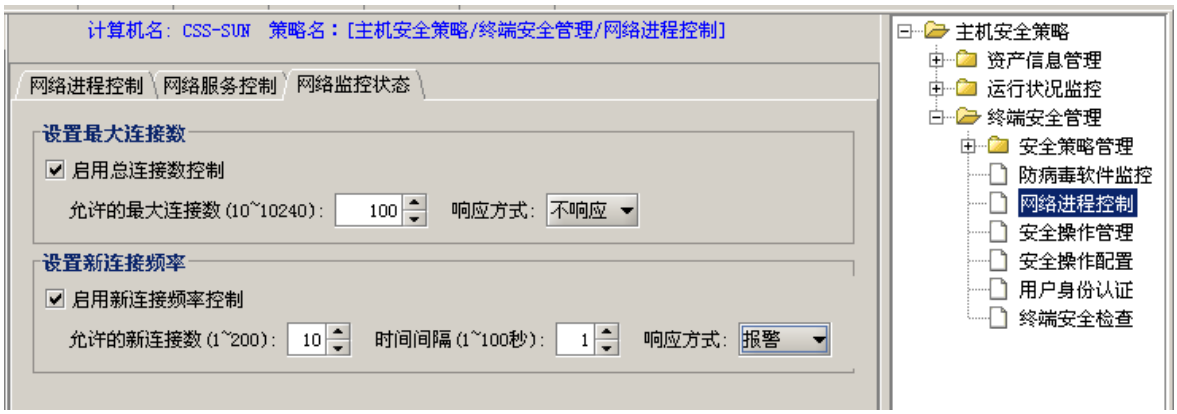


图 5-93　网络监控状态

5.6.3.4　安全操作管理

安全操作管理能够及时清理系统在处理敏感信息所遗留的临时文件，包括 Word、Excel、Powerpoint 等通用办公软件所产生的临时文件、网络访问所遗留的 Cookie 文件、网页浏览所产生的历史纪录、注册表的临时键值等相关内容，由策略统一配置安全清除的时间间隔。具体操作如下：

在安全管理中心中，用鼠标单击“主机安全策略”→“终端安全管理”→“安全操作管理”，进入安全操作管理界面，如图 5-94 所示。选择清除内容和间隔时间后，将策略应用到指定的组织或计算机。客户端收到策略后，在指定的时间内自动清除设定项。

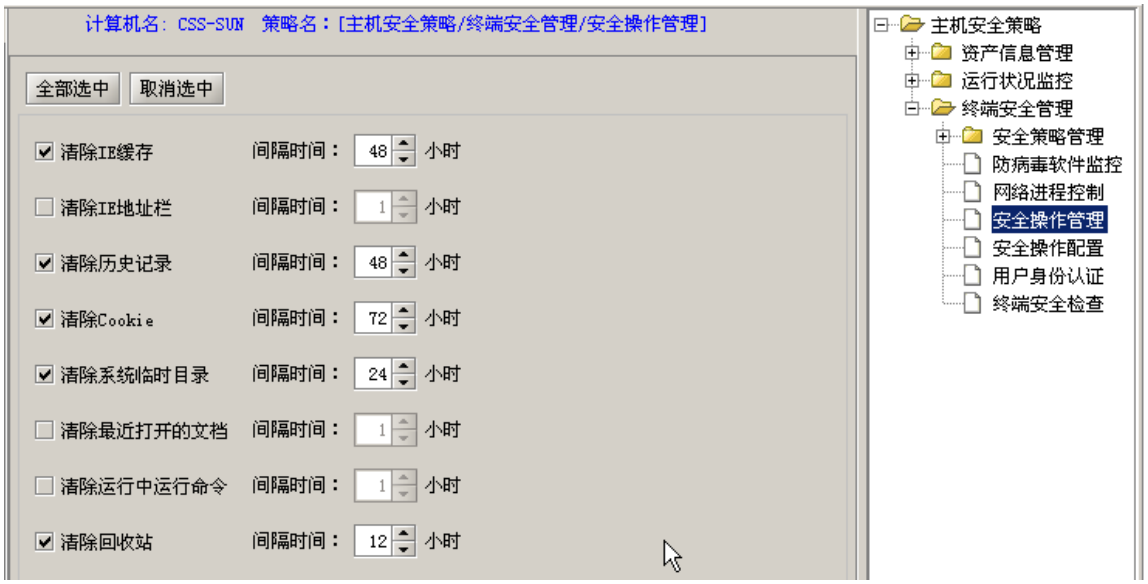


图 5-94　安全操作管理

注意：如果在“清除运行中运行命令”后面设置“间隔时间”，到时该命令没有生效，这时需要将客户端注销或者重启，该命令才会生效。

5.6.3.5　安全操作配置

用户删除涉密信息文件时，操作系统所带的删除工具已不能真正把数据从磁盘上删除，大多还可以通过数据恢复工具来恢复，给用户信息安全带来相当大的隐患。中软 UEM8.0 系统可以通过安全操作配置，设置安全删除时数据回添次数，这样实现涉密信息的安全删除。

在安全管理中心中，用鼠标单击“主机安全策略”→“终端安全管理”→“安全操作配置”，进入安全操作配置界面，如图 5-95 所示。输入“安全删除时的数据回填次数”，选择执行安全删除操作的快捷键“Shift+Delete”或者“Delete”。选择“Delete”时，必须同时勾选“Shift+Delete”。因选择“Delete”执行安全删除操作时风险较大，可能不小心按住“Delete”键，将导致删除的文件无法恢复，所以请慎重选择。最后，点击“应用到”按钮，把策略下发给选定的组织或计算机。

提示：数据回填次数：在对文件进行安全删除操作时，对存储该文件的磁盘空间反复写入其它数据的次数。如果数据回填次数添的较大，当安全删除较大的文件时，会感觉很慢。

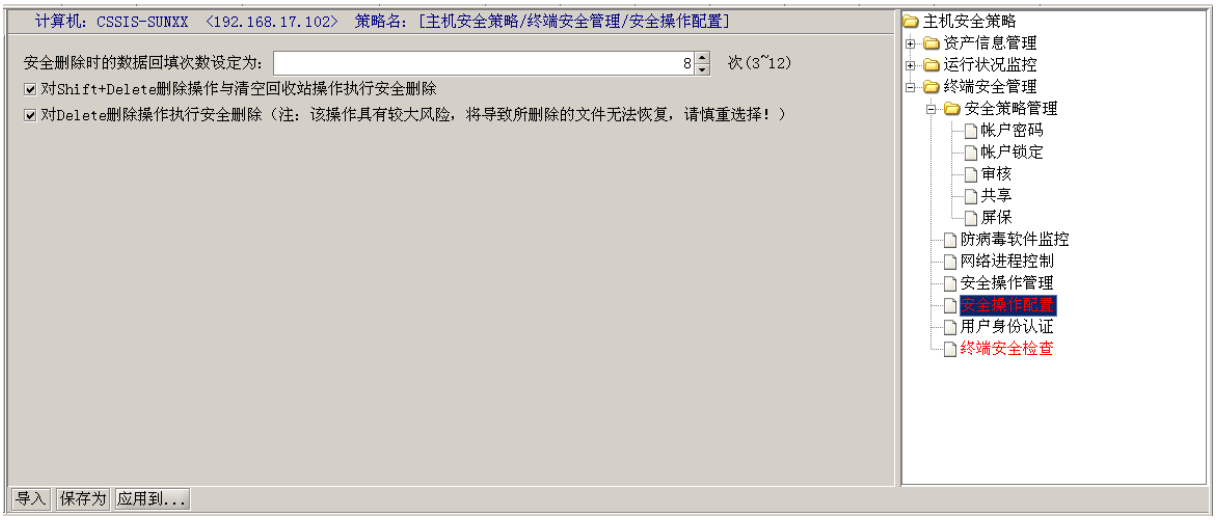


图 5-95　安全操作管理

5.6.3.6　用户身份认证

在安全管理中心中，用鼠标单击“主机安全策略”→“终端安全管理”→“用户身份认证”，进入用户身份认证界面，如图 5-96 所示。勾选用户身份，从下拉框中选择控制方式，然后把策略下发给选定的组织或计算机。

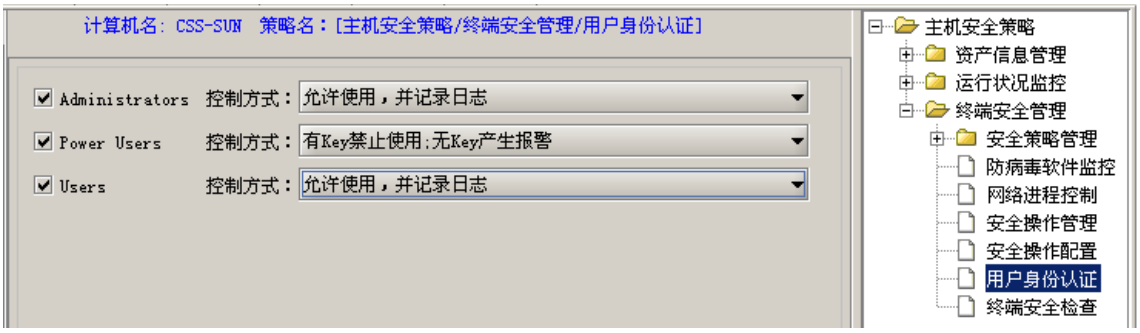


图 5-96　用户身份认证

提示：客户端分两个版本,有 key 版本和 nokey 版本。如果客户端安装的是有 key 版本，当 Power Users 用户选择“有 Key 禁止使用，无 Key 产生报警”这个选项时，就不能登录。反之，客户端能够登录，但产生报警信息。

5.6.3.7　终端安全检查

■　**操作系统补丁检查**

1．在终端安全管理中，用鼠标单击“终端安全管理”→“终端安全检查”→“操作系统补丁检查”，进入操作系统补丁检查策略设置界面，如图 5-97 所示。

图 5-97　设置操作系统补丁检查策略

在“操作系统补丁检查”界面，首先检查终端大补丁安装情况。从下拉框中选择操作系统的最低补丁，如果没有达到最低要求，可禁止连接网络或禁止使用 U 盘。

在下面的补丁列表中，点击表头下面的空白框，然后单击右边出现的浏览按钮 ...，会弹出查询条件框。输入查询条件后，将在补丁列表中过滤出所要查看的补丁。另外，单击表头右边的向上、或向下小箭头，可以实现该列的升序或降序排列，如图 5-98 所示。

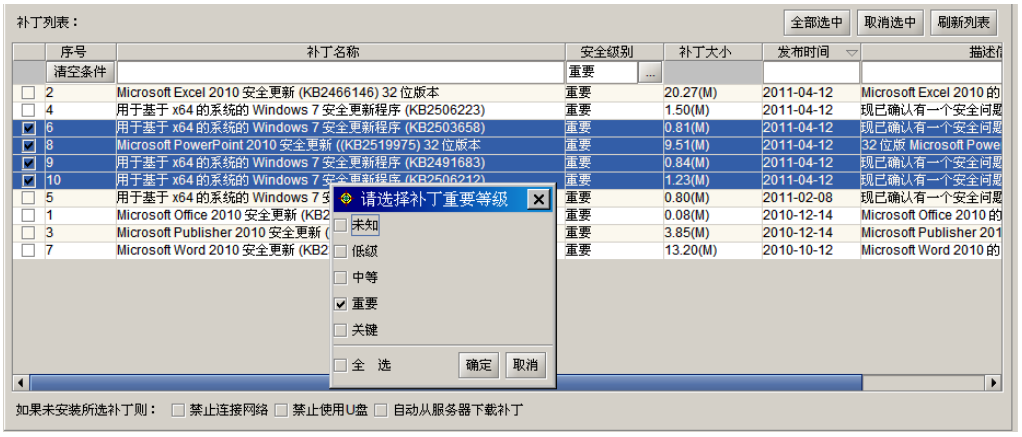


图 5-98　补丁排序和过滤图

用户可以根据自己的需要，选择某些具体补丁，设置“如果未安装禁止连接网络”，“禁止使用 U 盘”或者“自动从服务器下载补丁”等，最后将策略下发。

提示：禁止连接网络：是指禁止客户端与 UEM 服务器和补丁服务器以外的其它网络连接。

■ 防病毒软件检查

单击“终端安全检查”中的“防病毒软件检查”标签页，进入“防病毒软件检查”策略设置界面，如图 5-99 所示。用户可以设置“如果防病毒软件未运行，禁止连接网络”或者“防病毒软件超过设定的天数未更新，禁止使用 U 盘”，最后将策略应用到指定的组织或计算机。

提示：该系统对监测不到防病毒软件更新时间的，认为符合要求，允许连接网络。

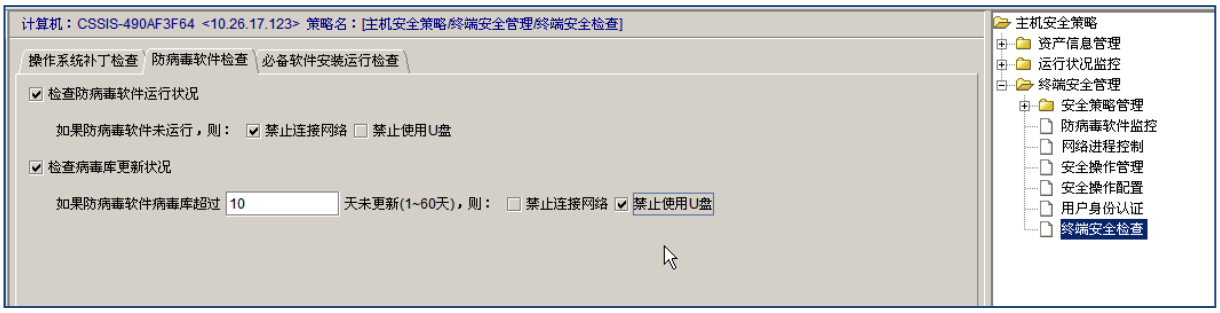


图 5-99　设置防病毒软件检查策略

■ 必备软件安装运行检查

1. 单击“终端安全检查”中的“必备软件安装运行检查”标签页，进入到“必备软件库管理”与“必备软件安装运行检查”策略设置界面，如图 5-100 所示。上面为必备软件库列表，下面策略软件列表，都能按关键字段检索和排序。

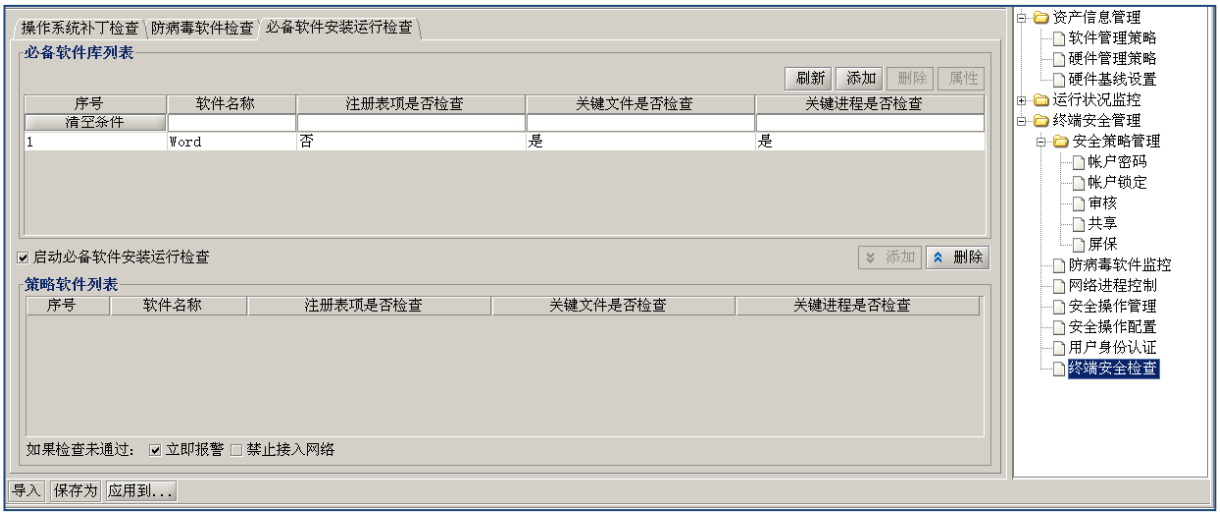


图 5-100　必备软件安装运行检查

2. 单击上面的“添加”按钮，弹出“添加必备软件”界面，向必备软件库中增加新的必备软件如图 5-101 所示。输入任意的“必备软件名称”，选择是否启动注册表项检查、关键文件检查、关键进程检查，这三项可以单选，也可以多选。然后，单击各个“添加”按钮，分别添加各检查项的路径或具体值，它们将显示在检查项的列表中，用户可以修改和删除这些检查项列表。最后，单击“确定”按钮，返回前面的“必备软件安装运行检查”界面。

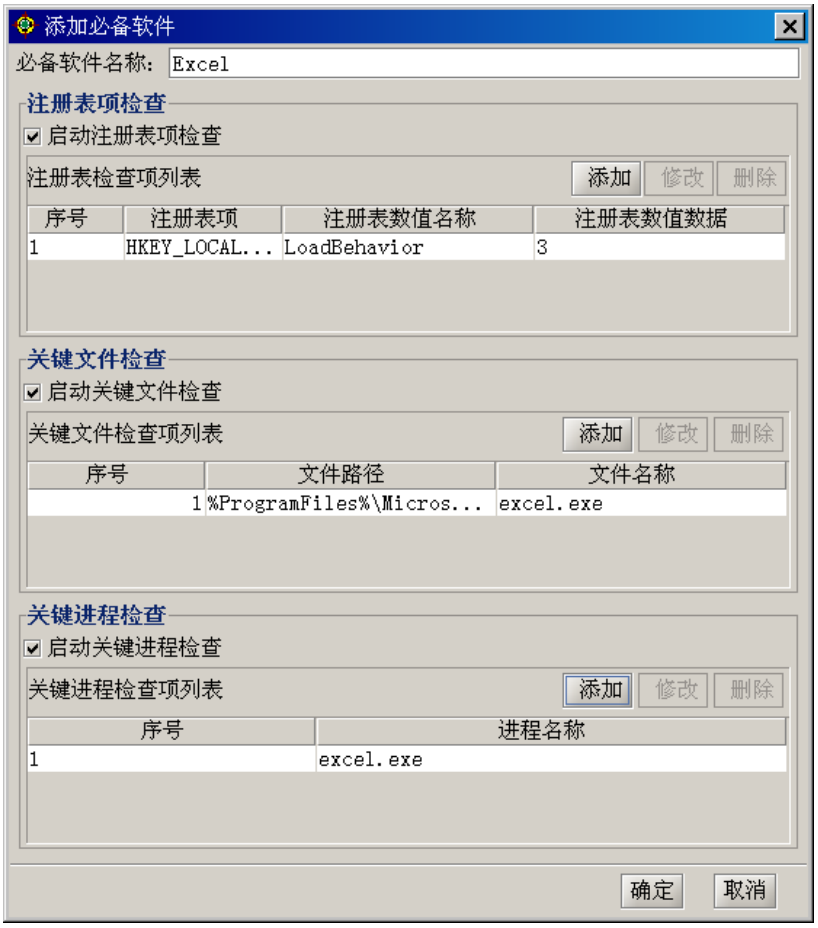


图 5-101　添加必备软件界面

3. 在“必备软件库列表”中，可以看到刚添加的软件列表。选择某一软件，单击下面的“添加”按钮，添加到策略软件列表中，如图 5-102 所示。

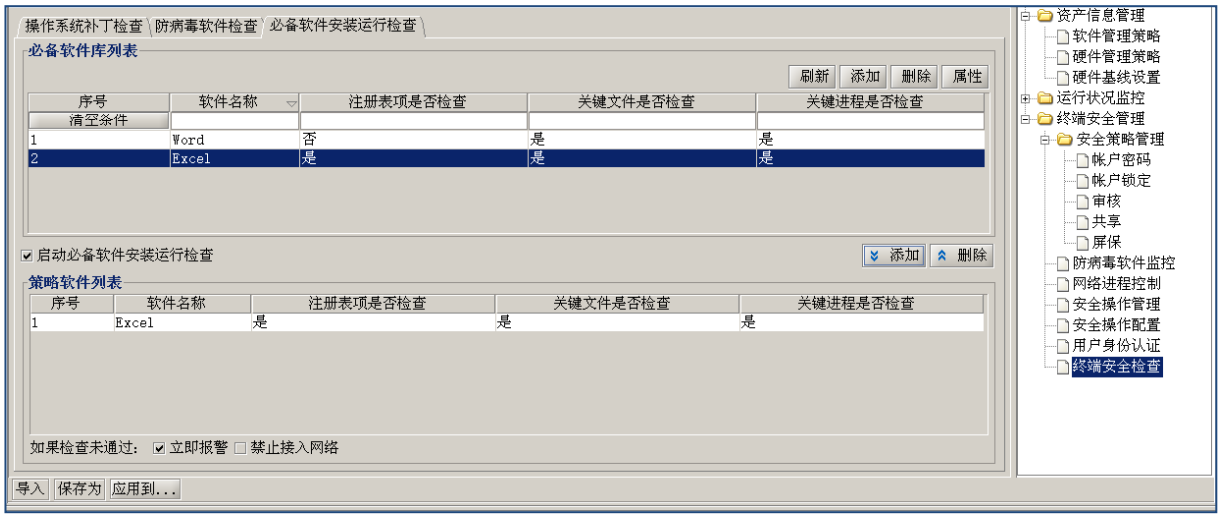


图 5-102　添加到策略软件列表

4. 按照同样的方法，添加多个必备软件至必备软件库中，如果需要对其执行安装运行检查，可进一步将其添加至策略软件列表中”。最后，单击“应用到”按钮，将策略下发到指定的组织和计算机。终端计算机收到策略后，如果没有启动必备软件进程，或者在指定的位置下没有发现注册表项和关键文件，或者注册表数值数据存在与策略设置不符的情形，都会按策略设置报警或禁止接入网络。

提示：

1. 当策略下发后，系统监测到客户端“必备软件进程”没有启动时，产生一条告警信息。如果启动“必备软件进程”后，再次关闭该进程，就会再产生一条告警信息。告警信息可以在统计审计分析中查看。

2. 进行注册表项添加时，注册表数值数据可以为空，在这种情况下只检查注册表数值是否存在，而不再进行注册表数值数据的匹配处理。

5.7 远程管理

在安全管理中心中，单击“远程管理”，可以查看在线主机的驱动信息、硬件环境、进程信息和内存信息等，并能对在线主机的进程、服务和共享文件夹进行远程管理。这里重点讲一下远程管理和远程协助，对远程信息查看做略讲。

5.7.1 驱动信息

在“远程管理”界面中，任选一在线主机，单击“驱动信息”，稍等，出现远程客户端驱动信息的详细列表，如图 5-103 所示。在这里可以查看远程客户端安装的所有驱动程序。

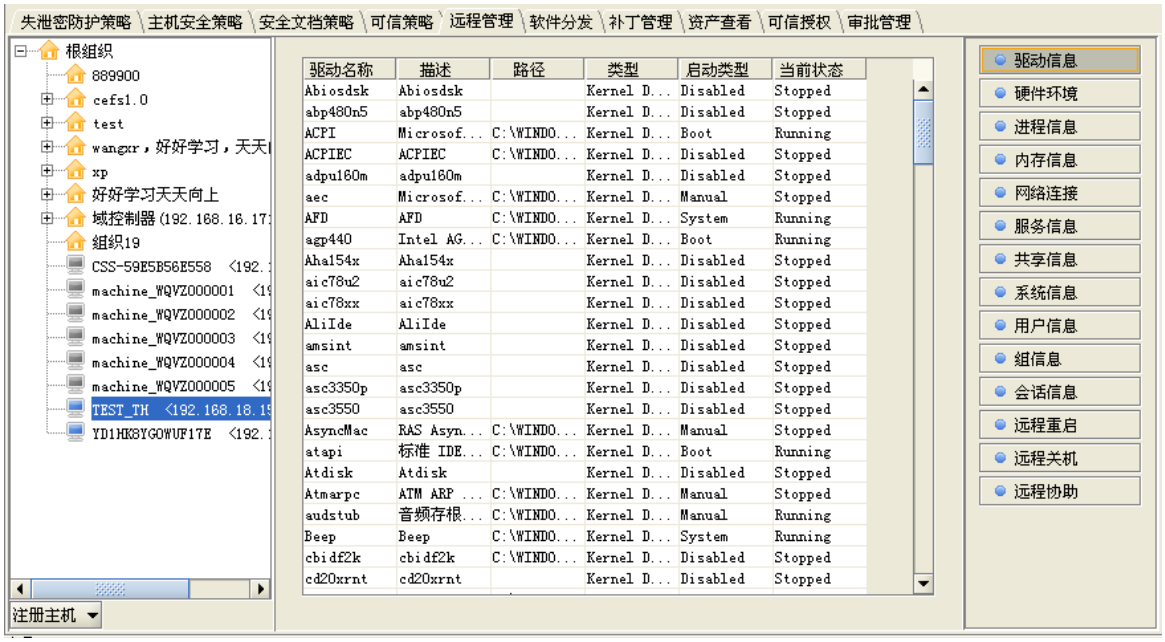


图 5-103　远程客户端驱动信息

5.7.2　硬件环境

在“远程管理”界面中，任选一在线主机，单击“硬件环境”，稍等，出现远程客户端所有硬件列表，如图 5-104 所示。在这里可以查看远程客户端使用什么样的硬件。

图 5-104　远程客户端硬件信息

5.7.3　进程信息

1. 在“远程管理”界面中，任选一在线主机，单击“进程信息”，开始获取进程信息，如图 5-105 所示。稍等，出现远程客户端进程信息的详细列表。

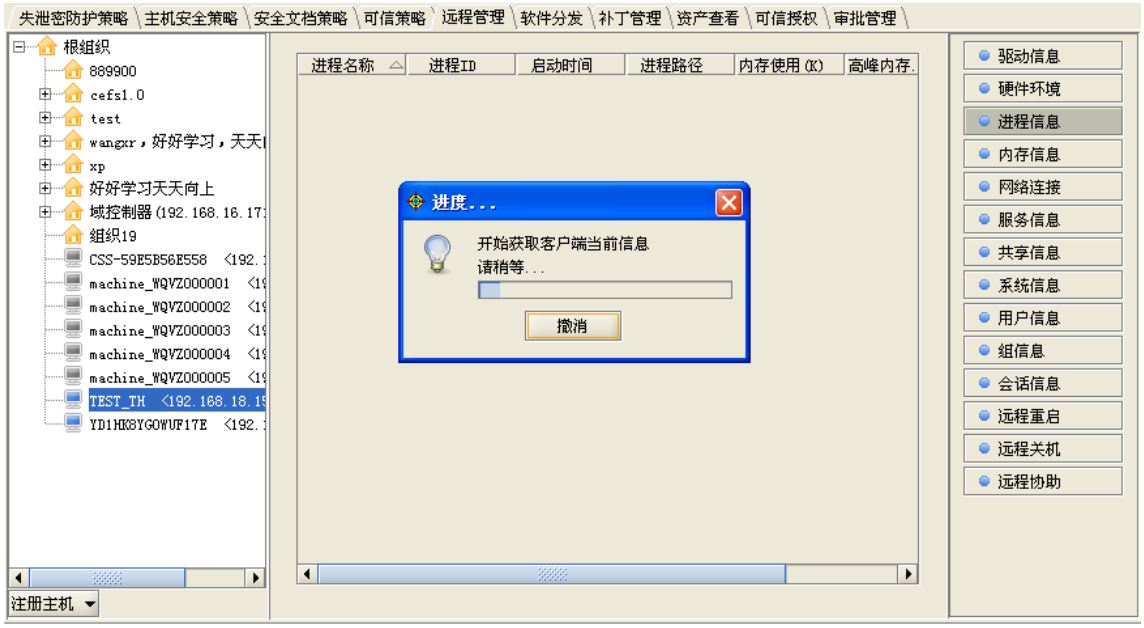


图 5-105　　获取系统进程信息

2. 点击列表项名称后面的小箭头，可以按升序或降序排列，方便查看，如图 5-106 所示。

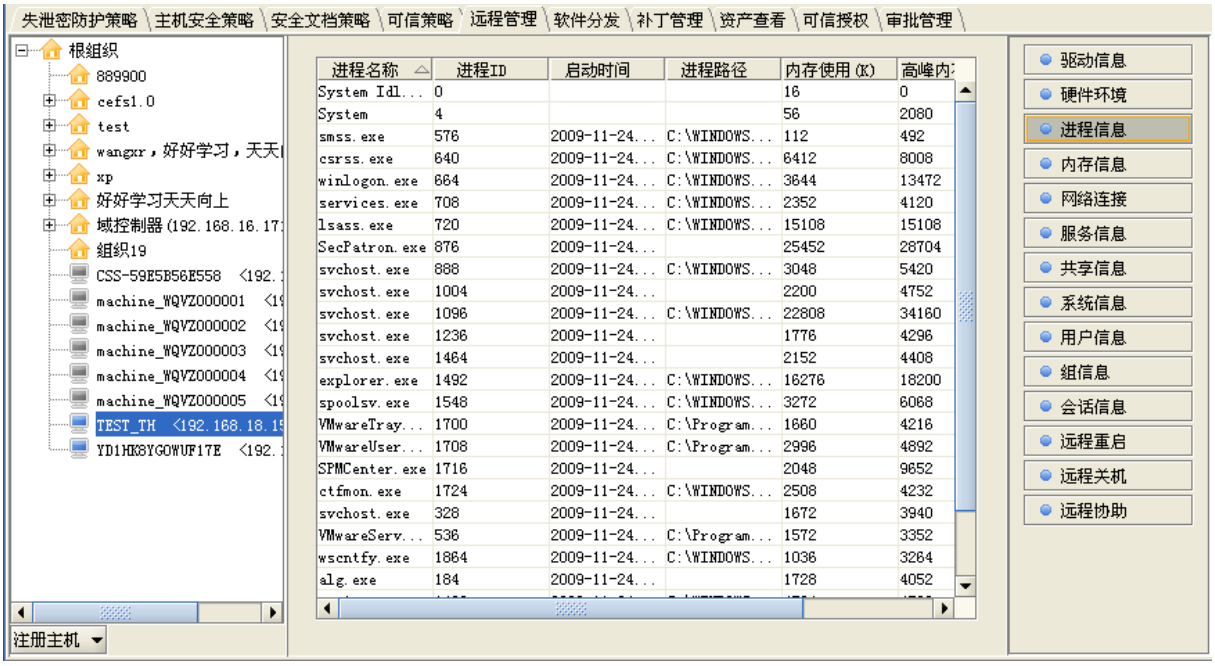


图 5-106　系统进程详细列表

3. 单选某些进程，单击右键菜单，执行“结束进程”命令，可以中止该进程，实现计算机的远程管理，如图 5-107 所示

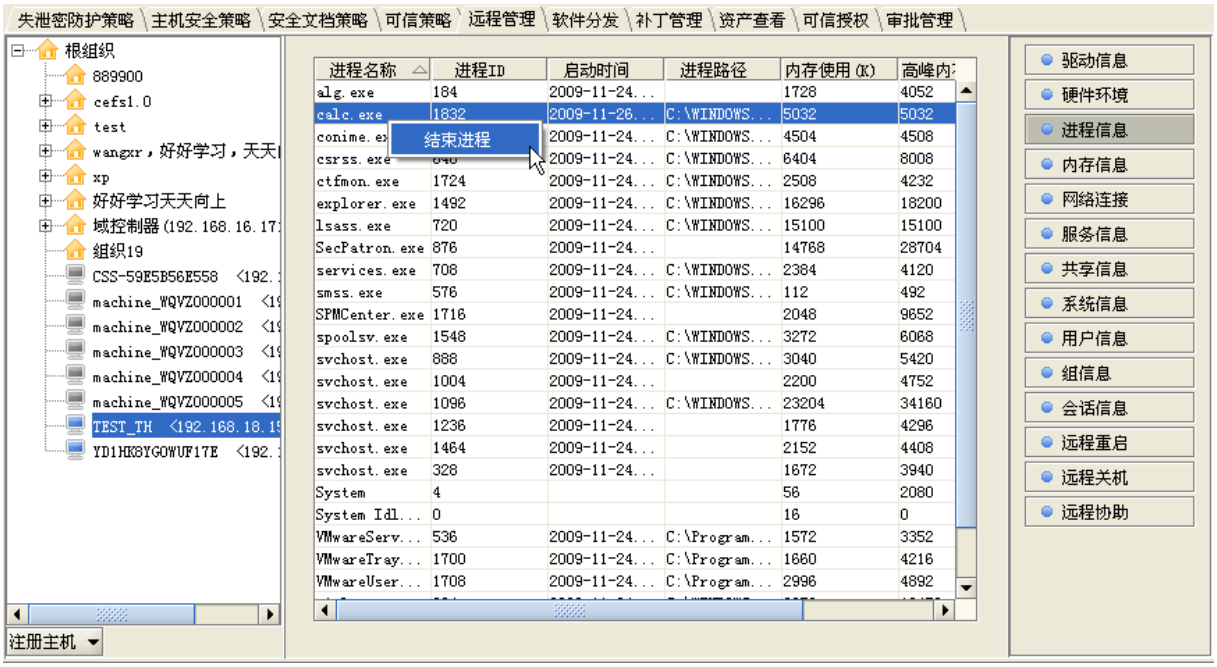


图 5-107　远程结束计算机进程

5.7.4　内存信息

在“远程管理”界面中，任选一在线主机，单击“内存信息”，稍等，出现远程客户端内存信息列表，用户可以查看，如图 5-108 所示。

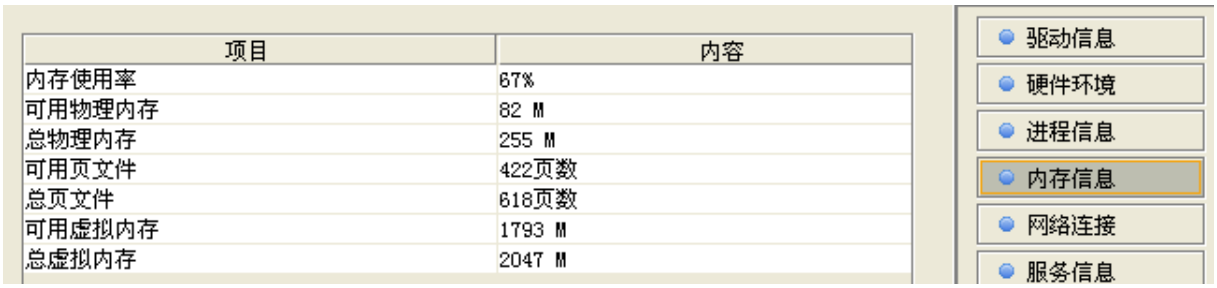


图 5-108　　查看远程客户端内存信息

5.7.5　网络连接

在“远程管理”界面中，任选一在线主机，单击“网络连接”，稍等，查看远程客户端网络连接情况，如图 5-109 所示。

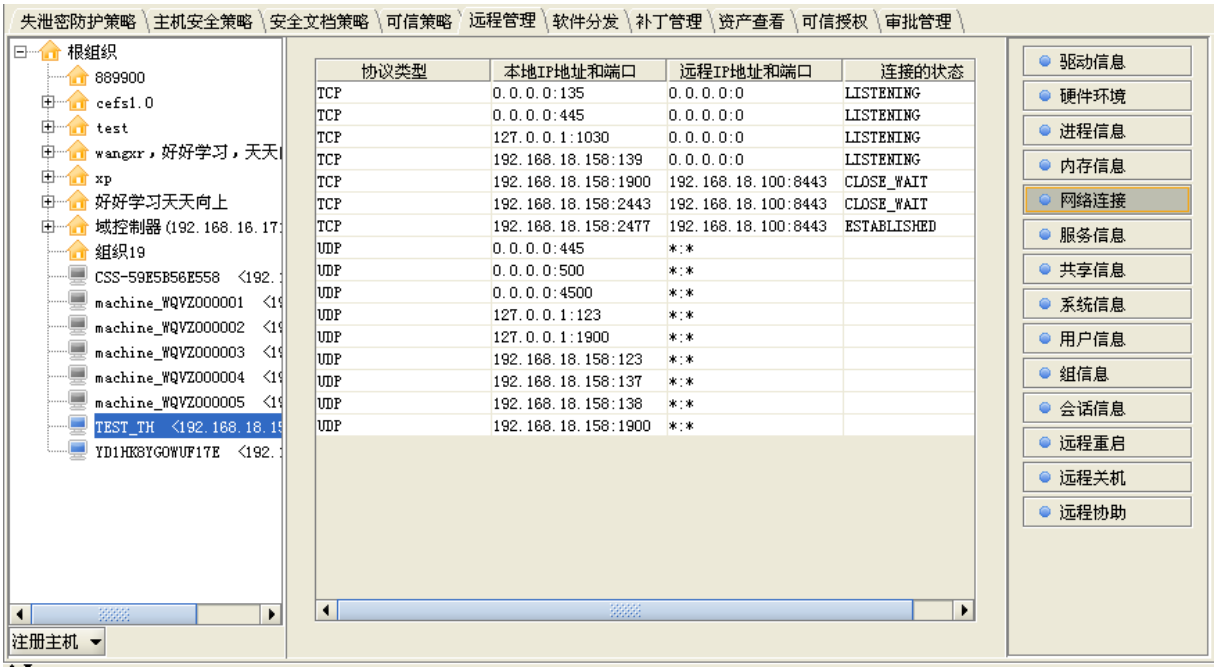


图 5-109　　查看远程客户端网络连接

5.7.6　服务信息

1. 在“远程管理”界面中，任选一在线主机，单击“服务信息”。稍等，出现远程客户端服务信息的详细列表，如图 5-110 所示。单击列表项下面箭头，可以按升序或降序排列，方便用户查看。

图 5-110　服务详细信息

2. 选择某一服务项，单击“当前状态”的下拉框，可以远程改变该服务的当前状态（Paused、Running、Stopped、Resume），如图 5-111 所示。

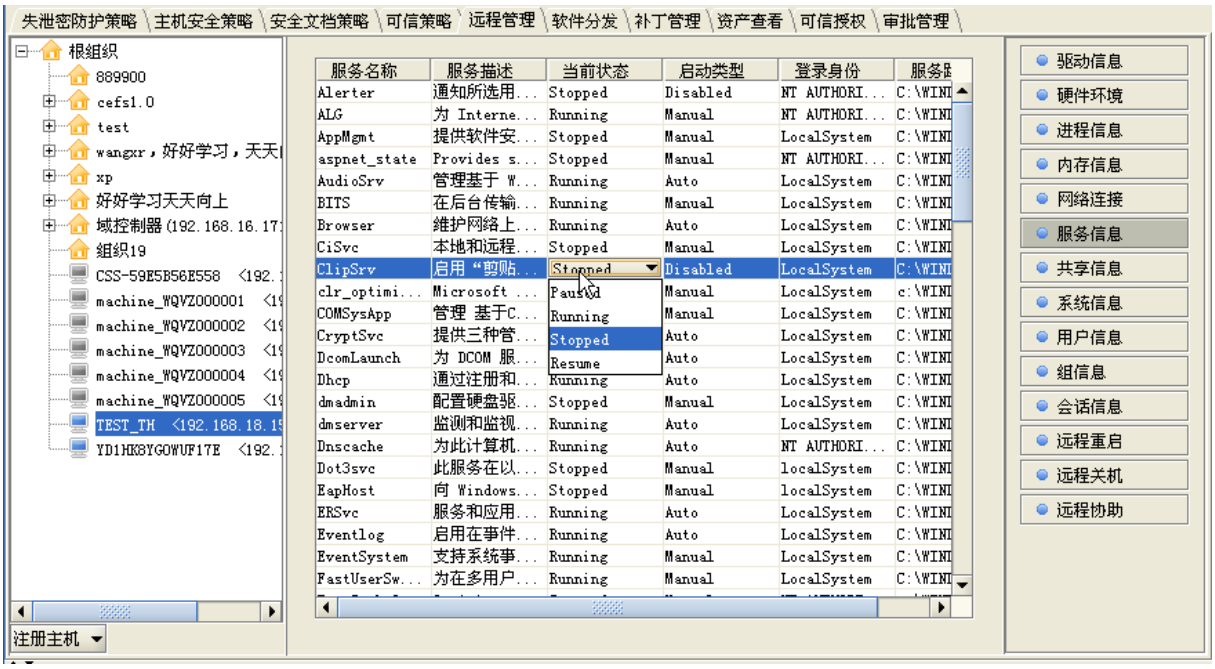


图 5-111　改变服务的当前状态

3. 选择某一服务项，单击“启动类型”的下拉框，可以远程改变该服务的启动类型（Disabled、Manual、Auto），如图 5-112 所示。

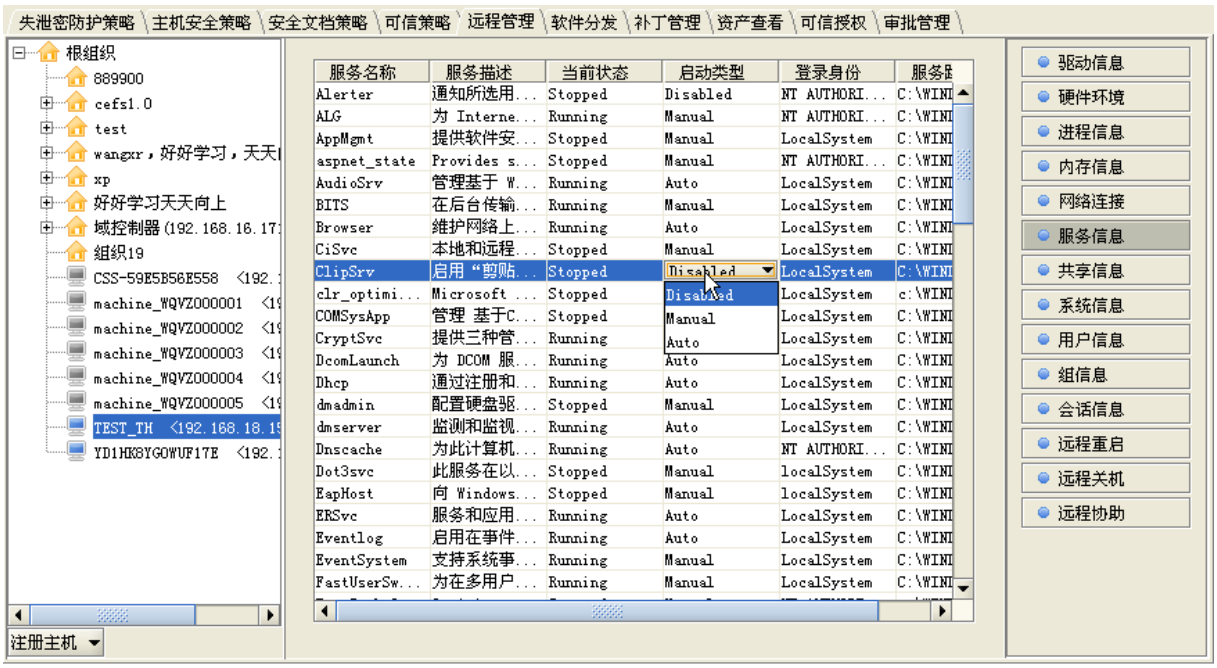


图 5-112　改变服务的启动类型

5.7.7　共享信息

1. 在“远程管理”界面中，任选一在线主机，单击“共享信息”。稍等，出现远程客户端共享信息的详细列表，如图 5-113 所示。

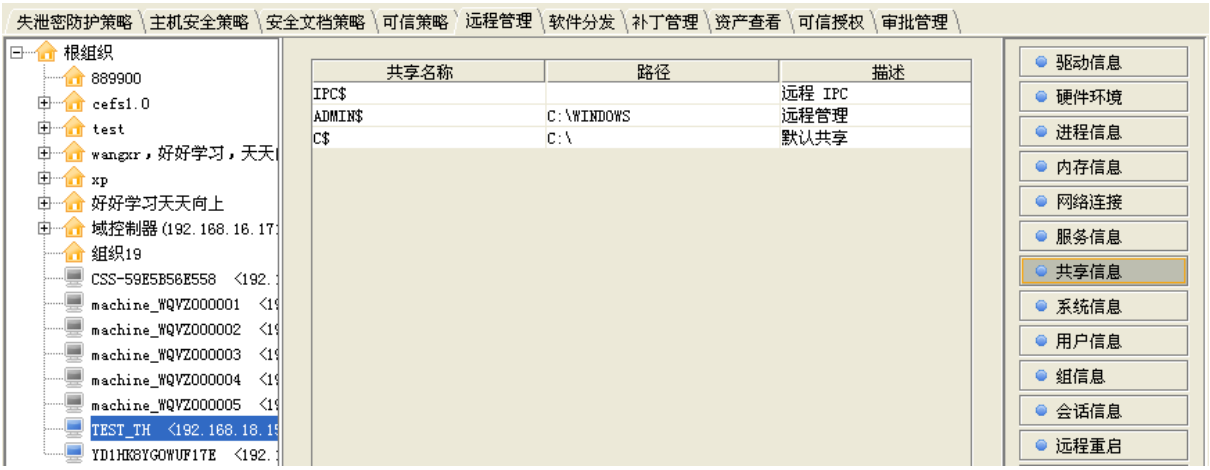


图 5-113　共享信息的详细列表

2. 单选或多选某些进程，单击右键菜单，执行“取消共享”命令，可以远程取消该共享，实现计算机的远程管理，如图 5-114 所示。

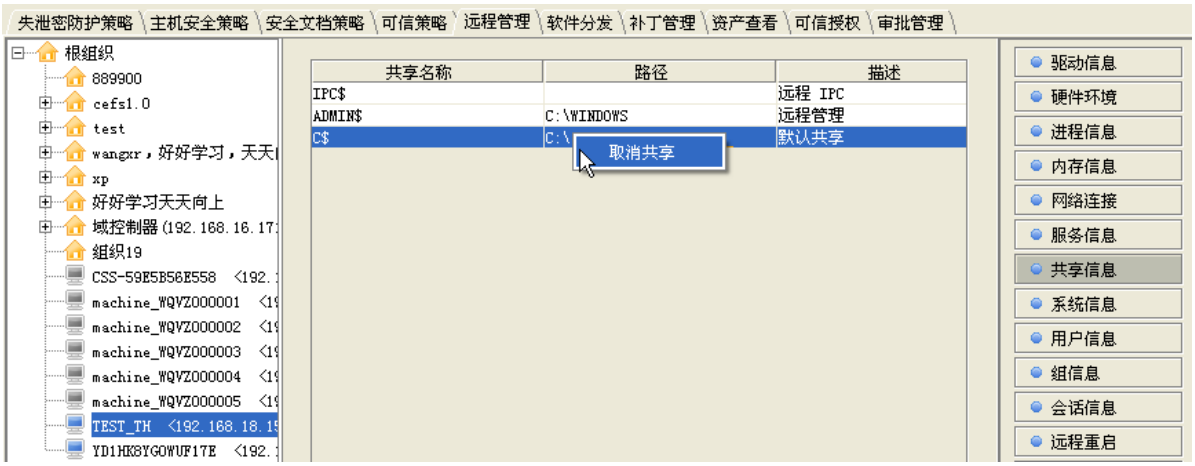


图 5-114　远程取消共享

5.7.8　系统信息

在“远程管理”界面中，任选一在线主机，单击“系统信息”，稍等，查看远程客户端系统信息，如图 5-115 所示。

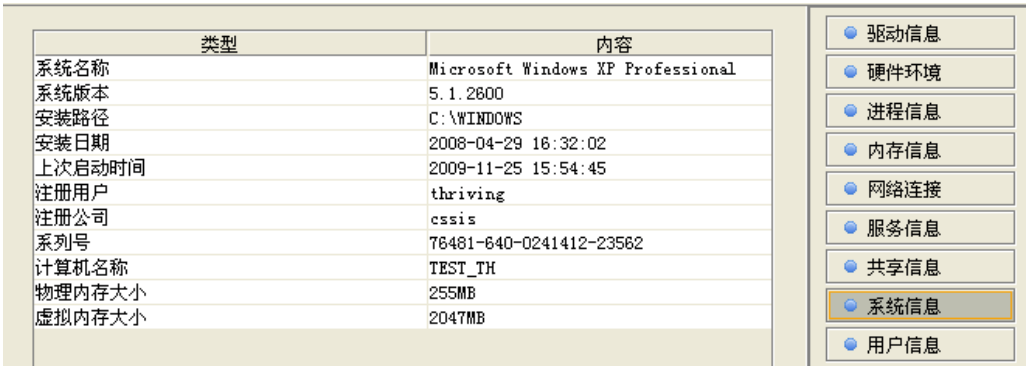


图 5-115　获取远程客户端系统信息

5.7.9　用户信息

在“远程管理”界面中，任选一在线主机，单击“用户信息”，稍等，查看远程客户端用户信息，如图 5-116 所示。

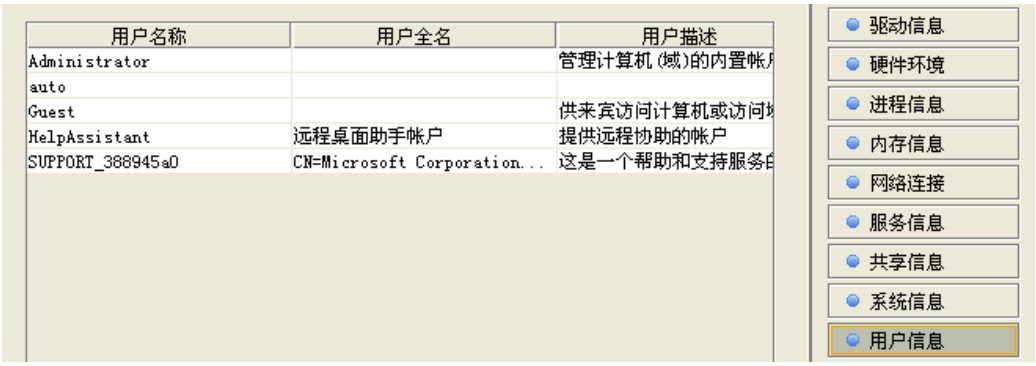


图 5-116　获取远程客户端用户信息

5.7.10　组信息

在“远程管理”界面中，任选一在线主机，单击“组信息”，稍等，查看远程客户端组信息，如图 5-117 所示。

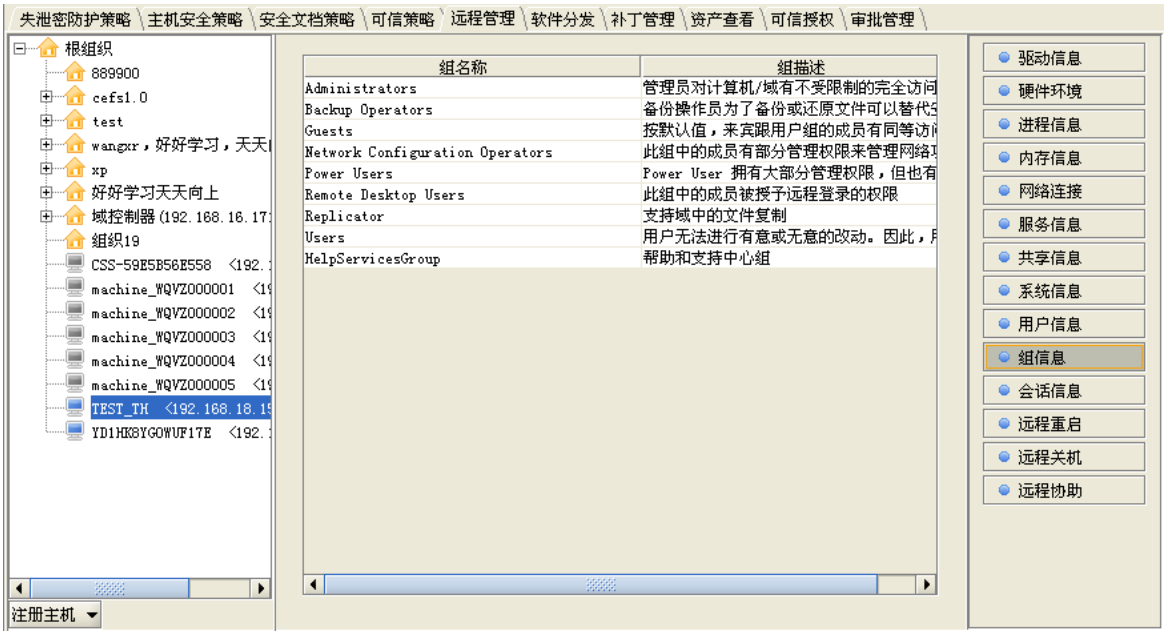


图 5-117　获取远程客户端组信息

5.7.11　会话信息

1. 在“远程管理”界面中，任选一在线主机，单击“会话信息”。稍等，出现远程客户端会话信息的详细列表，如图 5-118 所示。

图 5-118　会话信息

2. 在列表中选定某一会话信息，单击右键菜单，执行“注销会话”命令，可以远程注销该客户端的当前登录账户。另外，点击右键菜单也可以获取活动窗口，如图 5-119 所示。

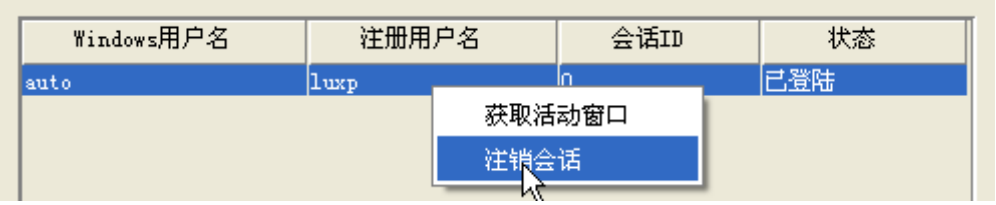


图 5-119　远程注销客户端

5.7.12　远程重启

在“远程管理”界面中，任选一在线主机，单击“远程重启”，出现确认框，如图 5-120 所示。确定后即可远程重启客户端。

图 5-120　远程重启客户端

5.7.13　远程关机

在“远程管理”界面中，任选一在线主机，单击“远程关机”，出现确认框，如图 5-121 所示。确定后即可远程强制客户端关机。

图 5-121　远程关闭客户端

5.7.14　远程协助

（1）在“远程管理”界面中，选择某一需远程协助的在线主机，单击“远程协助”。稍等，出现“启动远程协助成功!”消息框，然后出现远程协助邀请提示框，如图 5-122 所示。单击“是（Y）”后，屏幕出现等待状态，等待客户端应答。

图 5-122　远程协助邀请提示框

（2）这时客户端也出现远程协助提示框，如图 5-123 所示。客户端单击“是（Y）”后，即可与控制台建立远程协助连接。控制台管理员将能查看客户端的屏幕，协助其完成工作。

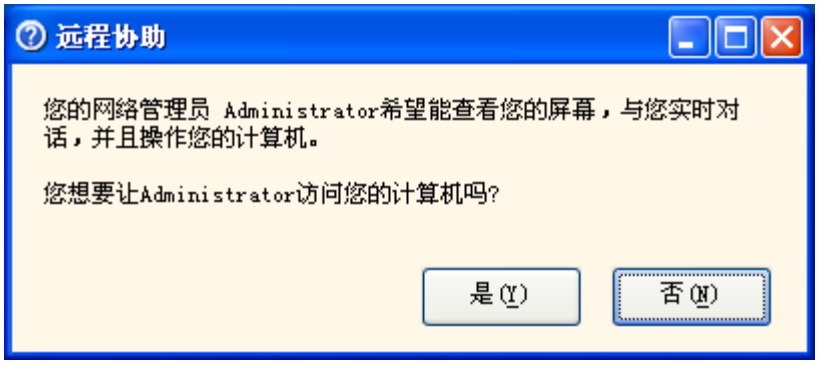


图 5-123　客户端远程协助提示框

（3）建立远程连接后，客户端可以和控制台管理员进行网络通话，如图 5-124 所示。左边显示的控制台消息框，右边显示的是客户端的桌面和消息框，有什么问题通过消息框进行交流。

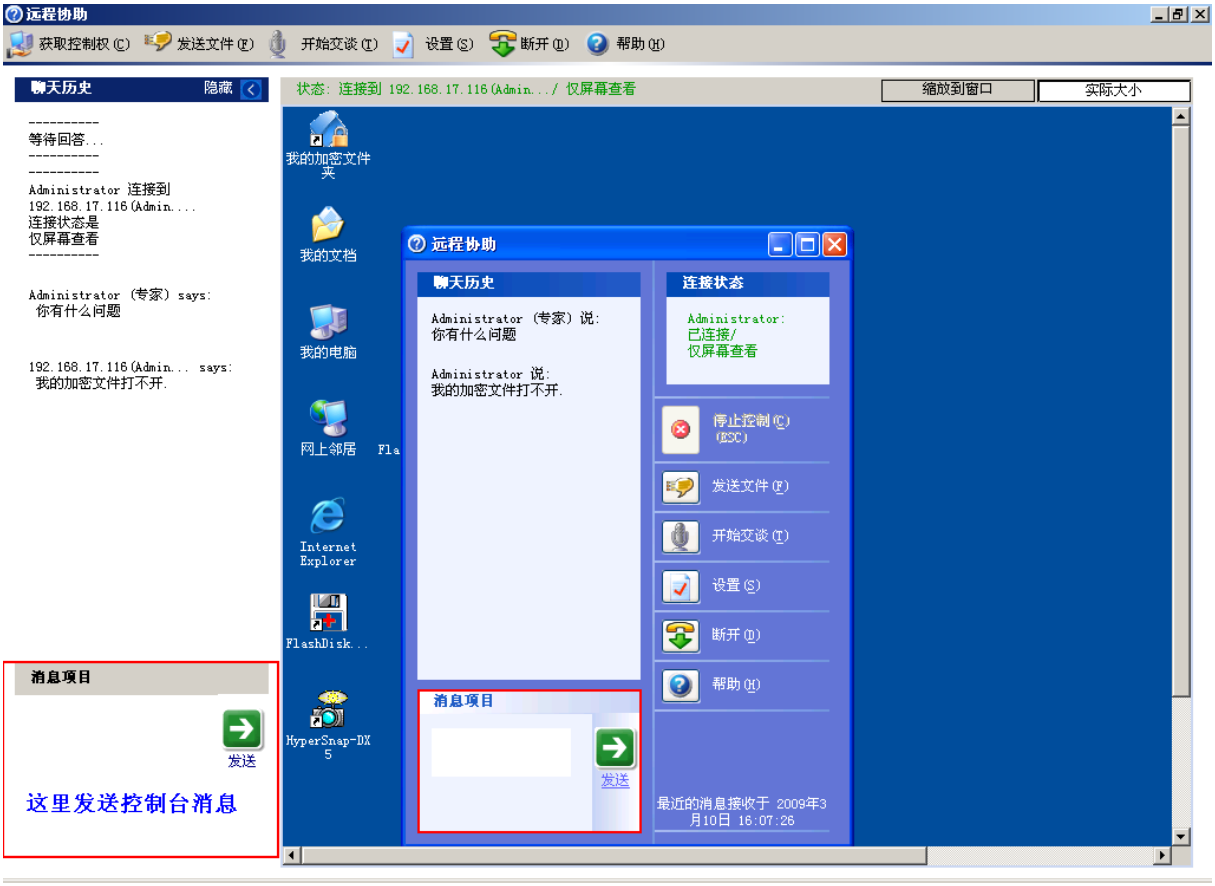


图 5-124　控制台远程协助桌面

（4）如果在控制台管理员的协助下，客户端仍然无法解决某些问题，这时管理员可以点击左上角的“获取控制权”菜单，等客户端确定后，就可在控制台操控客户端计算机，帮助客户端解决问题，如图 5-125 所示。双方都可以在任何时候通过按 ESC 键或者包含 ESC 的组合键来停止控制。

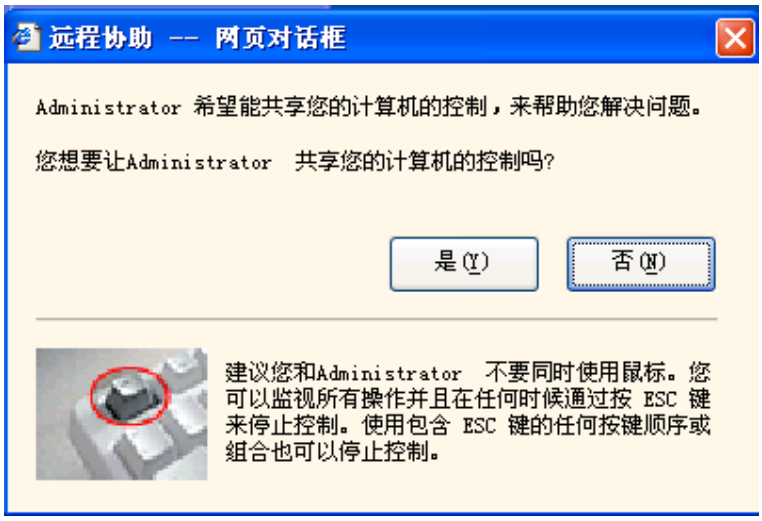


图 5-125　远程客户端确认框

（5）另外远程协助时，双方还可以通过网络发送文件，进行音频交谈等，这里不再详讲。最后，别忘了远程协助结束后，断开连接。

5.7.15　远程日志

（1）在“远程管理”界面中，选择某在线主机，单击“远程日志”，确定后，下发客户端上传运行日志命令，如图 5-126 所示。

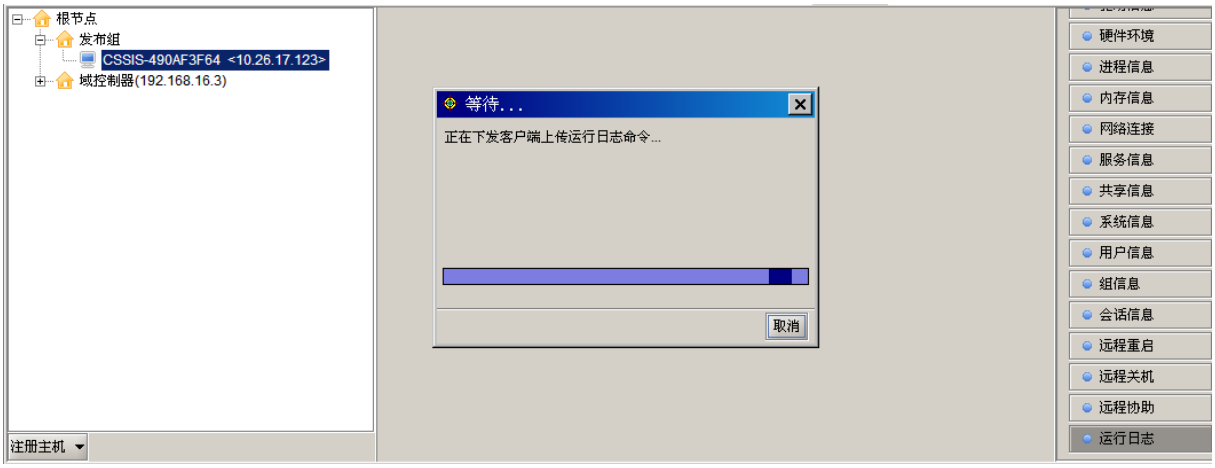


图 5-126　下发客户端上传运行日志命令

（2）稍等，选择日志上传文件的保存位置，如图 5-127 所示。该客户端的所有运行日志，将以默认 ConsoleLog.cab 文件形式，上传到控制台指定的保存位置。上传文件一般比较大，可能需要一会儿时间，请耐心等待。上传结束后，控制台管理员可以打开 ConsoleLog.cab 文件查看。

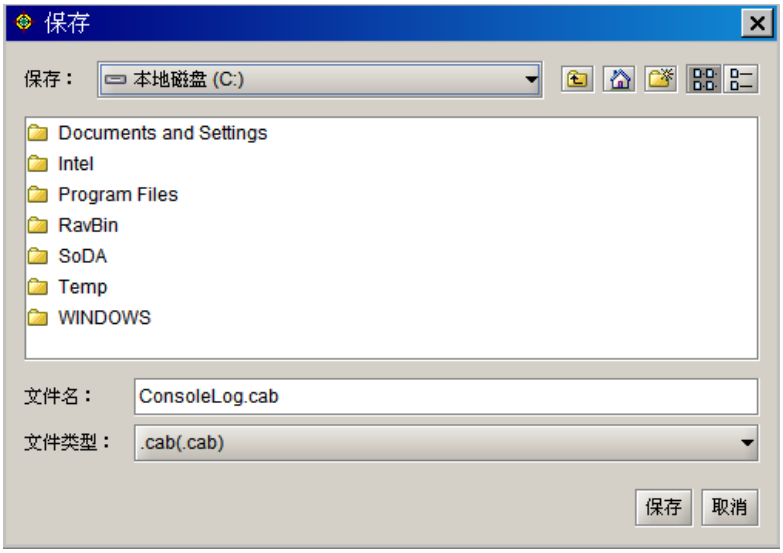


图 5-127　选择客户端运行日志的上传位置

5.8　软件分发

软件分发管理能够实现各种软件安装包集中统一的自动分发，大大简化企业大规模软件分发和部署的复杂度，提高工作效率。软件分发管理可定义软件分发的范围（哪些主机可安装），支持软件包在终端机上按设定的时间自动安装，以及对标准格式的安装包在终端机上的安装结果进行跟踪。

在安全管理中心中，用鼠标单击“软件分发”，进入软件分发界面，如图 5-128 所示。上半部分为软件包列表框，负责上传目录的添加，软件包的创建、修改和删除工作。下半部分为任务列表框，负责下发任务的创建、修改和删除工作。

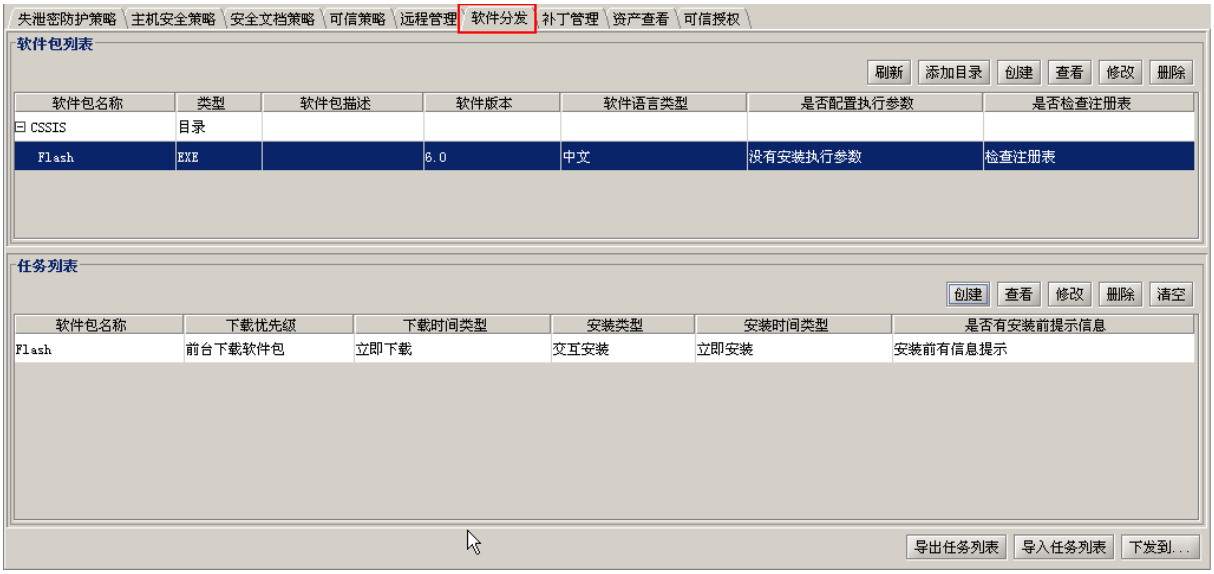


图 5-128　　软件分发页面

5.8.1　软件包制作和管理

1. 在软件分发界面，单击上面的“添加目录”按钮，弹出上传目录输入框，输入目录名称后，单击“添加”按钮退出，如图 5-129 所示。

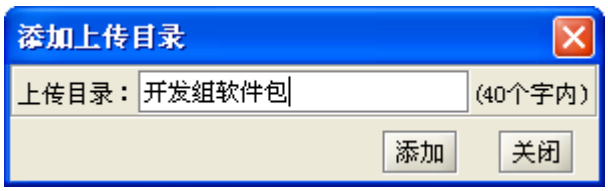


图 5-129　　添加上传目录

提示：上传目录是服务器上的一个特定目录，默认位置在\UEM\WBServer\filestore 下，这由服务器的贮存空间配置。

2. 在软件分发界面，如图 5-130 所示。单击上面的“创建”按钮，或者在软件包列表中单击右键菜单“创建软件包”，都可弹出软件包创建界面。

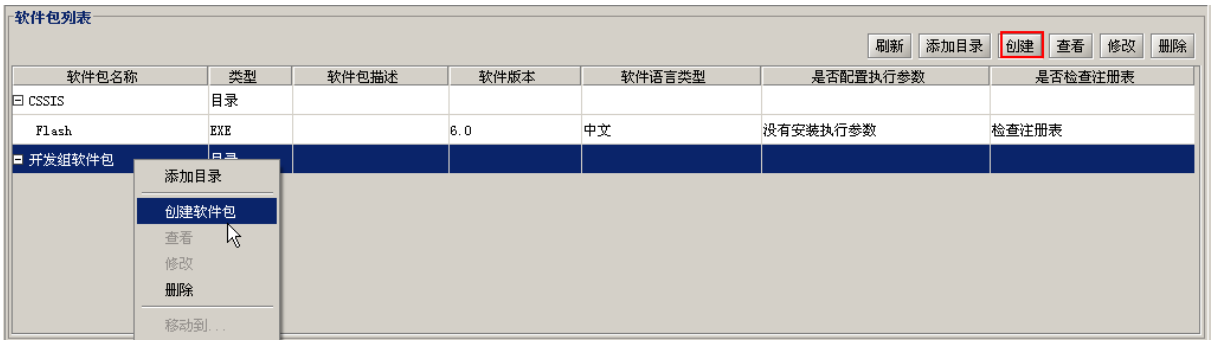


图 5-130　　单击“创建”菜单

3. 在创建软件包基本信息页面中，输入软件包名称、版本和语言类型等，如图 5-131 所示。单击“下一步”继续。

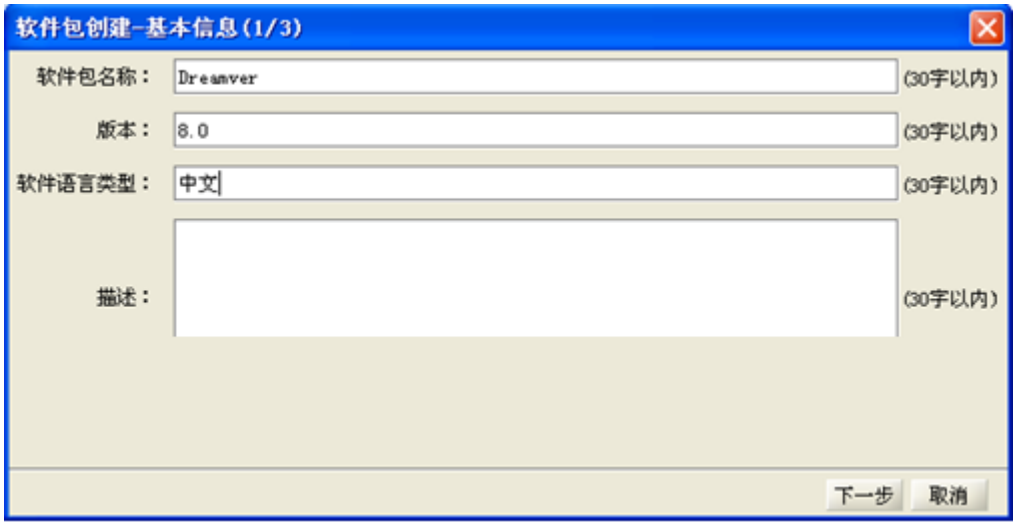


图 5-131　　创建软件包--基本信息

4. 在创建软件包源文件信息页面中，输入打包文件路径、主执行程序和参数配置，如图 5-132 所示。单击“下一步”继续。

提示：

（1）BAT 和 MSI 的软件包没有执行权限配置项，界面上不显示。只有 EXE 软件包，才有执行权限配置项。如果不配置，客户端权限低于软件包安装权限的话，就不能安装。这时，不同的客户端可能会出现不同的提示信息，请用户按照提示信息去做。

（2）如果主执行程序为 EXE 和 BAT 文件类型，建议输入注册表项和注册表值，否则，软件包安装成功与否，可能会有判断误差。如果主执行程序为 MSI 文件类型，不必检查注册表配置。

（3）创建文件包时，会将打包文件路径下的所有文件都打包。所以，打包文件路径下文件不能太混乱，一定要清除一些与该包无关的文件。

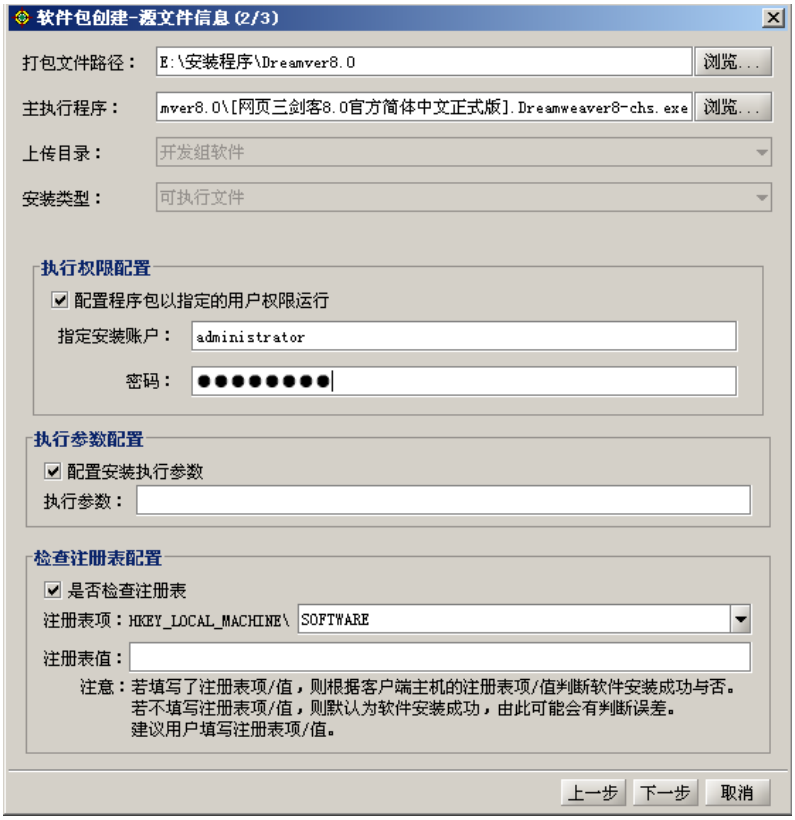


图 5-132　　创建软件包—源文件信息

5. 在创建软件包环境要求页面中，设置基本环境，并选择系统及版本环境要求，如图 5-133 所示。单击“完成”按钮。

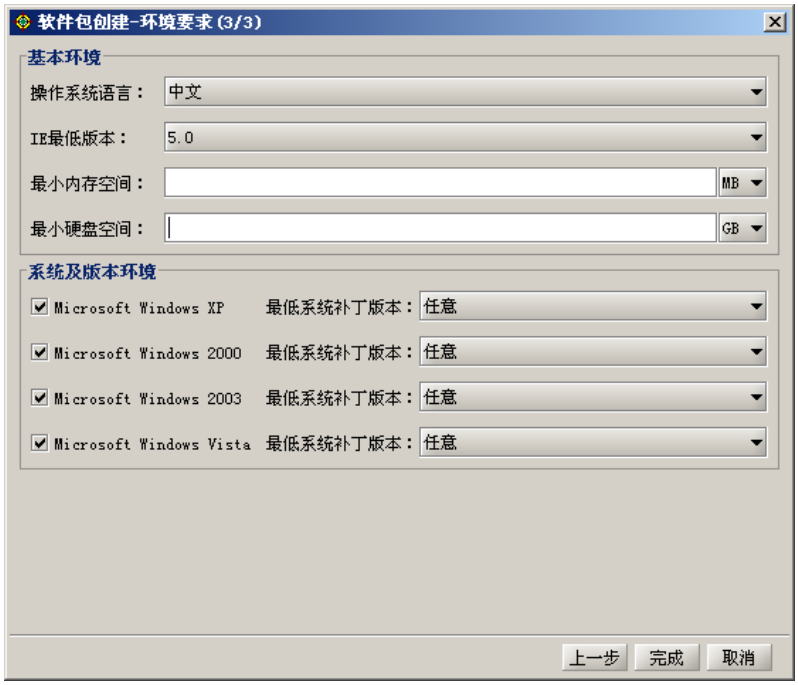


图 5-133　　创建软件包——环境要求

6. 上传软件包过程中，如果软件比较大，可能等待制作和上传的时间会长一些，如图 5-134 所示。制作完成后，弹出消息框，如图 5-135 所示。

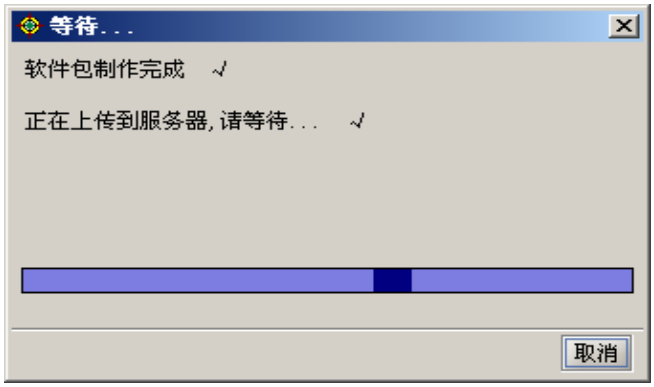


图 5-134　制作上传软件包

图 5-135　软件包制作成功

7. 软件包制作完成后，在软件包列表框中，可以看到刚制作的软件包，如图 5-136 所示。

图 5-136　显示新建的软件包

8. 选择某软件包，可通过右键菜单“移动到”，转移软件包位置，如图 5-137 所示。

图 5-137　移动软件包位置

9. 在软件包列表中选择某软件包，单击“修改”按钮，或单击右键菜单“修改”，都可弹出软件包修改界面，通过不同的选项卡对软件包设置进行修改，如图 5-138 所示。另外，单击“查看”按钮，可以查看软件包内容，但不能修改。如果单击“删除”按钮，可删除软件包。

提示：

（1）　选中的一条或多条软件包信息可以批量删除。

（2）　不支持同时删除软件包和目录，支持多个软件包移动目录。

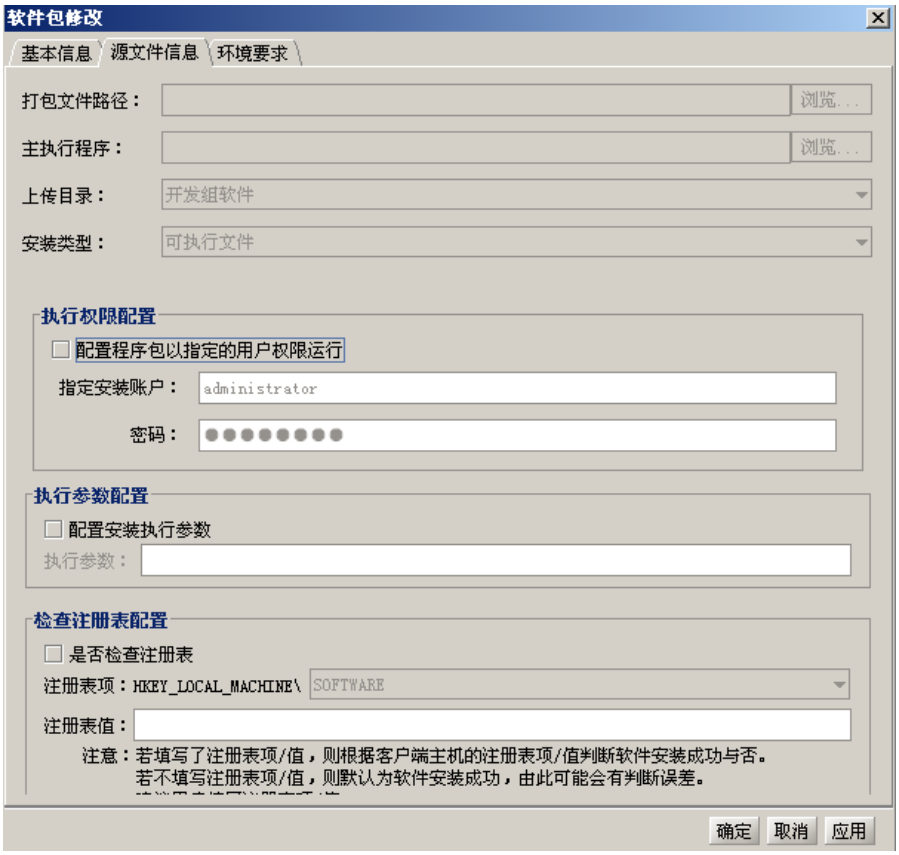


图 5-138　修改软件包

5.8.2　软件包下发

1. 在软件包列表中选择某软件包，单击右键菜单“创建任务”，或者单击任务列中的“创建”按钮，弹出软件包选择界面，如图 5-139 所示。如果已经选中了软件包，该界面不可选，直接单击“下一步”。

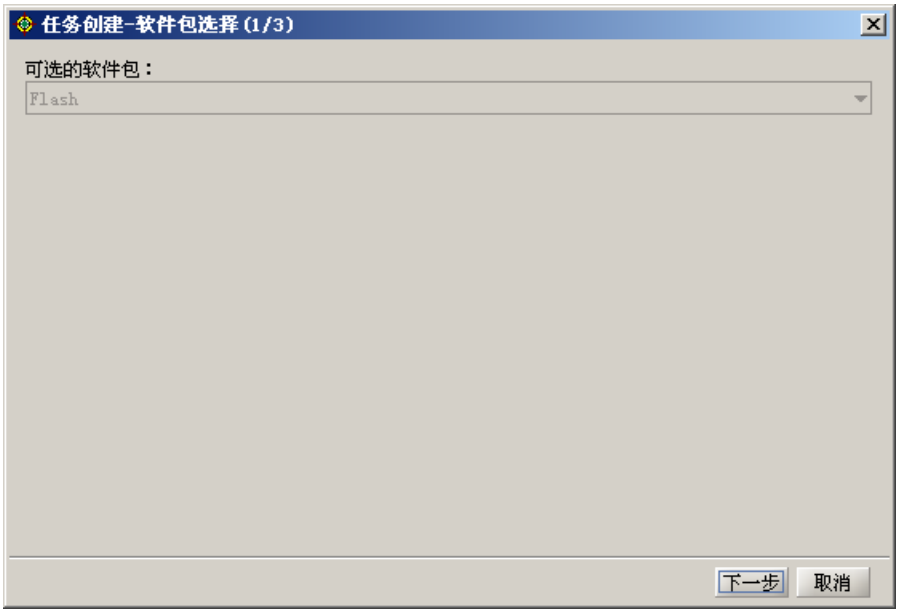


图 5-139　　选择软件包

2. 在下载属性页面，通过下拉框选择下载优先级和下载时间类型，如图 5-140 所示。单击“下一步”继续。

下载优先级分为：前台下载软件包、后台高优先级下载软件包、后台中优先级下载软件包和后台低优先级下载软件包。

下载时间类型支持：立即下载、时间点下载、分段时间下载。

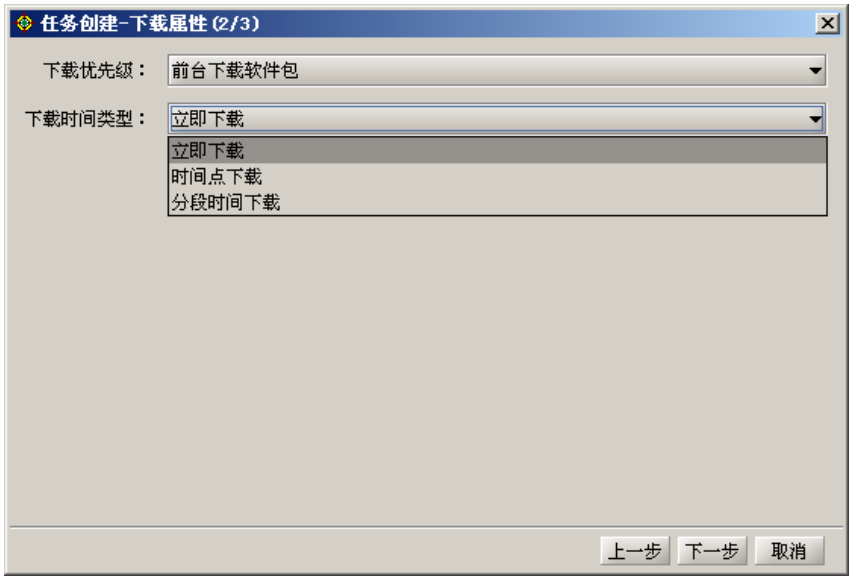


图 5-140　　选择下载属性

3. 在安装属性页面，选择“开始安装时消息通知客户端”，并输入消息内容。通过下拉框选择安装类型和安装时间类型（立即安装、时间点安装和 n 分钟后安装），如图 5-141 所示。最后，单击“完成”按钮。

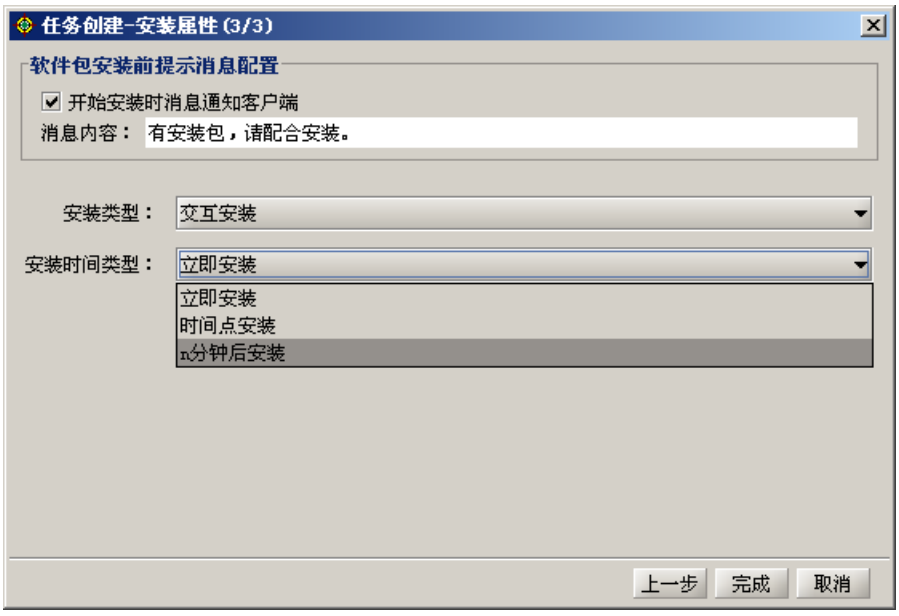


图 5-141　　选择安装属性

4. 在任务列表中，可以看到刚添加的任务，如图 5-142 所示。选中某任务列表项，单击“修改”按钮，或者单击右键菜单“修改”，可以对任务列表项进行修改。单击“查看”按钮，只能对任务列表进行查看，不能修改。单击“删除”按钮，可删除选中的任务列表项。

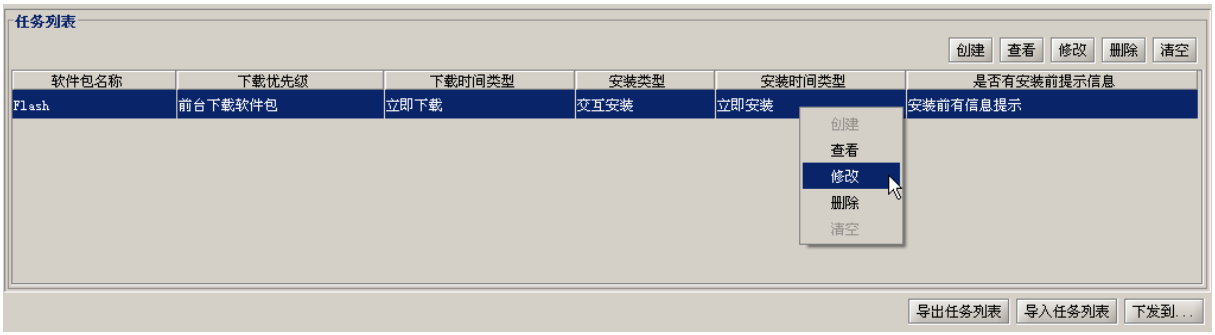


图 5-142　　编辑任务列表

5. 选中某任务列表，单击下面的“下发到…”按钮，在任务名称框中，输入任务名称（或按默认名称），如图 5-143 所示。随后弹出计算机选择框，勾选要下载到的计算机，最后，单击“确定”按钮，既可将任务下发，如图 5-144 所示。

提示：如果下发任务时，软件包列表中已删除该软件包，此时系统会做判定，给出提示。

图 5-143　　输入下发任务名称

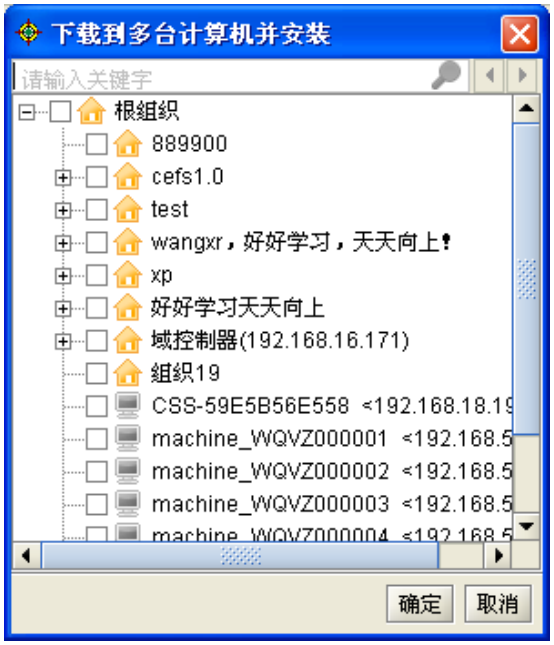


图 5-144　　选择要下载到的计算机

6．为方便用户使用，我们可以单击下面的“导出任务列表”按钮，将当前的任务列表导出为*。XML 文件保存。另外，在需要的时候，可单击“导入任务列表”按钮，清空当前任务列表，导入保存的任务列表，如图 5-145 所示。导入时，如果软件包列表中已删除某些软件包，系统会做出判断，与此相关的任务不再导入。

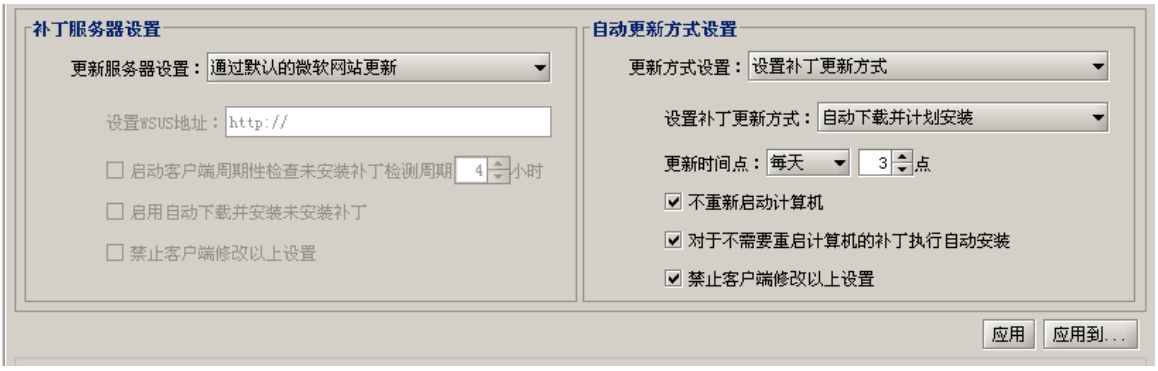
图 5-145　导入任务确定框

5.9　补丁管理

1．在安全管理中心中，用鼠标单击功能菜单项“补丁管理”，进入补丁分发管理界面。上半部分为补丁服务器和客户端更新方式设置，右侧是关于客户端的更新方式设置，下半部分显示客户端补丁列表，如图 5-146 所示。

图 5-146　补丁分发管理

2．设置补丁更新服务器和自动更新方式。设置完成后，单击“应用到”按钮，将策略下发到组织或计算机，如图 5-147 所示。



5-147　补丁服务器和更新方式设置

补丁服务器设置：补丁更新服务器可以设为“通过默认的微软网站更新”或“指定更新服务器地址”。如果设置为“通过默认的微软网站更新”，则客户端自动从微软网站获取补丁，不需设置检测未安装补丁周期；如果设置为“通过设定的补丁服务器更新”，则客户端从设定的补丁服务器上获取补丁列表。这时需要输入 WSUS 补丁服务器地址，设置检测周期。

自动更新方式设置：自动更新方式由控制台设置下发或者允许用户自定义。如果由控制台设置策略下发，那么可以选择的自动更新方式为：通知下载并通知安装、自动下载并通知安装和自动下载并计划安装，其中计划安装时，还要设置具体的更新时间点。

禁止客户端修改以上设置：是指禁止客户端通过注册表修改所连接的补丁服务器，或者禁止客户端修改控制台下发的补丁自动更新方式。

3. 在补丁列表框中，点击“下发获取补丁命令”，可以显示补丁服务器上的所有补丁，或者客户端未安装的补丁，如图 5-148 所示。最后，勾选要下发的补丁（不是拖选），可以将补丁下载到多台计算机并安装。

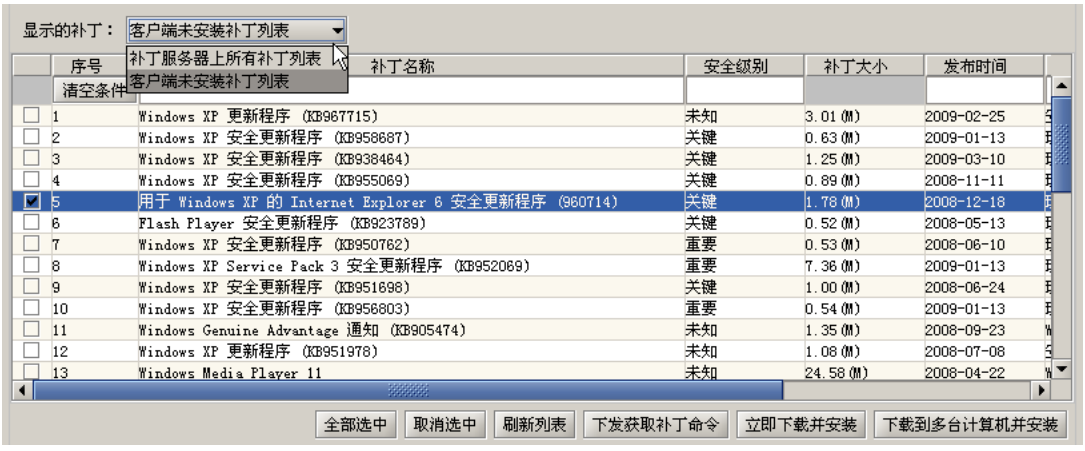


图 5-148　客户端未安装补丁列表

点击表头“补丁名称”、“安全级别”、“发布时间”，可以使该列内容按升、降序排列；点击“补丁名称”或“安全级别”下面的空白框，然后单击空白框右边的浏览按钮，输入查询条件，可以按条件查询。

4. 补丁下发后，可以在“统计审计分析”的“补丁安装情况统计”中查看。

5.10 资产查看

1. 在安全管理中心中，用鼠标单击“资产查看”标签项，进入资产信息查看界面。选定组织结构视图中某主机，可以查看该主机的硬件信息，如处理器、硬盘、内存、光驱和声卡具体型号，如图 5-149 所示。

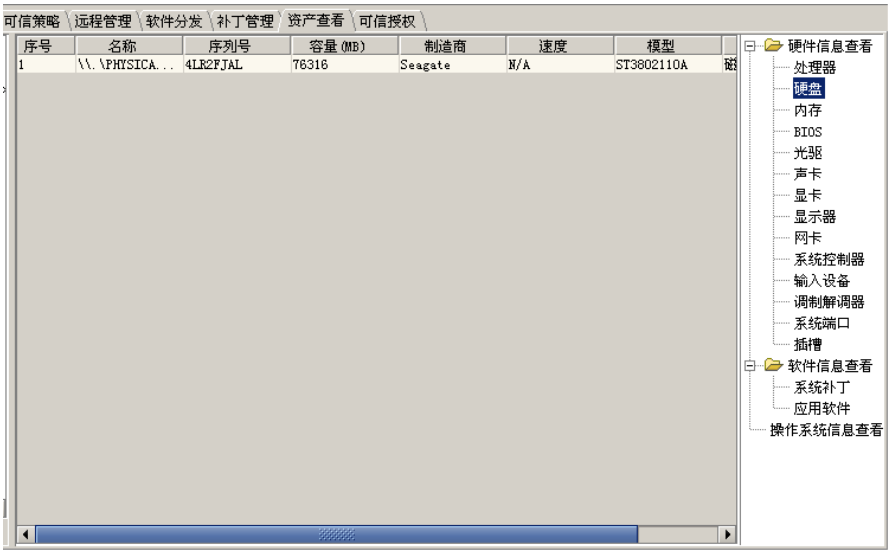


图 5-149　　硬件信息查看

2. 同样方法，可以查看该主机的软件信息，如安装的应用软件、系统补丁，如图 5-150 所示。安装时间和厂商未知，就不显示。在统计审计分析的软件统计中，对于未知的安装时间，默认为 1970-01-01，便于用户按时间条件查询。

图 5-150　　应用软件查看

5.11 安全文档策略

安全文档策略是指自动地、用指定的加密（解密）算法、用指定的密钥，对指定的文件实行加密和解密操作，从而达到保护文件的目的。

用户在操作过程中，不改变对文件的访问（打开或关闭）习惯，整个加密（解密）操作过程是自动完成的，用户毋须显式地指明算法、密钥和被操作的文件名。加密中所用到的算法、密钥，是事先设定的、存在系统的环境变量中，而不是在加密（解密）过程中指定的。系统根据“加密策略”自动识别什么文件需要进行加密/解密操作，哪些不需要。

安全文档策略利用透明加解密技术和访问控制，向整个系统提供实时的、透明的、动态的数据加解密服务。文件数据在储存设备(例如磁盘)上以密文形式存储，当需要读取该加密文件的数据内容时，通过基于文件指纹智能识别技术和基于文件名识别技术的有机结合,实时进行解密。这样，系统在授权情况下，可以透明地以明文形式读写该加密文件的数据，实现了安全性和方便性的完美地结合。

安全文档策略作为一个独立的功能模块，其授权通过服务器硬件加密锁控制。主要包含几个方面：加密进程控制、自解密控制、文档备份策略、剪贴板控制、截屏软件黑白名单、非加密进程系统参数设置、文件服务器放开设置、安全文档离线策略。

5.11.1 加密进程控制

加密进程控制就是通过控制客户端指定的进程，实现文档的自动加解密。加密和解密过程在后台进行，对用户透明，不改变用户使用习惯。但对没有下发此策略的用户来说，则不能访问已经加密过的密文，这样实现了文件的安全加解密。

所谓加密进程，指通过该进程产生或修改后的文件均会被自动加密。在加密进程控制策略中，用户需要首先将指定的进程加入到安全文档进程库，然后再将其下发给客户端。

在安全管理中心中，选择某人员（或策略集、群组策略），单击“安全文档策略”→“加密进程控制”，进入加密进程控制界面，如图 5-151 所示。

图 5-151　加密进程控制

5.11.1.1 启用加密进程策略

加密进程控制有两种方式：如果选择“启用进程加密策略”，则指定的进程访问文件时进行控制；如果不选择“启用进程加密策略”，则指定的进程访问文件时不进行控制，加密策略不起作用。

5.11.1.2 进程库管理

在加密进程控制界面中，点击“进程库管理”按钮，对进程库进行添加或删除操作。该系统已经在加密进程库中添加了常用进程，如办公软件、制图软件等，对于不同企业的用户，可根据自身需要，对进程库进行修改。添加、删除进程操作如下：

（1）在安全文档进程库管理页面中，右键单击进程库的树形结构，选择“添加类别”或“添加进程”，并输入类型和进程名称，如图 5-152 所示。

在添加进程时，可以单击右边的浏览按钮“...”，选择进程路径和进程名称，进程版本和进程描述可以自动获取。勾选“是否签名”，输入起始位置和签名长度。输入缺省预加密文件类型，多个类型之间用“|”隔开，也可以只输入*.:all:来表示所有后缀类型。最后，单击“添加”按钮，将进程添加到进程库中。

例如：单击浏览按钮“...”，选择 WINWORD.EXE 进程，进程版本和进程描述自动获取，勾选“是否签名”框，采用默认起始位置和签名长度，并输入缺省预加密文件类型“*.doc|*.docx”。最后，单击“添加”按钮，将 WINWORD.EXE 进程添加到进程库中。

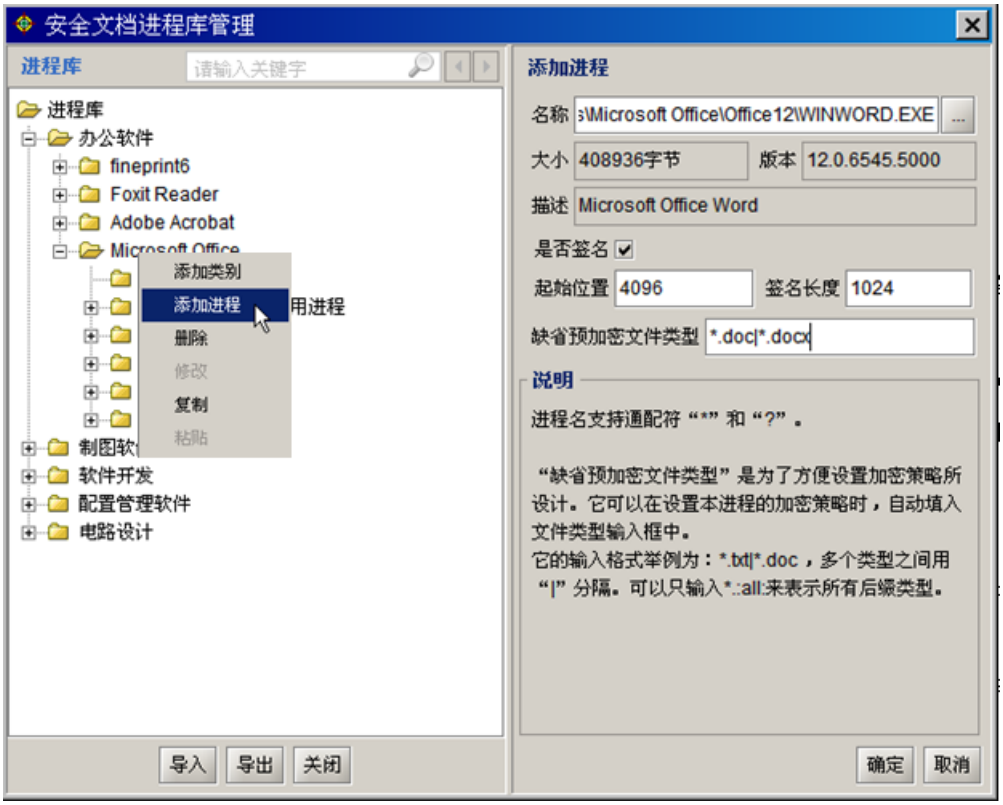


图 5-152　添加 Winword.exe 进程库管理

提示：

（1）如果不签名，不针对进程版本控制，只判断进程名。例如：下发 word2003 的进程，也可以控制 word2007。但是，客户端可以通过更改进程名，访问不该访问的文档。

（2）如果签名，是针对进程版本控制的。例如：下发 word2003 的进程，就不能控制 word2007。在输入签名值的起始位置和签名长度时，一定要注意文件长度，一般情况下采用默认值即可。

（3）预加密文件类型是指启用某进程时，只要访问指定后缀类型的文件，文件即被加密。而对于其他文件，只有加密进程写文件时才被加密。此处设置预加密文件类型，是为了方便设置加密策略所设计，它可以在设置本进程的加密策略时，自动填入文件类型输入框中，详见加密策略的下发。

（4）进程库中允许存在同名进程，同名进程以不同的签名值区分。如果同时下发多个同名进程策略（签名或不签名），只要有一个进程被匹配上（不签名），则认为该进程为加密进程。

（2）进程库管理增加进程名搜索功能，该功能支持模糊查询，用户可以在上面的搜索框中输入进程名，单击搜索按钮进行查询，将搜索结果定位于第一个进程匹配处，如图 5-153 所示。单击左右箭头，进入上一个或下一个进程匹配处。

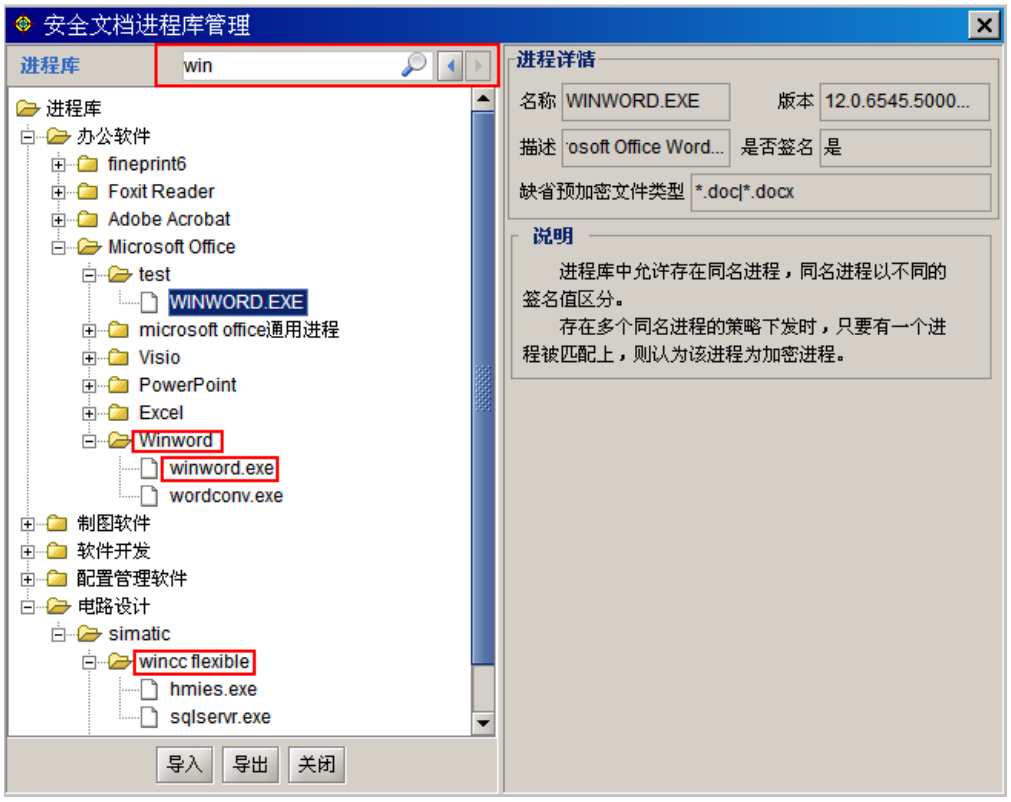


图 5-153　进程名搜索

（3）单击右键菜单，选择“修改”菜单项，可以对选定的进程进行修改。对于自己不需要进程或类别，也可以通过右键菜单删除，如图 5-154 所示。

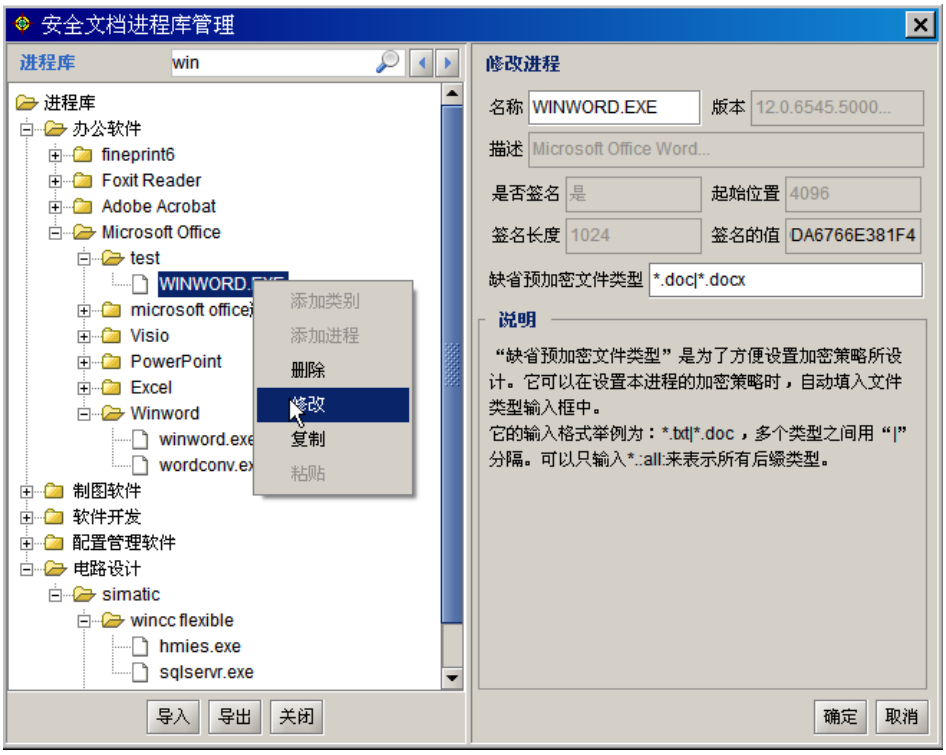


图 5-154　修改进程名

（4）另外，进程库支持导入和导出操作，可以将进程库导出保存为*.xml 文件，如图 5-155 所示。

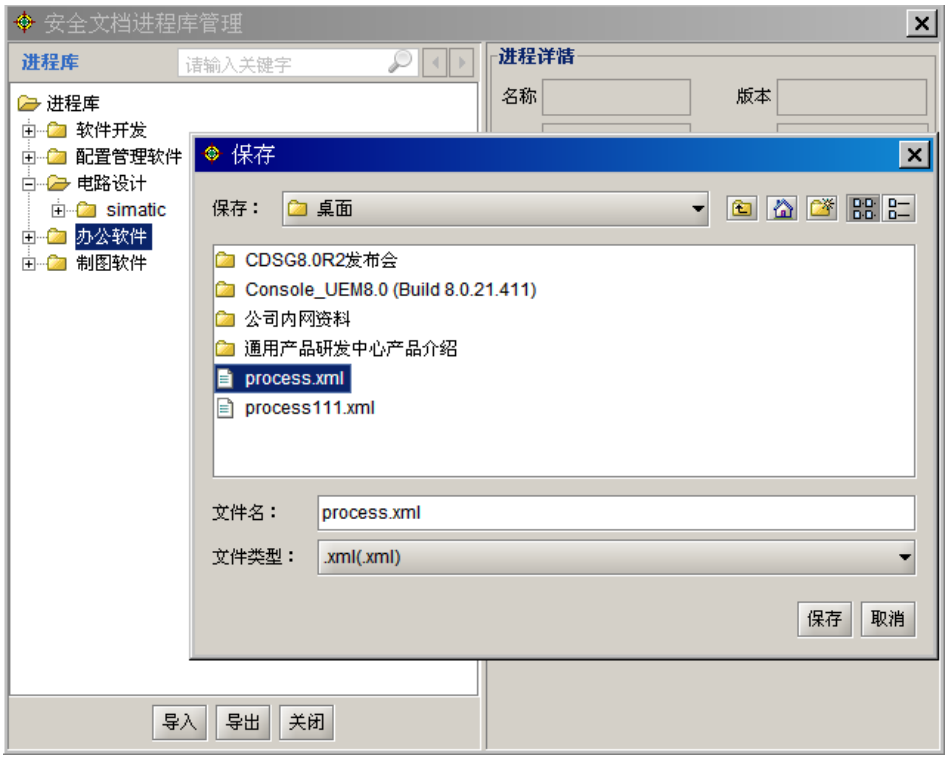


图 5-155　进程库导入和导出操作

5.11.1.3 加密策略的下发

在“加密进程控制”界面，选择要控制的进程和加密策略。一般用户只需基本设置，“允许解密”是必选项，然后选择加密文件类型，是所有类型文件都加密，还是指定类型文件加密。最后，单击下面的“应用”按钮，将策略下发给指定的人员，如图 5-156 所示。

图 5-156　加密进程基本设置

策略的基本设置允许解密是必选项，可以设置所有类型加密或指定类型加密。指定类型加密是只对指定类型的文件加密，其他类型的文件不加密。当指定文件类型加密时，预加密类型与加密类型完全相同，预加密类型设置无效。写权限是软件进程在打开文件时本身的属性，不是用户设置的。例如：winword.exe 是写权限打开文件；notepad.exe 是读权限打开文件。

高级设置项是为了满足某些用户的特殊需要，使用时请慎重，请专业技术人员设置，如图 5-157 所示。

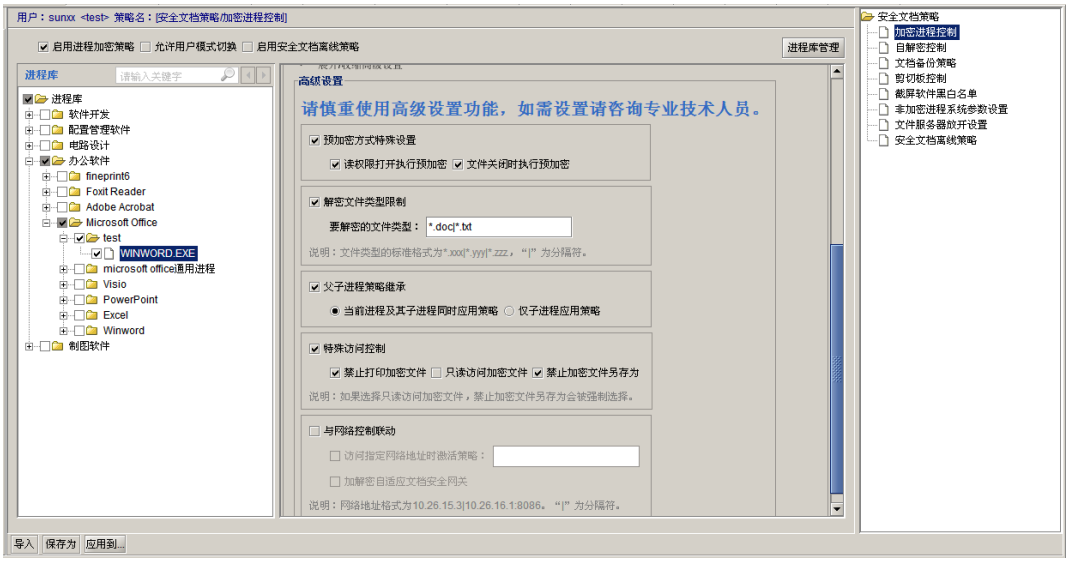


图 5-157　加密进程高级设置

选项说明：

（1）预加密方式特殊设置：读权限打开时执行预加密，或关闭时执行预加密。

（2）解密文件类型限制：指定要解密的文件类型，加密进程可以明文打开此类型的加密文件，其他类型的加密文件，打开会看到密文。

（3）父子进程策略继承：某些软件启动一个主进程，同时会启动一些子进程。为下发策略方便，将当前进程与子进程应用相同的策略。

（4）特殊访问控制：对加密文件的访问可做单独控制，例如：只读，另存，打印。

（5）与网络控制联动：设置当前进程访问指定 IP 时，才变成加密进程；其他情况下都是一个普通的非加密进程。

5.11.1.4 模式切换控制

针对安全文档的工作状态，为客户端设置两个模式：工作模式和普通模式。

- ✧ 工作模式：指安全文档内核处于工作状态。
- ✧ 普通模式：指安全文档内核停止工作。

默认情况下为工作模式，即安全文档处于工作状态。

管理人员可以在控制台下发策略，控制客户端能不能进行模式切换，如图 5-158 所示。

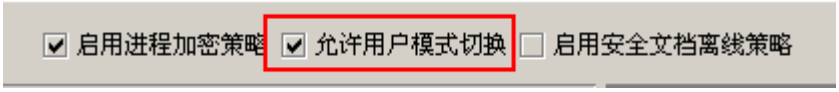


图 5-158　工作模式控制策略

默认情况下不允许模式切换，客户端托盘菜单中没有模式切换的菜单项。

在控制台下发允许模式切换策略，客户端托盘菜单中会显示模式切换的菜单项。用户可通过点击对应的菜单项，进行模式的切换，从而使安全内核处于离开或工作状态。

如果当前客户端为工作模式，显示“切换为普通模式”；如果当前客户端为普通模式，显示“切换为工作模式”，如图 5-159 所示。

图 5-159　模式切换—当前模式为工作模式的菜单项

提示：如果控制台允许模式切换，并且客户端设为普通模式，当管理员再下发安全文档策略时，策略将不生效。

5.11.2 自解密控制

控制台可设置某些客户端在本地自解密密文文件，生成明文，同时产生自解密日志，以便审计。安全文档策略中，有自解密控制策略项，如图 5-160 所示。

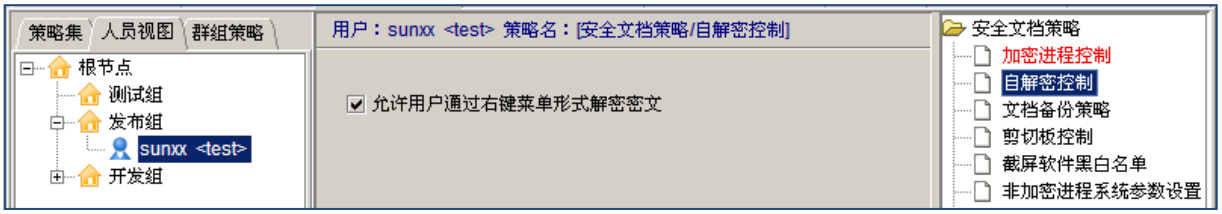


图 5-160　自解密控制策略

当控制台下发允许客户端自解密策略后，在客户端用右键点击密文文件，会出现“安全文档”→“解密”菜单项。点击该菜单项，所选文件全部解密成功时不弹提示框，当所选文件中有解密失败的文件时会弹提示框。

本系统允许用户同时自解密多个加密文件，但是如果自解密文件过多，会将部分文件请求去除，因此对于过多文件自解密，请分次操作。

提示：如果客户端选择自解密的多个文件中有密文和明文，或者选择有文件夹，将不出现“自解密”菜单项。

5.11.3 文档备份策略

安全文档在加密文件时可能出现意外，需要将未破坏前的文件进行备份保存，防止用户文件遇到不可修复的错误而造成损失。系统操作员通过控制台策略设置界面，可以设置加密文件备份策略；如果管理员允许用户设置备份策略，客户端用户也可以设置加密文件备份策略。

在文档备份策略界面，勾选“启用备份功能”，设置定时备份策略，包括备份路径、备份的文件类型、同一文件最大备份数、备份周期、备份时间点等，如图 5-161 所示。

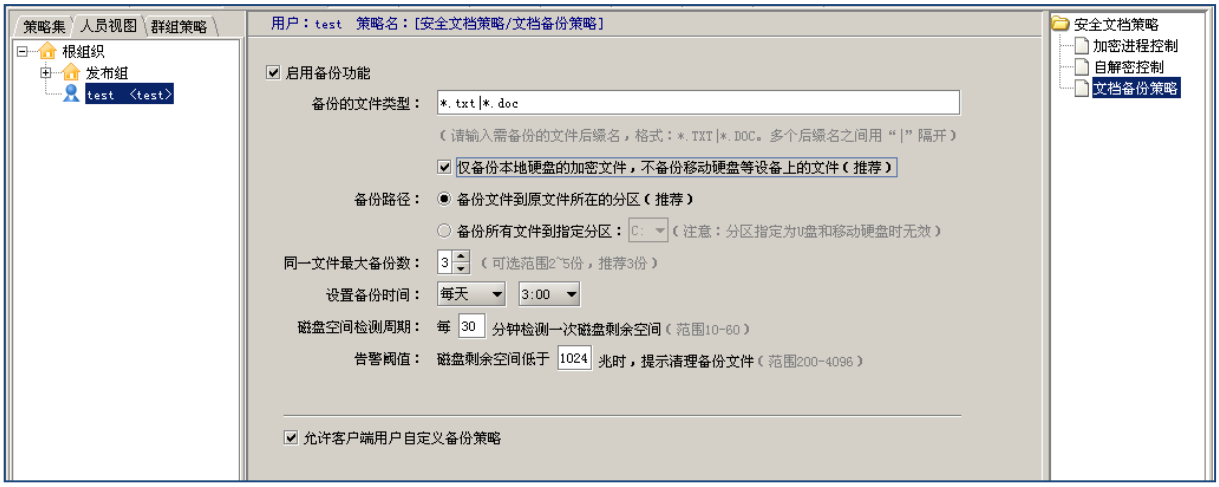


图 5-161　文档备份策略

选项说明:

（1）勾选“启用备份功能”，该页面中其他所有输入项、选择项可用；不勾选，则全部不可用。

（2）“设置备份时间”时，最好在客户端参数设置中，将客户端和服务器时间同步。然后，从下拉框中选择，定时备份的周期和时间点。

（3）备份文件份数最小为 2 份，最大为 5 份。当备份份数低于 2 份时，备份文件保存的最后一份拷贝，可能是已经损坏的文件，失去了备份的意义；当备份份数高于 5 份时，保存了大量的历史文件，这些文件可能只是工作的中间产品，保留越多，意义越小，反而占用了大量的磁盘空间。所以，推荐设置为 3 份，保证文件安全性与磁盘占用的平衡。

（4）选择“备份文件到原文件所在的分区（推荐）”，同时勾选“仅备份本地硬盘的加密文件，不备份移动硬盘等设备上的文件（推荐）”，那么仅备份本地硬盘的加密文件到原分区，不备份移动硬盘等设备上的文件。

（5）选择“备份所有文件到指定分区”，分区指定为 U 盘和移动硬盘时无效。

（6）当选中“允许客户端用户自定义备份策略”的时候，通过控制台设置的策略将作为客户端的缺省备份策略；如果客户端用户自行设置了备份策略，将按照客户端用户自定义的策略实施备份。

提示:

1. 备份路径选择“备份文件到原文件所在的分区（推荐）”时，服务器会检测客户端上所有有盘符的磁盘。这时硬盘保护区、可信磁盘、移动硬盘都会被检测。如果这些磁盘的磁盘空间小于控制台设置的阈值都会在客户端报警提示。

2. 备份路径选择“备份文件到原文件所在的分区（推荐）”时，并且不勾选“仅备份本地硬盘的加密文件，不备份移动硬盘等设备上的文件（推荐）”，这时会对本地硬盘、移动硬盘、可信磁盘或硬盘保护区上的加密文件执行备份，不会对网络硬盘上的加密文件执行备份。服务器除了检测本地磁盘的磁盘空间外，还会检测移动硬盘、可信磁盘和硬盘保护区的磁盘空间。如果不对移动硬盘、可信磁盘和硬盘保护区进行加密文件操作，就不检测这些磁盘的存储空间。

3. 备份的加密文件名长度限制最长为 180 个字符（包括后缀），超过 180 个字符可能会备份不成功。

4. 如果没有启用安全文档的加密进程控制，设置的备份策略无效。备份策略针对的是启用加密进程产生的加密文件，防止恢复时出错而设置的备份。

5.11.4 剪贴板控制

安全文档系统对于加密进程和非加密进程的复制粘贴进行了严格控制，不允许从加密进程向非加密进程复制、拖拽数据。该控制某些用户觉得太严格，此处提供配置功能，允许用户自由设置加密进程和非加密进程白名单。

在“剪贴板控制”界面中，根据用户需要设置加密进程、非加密进程，以及剪贴板控制长度，如图 5-162 所示。

启用加密进程剪贴板放开设置，添加的加密进程，将根据放开的设置项，允许向非加密进程拷贝、拖拽数据，或进行截屏操作。启用非加密进程剪贴板放开设置，那么添加的非加密进程，将根据放开的设置项，允许加密进程向其拖拽、粘贴数据，或插入加密对象文件。启用剪贴板长度限制，超出限制的长度时，将不执行拷贝、粘贴工作。

提示:

1. 如果同时启动多个进程，有的允许截屏，有的不允许截屏，那么截屏的结果按照最严格的控制。比如，加密进程 A，允许截屏；加密进程 B，不允许截屏；A，B 都启动后，截屏后的内容也不能贴到非加密进程中。

2. 某些软件本身不支持拷贝、拖拽操作，与下发的策略没有关系。

3. 剪贴板长度限制，这个长度只是一个近似值，字符或字节数与具体软件有关。

图 5-162　剪贴板控制界面

5.11.5 截屏软件黑白名单

安全文档在针对拷屏键进行控制的基础上，增加对专业拷屏软件的控制。在“截屏软件黑白名单”设置界面中，添加截屏软件进程名，将策略应用下发，如图 5-163 所示。黑名单指定的拷屏软件，将在加密进程启动情况下被禁止运行。白名单指定的拷屏软件不受控制。

如果下发了截屏软件黑名单设置，当启动任意加密进程时，黑名单中的截屏软件会强制退出；如果下发了截屏软件黑名单设置，当任意加密进程正在运行中，黑名单中的截屏软件无法启动；如果在加密进程剪贴板放开设置中，设置了加密进程 A 允许截屏，即使下发了截屏软件黑名单设置，启动和使用加密进程 A，截屏软件仍可以自由使用。

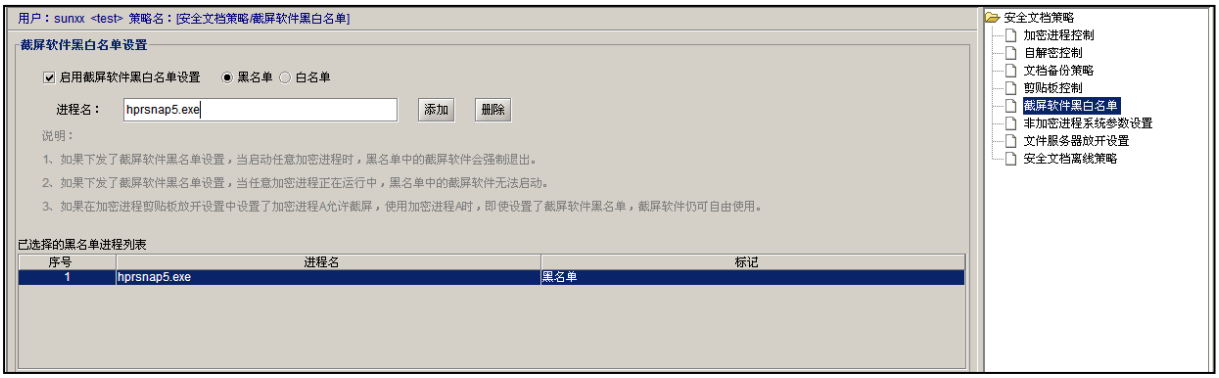


图 5-163　截屏软件黑白名单设置

5.11.6 非加密进程系统参数设置

在“非加密进程系统参数设置”中，添加非加密进程名，如图 5-164 所示。在设置的非加密进程中，对加密文件不做只读保护，或与加密进程可共享打开加密文件。该项功能属高级设置，使用时请慎重，请技术人员指导。

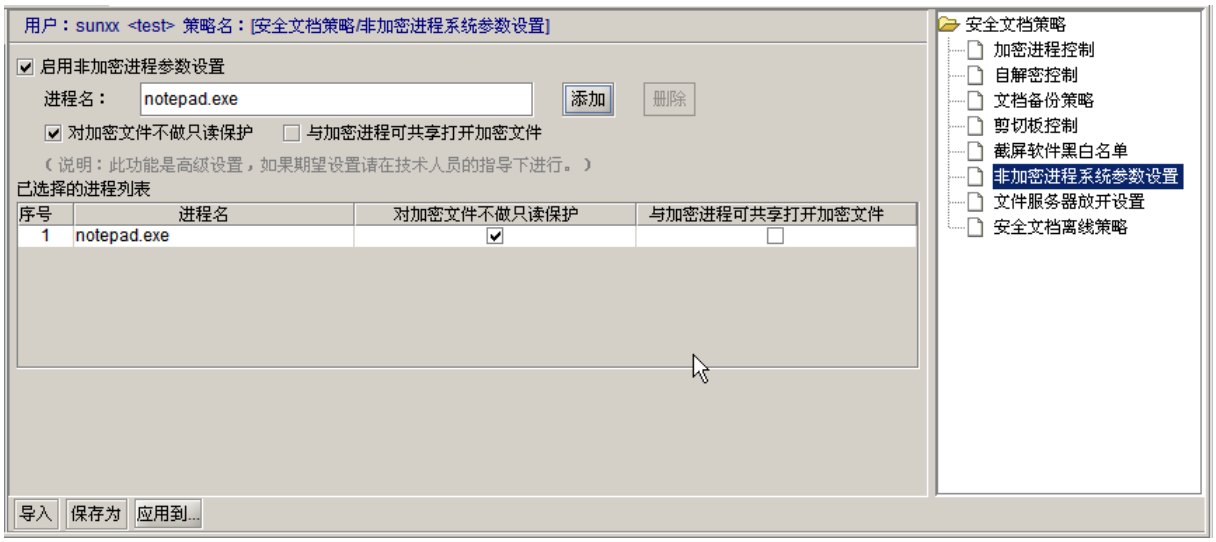


图 5-164　非加密进程系统参数设置

5.11.7 文件服务器放开设置

在“文件服务器放开设置”中，添加文件服务器放开路径（网络共享目录），如图 5-165 所示。策略应用后，加密进程向放开路径下保存文件时，文件不再被加密。将生成的加密文件拖到放开路径下，依然是加密的。

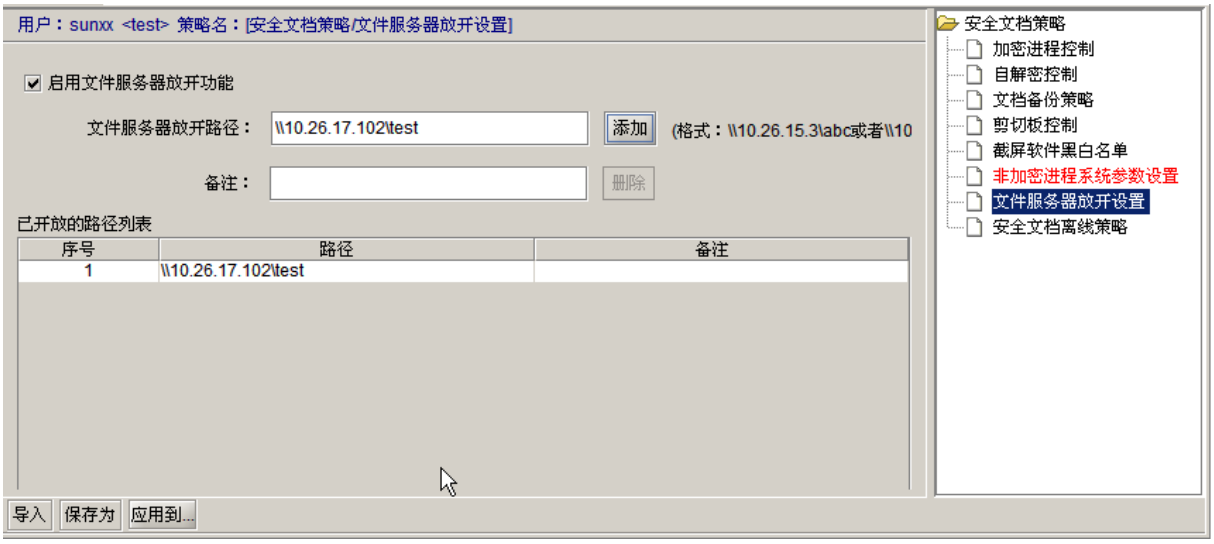


图 5-165　文件服务器放开设置

5.11.8 安全文档离线策略

设置安全文档离线策略，首先要在“加密进程控制”界面中，启用安全文档离线策略，如图 5-166 所示。

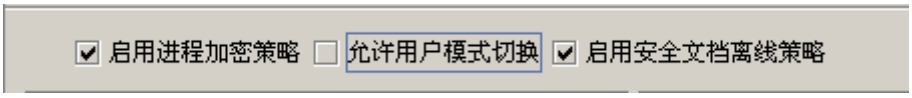


图 5-166　离线时强制切换到普通模式

在安全文档离线策略设置中，如果设置“离线后强制切换到普通模式”，客户端离线后，安全文档内核停止工作，所有的加密文件均不能使用。当客户端再次上线后，会自动切换到工作模式，安全文档内核重新工作。如图 5-167 所示。

图 5-167　安全文档离线策略设置

如果选择离线后有条件使用加密文件，并且设置加密文件生效时间，那么用户离线后，在加密文件的生效时间内，根据用户设置，有条件使用加密文件。例如：只读访问加密文件，禁止打印加密文件，禁止自解密加密文件等；另一种情况，用户离线后，在加密文件的生效时间外，不能使用加密文件，且新生成的文件不加密。

如果选择离线后有条件使用加密文件，不设置加密文件生效时间，那么用户离线后，不受时间限制，根据用户的设置，有条件使用加密文件。

5.11.9 安全文档工具的使用

5.11.9.1 灾难恢复工具

用户在使用过程中，为了防止系统出现意外或者客户端卸载后，原来加密的文档打不开，安全文档系统提供了灾难恢复工具。

例如：如果下发了 Winword 加密进程，Winword 应用程序在使用过程中会调用很多模板，这些模块也会自动加密。当卸载了 UEM 客户端或者停用安全文档功能模块后，Winword 因模板加密不能使用。这时就可以用灾难恢复工具恢复，当然也可以重新安装 Office 系统解决。

（1）运行安装程序包 Tools_UEM8.0 中的灾难恢复工具 EfsRecorver.exe，出现身份认证界面。认证方式有两种：管理员身份认证和动态口令认证。

如果是 UEM 系统管理员或者具有管理员权限（所有管理员帐户都可以），既采用“管理员身份认证”模式。输入用户名和密码后，点击“确定”按钮，启动灾难恢复工具，如图 5-168 所示。

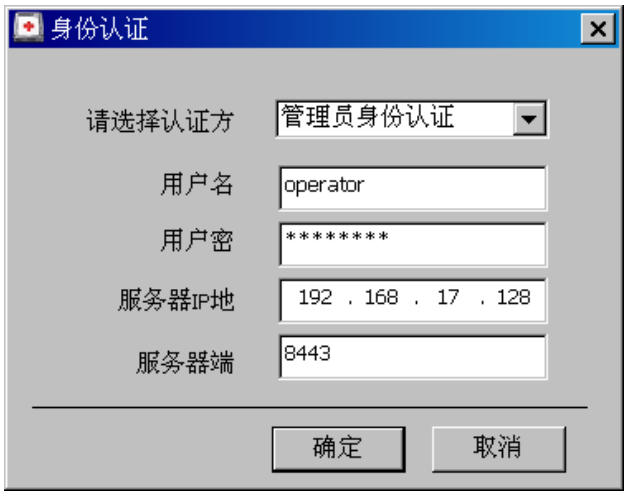


图 5-168　管理员身份认证界面

如果是普通用户，则将生成的随机码发给管理员，管理员允许后将生成的验证码返回给用户，那么用户就可用此验证码启动灾难恢复工具，如图 5-169 所示。参见“灾难恢复动态中令管理”章节。

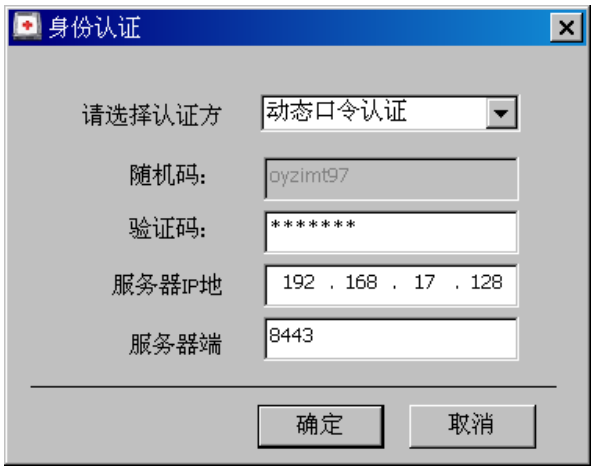


图 5-169　动态口令身份认证界

（2）在灾难恢复主界面，设置路径和不同参数，点击“开始”按钮，开始进行指定目录的扫描。扫描到加密文件后，自动对其解密，同时在主界面中显示扫描、恢复结果，如图 5-170 所示。

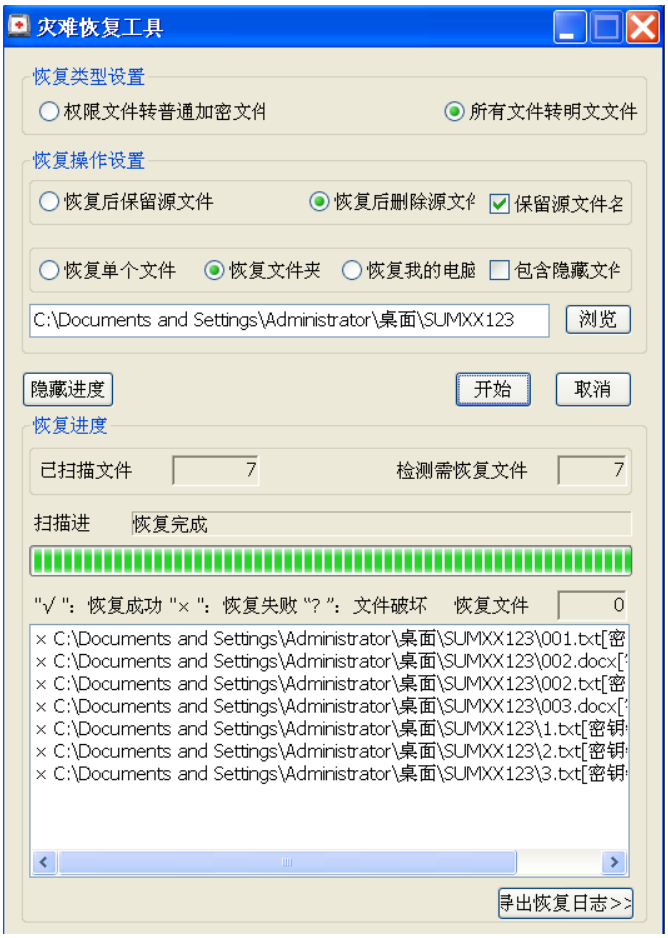


图 5-170　灾难恢复工具主窗口

注意：使用灾难恢复工具时，一定要保证原来的 UEM 服务器没有卸载，数据库还存在，并且原来装客户端的机器与服务器网络畅通，否则不会出现恢复主界面，也不可能恢复成功。

5.11.9.2 扫描加密工具

扫描加密工具 EFSScanEncryptTool.exe，用于对客户端指定目录下、指定扩展名的文件进行扫描并且加密。双击运行扫描加密工具，运行主界面如图 5-171 所示。

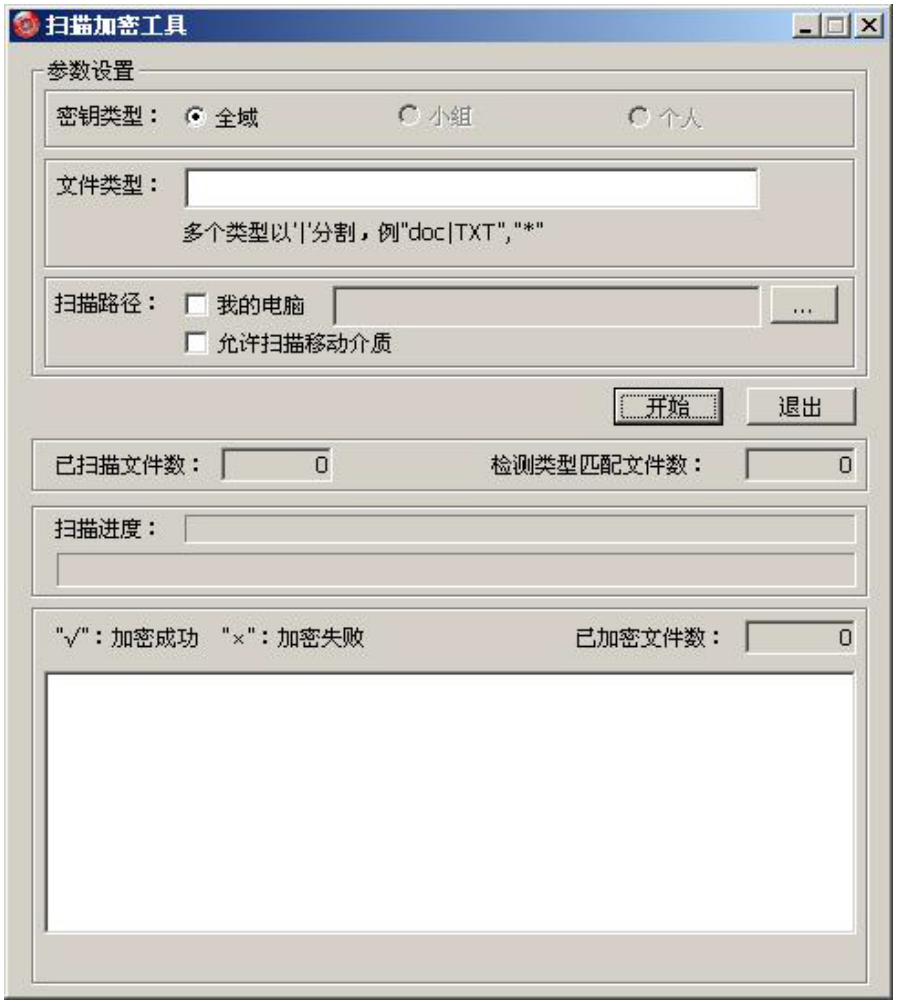


图 5-171　扫描加密工具

在扫描加密工具中，需要指定要扫描加密的文件扩展名、扫描的路径等参数，点击“开始”按钮后，进行扫描加密工作。扫描结束后，在主界面中将显示扫描加密结果。

5.12 安全文档隔离管理

隔离管理分为“个人隔离”和“部门隔离”。“个人隔离”是对用户下发个人隔离策略，该用户产生的指定类型文件为隔离文件（个人隔离），此类文件用户自己可以自由访问，其他用户不能访问。“部门隔离”是将一个或者多个部门添加到一个隔离范围中，这一隔离范围内的用户产生的指定类型文件为隔离文件（部门隔离文件），此类文件可以被范围内的用户自由访问，范围之外的用户禁止访问。

5.12.1 隔离策略

◆ **个人隔离**

（1）在安全管理中心中，单击“安全文档隔离管理” → “隔离策略”→“个人隔离”，进入个人隔离策略设置界面，如图 5-172 所示。

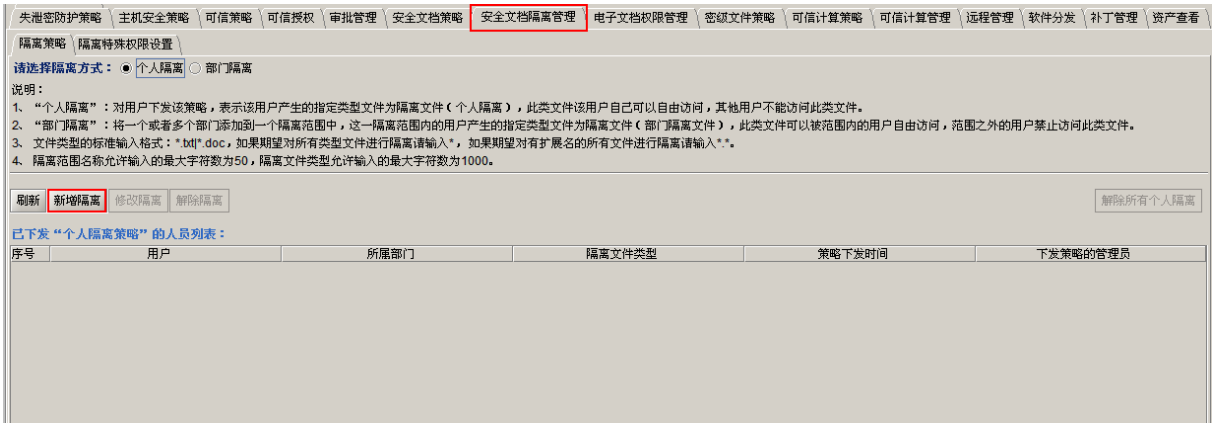


图 5-172　个人隔离管理界面

（2）单击下方的“新增隔离”按钮，添加隔离文件类型（加密进程控制的文件类型），选择要隔离的人员，如图 5-173 所示。文件类型的标准输入格式为*.txt|*.doc，如果期望对所有类型文件进行隔离请输入*（包含所有有扩展名的文件及无扩展名的文件），如果期望对有扩展名的所有文件进行隔离请输入*.*。

提示:

（1）隔离策略包括个人隔离策略和部门隔离策略，隔离策略和群组策略不能同时存在，下发隔离策略的用户不能再下发群组策略，同时，下发群组策略的用户也不能再下发隔离策略；在 UEM 组织机构中，下发隔离策略的用户不能迁移，更改节点位置；同时，没有下发隔离策略的用户，要迁移到的地方有隔离策略，系统也不让迁移。

（2）隔离文件是在安全文档的基础上做进一步的隔离控制，所以在下发隔离文件策略前，必须下发安全文档策略。同时，隔离文件类型必须是启用加密进程控制的文件类型，否则生成的文件是普通文件，而不是安全文档，更谈不上是隔离文件。

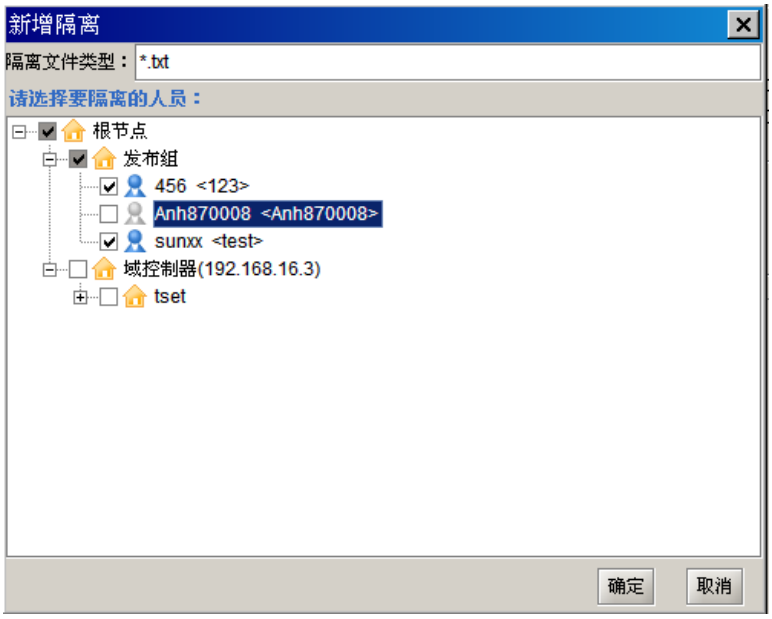


图 5-173　新增隔离策略

（3）单击“确定”按钮，提示策略应用成功。这时，收到策略的客户端用户，以后生成的指定类型的文件为隔离文件，用户自己可以自由访问，其他用户禁止访问。隔离文件图标和安全文档也不一样，如图 5-174 所示。

隔离文件　　安全文档

图 5-174　隔离文件图标

（4）在“个人隔离策略列表”中，可以看到新增的个人隔离策略，如图 5-175 所示。选择某条个人隔离策略，单击“修改策略”按钮，可以修改隔离文件类型。确定后，将修改后的个人隔离重新应用下发。

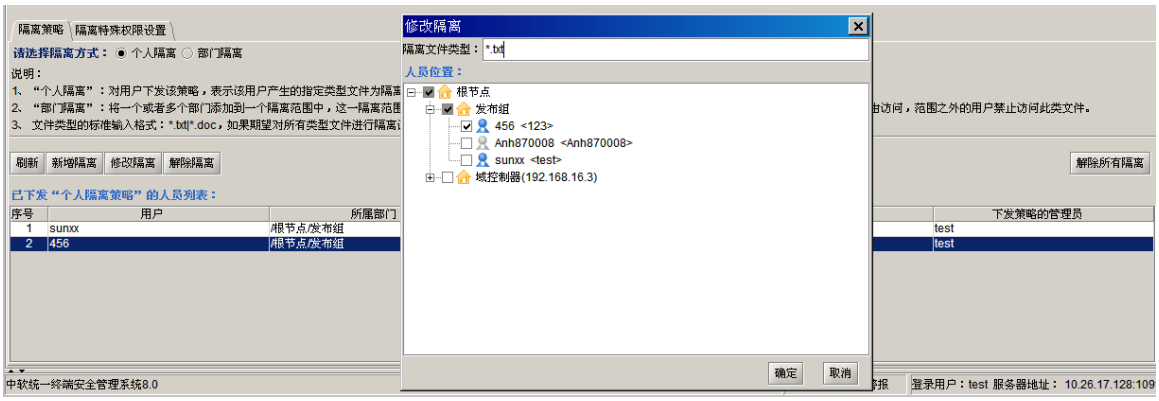


图 5-175　修改个人隔离策略

（5）如果要删除某用户的个人隔离策略，在“个人隔离策略列表”中，选中某用户个人隔离策略，单击“解除隔离”按钮，将此策略删除，如图 5-176 所示。也可单击右边的“解除所有隔离”按钮，将列表中的所有个人隔离策略一次性解除。

个人隔离策略解除后，原来产生的个人隔离文件，只有自己能够打开使用，保存后变为普通安全文档；如果将该用户添加到部门隔离范围中，它打开的原来个人隔离文件就变成了部门隔离文件，可以由部门里的每个人打开使用。

提示:

如果某用户有个人隔离策略，欲将该用户添加到部门隔离策略范围中，需要先解除该用户的个人隔离策略，然后才能将用户添加到部门隔离策略范围中。也就是说，某用户要么有个人隔离策略，要么有部门隔离策略，不能同时有个人隔离策略和部门隔离策略。当用户具有部门隔离策略时，也只能拥有一个部门隔离策略，不能同时隶属于两个部门策略。

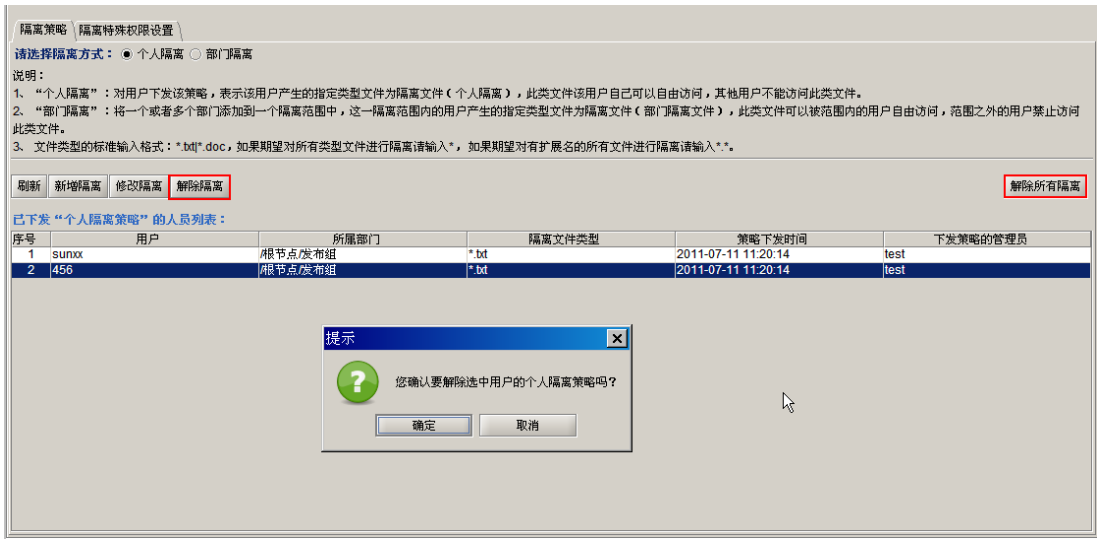


图 5-176　解除个人隔离策略

◆ **部门隔离**

（1）在安全管理中心中，单击“安全文档权限管理”→“隔离管理”→“部门隔离”，进入部门隔离策略设置界面，如图 5-177 所示。

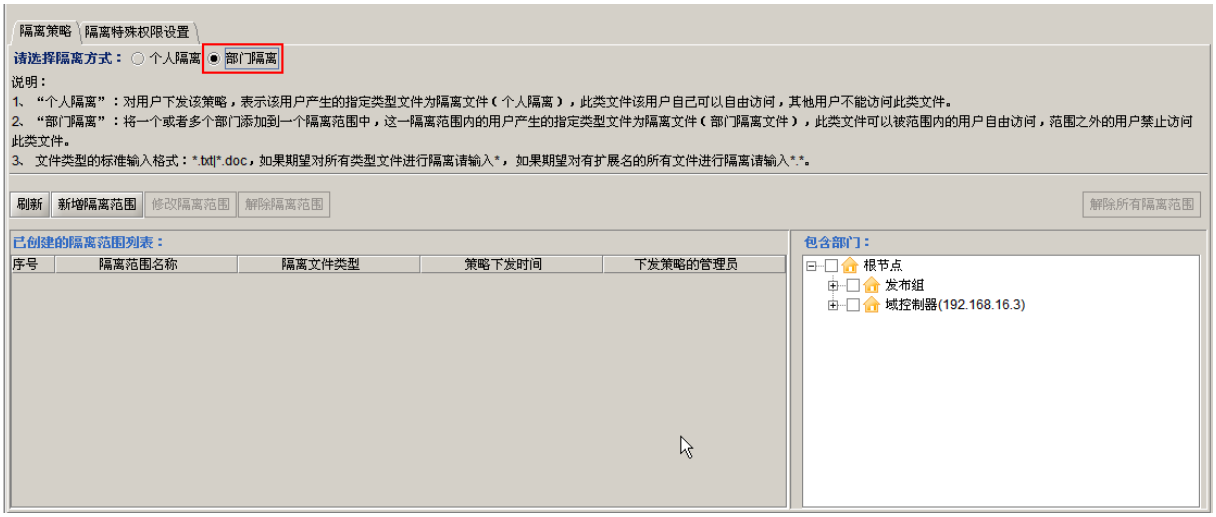


图 5-177　部门隔离管理界面

（2）单击下方的“新增隔离范围”按钮，输入隔离范围名称和隔离文件类型，并选择隔离范围，如图 5-178 所示。文件类型的标准输入格式为*.txt|*.doc，如果期望对所有类型文件进行隔离请输入*，　如果期望对有扩展名的所有文件进行隔离请输入*.*。

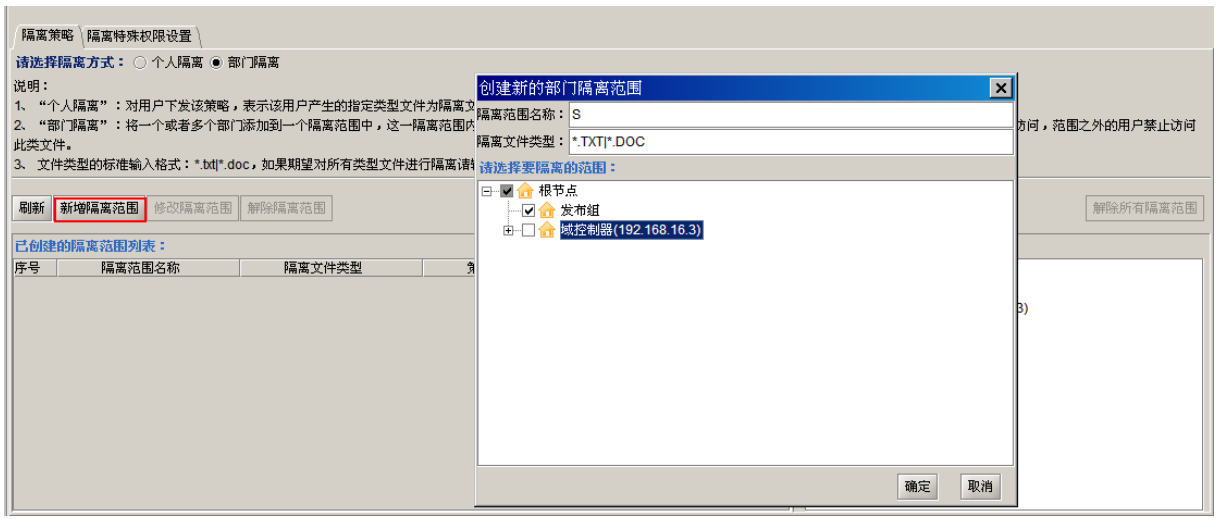


图 5-178　新增隔离范围

（3）如果新增隔离范围中，某些用户有个人隔离策略，提示解除这些用户的个人隔离策略，如图5-179 所示。这时，管理员需要回到个人隔离界面，将这些用户的个人隔离策略解除，然后再制定部门隔离策略。

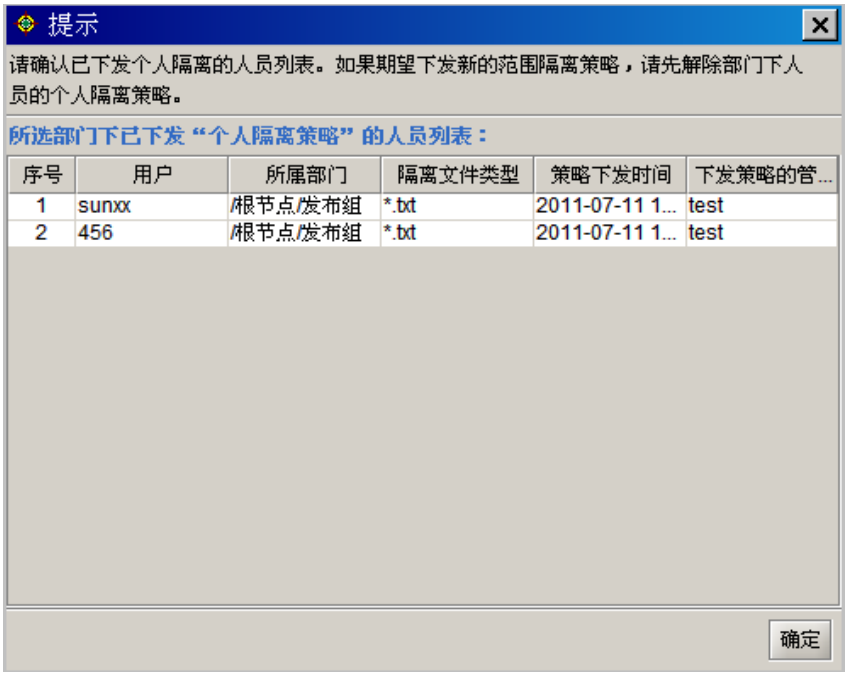


图 5-179　提示解除某些个人隔离策略

（4）部门策略制定成功后，展示在下方的隔离范围列表中，右边显示包含的具体部门，如图 5-180 所示。这时，隔离范围内的用户产生的指定类型文件为隔离文件（部门隔离文件），此类文件可以被范围内的用户自由访问，范围之外的用户禁止访问此类文件。

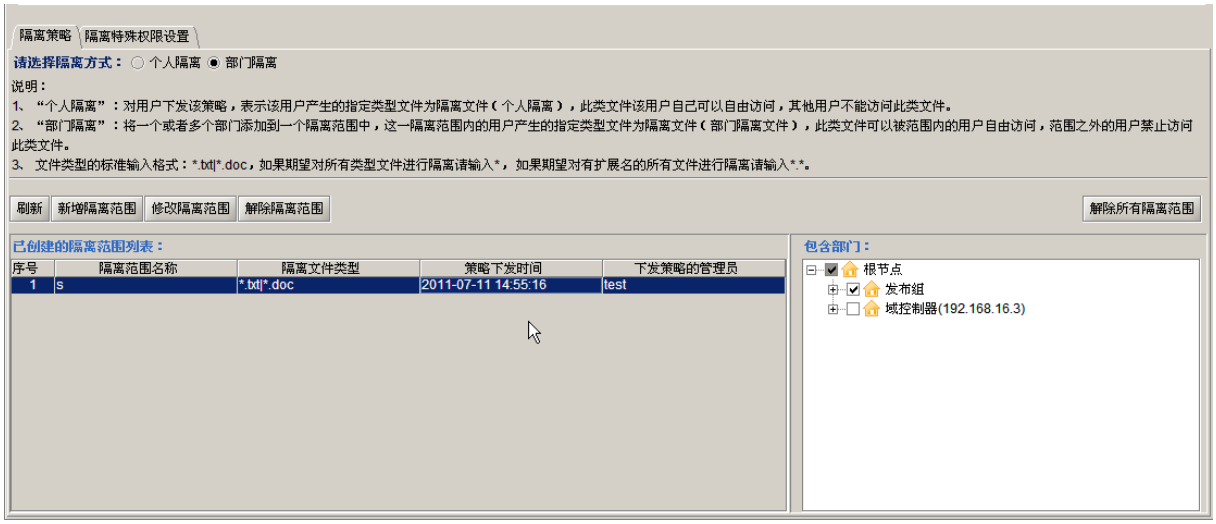


图 5-180　部门策略列表

（5）选择某部门隔离策略，单击“修改隔离范围”按钮，可以修改部门隔离策略的文件类型和隔离范围，如图 5-181。确定后，此策略重新应用下发。那么，隔离范围内的用户产生的**新指定类型文件**为隔离文件（部门隔离文件），此类文件可以**被新范围内**的用户自由访问，并且对该部门以前产生的隔离文件也可以自由访问。 也就是说，部门隔离文件只与隔离范围有关，是这个范围就能访问，不是这个范围就不能访问，它与文件类型没有太大关系，文件类型只控制以后生成的该类型文件是部门隔离文件。

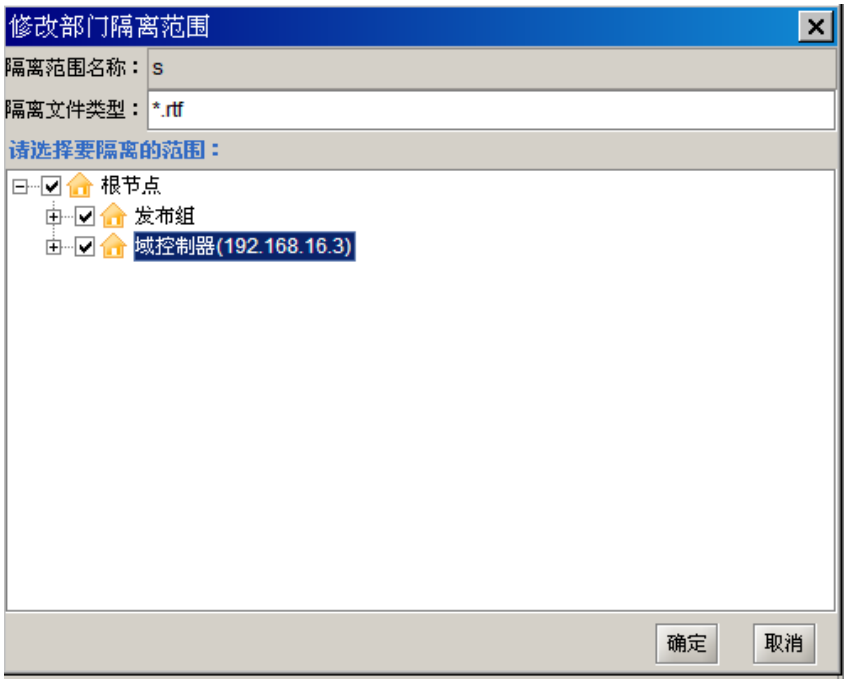


图 5-181　修改部门隔离策略

（6）如果要删除某部门的隔离策略，选定该策略后，单击“解除隔离范围”按钮，将此策略删除，如图 5-182 所示。也可单击右边的“解除所有隔离范围”按钮，将列表中的所有部门隔离策略一次性解除。

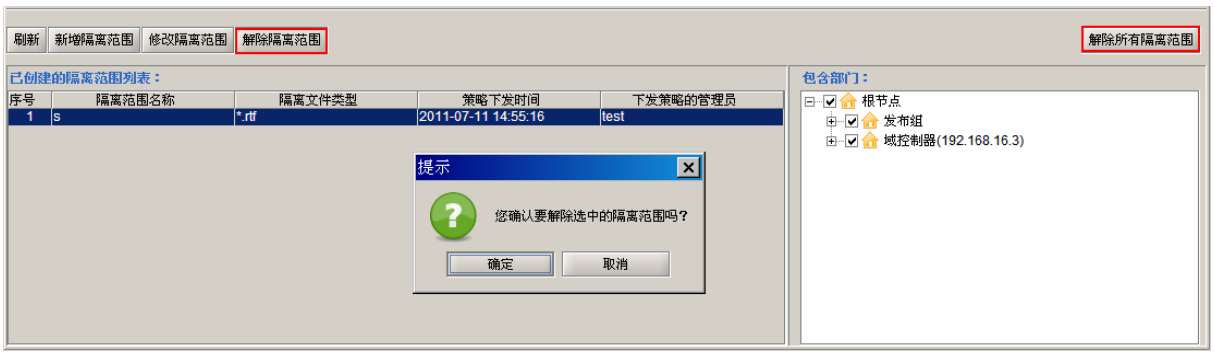


图 5-182　解除部门隔离策略

部门隔离策略解除后，原来的部门隔离文件，若曾经被当前用户成功访问，则即使解除部门策略，当前用户仍然可访问该隔离文件，但修改后再保存时，就会转变为普通安全文档。

5.12.2　隔离特殊权限设置

隔离特殊权限设置是将组织结构中某些特别人员或群组启用强制访问控制策略，使他们能够访问指定范围内用户产生的个人隔离文件和部门隔离文件，从而满足管理上的需要。

（1）在安全管理中心中，单击“安全文档隔离管理”→“隔离特殊权限设置”，进入隔离特殊权限设置界面。在左侧选择人员或群组，在右侧单击“强制访问控制”，在中间显示区勾选“是否启用强制访问控制”，然后在列表框中选择接受强制访问的人员或组织，如图 5-183 所示。

图 5-183　制定强制访问控制策略

（2）单击下方“应用到”按钮，将强制访问控制策略应用下发，如图 5-184 所示。这样，收到策略的客户端可以访问指定范围内用户产生的个人隔离文件和部门隔离文件。

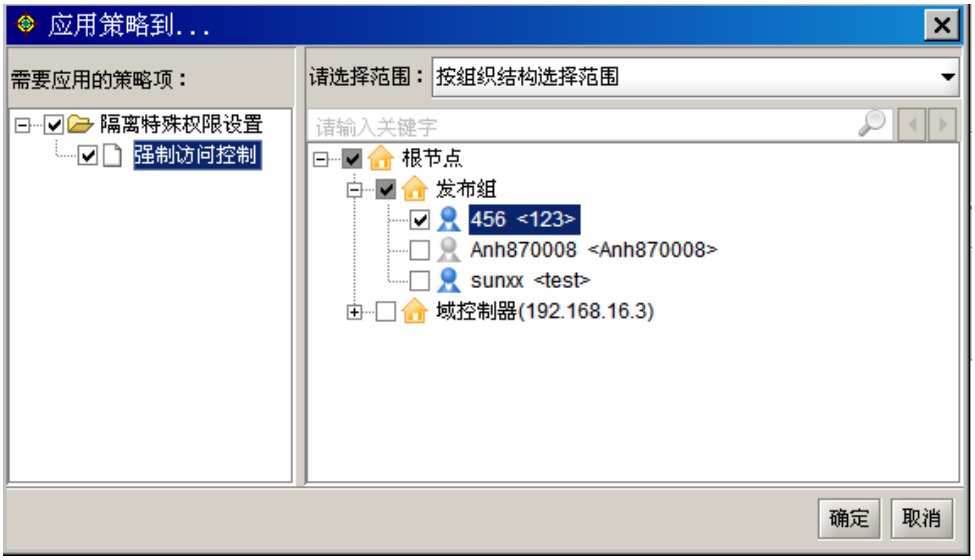


图 5-184　应用强制访问控制策略

5.13 电子文档权限管理

电子文档权限管理能对文档进行细分化的权限设置，确保重要文件在特定授权范围内进行指定操作，同一文档可以针对不同用户设置不同权限。

主动授权文件是用户主动制作生成的一种加密文件，此类文件本身带有一些制作者主动设置的使用权限，用户访问该文件时受文件中设置的使用权限控制。“主动授权文件”可以通过在线审批方式制作，而对于下发了离线制作主动授权文件策略的用户，也可以通过离线方式自主制作“主动授权文件”。

◆ 自审批授权控制

（1）在安全管理中心中，单击“电子文档权限管理”标签页，在左侧选择人员或群组，在右侧单击“自审批授权控制”，在中间显示区勾选“允许用户通过右键菜单形式制作主动授权文件”，然后选择允许制作主动授权的文件类型——隔离文件或非隔离文件，如图 5-185 所示。非隔离文件不包括密级文件和用“我的加密文件夹”加密的文件。

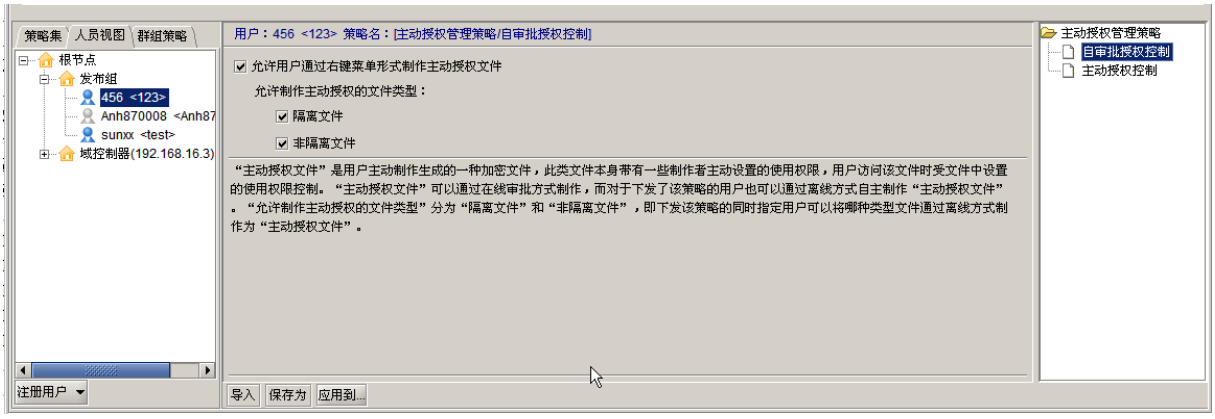


图 5-185　自审批授权控制

（2）单击下方“应用到”按钮，将主动授权控制策略应用下发，如图 5-186 所示。这样，收到策略的客户端就可通过右键菜单形式离线制作主动授权文件。参见客户端电子文档权限管理部分。

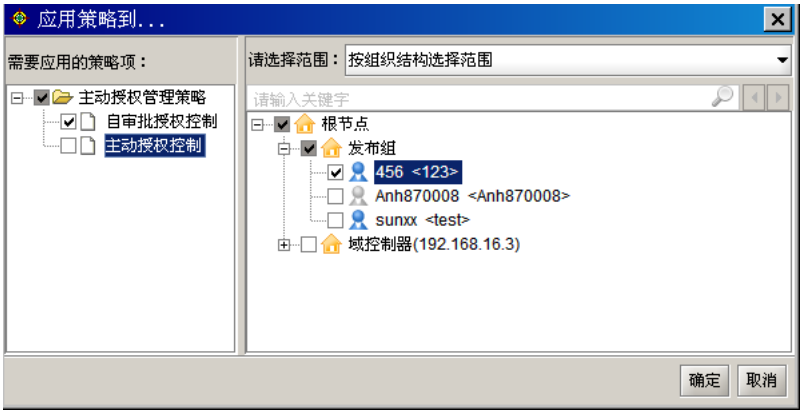


图 5-186　下发自审批授权控制策略

◆ 主动授权控制

（1）在主动授权管理策略中，单击右侧“主动授权控制”，进入主动授权控制界面，如图 5-187 所示。在这里设置允许打印的主动授权文件，打印输出的水印内容、字体、字号、字形、颜色以及时间等。

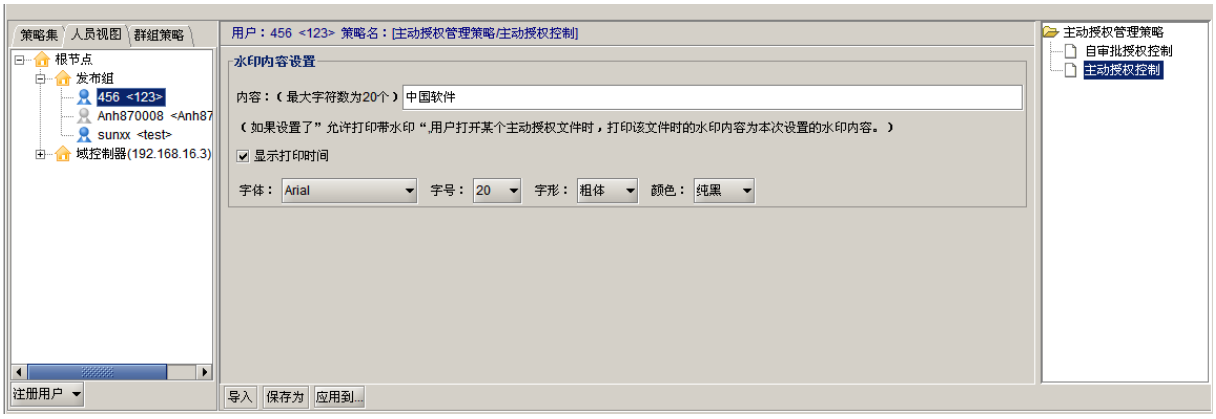


图 5-187　主动授权控制

（2）单击下方“应用到”按钮，将主动授权控制策略应用下发，如图 5-188 所示。这样，收到策略的客户端制作的主动授权文件，如果允许打印时，就可打印出设置的水印内容。

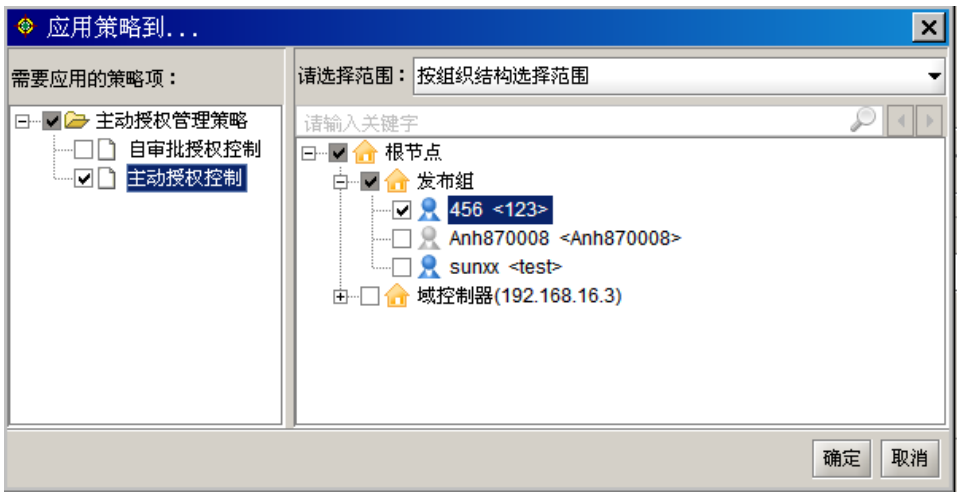


图 5-188　下发主动授权控制策略

5.14 扫描执行管理

扫描执行管理是通过控制台向客户端下发扫描加密命令，客户端收到命令后启动安全内核，对指定扩展名的文件进行全盘扫描，如遇未加密的文件进行加密操作。在整个扫描加密过程中，管理员可以查看客户端当前的扫描加密执行状态，启动、暂停、继续或终止任一次扫描加密任务。管理员也可查看每台计算机的扫描加密历史记录，并对客户端的扫描状态和扫描历史信息进行统计审计分析。

5.14.1 扫描执行管理界面

在安全管理中心中，用鼠标单击功能菜单项“扫描执行管理”，进入扫描执行管理界面，如图 5-189 所示。

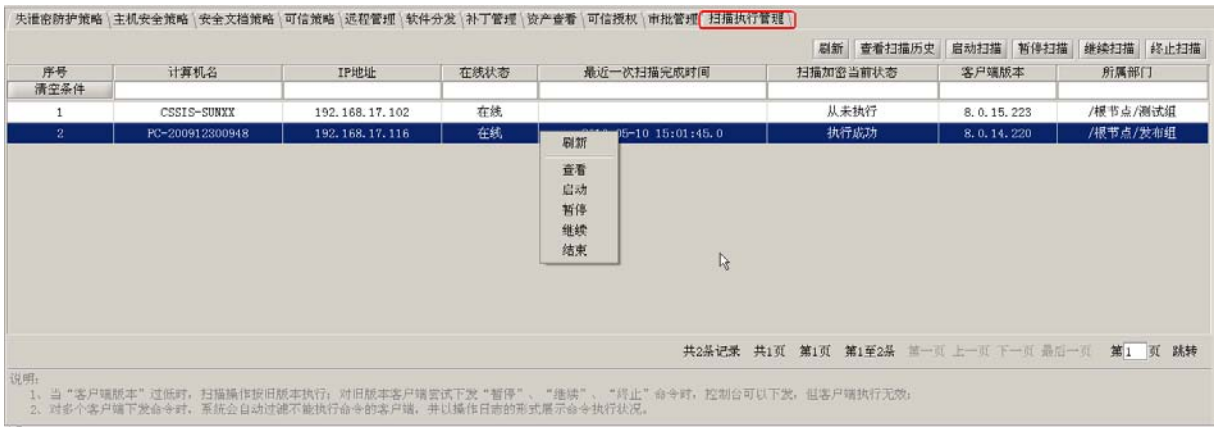


图 5-189　扫描执行管理界面

界面分为三部分，即工具栏、信息显示区和分页区，控制台以表的形式在信息显示区展示出所有计算机的扫描加密执行情况，包括：“计算机名” 、“IP 地址”、“在线状态”、“最近扫描的完成时间”、“扫描加密当前状态”、“客户端版本”、“所属部门”等。工具栏包括：启动扫描、暂停扫描、继续扫描、终止扫描、查看扫描历史等，单击信息列表右键菜单也显示相应功能菜单。

客户端在线状态分两种：在线和离线。客户端“在线”时，对计算机下发命令后，客户端接收到命令后，即可执行相应的扫描任务；客户端“离线”时，对计算机下发命令后，待客户端下一次上线，并从服务器端成功接收到命令后，才会执行相应的加密扫描任务。

5.14.2 启动扫描加密

1. 在扫描执行管理界面，选中某计算机，选择工具栏“启动扫描”按钮或者右键快捷菜单中的“启动”项，进入“扫描加密参数设置”界面，如图 5-190 所示。

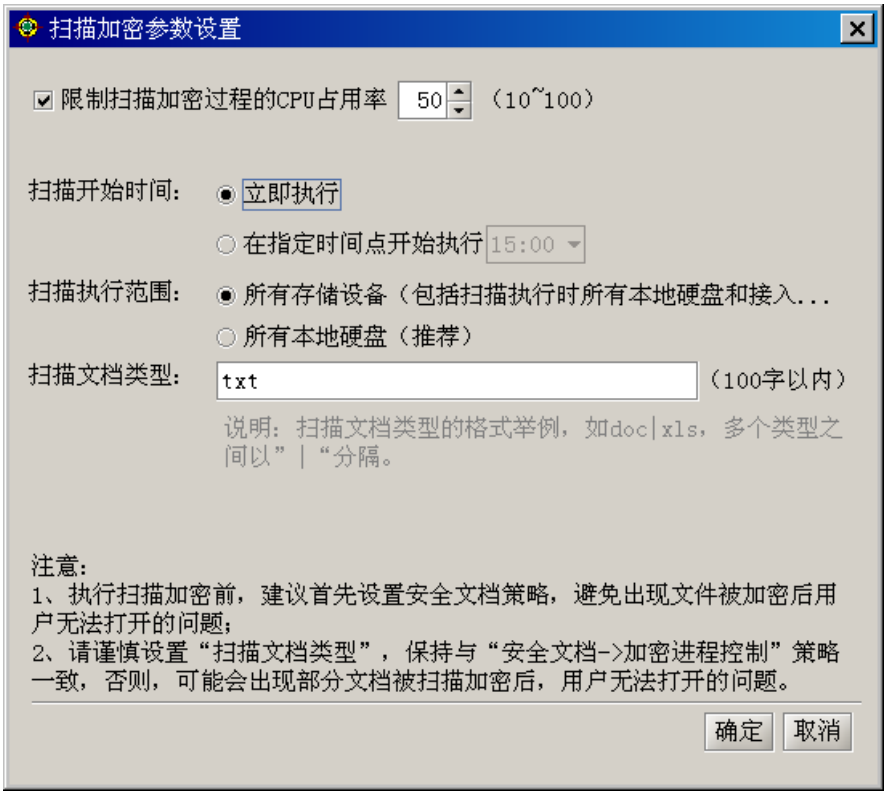


图 5-190　扫描加密参数设置

选项说明：

“CPU 占用率”为可选项。通过此项设置，对客户端扫描过程中出现 CPU 占用率过高的情况进行控制。如果 CPU 占用率超出设置的值，则客户端会强制停止扫描。

“执行开始时间”包括两种方式：立即执行和自定义时间点，根据需要确定。

“扫描范围”包括两种方式：扫描计算机所有存储设备和所有本地硬盘，建议选择所有本地硬盘。

“扫描文件类型”是通过设置文件类型，对扫描的文件进行过滤。如：输入“doc|txt|xml”，表示仅对文件后缀名为.doc、.txt 和.xml 的文件进行扫描加密，其余格式的文件不扫描。

提示：

（1）如果输入的后缀名中包含“exe”时，弹出错误提示框。请用户不要对扩展名为 exe 的文件进行加密操作，它可能影响到 WINDOWS 操作系统正常运行。

（2）扫描加密过程中，对回收站内的文件不扫描加密。

2. 参数设置完成后，单击设置界面中“确定”按钮，会弹出提示框，如图 5-191 所示。再次“确定”后，将启动扫描命令下发至选择定的计算机 。客户端计算机收到命令后，启动扫描进程。

安全文档扫描进程启动后，会自动调用进程保护接口，防止进程被客户端用户人为杀掉。进程退出后，自动将自己的进程号从保护列表中去掉。

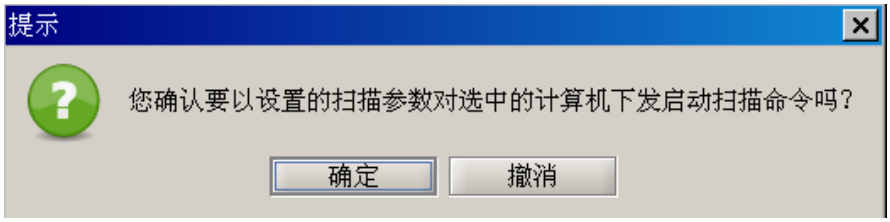


图 5-191　启动扫描命令提示框

计算机“扫描加密的当前状态”值不会立刻发生变化。待命令下发一段时间后，控制台会从服务器获取新的数据刷新列表，计算机“扫描加密的当前状态”值才会发生变化。

对于“在线”计算机，只有在执行“启动扫描”命令前，“扫描加密当前状态”值为“从未执行”、“已终止扫描”、“已成功完成扫描”或者“扫描失败”的计算机，并且客户端成功获取到启动扫描命令，此时“扫描加密的当前状态”值才会变为“正在扫描”，否则值保持不变。

对于“离线”的计算机，需等该计算机上线后，成功接收到服务器的“启动扫描”命令后，才会执行相应的扫描任务，所以此时离线的计算机记录中，“扫描加密当前状态”的值并不发生变化。

提示：

1、当“客户端版本”过低时（R7 以前的版本），扫描操作按旧版本执行；对旧版本客户端尝试下发“暂停”、“继续”、“终止”命令时，控制台可以下发，但客户端执行无效；

2、对多个客户端下发命令时，系统会自动过滤不能执行命令的客户端，并以操作日志的形式展示命令执行状况。

3. 控制台下发启动扫描命令后，服务器返回执行结果，可以在控制台操作日志中查看，如图 5-192 所示。

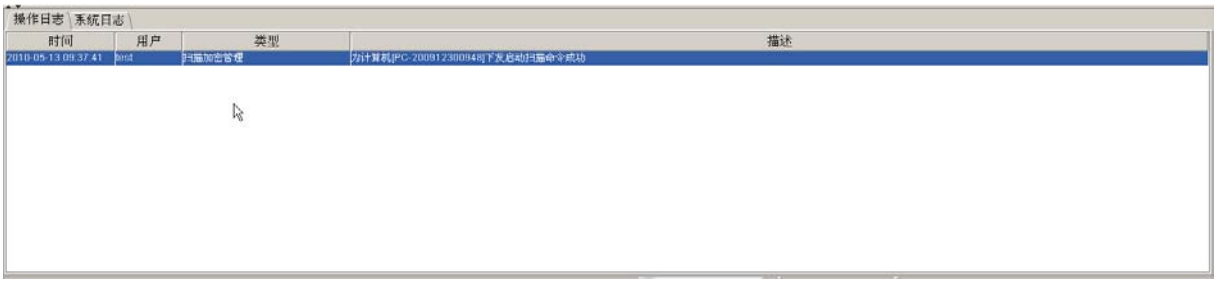


图 5-192　控制台操作日志

5.14.3 暂停扫描加密

对于正在执行扫描命令的在线客户端，用户可以通过控制台下发“暂停扫描”命令。客户端收到命令后，暂停扫描任务的执行。

1. 在扫描执行管理界面，选中正在扫描的计算机，选择工具栏“暂停扫描”按钮或者右键快捷菜单中的“暂停”项，下发“暂停扫描”命令，如图 5-193 所示。

图 5-193　下发暂停扫描命令

2. 客户端收到“暂停”命令后，执行暂停操作。

计算机的“扫描加密当前状态”不会立刻发生变化。待命令下发一段时间后，控制台会从服务器获取新的数据刷新列表，计算机“扫描加密的当前状态”值才会发生变化。

对于“在线”的计算机，只有在执行“暂停扫描”命令前，“扫描加密当前状态”值为“正在执行”，并且客户端成功获取到暂停命令，这时“扫描加密当前状态”值才会变为“暂停扫描”，否则值不会改变；对于“离线”的计算机，不能执行暂停命令。

3. 控制台下发暂停扫描命令后，服务器返回执行结果，可以在控制台操作日志中查看，如图 5-194 所示。

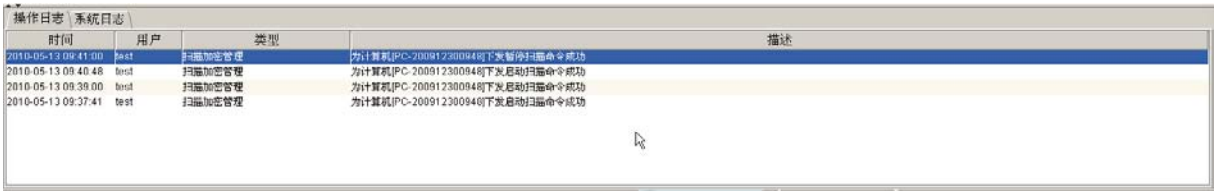


图 5-194　控制台操作日志

5.14.4 恢复扫描加密

对于暂停扫描状态的在线客户端，用户可以通过控制台下发“继续扫描”命令。客户端收到命令后，重新启动扫描进程，执行扫描任务。

1. 在扫描执行管理界面，选中“暂停扫描”状态的计算机，选择工具栏“继续扫描”按钮或者右键快捷菜单中的“继续”项，下发“继续扫描”命令，如图 5-195 所示。

图 5-195　下发继续扫描命令

2. 客户端收到“继续扫描”命令后，重新启动扫描进程。

计算机的“扫描加密当前状态”不会立刻发生变化。待命令下发一段时间后，控制台会从服务器获取新的数据刷新列表，计算机“扫描加密的当前状态”值才会发生变化。

对于“在线”的计算机，只有在执行“继续扫描”命令前，“扫描加密当前状态”值为“暂停扫描”，并且客户端成功获取到继续扫描命令，这时“扫描加密当前状态”值才会变为“正在扫描”，否则值不会改变；对于“离线”的计算机，不能执行继续命令。

3. 控制台下发继续扫描命令后，服务器返回执行结果，可以在控制台操作日志中查看，如图 5-196 所示。

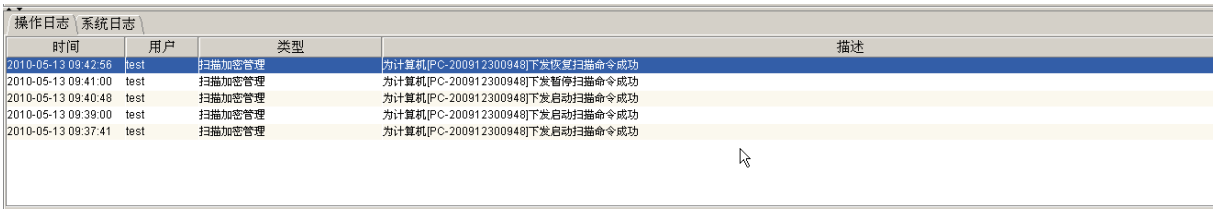


图 5-196　控制台操作日志

5.14.5 终止扫描加密

对于“正在扫描”或者“暂停扫描”的客户端，用户可以通过控制台下发“终止扫描”命令。客户端收到命令后，强制停止扫描进程执行。

1. 在扫描执行管理界面，选中“正在扫描”或“暂停扫描”状态的计算机，选择工具栏“终止扫描”按钮或者右键快捷菜单中的“结束”项，下发“终止扫描”命令，如图 5-197 所示。

图 5-197　下发终止扫描命令

2. 客户端收到“终止扫描”命令后，强制终止扫描进程执行。

计算机的“扫描加密当前状态”不会立刻发生变化。待命令下发一段时间后，控制台会从服务器获取新的数据刷新列表，计算机“扫描加密的当前状态”值才会发生变化。

对于“在线”的计算机，只有在执行“终止继续扫描”命令前，“扫描加密当前状态”值为“正在扫描”或“暂停扫描”，并且客户端成功获取到终止扫描命令，这时“扫描加密当前状态”值才会变为“执行成功”，否则值不会改变。

对于“离线”的计算机，需等该计算机上线后，成功接收到服务器的“终止扫描”命令后，才会执行相应的扫描任务，所以此时离线的计算机记录中，“扫描加密当前状态”的值并不发生变化。

3. 控制台下发终止扫描命令后，服务器返回执行结果，可以在控制台操作日志中查看，如图 5-198 所示。

图 5-198　控制台操作日志

5.14.6 查看扫描加密历史记录

1. 在扫描执行管理界面，选中某一计算机，选择工具栏“查看扫描历史”按钮或者右键快捷菜单中的“查看”项，查看该计算机执行的所有扫描记录，如图 5-199 所示。

图 5-199　查看扫描历史

选择一个或者多个计算机，若选择一行记录时，工具栏“查看扫描历史”按钮和右键快捷菜单中的“查看”项处于可用状态；若选择多行记录，则“查看扫描历史”按钮和“查看”项不可用。工具栏其他按钮以及菜单项其他项均处于可用状态。直接双击某行记录，也可进入扫描加密历史记录界面。

2. 在扫描加密历史记录界面，用户可以根据过滤条件对历史记录进行查询、查看，如图 5-200 所示。

图 5-200　扫描加密历史记录

5.15 密级文件策略

密级文件是基于密级标识的安全文件，与安全文档一样都是以透明加解密技术为基础，同时，密级文件共用了安全文档的加密进程策略管理机制。密级文件策略作为 UEM 系统独立的功能模块，其模块授权方式是通过 licence 控制的。授权密级标识文件，必须授权安全文档管理；但授权安全文档管理，可不授权密级标识文件。

有密级标识功能的客户端，其生成的文件有三种状态：非加密文件、普通加密文件和密级文件，它们之间有一个变化过程。简单地说：文件初始状态即非加密文件，加密进程将非加密文件加密成普通加密文件，用户可以申请将普通加密文件变成密级文件。

密级文件有四个级别：普通、秘密、机密、绝密，同时还有使用范围限制。在前面“添加用户”章节，我们讲过用户自身也有密级。当用户访问密级文件时，受“密级文件策略”限制。

在安全管理中心，单击“密级文件策略”→“密级文件访问控制”策略，进入密级文件访问控制设置页面，如图 5-201 所示。

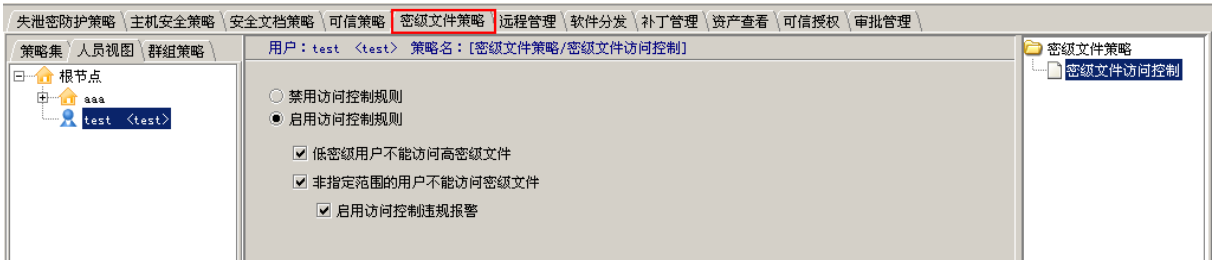


图 5-201　密级文件访问控制策略

当选择“禁用访问控制规则”时，策略应用成功后，客户端用户可以访问任意密级的文件。

当选择“启用访问控制规则”时，必须勾选“低密级用户不能访问高密级文件”和“非指定范

围的用户不能访问密级文件”两项其中的一项或全部，并可同时勾选“启用访问控制违规报警”。如果勾选全部并启用报警，只对“非指定范围的用户不能访问密级文件”违规时，产生报警。

提示：

（1）审批员打开下载的待审批文件时，不受“密级文件策略”限制，可打开任意密级的待审批文件。如果将待审批文件直接拷贝给审批员，就要接受“密级文件策略”的限制，低密级审批员可能打不开高密级的待审批文件。

（2）密级文件创建、修改、销毁等参见客户端操作部分。

5.16 审批管理

启用加密进程加密的普通加密文件，如果客户端没有自解密功能，带出时需要经过审批（在线审批或离线审批），才能变成解密只读文件；客户端用户申请将普通加密文件转化成密级文件，或者修改、销毁密级文件时，也要经过审批；客户端制作可信磁盘，也要审批。审批过程需要有一定的审批规则，我们在审批管理中设置规则，指定待审批的组织、审批员、审批内容和优先顺序。

在安全管理中心中，用鼠标单击“审批管理”，进入审批管理界面，如图 5-202 所示。

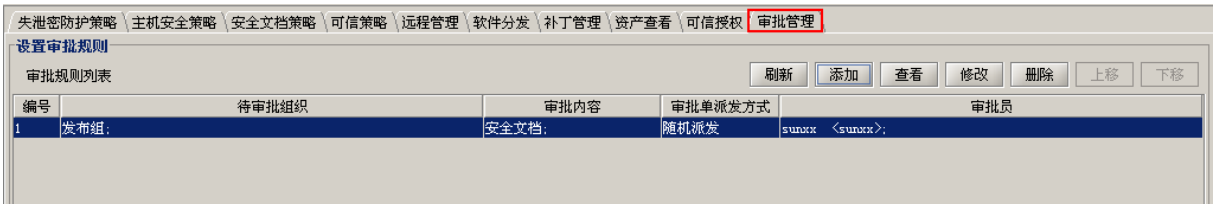


图 5-202　审批管理界面

5.16.1　添加审批规则

1. 在审批管理页面，单击“添加”按钮，弹出选择待审批的组织界面，如图 5-203 所示。勾选待审批的组织后，单击“下一步”。

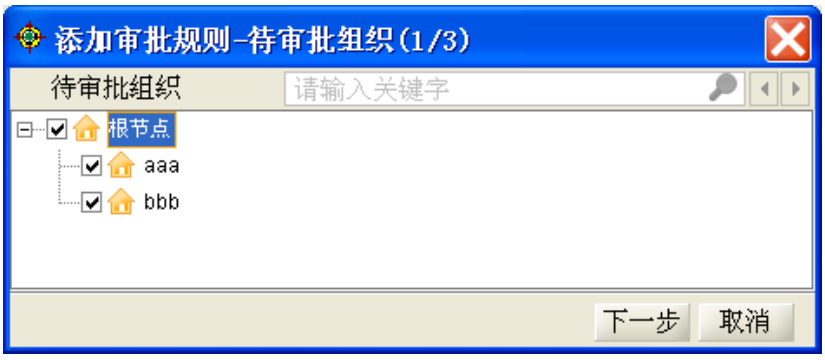


图 5-203　选择待审批的组织

2. 在设置审批内容界面中，勾选要审批的内容，单击“下一步”继续，如图 5-204 所示。审批内容受 License 控制，当某项功能未授权时，其对应的被审批对象不能出现在审批内容的可选项中。

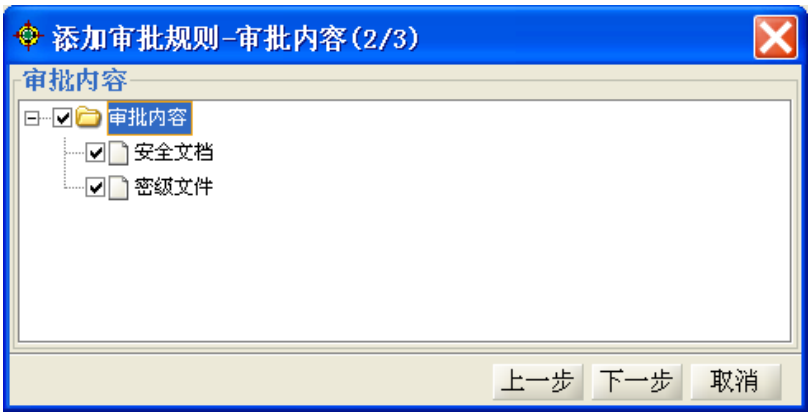


图 5-204　选择审批内容

3. 在设置审批员界面中，选择某组织下的某些人员做为审批员，如图 5-205 所示。最后，单击“确定”按钮，完成退出。

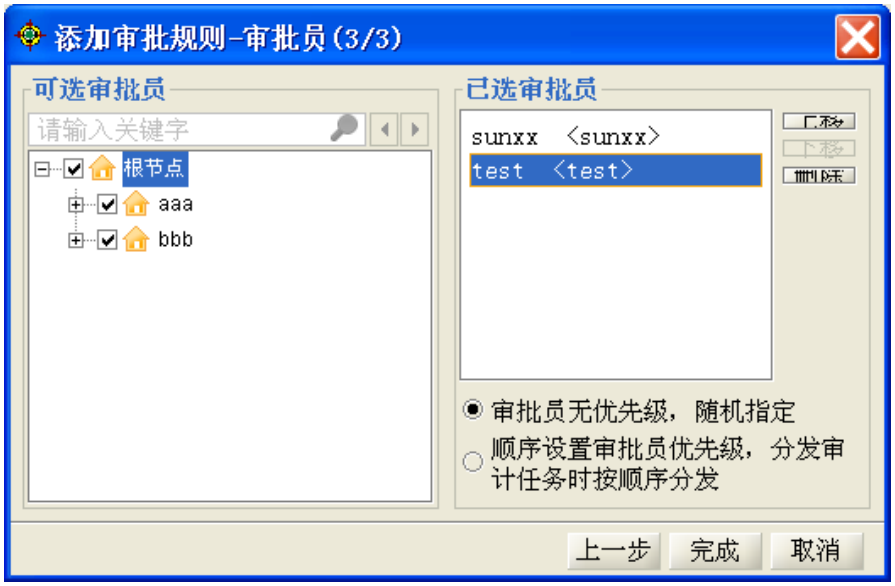


图 5-205　选择审批员

提示：

（1）设置审批员时，可以自己审批自己，控制台不做判断。但服务器派发审批单时，会自动被过滤掉的。

（2）设置审批员可以无优先级，随机指定。也可以按顺序设置优先级，按“上移”或“下移”按钮，改变审批员优先级顺序，分发审计任务时按列表顺序分发。

（3）审批员最多允许 50 个。当勾选的用户超过 50 个时，点击“确定”按钮，将给出提示，不允许添加该规则。

4. 回到审批管理界面，可以看到刚建立的审批规则，如图 5-206 所示。请用户参照上面方法，建立自己需要的审批规则。

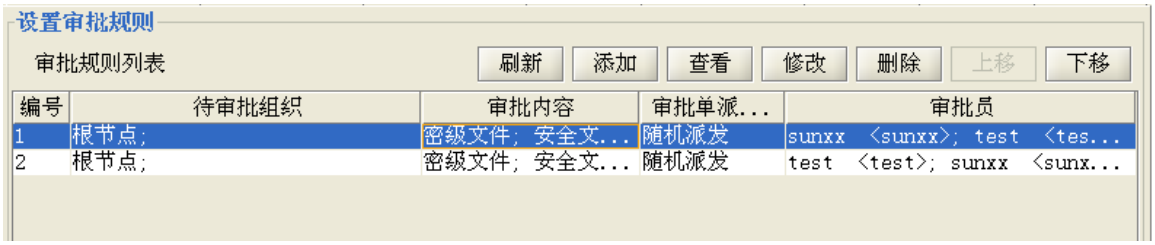


图 5-206　新建审批规则列表

5.16.2　修改审批规则

在审批规则列表中，选择某一规则，单击“修改”按钮，进入修改审批规则界面，如图 5-207 所示。打开标签页“待审批组织”、“审批内容”、“审批员”，修改具体内容项，最后单击“确定”按钮退出。

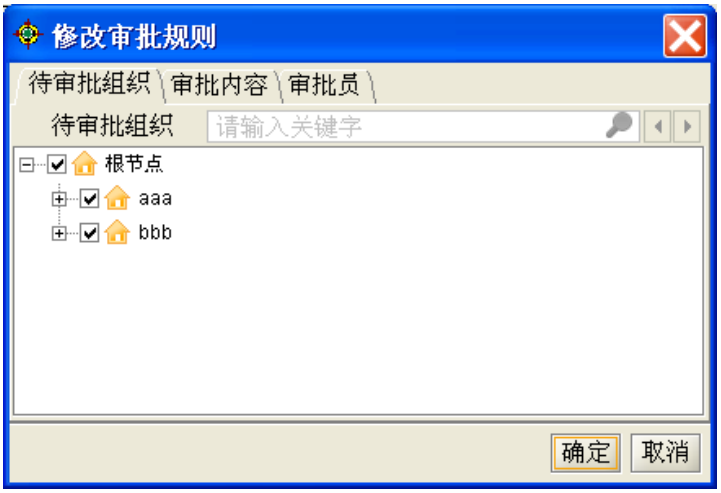


图 5-207　修改审批规则

5.16.3　删除审批规则

在审批规则列表中，选择某一规则，单击“删除”按钮，弹出确认框，如图 5-208 所示。确定后，即可将本规则删除。

图 5-208　删除审批规则

5.16.4　查看审批规则

在审批规则列表中，选择某一规则，单击“查看”按钮，即可查看本规则的详细信息，如图 5-209 所示。

图 5-209　查看审批规则

5.16.5　多个审批规则之间的关系

在审批管理中，用户可以根据自己的需要建立多个审批规则，如图 5-210 所示。

图 5-210　审批规则列表

1．在审批规则列表中，各个规则之间可以重叠和冲突，控制台不做判断。

2．各规则之间以编号设置优先级。编号小的规则优先于编号大的规则，出现冲突时，以编号小的规则为准。用户新添加的规则始终放在最前面（编号小），优先于原来添加的规则。

3．通过“上移”、“下移”按钮，可以改变规则的排列位置，也就是编号，这样就改变了审批规则的优先级。

5.17 可信授权

移动存储介质由于具有灵活性、方便性的特点，在企业信息化过程中迅速得到普及应用。但越来越多的敏感信息、秘密数据和档案资料存贮在移动存储介质里，给企业信息资源带来了相当大的安全隐患。该系统借助于注册授权、身份验证、密级识别、锁定自毁、驱动级加解密、日志审计等技术手段，对移动存储介质从购买、使用到销毁整个过程的管理和控制，使“未授权的移动存储器拿进来使不了”、“授权的移动存储器拿出去不能用”，真正做到了对移动存储介质的有效防护。

可信授权模块用于对移动存储介质进行入库管理、注册授权、激活、解锁、回收、可信磁盘的信息查看等操作，包括磁盘库存管理、磁盘授权管理和授权信息管理。UEM8.0 支持可信磁盘跨服务器访问，也就是在 A 服务器授权的可信磁盘,在 B 服务器管理的主机上也能使用。

5.17.1 磁盘库存管理

在安全管理中心中，用鼠标单击“可信授权”标签项，进入“磁盘库存管理”界面，如图 5-211。

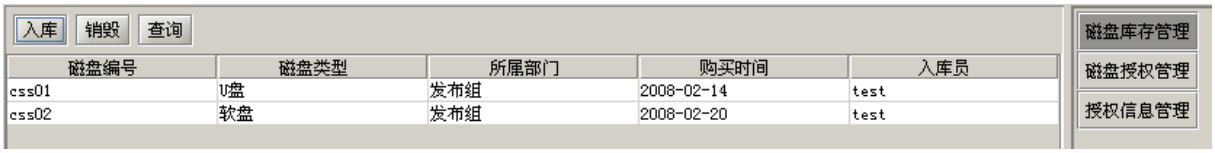


图 5-211　磁盘库存管理

5.17.1.1　入库

对于一个新的移动存储介质，在进行授权之前，首先需要将其登记入库。

点击菜单“磁盘库存管理”→“入库”，将弹出“磁盘入库”对话框，如图 5-212 所示。

图 5-212　磁盘入库

输入磁盘的编号，从下拉框中选择磁盘的类型、购置日期和所属部门，最后点击“确定”按钮，即可将磁盘登记到磁盘库中。新添的磁盘记录将会自动显示在上面的磁盘列表中，如图 5-213 示。

图 5-213　磁盘库列表

5.17.1.2　销毁

对于已被损坏的或者不再使用的磁盘，从磁盘库列表中选择被物理销毁的磁盘，点击“销毁”按钮，将清除磁盘库中该磁盘的记录。在销毁前，请确认授权记录中是否还存在针对该磁盘的授权，如果有，系统将禁止销毁操作，如图 5-214 所示。否则，系统将提醒您确认是否真要销毁该磁盘，如图 5-215 所示。选择“确定”，磁盘记录将被从数据库中清除；选择“撤消”，将取消销毁操作。

图 5-214　销毁提示框

图 5-215　销毁确认框

5.17.1.3 查询

点击“查询”按钮，进行已入库的磁盘查询，如图 5-216 所示。设置检索条件，单击“确定”按钮，系统自动将符合条件的记录列表显示出来，如图 5-217 所示。

图 5-216　设置检索条件

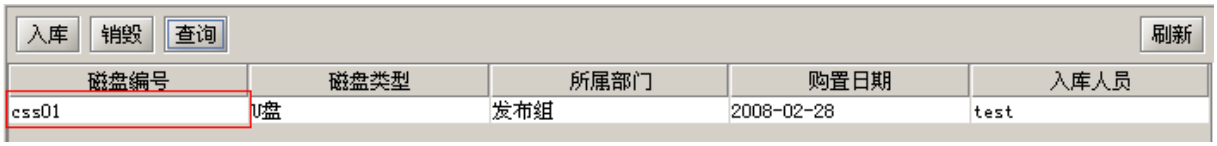


图 5-217　查询结果

5.17.2　磁盘授权管理

将磁盘登记入库以后，即可对其进行授权了。可信磁盘是经过 UEM 授权中心授权过的移动存储介质，只能在可信环境下使用，也就是只能在安装 UEM 系统客户端的主机上使用。可信磁盘有不同的工作模式，如下所述：

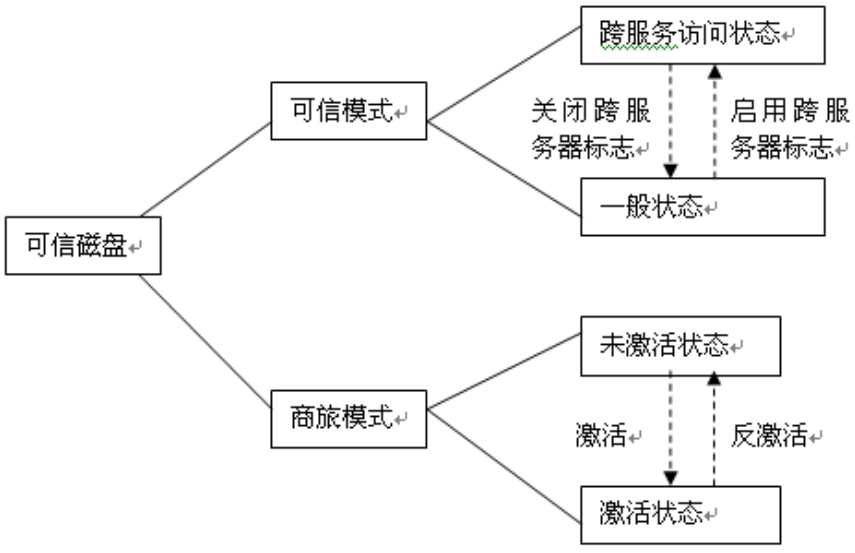
（1）可信模式：可信磁盘的一种工作模式，只能在可信环境中使用，在普通环境中无法使用。

- 可信模式一般状态：可信模式的缺省状态，不能跨服务器使用，只能在授权服务器所管理的主机上使用。访问范围受授权范围、主机密级的限制。可以在控制台通过启用跨服务器标志转换为跨服务器访问状态。（注：*在磁盘授权时被设定为无口令的可信磁盘不能转换为跨服务器访问状态*）。
- 可信磁盘跨服务访问状态：允许跨服务器访问，访问范围受服务器授权时用户编号、主机密级的限制。可以在控制台通过关闭跨服务器标志转换为一般状态。

（2）商旅模式：可信磁盘的一种工作模式，用于和外界进行数据交互。

- 商旅未激活状态：在可信环境下能读也能写，在普通环境下不能访问。可以在控制台通过激活操作转换为激活状态。
- 商旅激活状态：在可信环境下只读不能写，在普通环境下能读也能写。可以在控制台通过反激活操作转换为未激活状态。

下面为可信磁盘的工作状态示意图。



点击“可信授权”→“磁盘授权管理”，下面进行磁盘的授权、激活、回收、解锁、启用跨服务器等具体操作。

5.17.2.1　制作可信盘

制作可信盘就是对普通移动存储介质进行授权，使之变成可信移动存储介质。如果对客户端下发“禁止使用移动存储设备”策略后，普通的移动存储介质将不能使用，只能可信移动存储介质通过客户端正常加载后，才能够使用。

点击“制作”功能项，进入可信磁盘授权页面，如图 5-218 所示。客户端也可通过在线审批方式制作可信磁盘。参见客户端可信介质的管理部分。

1. 在常规选项卡中选择要制作的磁盘设备、磁盘类型、使用范围、磁盘编号和责任人。

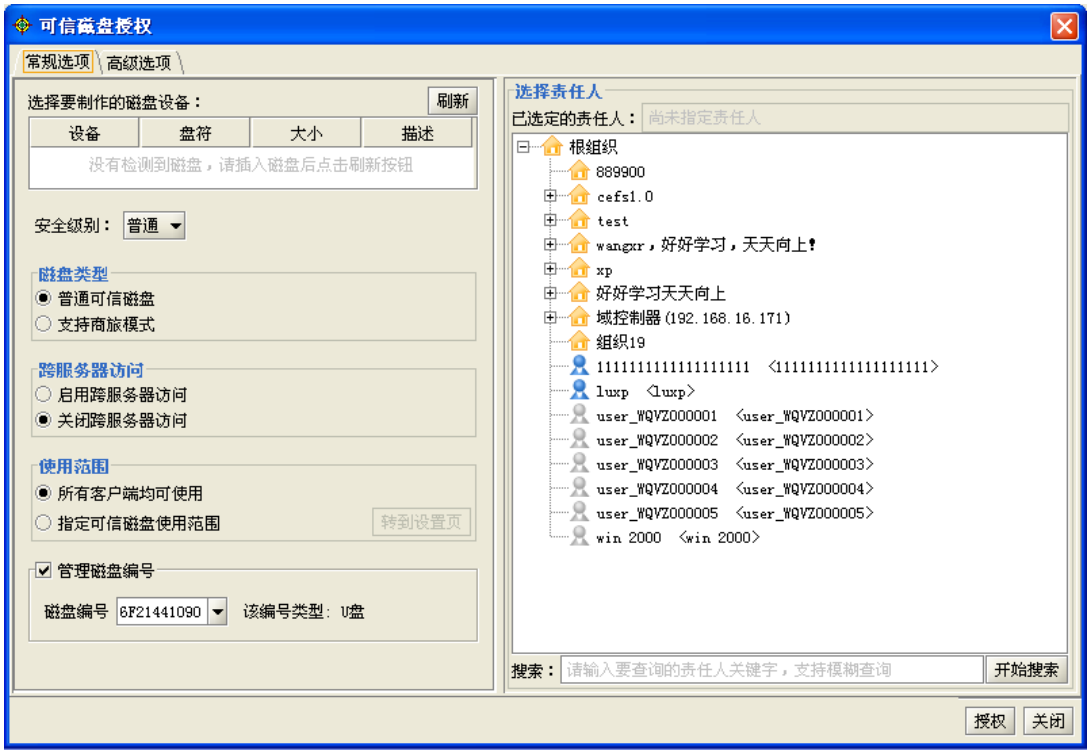


图 5-218　可信磁盘授权—常规选项

■　**选择要制作的磁盘设备**

将移动盘插入到控制台主机，点击“刷新”按钮，在磁盘设备列表中显示了所有接入当前主机的移动盘的相关信息，包括设备名称、对应的磁盘盘符、磁盘的大小以及磁盘的类型描述。其中“描述”一列可以有三种值：可移动磁盘名称、磁盘分区和软盘。如果选择某个磁盘，则对该磁盘的所有分区进行授权；如果选择的是某分区，则仅对选中的分区进行授权。系统默认选择的是列表中位于第一行的磁盘。

■　**安全级别**

安全密级提供了四个安全级别，按级别由低到高依次为普通、秘密、机密和绝密。用户可以根

据自己需要选择，系统默认为普通级别。

- **磁盘类型**

可信磁盘分为普通模式和商旅模式。

普通模式的可信磁盘只能在可信环境中使用，在普通环境中无法使用。也就是只能在授权服务器所管理的主机上使用，启用跨服务器后才可以跨服务器访问。

商旅模式可信磁盘用于和外界进行数据交互。未激活时，在可信环境下能读也能写，在普通环境下不能访问，启用跨服务器后才可以跨服务器访问；激活后，在可信环境下只读不能写，在普通环境下能读也能写，启用跨服务器后可以在跨服务器可信环境下只读。

- **跨服务器访问**

启用跨服务器访问：一般情况下，可信磁盘只能在授权服务器管理的客户端上使用，拿到别的服务器管理的客户端上，就不能使用。如果启用跨服务器访问后，只要授权服务器的用户编号一样，那么在 A 服务器上授权的可信盘，就可以在 B 服务器管理的客户端上使用。这里说的用户编号是指授权服务器的用户编号，同一单位的服务器用户编号一样，可以在控制台授权信息中查看。另外，可信磁盘在客户端使用时，也受密级的限制。

关闭跨服务器访问：可信磁盘的跨服务器状态变为原来的一般状态，只能在授权服务器管理的客户端上使用。

- **使用范围**

系统默认可信磁盘的使用范围是所有客户端均可使用。如果用户需要指定使用范围，那么就要转到设置页，在高级选项的使用范围中分别设置人员范围、组织范围和计算机范围。

- **管理磁盘编号**

不选择管理磁盘编号时，系统在授权时会给磁盘加默认编号。

选择管理磁盘编号，该盘已进行了入库登记，请在下拉框中选择编号。如果手动输入新的磁盘编号，会弹出提示框“您输入的磁盘编号还没有加到磁盘管理库中，是否添加到时磁盘管理库中”，单击“确定”后，进行入库操作。

- **选择责任人**

每个移动盘都需要选择一个用户，将其设置为责任人。在组织结构列表中选择某用户，该用户就成为该盘选定的责任人。如果记不清用户名称和所在的位置，也可以在搜索框输入相似的用户名，系统会自动搜索出类似的用户，显示在上面组织结构列表中。该搜索功能支持模糊查询，如果输入“123”，系统会自动搜索出“123”、“12345”、“1237A”、“1234567”等相关的用户。

提示：

（1）常规选项除磁盘设备外，都具有记忆功能，能记录上次用户选择项，做为用户下次使用时的默认值。（2）如果用户只选择常规选项，不选择高级选项，系统会以高级选项中的默认值对磁盘进行授权。

2. 在高级选项卡中选择使用范围、基本信息、口令设置、加密算法、使用限制条件。

■ **使用范围**

该页面用于设置磁盘的使用范围，用户可以设置人员范围、计算机范围和组织范围，如图 5-219 所示。

对于每一个节点，其名称前面的☐显示了该节点的选中状态：完全选中（☑）、部分选中（☑）和未选中（☐）。如果节点为完全选中，表示允许该节点下的所有用户或主机使用该磁盘；如果为部分选中，表示仅信任该节点下的部分用户或主机；如果未选中，表示不信任该节点及其下所有子用户或主机。

提示：建议使用组织范围页面来指定磁盘的使用范围，若需要指定到特定的人员或计算机，请选择人员或计算机范围页面。

图 5-219 可信磁盘高级选项—使用范围

■ **基本信息**

基本信息设置界面，如图 5-220 所示。

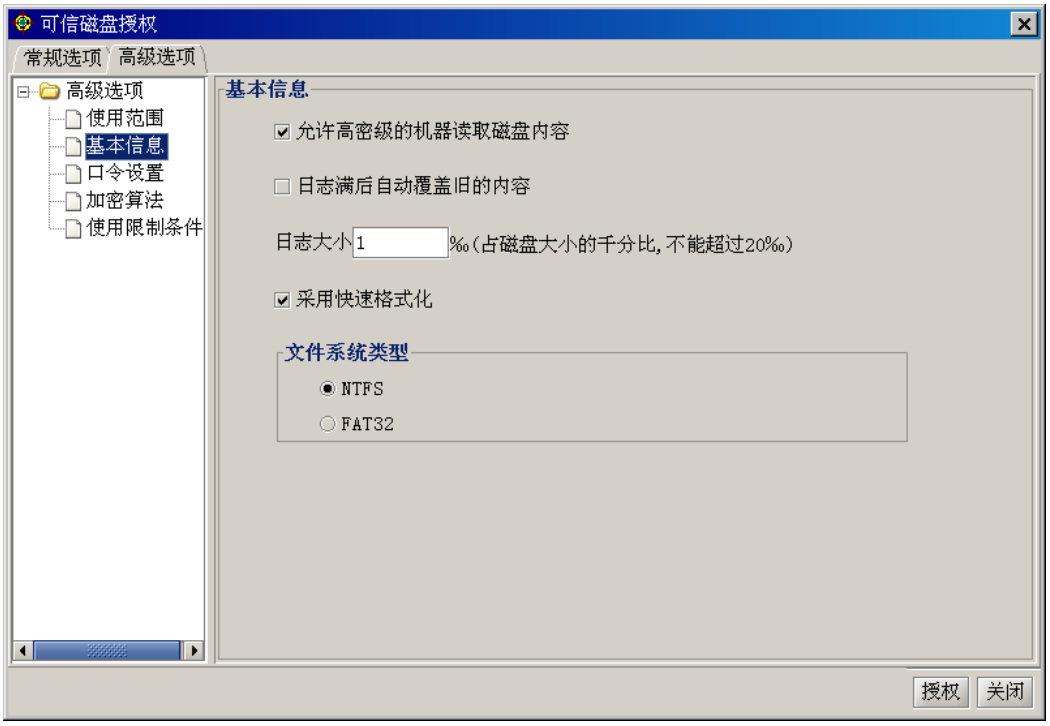


图 5-220　可信磁盘高级选项——基本信息

如果想在高密级的主机上也能查看低密级磁盘上的数据，请选中“允许高密级的机器读取磁盘内容”；否则将禁止使用。在低密级的主机上，高密级磁盘会自动被禁止使用。同密级的主机和磁盘可以读写，不同密级有限制。

选项“日志满后自动覆盖旧的内容”，用于设置磁盘上的日志数据区被写满后的处理方式。可信盘离开授权服务器在外使用时，其使用日志将被记录在可信磁盘的日志数据区。如果选择自动覆盖，则在日志区被写满后，新的日志将冲掉旧的日志；否则，放弃新的日志。

选项“日志大小”用于设定日志数据区的大小，此处填入的数字表示日志区占用整个磁盘大小的千分比。

“采用快速格式化”项用于决定在制作磁盘的文件系统格式过程中，是否采用随机数填充空白区域。经随机数填充后的磁盘，能有效地抵制恶意地对磁盘数据格式的解析，因此，如果磁盘的安全密级比较高，建议不采用快速格式化。

选项“文件系统类型”是指将可信盘格式化为 NTFS 文件系统格式，还是 FAT32 文件系统格式，系统默认是 NTFS 文件系统格式。

■ **口令设置**

口令设置界面，如图 5-221 所示。

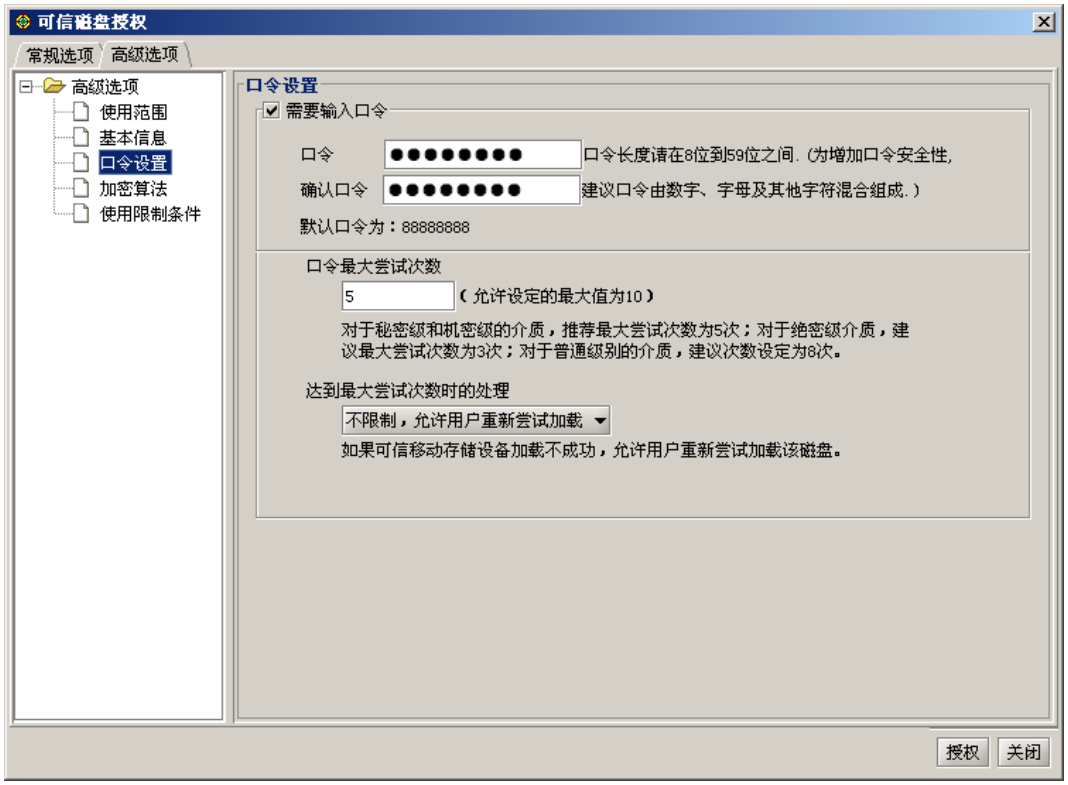


图 5-221　可信磁盘高级选项—口令设置

选中“需要输入口令”，则该磁盘在接入终端使用时，用户必须输入认证口令才可使用该磁盘，系统默认口令为 88888888，用户可以任意更改。如果不选择口令，系统将采用一随机数作为口令，进行数据加密，当磁盘接入可信终端上时，系统会自动加载，方便用户使用。但是，对于支持商旅模式的可信磁盘，必须设定认证口令。没有口令，也不支持跨服务器操作。

选项“口令最大尝试次数”用于限定用户所能连续尝试使用口令的次数。依据保密规定，对于秘密级和机密级的介质，推荐的最大尝试次数为 5 次；对于绝密级介质，推荐的最大尝试次数为 3 次；对于普通密级的介质，推荐的最大尝试次数为 8 次。

如果用户超过了限定的口令尝试次数，系统提供了三种自我保护方式：

不限制，允许用户重新尝试加载：如果可信移动存储设备加载不成功，允许用户重新尝试加载该磁盘，不需要拔除设备。

锁定，禁止使用：锁定可信移动存储设备，该设备必须到授权中心解锁后方可再使用。

自动破坏数据，不可恢复：销毁该可信移动存储设备中的数据，用户将无法恢复存储在其中的数据。为安全起见，建议在高密级的设备中使用。

注意：自毁后的磁盘数据将不可恢复，在保密要求不是很高的情况下，请慎重选择使用自毁的自我保护方式。

■ **加密算法**

加密算法设置界面，如图 5-222 所示。

此处用于设置磁盘中的数据加密方式，其中可以选择的加密算法有：AES、BLOWFISH、CAST5、SERPENT、TRIPLE DES 和 TWO FISH；可以选择的散列算法有：SHA1 和 RIPEMD-160。

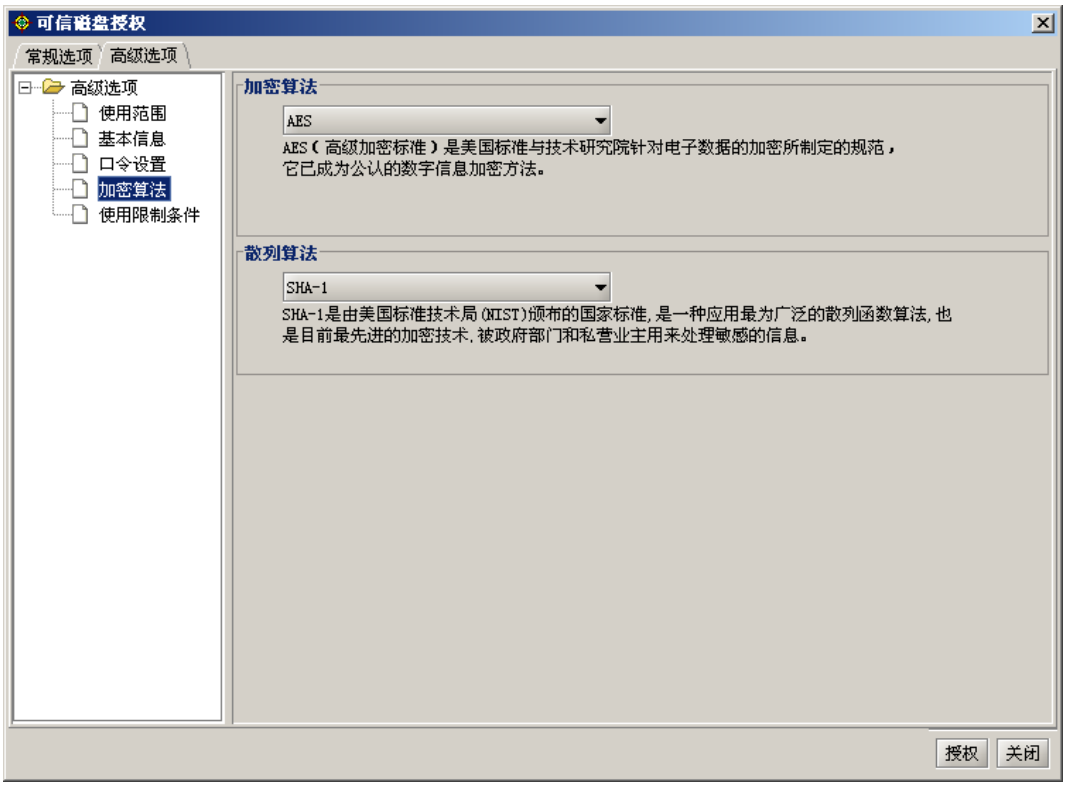


图 5-222　可信磁盘高级选项—加密算法

■　使用限制条件

使用限制条件设置界面，如图 5-223 所示。

可信移动存储管理系统提供了两种磁盘使用限制条件：使用次数和使用日期。授权后的可信磁盘每正常加载一次，使用次数将自动减 1。当其变为 0 次后，磁盘的使用将会被控制。

如果系统没有设定时间同步的话，因用户可以自行更改系统的日期，在一定程度上可以绕开使用日期的限制，所以，推荐采用使用次数作为限制条件。

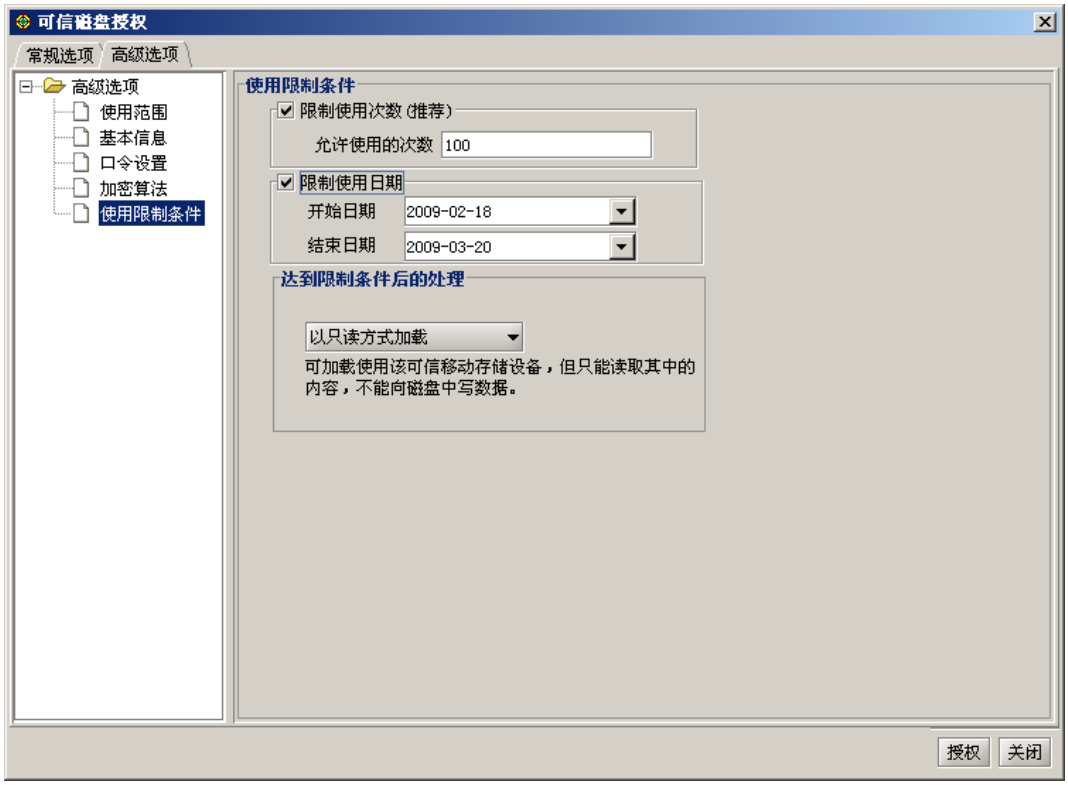


图 5-223　可信磁盘高级选项——使用限制条件

当磁盘达到使用限制条件后，系统提供了三种自我保护方式：以只读方式加载、锁定和自动破坏数据。当以只读方式加载时，用户可以查看磁盘中的内容，但不能再往磁盘中写入任何数据；选择“锁定”，则该磁盘将被禁止使用，必须到授权中心解锁后才能再使用；选择“自动破坏数据”，存储在磁盘中的数据将被破坏，不可恢复。

提示：高级选项中除磁盘口令外，都具有记忆功能，能记录上次用户选择项，作为用户下次使用时的默认值。如果不退出可信授权界面继续授权的话，磁盘口令默认为上次授权口令，不再是 88888888。

3. 当所有选项都选择完成后，单击“授权”按钮进行授权。授权成功后，系统会有提示，如图 5-224 所示。

图 5-224　可信磁盘授权成功

5.17.2.2　激活

如果用户想通过可信磁盘带出数据，请先到授权中心申请制作支持商旅模式的可信磁盘。

用户将支持商旅模式的可信磁盘接入客户端，完成数据的拷贝后，如准备带出使用，需要在控制台对其进行激活。若经控制台允许，也可在客户端本地进行激活和反激活操作。

（1）单击“磁盘授权管理”→“激活”，系统将弹出磁盘激活确认对话框，如图 5-225 所示。

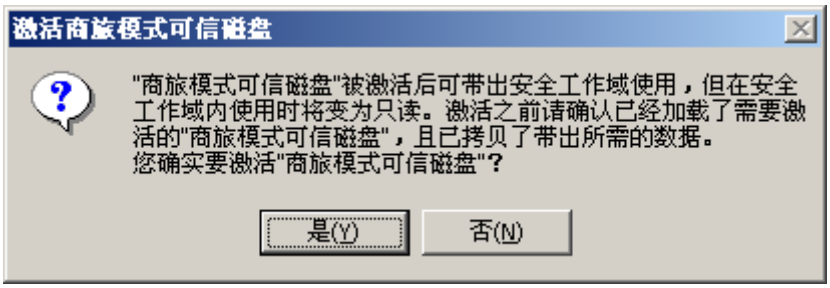


图 5-225　商旅模式可信磁盘激活确认对话框

（2）选择“是”完成激活操作；选择“否”，将放弃激活操作。激活成功后出现提示框，如图 5-226 所示。

图 5-226　磁盘激活成功

注意：

- 激活后的商旅磁盘在安全工作域内将变成只读模式，请确定所需数据已拷贝完全后再执行激活操作。
- 激活后的商旅磁盘在普通终端上加载成功后，可以进行正常的读、写操作。

5.17.2.3　商旅磁盘的使用

商旅磁盘上有一个可信磁盘管理程序 WBTSTravel.exe，将商旅磁盘接入普通终端时，如果普通终端允许自动播放功能，操作系统将自动执行文件 WBTSTravel.exe，否则，需用户手动运行该文件。该程序启动后，在操作系统的托盘区新添一图标。

在图标上点击鼠标右键，选择“加载可信磁盘”，如果事先没在控制台进行激活，会自动启用激活向导，如图 5-227 所示。用户将生成的随机码发送给控制台管理人员，管理人员利用可信授权管理中的“验证码生成管理器”生成验证码，发送给商旅磁盘使用者。然后，用户输入验证码和磁盘密码后，单击“确定”按钮，完成可信磁盘的加载。验证码的生成参见激活验证码章节。

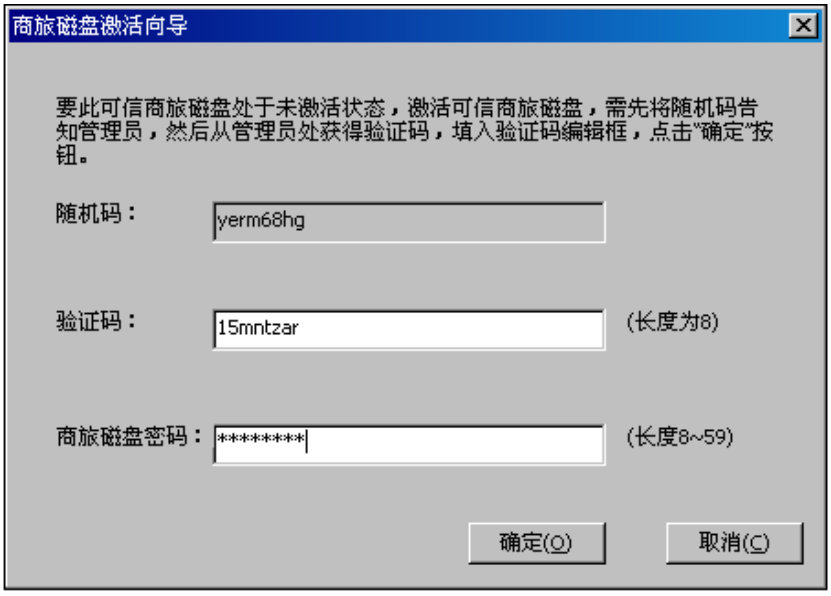


图 5-227　商旅磁盘激活向导

如果商旅磁盘事先在控制台进行了激活，加载时将弹出口令输入对话框，如图 5-228 所示。输入设定口令，点击“确定”按钮即可完成商旅磁盘的加载；点击“取消”，放弃加载操作。加载完成后，可以在“我的电脑”中看到新添了一个盘符，对此我们可以进行读写操作。

加载成功后，系统将日志记录到商旅磁盘日志区，日志格式同加载日志格式，当商旅磁盘连接控制台后，现有的日志导入程序会将日志自动上传到服务器。

图 5-228　输入口令对话框

5.17.2.4　反激活

反激活就是将已激活的商旅磁盘恢复到未激活状态，如图 5-229 所示。反激活成功后，只能在可信终端上使用，在普通终端上不能使用。

图 5-229　磁盘反激活成功

5.17.2.5　回收

对于已带出使用过的可信磁盘或者不需再使用的可信磁盘，需要收回其授权。在磁盘授权管理中，选择接入系统的可信磁盘，单击“回收”，即完成对磁盘授权的回收，如图 5-230 所示。

图 5-230　磁盘授权回收

对于非商旅模式可信磁盘，此操作将清除磁盘上的所有数据，将磁盘格式化为普通磁盘，同时清除授权记录；对于商旅模式的可信磁盘，该操作会提取存储于该磁盘中的日志信息，清除授权记录，同时将磁盘制作成普通格式磁盘。

5.17.2.6　解锁

可信磁盘可能会因为各种违规操作：如口令尝试过多、超过了使用次数、超过了使用期限等，导致可信磁盘被锁定。在这种情况下，我们需要解除其锁定。选择被锁定的可信磁盘，点击“解锁”，将解除对磁盘的锁定状态。

如果因为达到了限制使用次数而锁定，则在解锁时将允许管理员增加磁盘的使用次数，以保证用户能继续使用磁盘，如图 5-231 所示：

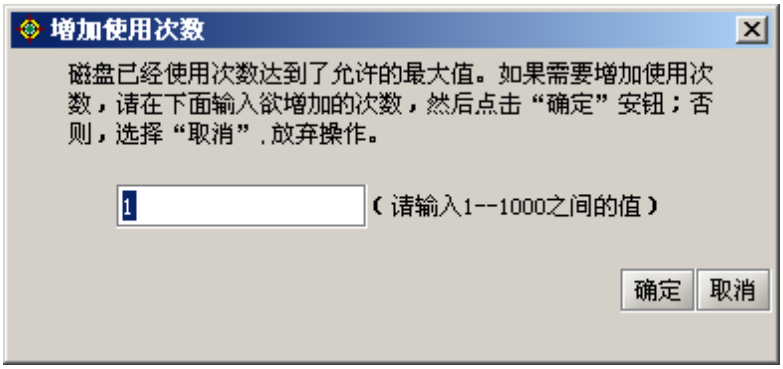


图 5-231　增加使用次数

如果因为超过了使用截止日期而导致磁盘锁定，则在解锁时将允许管理员设置新的截止日期，以保证用户能继续使用磁盘，新的截止日期不能早于当天，如图 5-232 所示：

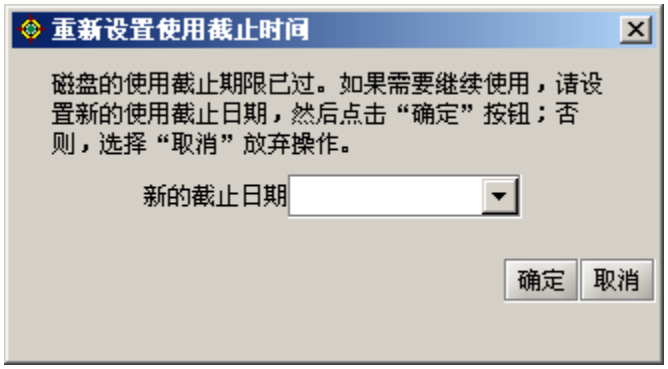


图 5-232　延长使用日期

5.17.2.7　启用跨服务器

在磁盘列表中选定某可信盘，单击“启用跨服务器”操作，弹出提示框，如图 5-233 所示。确定后，该可信盘就可实现跨服务器访问。

一般情况下，可信磁盘只能在授权服务器管理的客户端上使用，拿到别的服务器管理的客户端上，就不能使用。如果启用跨服务器访问后，只要授权服务器的用户编号一样，那么在 A 服务器上授权的可信盘，就可以在 B 服务器管理的客户端上使用。这里说的用户编号是指授权服务器的用户编号，同一单位的服务器用户编号一样，可以在控制台授权信息中查看。另外，可信磁盘在客户端使用时，也受密级的限制。

图 5-233　启用跨服务器操作提示框

5.17.2.8　关闭跨服务器

单击“关闭跨服务器”操作，出现提示框，如图 5-234 所示。确定后，该可信磁盘的跨服务器状态变为原来的一般状态，只能在授权服务器管理的主机上使用。

图 5-234　关闭跨服务器操作

5.17.2.9　重置口令

如果在创建可信盘时设置了口令，那么在授权服务器连接的控制台上，可以进行重置口令操作，如图 5-235 所示。

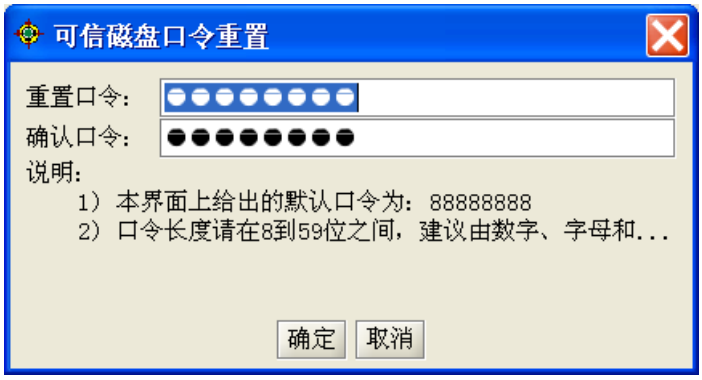


图 5-235　重置口令

5.17.2.10　激活验证码

如果商旅盘在普通终端上使用时，没有事先在控制台激活，可将商旅盘加载激活时生成的随机码，发送给控制台管理人员，管理人员利用验证码生成管理器生成验证码，方便商旅盘激活使用，如图 5-236 所示。

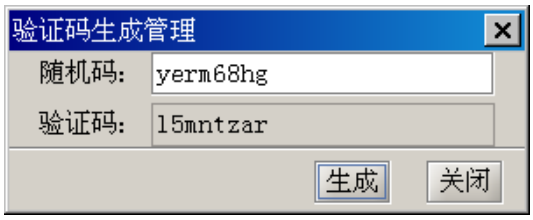


图 5-236　验证码生成管理器

5.17.3 授权信息管理

在“授权信息管理”中，可以看到所有有效的授权记录列表。

5.17.3.1 查看

选定其中的一项，双击或者单击“查看”，可以浏览授权记录的详细信息。

详细信息分四个页面显示：基本信息页显示了除授权范围外的所有信息；授权用户页显示了磁盘被授予给哪些用户使用；授权主机页显示了该磁盘可以在哪些主机上使用；授权组织页显示了该磁盘授予给哪些部门使用。基本信息页面示例如图 5-237 所示：

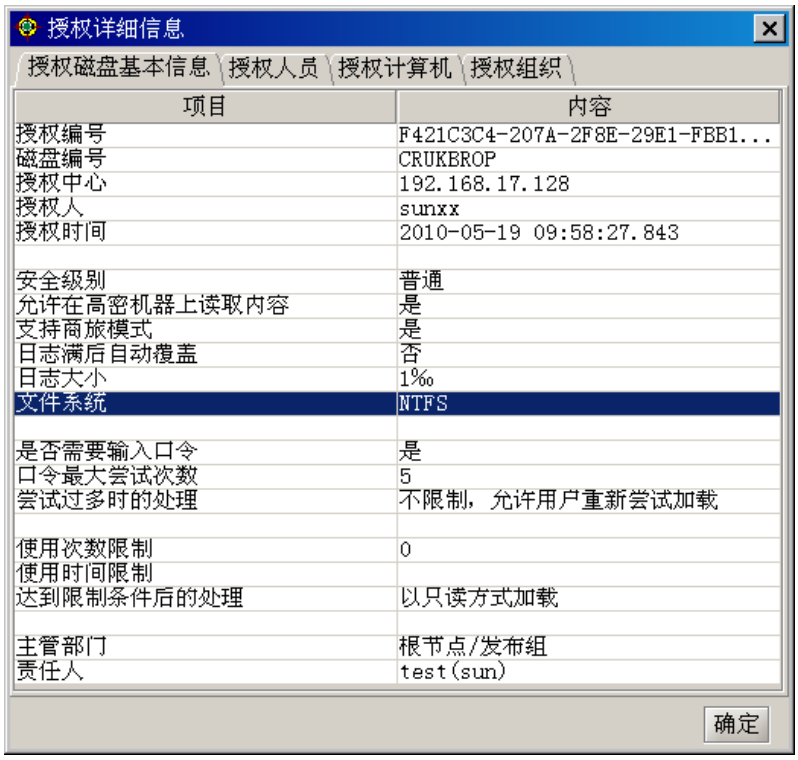


图 5-237　授权磁盘基本信息

5.17.3.2 撤销

在某些情况下，比如物理磁盘丢失了、被损坏了或者因为误操作导致磁盘上的授权信息被破坏了，这时，该磁盘的授权记录将无法被回收。为了清除这类信息，可以选择撤销授权操作。选择准备撤销授权的记录项，然后点击“撤销”，系统将弹出一个确认对话框，如图 5-238 所示。

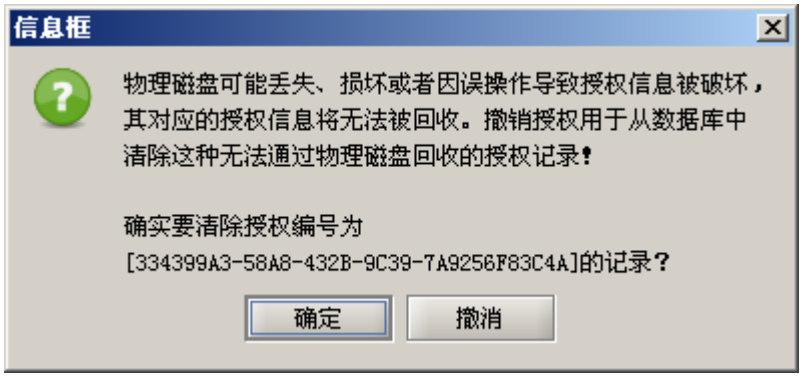


图 5-238　撤销授权确认框

单击“是”，则从数据库中清除该条授权记录；点击“否”，取消操作。

5.17.3.3 查询

单击“授权信息管理”→“查询”，设置检索条件，可以列出符合条件的授权记录信息，如图5-239、5-240所示。

图5-239　查询磁盘授权记录

图5-240　显示查询结果

5.18 可信移动存储介质策略

可信策略是针对可信移动存储介质制定的策略，它可以监控在可信盘上的文件操作，包括文件拷出、拷入、创建、重命名、删除、读取和写入等操作。

5.18.1　文件操作监控

1. 选择“可信策略”下的“文件操作监控”，进入文件操作监控设置界面。若单击“文件创建操作监控”标签页，选择“监控文件创建操作并记录日志”，然后单击“增加”按钮，对要监控的文件类型进行具体设置，如图5-241所示。

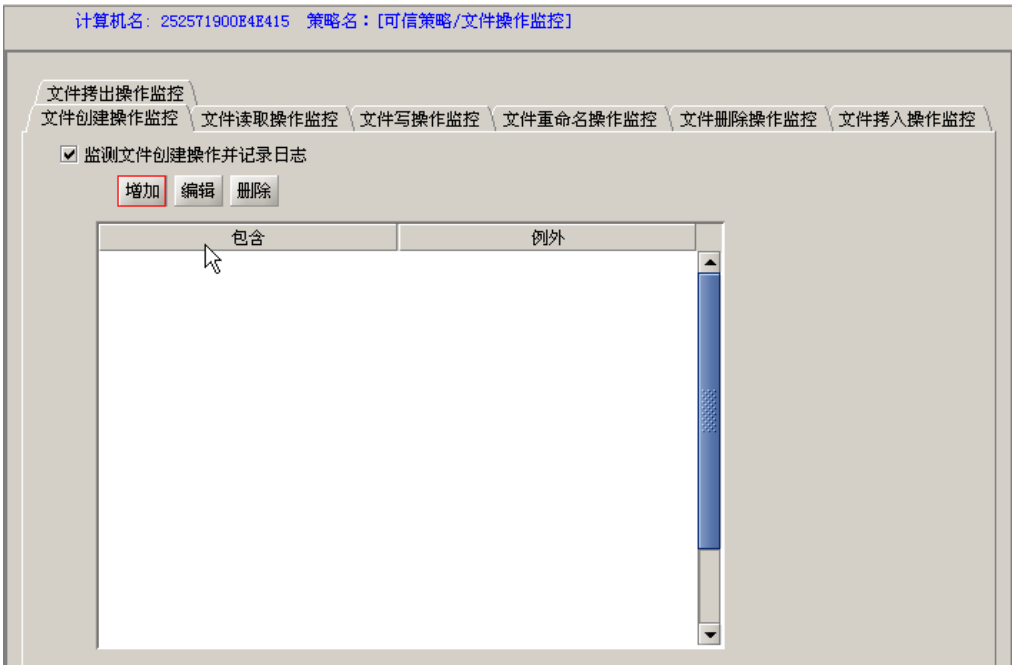


图 5-241　文件操作监控

2. 在“编辑要监测的文件”界面中，选择可信盘类型，输入路径和文件名，单击“确定”即可。如果在设定的路径下，有不需要监控的文件，可以单击“添加”按钮，在例外列表中输入例外文件名，如图 5-242 所示。

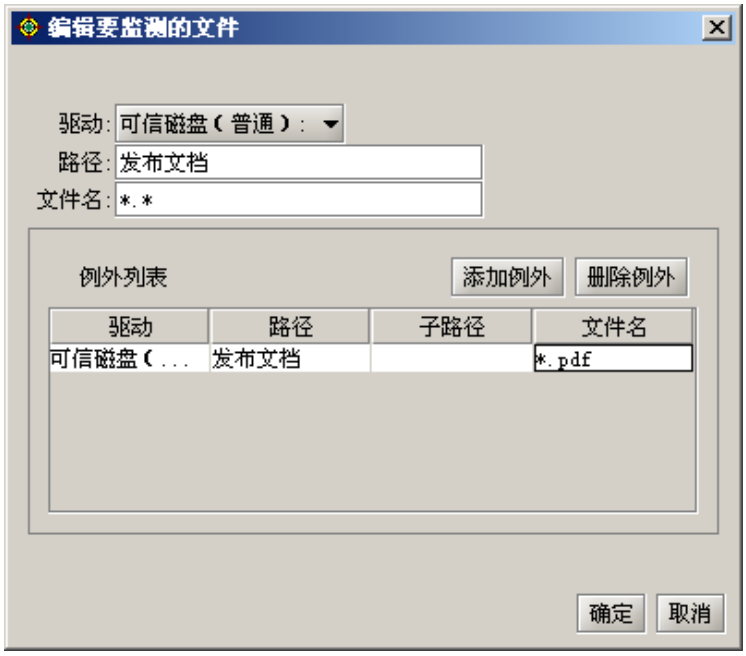


图 5-242　编辑要监测的文件

提示：路径的前面不输入盘符，开始和结束不能为“/”；文件名支持通配符。

3. 编辑好要监测的文件后，单击“确定”按钮，返回上一界面，可以看到刚添加的监控文件，如图 5-243 所示。

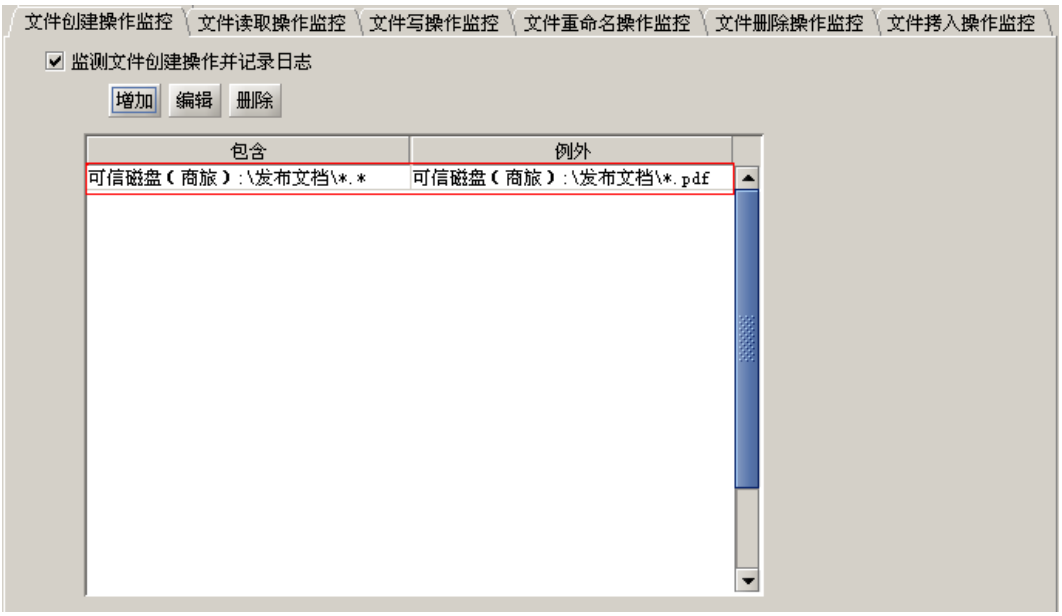


图 5-243　查看添加的监测文件

4. 策略下发成功后，客户端在可信盘上创建文件时，系统将监控设定的文件类型或文件名，并记录日志。

提示：

（1）在可信盘上的文件拷出和拷入操作，不需要设置文件类型，可以监控所有文件拷入、拷出操作，并记录日志。

（2）在可信盘上的文件重命名、删除、读和写操作，和创建文件的操作监控设置类似，这里不再叙述。

5.18.2　可执行文件控制

单击“可信策略”→“可执行文件控制”，进入可信盘可执行文件控制界面，如图 5-244 所示。在这里设置“禁止”或“允许”可信磁盘上的可执行文件，然后将策略应用下发。

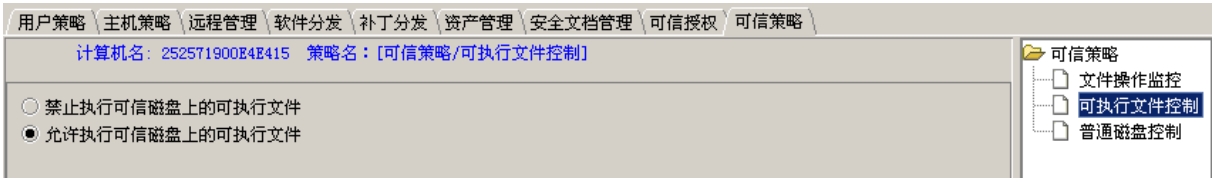


图 5-244　可执行文件控制

提示：此功能针对的是可执行文件，而不是批处理文件。如果是批处理文件，那么批处理文件中包含可执行文件也应在可信磁盘上，这样才能达到预期效果。

5.18.3　普通磁盘控制

单击“可信策略”→“普通磁盘控制”，进入普通磁盘控制界面，如图 5-245 所示。在这里设置普通移动存储设备的使用状态，然后将策略应用下发。

如果选择“禁止使用普通移动存储设备”并勾选“生成日志并产生警报信息”，那么在客户端尝试使用普通移动存储设备，或者尝试加载外单位可信磁盘时，就会生成报警信息和日志记录，可以在控制台的“报警信息”和“统计审计分析”→“可信移动”→“普通移动磁盘接入日志中”查看。

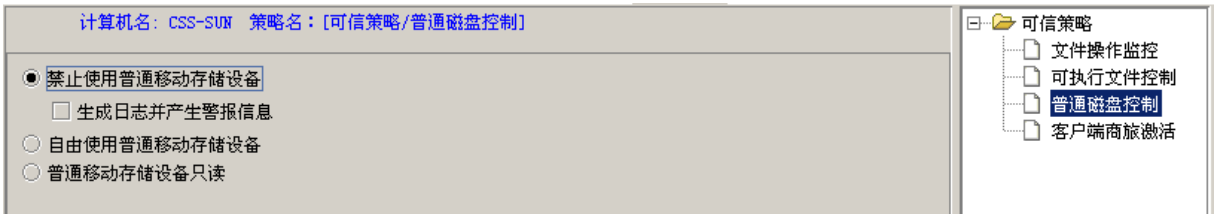


图 5-245　普通磁盘控制

提示：

该策略项是对计算机下发的，而“用户策略”中的“可移动介质控制”策略项是对人员下发的，如果这两个策略项相遇发生冲突时，系统将按照严格策略项执行。也就是说，如果一个策略项设置为“自由使用”，另一个策略项设置为“禁止使用”，那么系统将按照严格策略“禁止使用”执行。

5.18.4　客户端商旅激活

单击“可信策略”→“客户端商旅激活”，进入客户端商旅激活控制界面，在这里设置是否允许在客户端激活商旅磁盘，如图 5-246 所示。

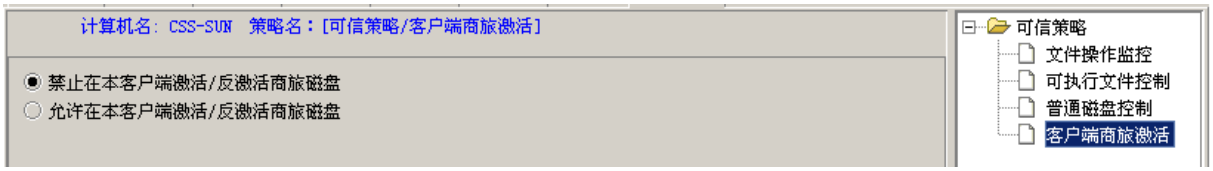


图 5-246　客户端商旅激活设置

默认情况下是不允许在客户端激活商旅磁盘的，如果为了客户端使用方便，将此策略放开的话，那么在客户端加载可信磁盘后，才会出现激活和反激活菜单，如图 5-247 所示。否则，不会出现这两项菜单，只能在控制台进行激活和反激活操作。

图 5-247　客户端商旅盘激活和反激活

5.19 可信计算

UEM 系统能够自动收集受控终端的运行进程信息，并对收集的进程信息实施分类管理。通过可信计算策略控制，防范关键进程的重命名行为；另外，UEM 系统对操作系统文件进行完整性校验，并实现强制访问控制，确保操作系统核心系统文件的安全，保证操作系统免被病毒或木马侵袭，实现操作系统的可信。

5.19.1 可信计算管理

在安全管理中心中，单击“可信计算管理”标签项，进入可信计算管理页面，可以进行“应用程序管理”和“核心文件库”的添加、删除、导入和导出操作，下面具体叙述。

5.19.1.1 应用程序管理

1. 在“可信计算管理”的“应用程序管理”界面，单击“添加”按钮，弹出“添加程序”操作框，如图 5-248 所示。单击“浏览”按钮，选择应用程序名称；单击下面的下拉框，选择程序分类，并添加描述信息（可选）。然后，单击“确定”按钮，将该程序添加到程序库列表中。

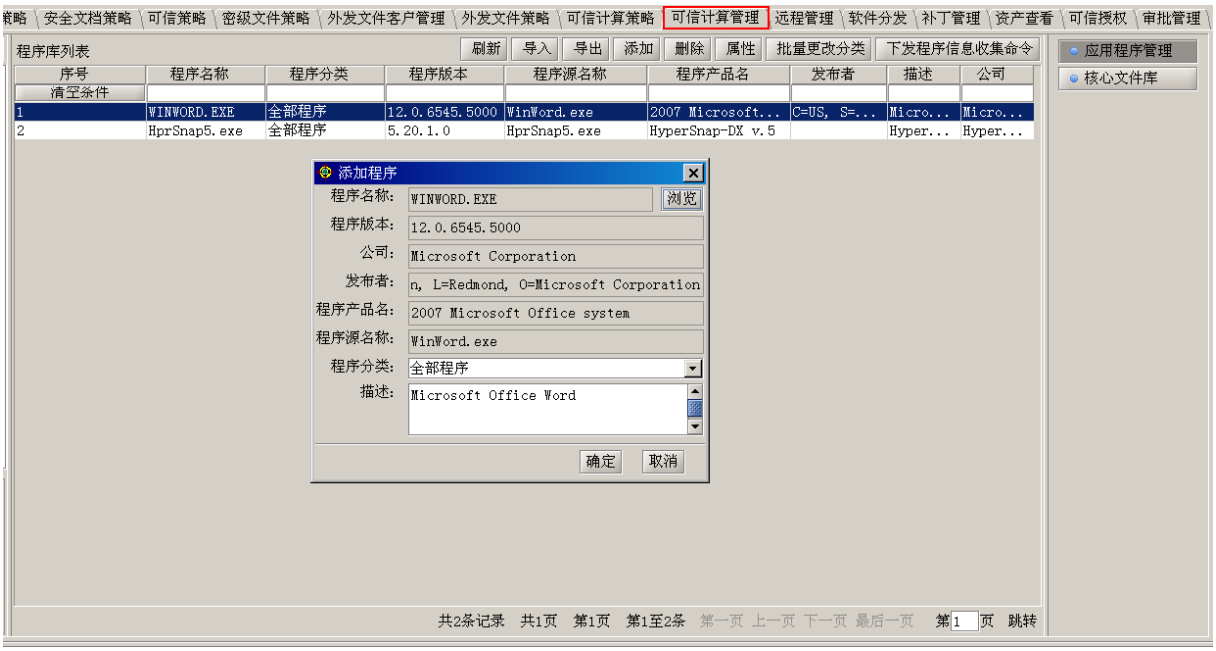


图 5-248　添加应用程序

2. 按此方法，在应用程序库中手动添加多个关键的应用程序。双击某一条程序记录，查看详细信息。单击下方的“上一条”、“下一条”按钮，可以逐条查看，如图 5-249 所示。如果确定某条程序记录不需要，可以单击右上方的“删除”按钮，将其删除。

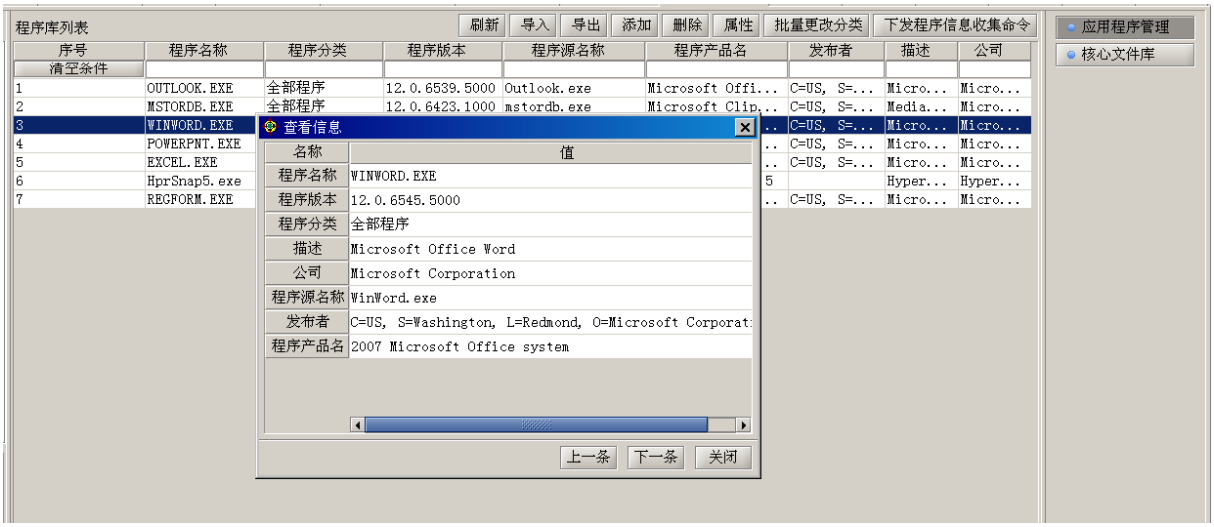


图 5-249　查看程序详细信息

3. 程序的收集除上面讲的手动单个添加外，还可以通过命令的方式批量获取。单击“下发程序信息收集命令”按钮，选择某计算机，单击“确定”按钮将命令下发，如图 5-250 所示。命令下发成功后，该计算机正在运行的程序信息将上传到可信计算管理应用程序库的“未分类程序”中。

提示：程序的收集也可以在“可信计算策略”界面，通过下发策略的方式获取客户端程序信息，详见“程序控制”章节。

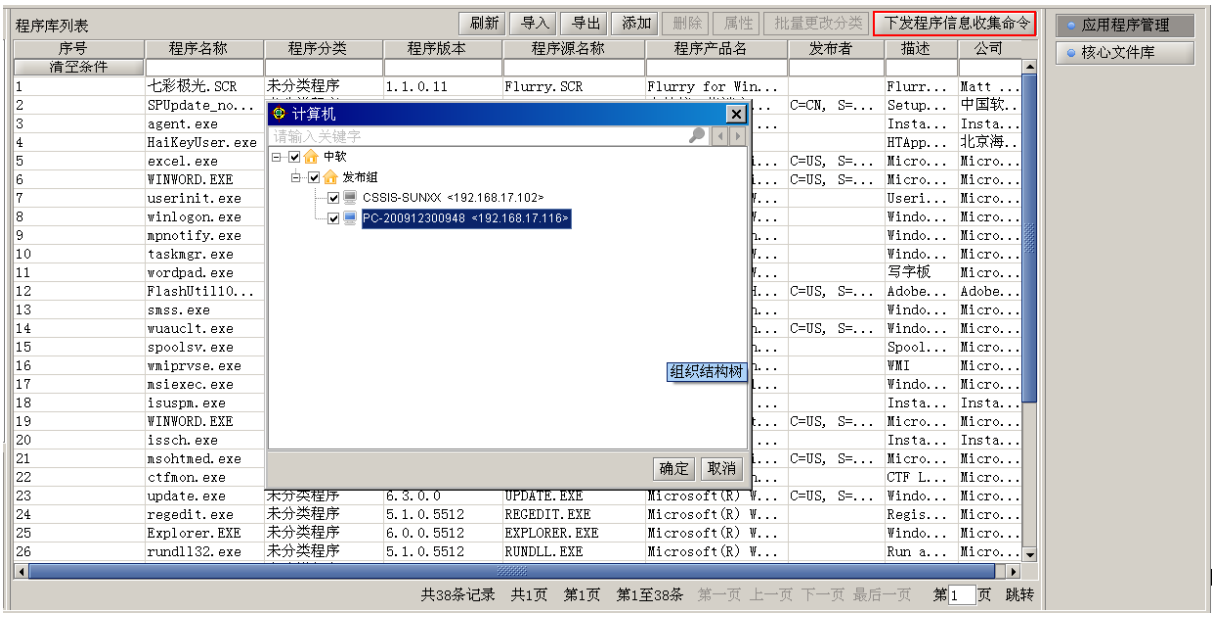


图 5-250　通过命令获取指定计算机程序信息

4. 当程序添加的比较多时，放在一起比较混乱，我们可以进行分类管理。在左侧框中，添加程序分类，设置默认匹配规则，如图 5-251 所示。默认程序库中已建立几个程序分类，并添加相应的程序。对于已经存在程序分类，用户也可以进行删除、修改操作。

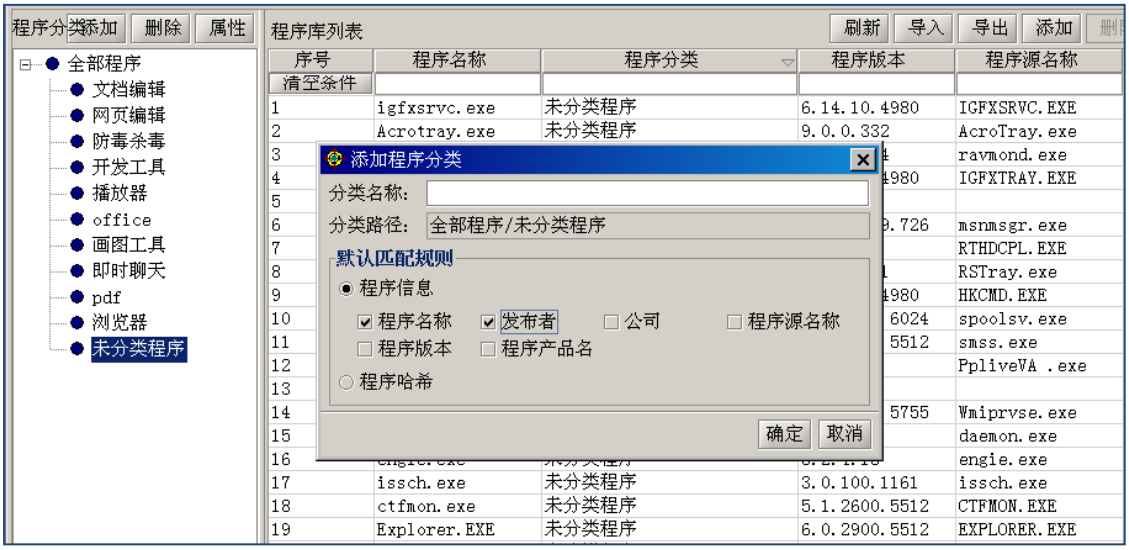


图 5-251　添加程序分类

5. 在程序库列表中选择某些程序，单击右上方的“批量更改分类”按钮，将选择的程序全部更改为指定的程序分类，如图 5-252 所示。也可选择某一个程序，单击右上方的“属性”按钮，单个更改程序分类。

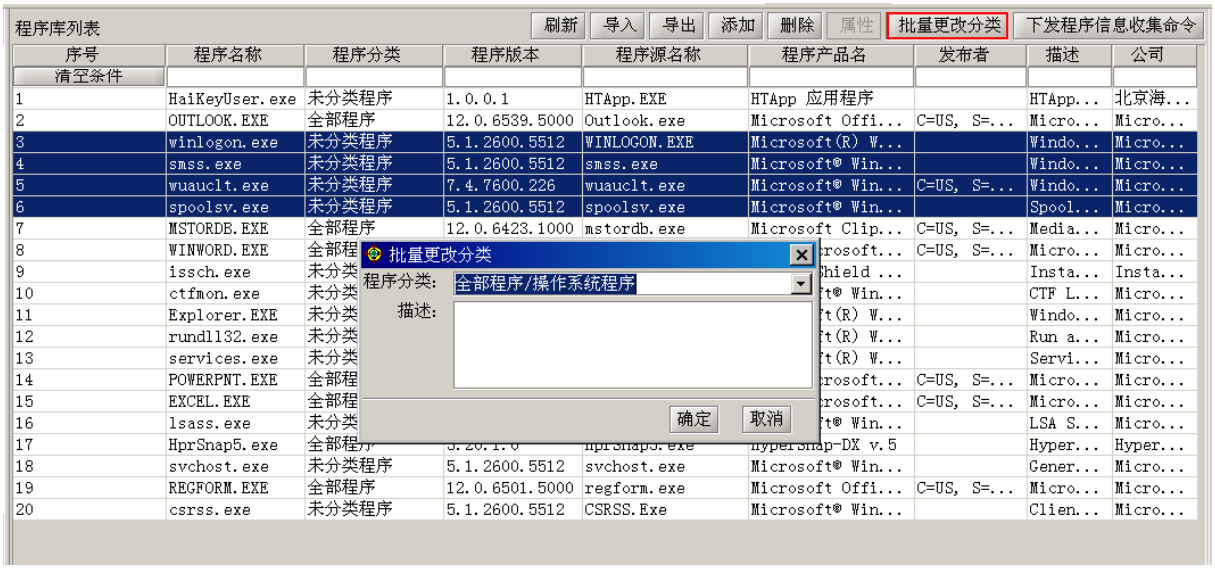


图 5-252　批量更改程序分类

6. 单击“程序名称”下面的空白框，输入检索条件，可以看到所有与之匹配的程序信息，如图 5-253 所示。程序库列表支持按条件检索，单击各表头上、下小箭头，可以按升降或降序排列。

图 5-253　程序库列表支持按条件检索

7. 最后，我们可以单击“导出”按钮，将全部程序库信息导出保存为*.xml 文件，如图 5-254 所示。相反，我们也可以将相应信息，批量导入到程序库列表中。导入时，如果用户选择“删除原有程序及分类”选项，则数据库中原有的进程及分类信息被删除后，才导入 xml 文件中的信息；如果用户不选择“删除原有程序及分类”，则将新的程序信息导入到未分类程序下面。

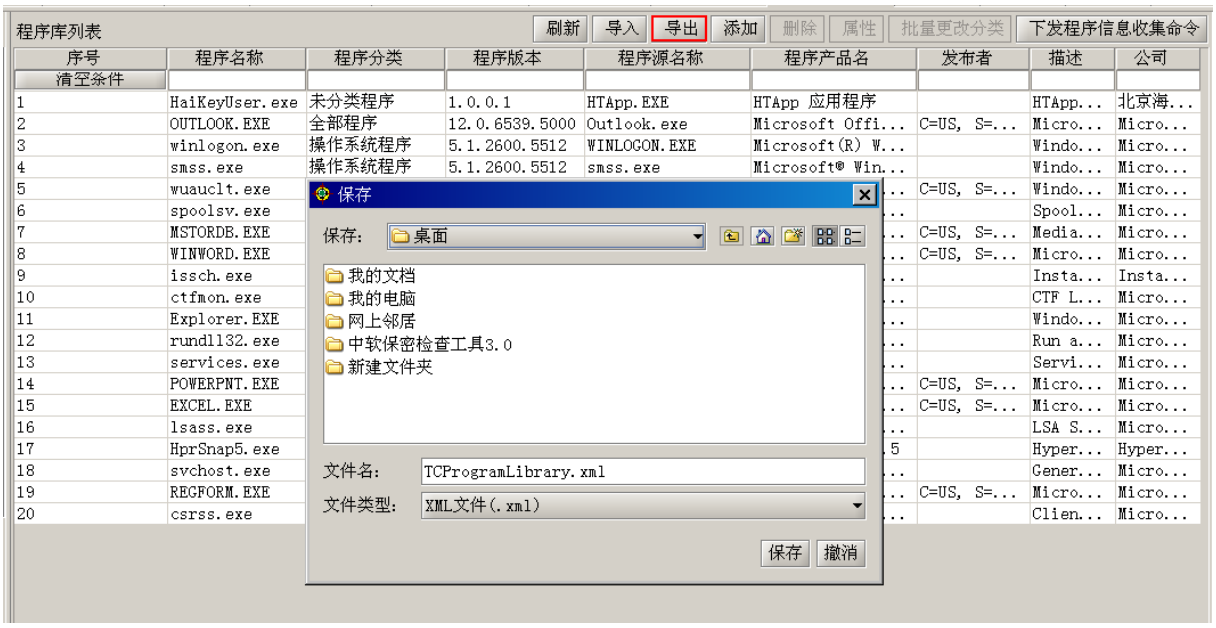


图 5-254　导出程序库列表信息

5.19.1.2 核心文件库

1. 在“可信计算管理” 的“核心文件库”界面，单击“添加”按钮，选取 windows、\windows\system、\windows\system32 这三个目录下的文件*.exe 或*.dll，如图 5-255 所示。确定后，将该核心文件添加到核心库文件列表中。

提示：如果在 win2000 下，核心文件路径指 winnt、winnt\system、winnt\system32 这三个路径。

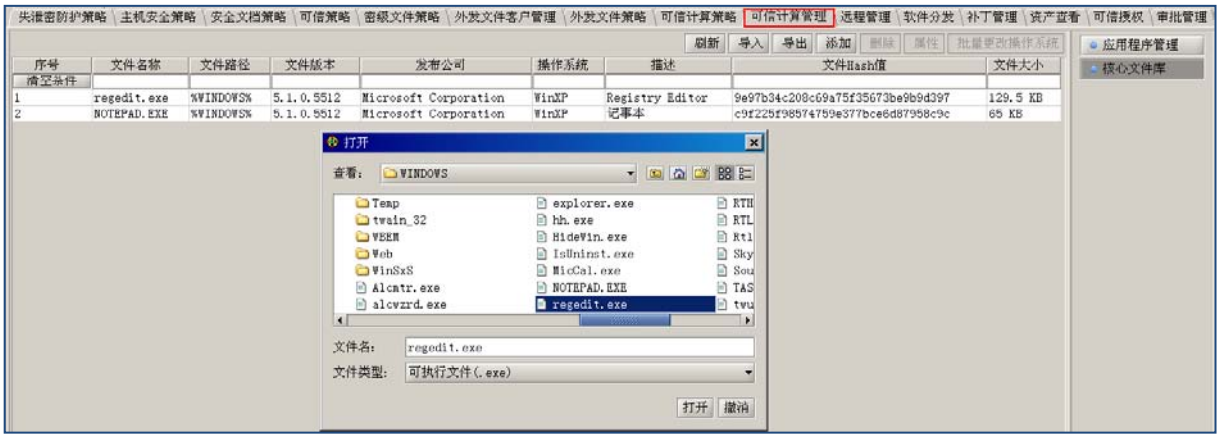


图 5-255　添加核心文件

2. 按此方法，在核心文件库中手动添加多个核心文件。双击某一条文件记录，查看详细信息。单击下方的“上一条”、“下一条”按钮，可以逐条查看，如图 5-256 所示。如果确定某条程序记录不需要，可以单击右上方的“删除”按钮，将其删除。

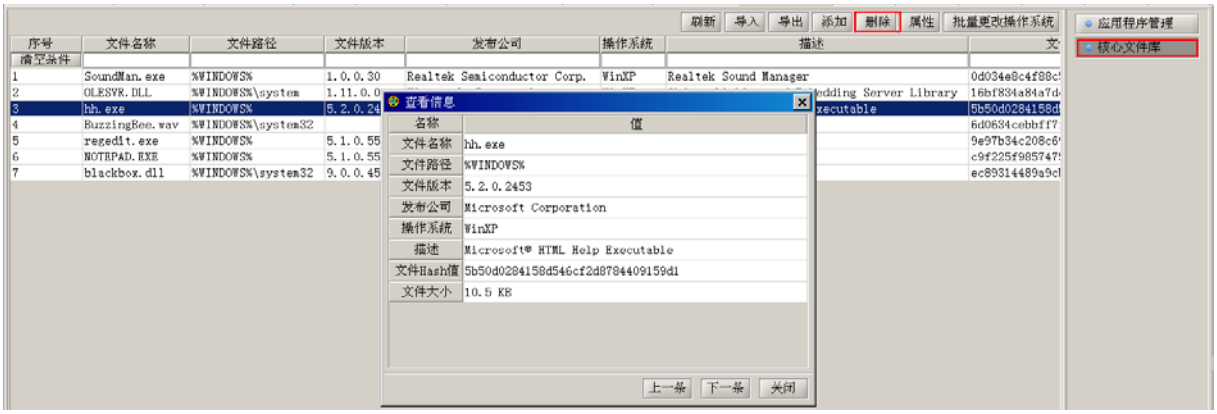


图 5-256　查看核心文件库列表

3. 核心文件的添加还可以通过下发命令的方式，批量获取客户端核心文件信息。单击“下发核心文件信息收集命令”按钮，弹出选择计算机和核心文件操作框，如图 5-257 所示。在左侧选择指定的计算机，在右侧选择核心文件。这些核心文件如果系统没有默认预设的话，管理员可以通过上方“手动添加”或者“浏览添加”按钮，一个一个添加。最后，单击“确定”按钮，将命令下发。

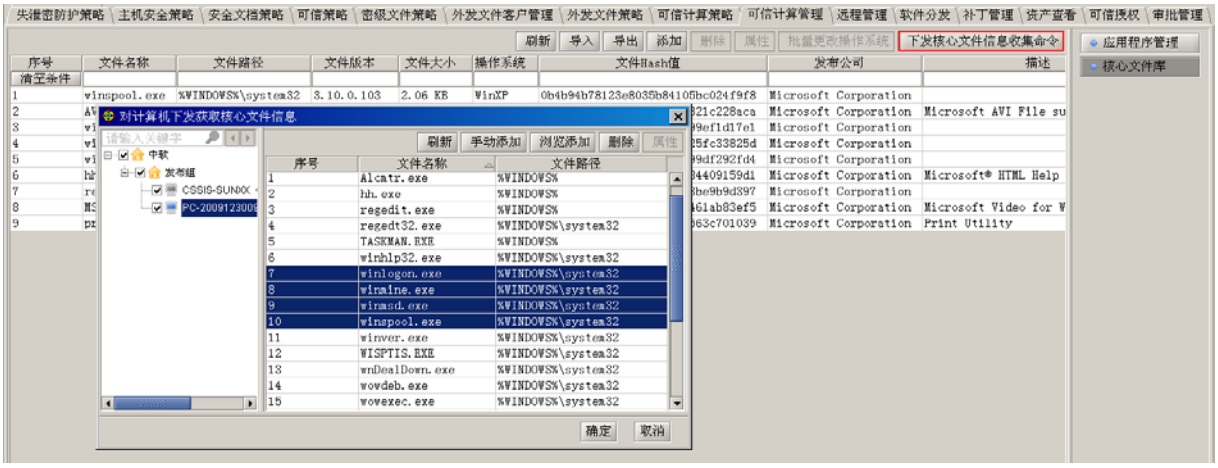


图 5-257　获取指定计算机核心文件

4. 收到命令的计算机，将指定路径下要求上传的核心文件信息上传至核心文件库。如果该计算机在指定路径下没有要求上传的核心文件，则不会上传。用户可以在“核心文件库”界面，单击“刷新”按钮，看到指定计算机上传的核心文件信息，如图 5-258 所示。

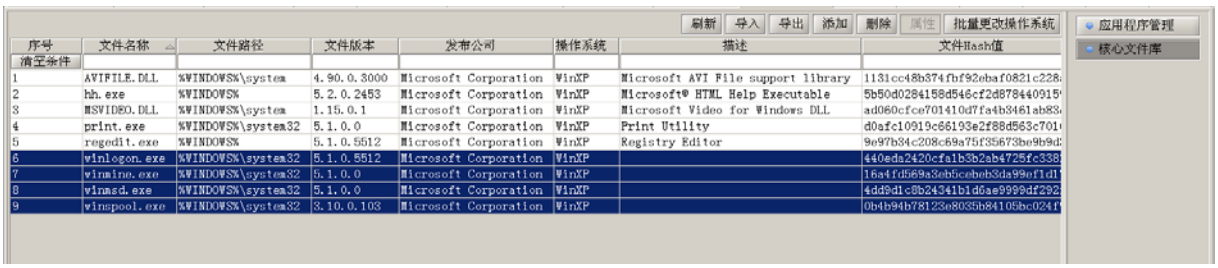


图 5-258　上传的指定计算机核心文件信息

5. 在核心文件库列表中，选择某些核心文件，单击右上方的“批量更改操作系统”按钮，将选择的核心文件全部更改为指定的操作系统，如图 5-259 所示。也可选择某一个程序，单击右上方的“属性”按钮，单个更改操作系统。

图 5-259　批量更改操作系统

6. 单击“操作系统”下面的空白框，输入检索条件“winxp”，可以看到所有与之匹配的文件信息，如图 5-260 所示。核心文件库列表支持按条件检索，单击各表头上、下小箭头，可以按升降或降序排列。

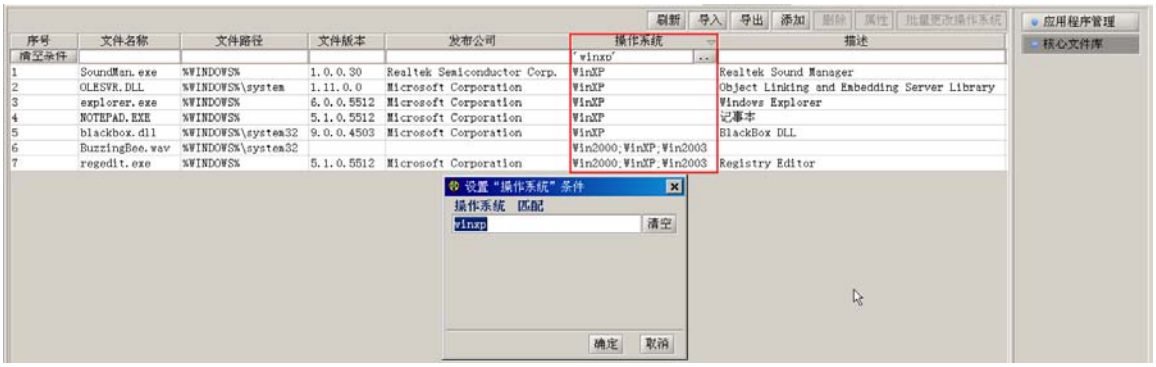


图 5-260　核心文件库支持按条件检索

7. 最后，我们可以单击“导出”按钮，将全部核心库文件导出保存为*.xml 文件，如图 5-261 所示。相反，我们也可以将相应信息，批量导入到核心文件库中。导入时，如果用户选择“删除原有核心文件”选项，则数据库中原有的核心文件信息被删除后，才导入 xml 文件中的信息；如果用户不选择“删除原有核心文件”，则将新的核心文件导入到原有核心文件的下面。

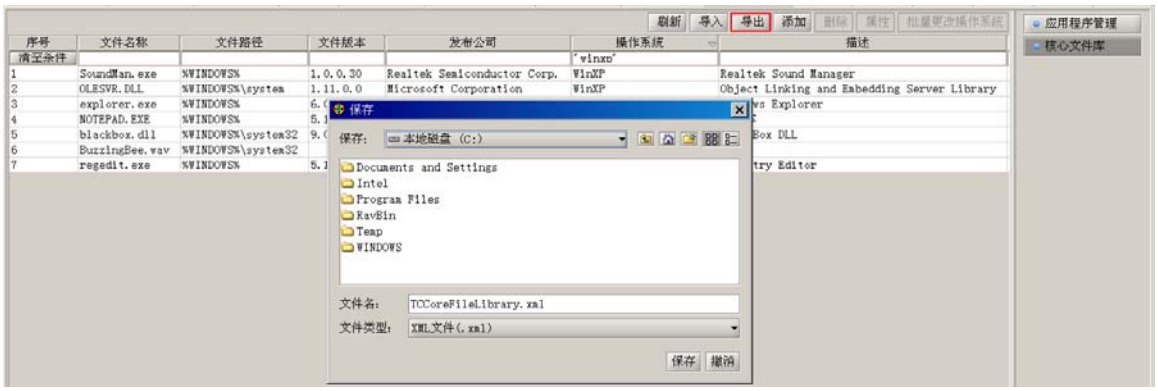


图 5-261　导出核心文件库

5.19.2 可信计算策略

在安全管理中心中，“可信计算策略”标签项，进入可信计算策略页面，在这里制定下发策略，进行关键程序控制和核心文件程序，下面具体叙述。

5.19.2.1 程序控制

1. 在“可信计算策略” 的“程序控制”界面，我们可以通过下发策略方式批量获取客户端程序信息，如图 5-262 所示。选择“启动程序收集”，将此策略应用下发后，收到策略的计算机将正在运行和以后运行的程序信息上传给服务器。

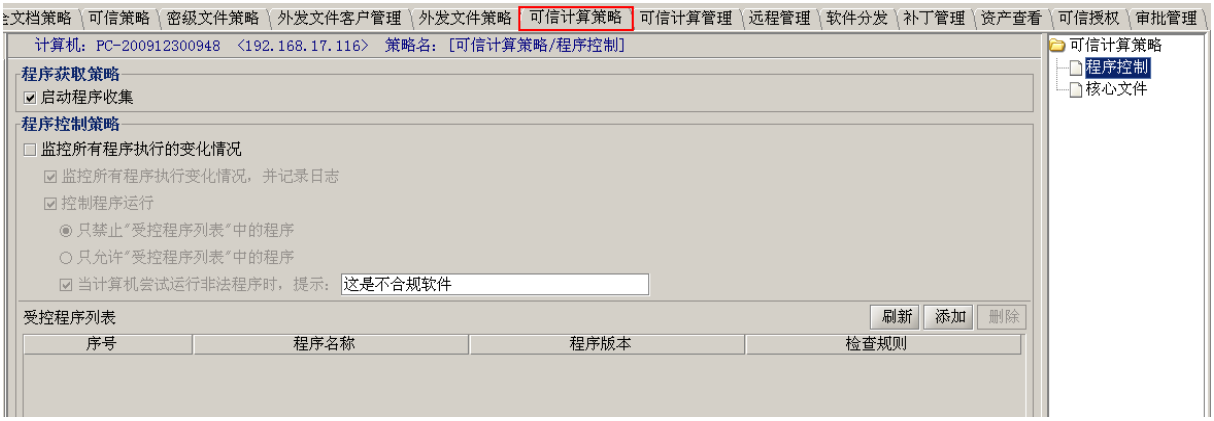


图 5-262　通过策略获取指定计算机程序信息

2. 在“可信计算管理”的“应用程序库”中，单击“刷新”按钮，可以在“未分类程序”下看到上传的程序信息，如图 5-263 所示。

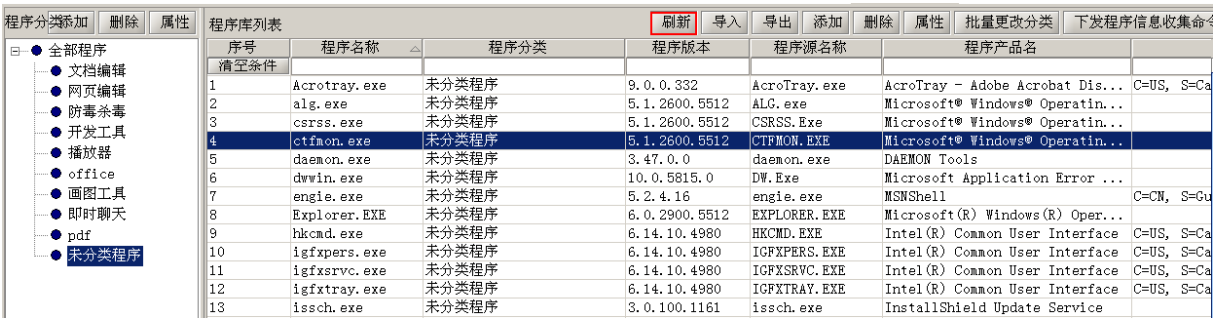


图 5-263　查看获取的程序信息

3. 返回到“可信计算策略” 的“程序控制”界面，制定程序控制策略，如图 5-264 所示。我们选择“监控所有程序执行变化情况，并记录日志”， 将策略下发成功后，收到策略的计算机所有运行程序的开启和关闭情况都有日志记录，可以在“统计审计分析”→“可信计算”→“进程运行状态日志”中查看。

图 5-264　监控所有程序执行变化情况

4. 如果要控制某些程序的运行，就要单击下方的“添加”按钮，从“应用程序库”中选择需要受控的程序 ，设置检查规则，添加到下面的受控程序列表中，如图 5-265 所示。这些检查规则之间是“与”的关系，只有都匹配上，该程序才执行相应的策略。如果单选“发布者”，不选择“程序名称”，那么所有与发布者相同的程序都要执行相应的策略，所以请用户设置匹配规则时一定要注意，是否同时检查程序名称。

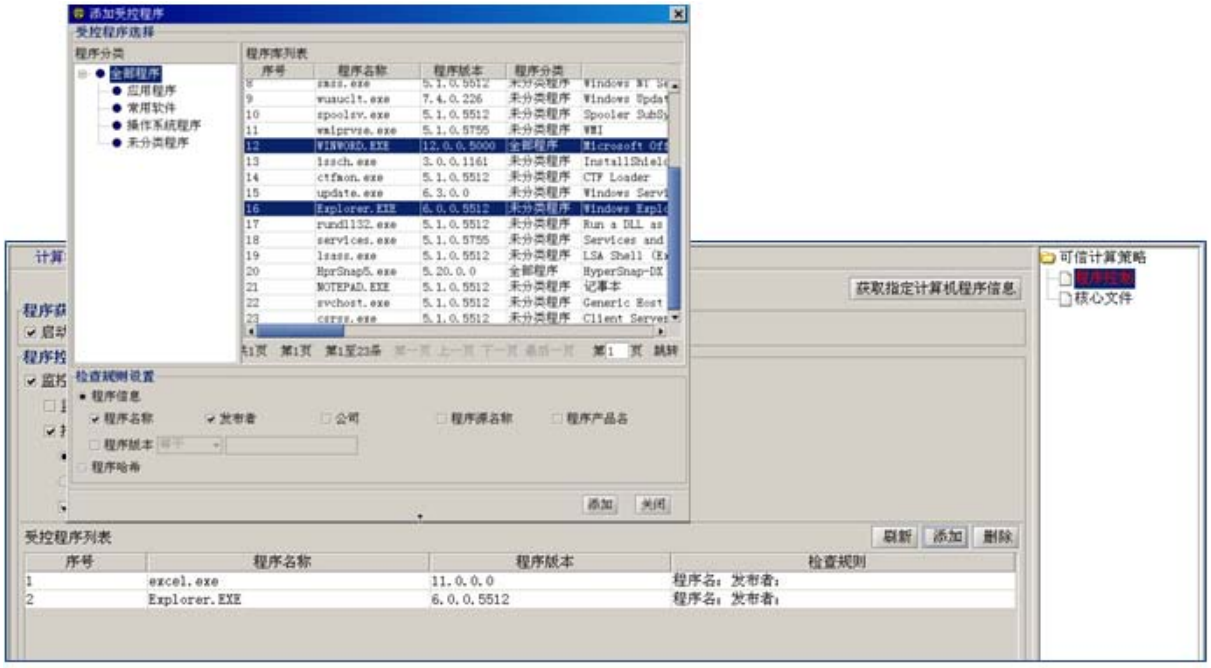


图 5-265　添加受控程序列表

5. 例如：我们下发“只禁止受控程序列表中的程序”，并设置当计算机尝试运行非法程序时，提示“这是不合规软件”，如图 5-266 所示。该策略下发成功后，收到策略的计算机尝试受控列表中的程序，并匹配上检查规则时，将弹出提示框，如图 5-267 所示。

提示：操作系统的一些文件是默认放开的，即使添加到受控程序列表中也不受控制。目前 UEM 系统默认放开的程序文件有：SMSS.EXE、CSRSS.EXE、LSASS.EXE、SERVICES.EXE、WINLOGON.EXE、EXPLORER.EXE、SVCHOST.EXE、TASKMGR.EXE、USERINIT.EXE、LOGONUI.EXE。

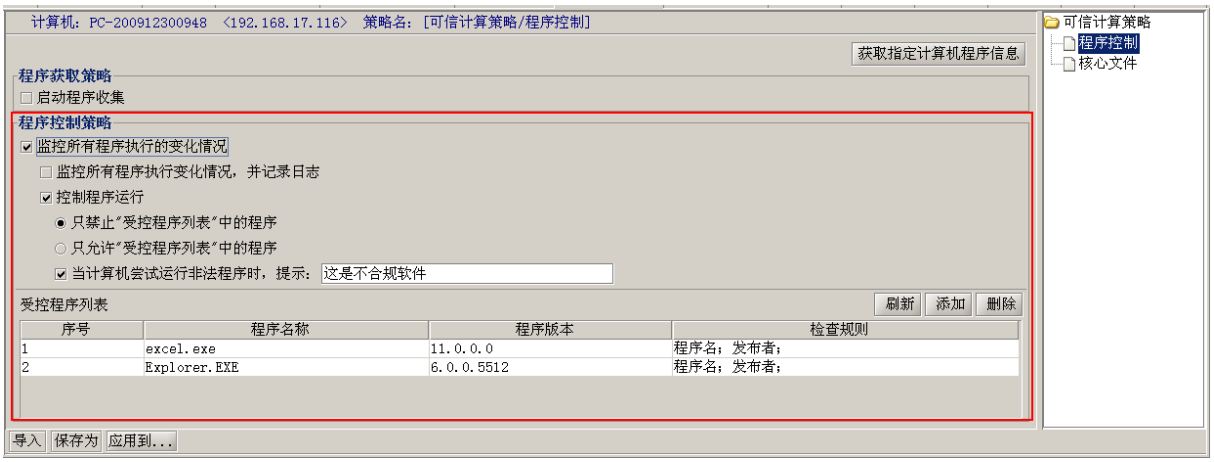


图 5-266　下发控制程序运行策略

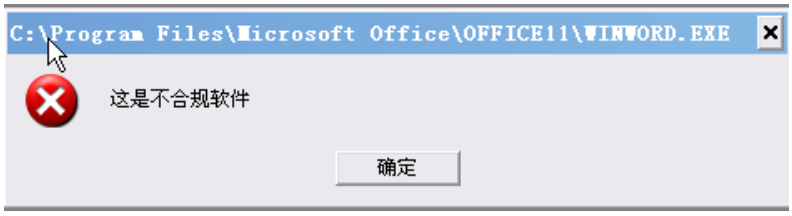


图 5-267　客户端计算机提示信息

5.19.2.2　核心文件控制

1. 我们在“核心文件库”管理中已经完成核心文件的添加工作，在“可信计算策略”的“核心文件控制”中，将制定核心文件控制策略，如图 5-268 所示。例如：选择“启用核心文件检查”→“启用报警”，并勾选“检查未通过，消息通知用户”。单击“应用到”按钮，将此策略下发指定的计算机。

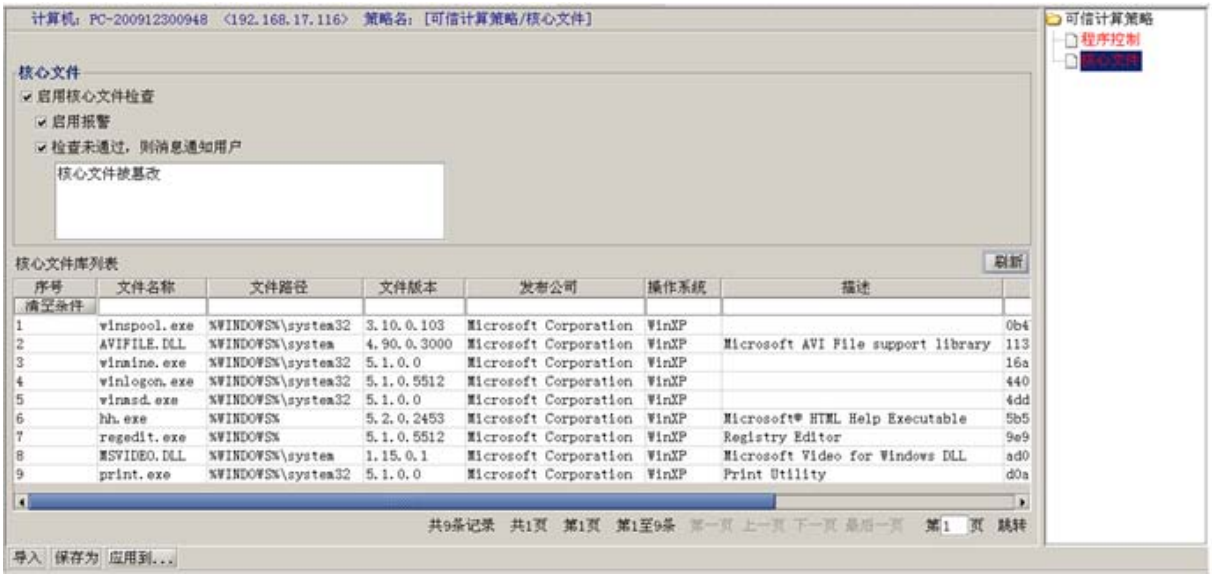


图 5-268　下发核心文件策略

提示：检查未通过是指下面核心文件库列表中的核心文件信息检查未通过，哈希值有变化。这里的核心文件库列表内容和可信计算管理中的核心文件库内容一致，添加、删除操作也要核心文件库管理中进行。

2. 收到策略的计算机，如果将核心文件库列表中的设定核心文件被非法程序篡改，系统重启或管理员下发策略时，系统就会报警，并弹出消息通知，如图 5-269 所示。这样防止了操作系统被病毒或木马感染，恶意侵犯操作系统的行为。报警方式支持邮件报警、短信报警和声音报警，需要在知识库管理章节配置。核心文件检查结果日志信息可以在“统计审计分析”→“可信计算”→“核心文件检查结果日志”中查看。

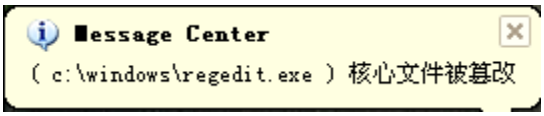


图 5-269　核心文件被篡改的消息通知

第六章　内网安全扫描

内网安全扫描是终端安全管理系统的一个组件，它的主要功能是扫描局域网内部的存活计算机信息，并对这些计算机进行合法性分析。其基本实现原理是，各个网段的代理向本网段发送探测数据，并收集数据提取存活主机信息，然后各网段代理分别将本网段数据信息发送至服务器，服务器在分析数据之后，通过控制台显示被探测到主机的相关信息。这些信息包括主机的 IP 地址、Mac 地址、是否安装 UEM 客户端等。在控制台中不合法接入的主机也将被标识，该组件还可以通过交换机阻断功能或 ARP 欺骗阻断功能来阻断这些不合法主机。内网安全扫描组件能记录扫描产生的日志信息，并且提供日志查询功能。

内网安全扫描默认由系统操作员执行，单击“内网安全扫描”，进入“内网安全扫描”主控界面，如图 6-1 所示。

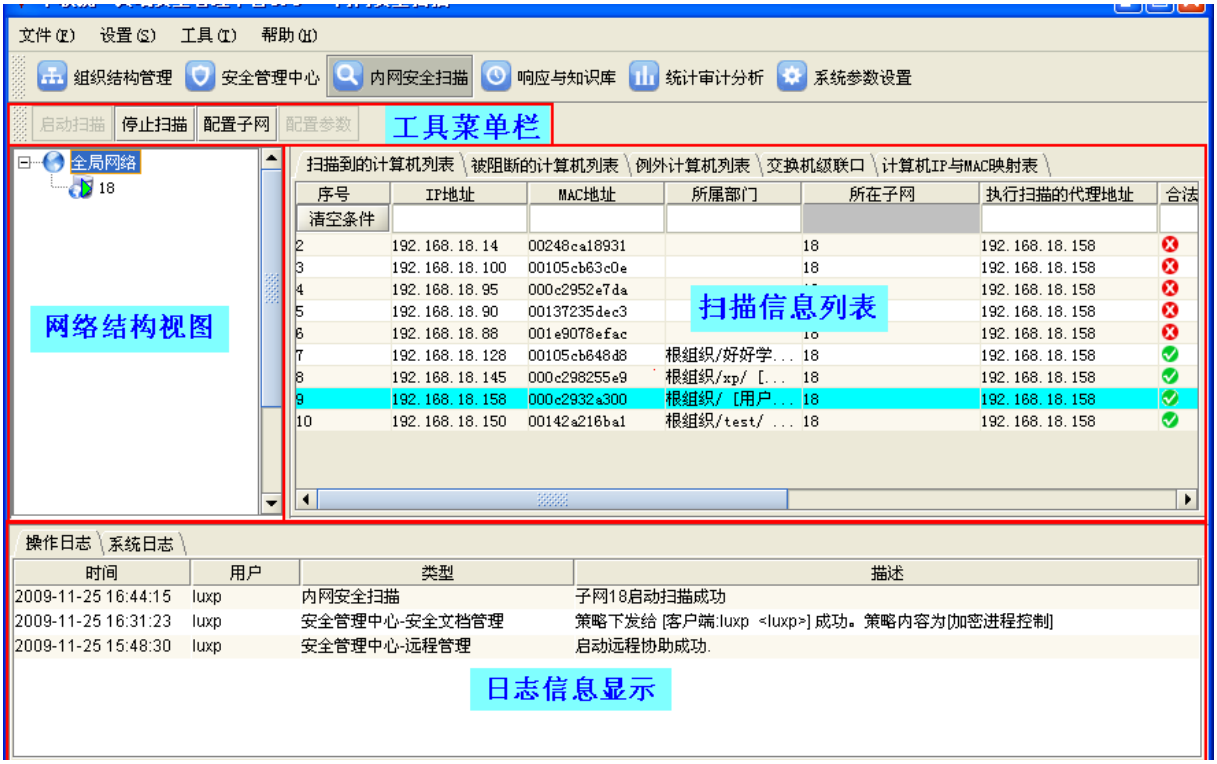


图 6-1　内网安全扫描主控界面

提示：

（1）在执行内网安全扫描前要首先配置子网和配置参数。

（2）如果要启用交换机阻断功能，交换机必须可控且支持 SNMP 协议，如何开启 SNMP 服务详见补充说明。

6.1 配置子网

6.1.1　添加子网信息

单击“配置子网”菜单项，进入子网配置界面，默认情况下没有任何子网信息。单击“添加”按钮，进入“添加子网”界面，如图 6-2 所示。

图 6-2　添加子网

◆　在子网信息输入框中输入“子网名称”、“网关地址”、“扫描起始地址”和“扫描结束地址”，其中“子网名称”是用户为了查看方便而输入的标识信息，为保证正确扫描网段信息，请务必将各字段信息填写正确。

◆　添加客户端代理地址。添加客户端代理之前，先添加扫描起始地址和结束地址等信息，根据这些信息得到这个网段可选的代理列表。单击“添加”按钮，弹出“选择代理地址”界面，如图 6-3 所示，列表中列出该网段所有可供用户选择的代理地址。用户可以在输入框中直接输入指定的客户端 IP 地址，将其添加到代理地址列表中；或者直接双击列表中可选的代理，即可添加到代理列表中。代理列表中的客户端会充当代理扫描其网段内机器信息。代理可以添加多个，各个代理地址按优先级排序（排在第一个的优先级最高）。当开始扫描时，内网安全扫描组件将按照代理优先级顺序启动代理扫描。若启用所有代理均失败，则该子网处于代理轮询状态，此时，一旦有某个代理机器上线，其将作为扫描代理扫描本网段信息。

图 6-3　选择代理地址

◆　ARP 欺骗阻断是通过客户端代理向其网段内的非法主机频繁发送 ARP 欺骗包来实现的。如果使用 ARP 欺骗阻断功能，则选中“启用 ARP 欺骗阻断功能”复选框。

◆　交换机阻断即关闭非法计算机与交换机之间的端口，使其与网络隔断。如果要启用交换机阻断功能，则选中“启用交换机阻断功能”复选框，并单击“添加”按钮，添加交换机信息，如图 6-4 所示。在弹出的添加交换机信息中输入交换机 IP 地址、共同体名、类型和 VLAN ID 值后。点击“测试”按钮，测试本主机是否有权限管理交换机，提示“成功”表示有权限，然后将此添加到交换机列表中。具体配置可参考以下所述。

图 6-4　添加交换机信息

假定子网 1 共有 50 台计算机并且占用了 2 台交换机。

第一台交换机为“思科”交换机，IP 地址为 192.168.100.1、交换机的读写共同体名为 private，本机所在 VLAN ID 为 13，则“本机交换机地址”和“共同体名”分别输入“192.168.100.1”、“private”，“交换机类型”选择“思科”，此时“共同体名格式”自动设置为“共同体名+@+VLAN ID”，“VLAN ID”输入“13”。然后点击“添加”将此交换机信息添加到交换机列表中。

第二台交换机为“华为”交换机，IP 地址为 192.168.100.2、交换机的读写共同体名为 private，本机所在 VLAN ID 为 13，则“本机交换机地址”和“共同体名”分别输入“192.168.100.2”、“private”，“交换机类型”选择“华为”，此时“共同体名格式”自动设置为“共同体名”，“VLAN ID”输入“13”。然后点击“添加”将此交换机信息添加到交换机列表中。

点击“测试”按钮可测试配置是否成功，如果提示“失败”，则有可能是本地计算机（即安装UEM服务器的计算机）没有权限管理这台交换机，或者是设置的共同体名不具备读写权限等等，这些情况都需要对交换机进行重新设置。

注意：

（1）使用交换机阻断时，需配置人员首先对本网络的拓扑结构、子网的划分、子网所连接的交换机以及交换机型号等信息了解清楚，这样才能保证内网安全扫描的阻断功能正常运行。

（2）在某些情况下，可控交换机的端口不是与计算机直接相连，而是连接集线器或是其他不可控交换机。在这些不可控设备下又连接多台计算机，当这多台计算机中有一台符合阻断条件时，客户端代理将关闭集线器与交换机之间的端口，于是集线器下方的这多台主机将全部被阻断，所以交换机的阻断功能应慎用。服务器和代理主机最好接在单独的交换机接口上，如果和不合法主机共接一个交换机接口，可能同时被阻断。

（3）如果某子网跨越了3个交换机，需要将这三个交换机全部输入到交换机列表中，一个都不可少。

交换机阻断和ARP欺骗阻断：

内网安全扫描采用两种方式实现对非法接入主机的阻断：即交换机阻断和ARP阻断。交换机阻断方式需要网管员配置交换机；ARP阻断方式则不需要。

若本局域网内子网结构划分清晰，交换机厂商及型号相对单一且HUB数量少，则建议采用交换机阻断方式；若网络结构复杂，交换机厂商及型号多样，则建议采用ARP欺骗阻断方式，这样能减轻配置交换机及配置内网安全扫描的负担。

亦可同时选择交换机阻断和ARP欺骗阻断方式，当同时选择这两种阻断方式时，系统将优先使用交换机阻断。只有当交换机阻断失败时，才会使用ARP欺骗阻断。

6.1.2　编辑子网信息

根据需要添加多个子网信息。在子网信息列表中，任选择一个子网，通过右键菜单或者下面的功能按钮，可以编辑、删除、查看子网信息，如图6-5所示。

◆　编辑子网，只有子网处于停止扫描状态，才可以进行编辑子网。在子网列表中选择要编辑的子网，通过右键菜单选择“编辑”选项或者点击“编辑”按钮，进行子网编辑。子网名称不可修改，“网关地址”、“扫描起始地址”和“扫描结束地址等可以修改，点击“添加”按钮，弹出“选择代理地址”界面，列表中列出该网段除了已添加到的代理列表之外所有可供用户选择的代理地址，可以添加新的代理地址到代理地址列表或者删除之前添加的代理地址。根据需要重新选择是否启用ARP欺骗阻断功能和交换机阻断功能。如果选择了启用交换机阻断功能，可以编辑交换机配置信息。

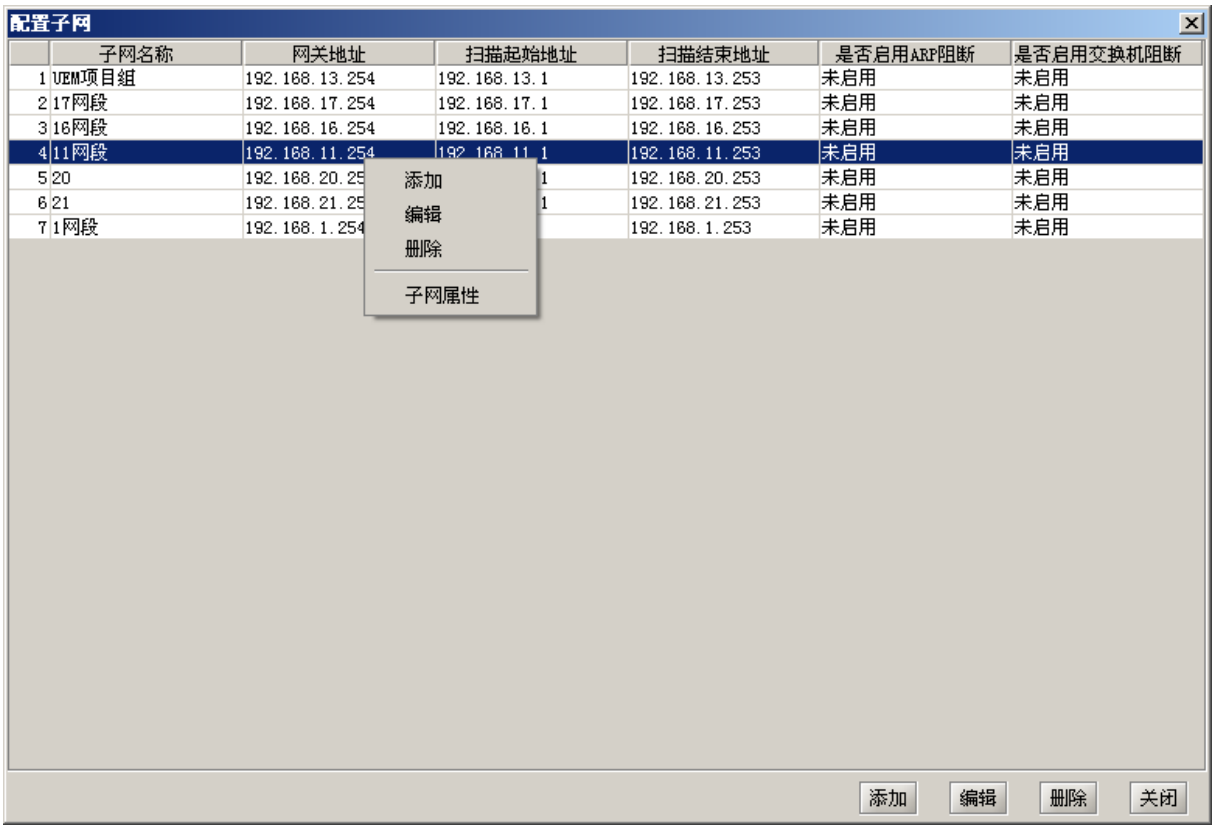


图 6-5　子网信息列表

◆　删除子网，只有子网处于停止扫描状态，才可以进行删除子网。删除子网时，在子网列表中选择要删除的子网，通过右键菜单选择“删除”选项或者点击“删除”按钮，进行子网删除。删除子网操作是不可恢复的操作，点击“确定”后，子网列表中的子网记录和“子网信息结构”视图中的该子网节点一起被删除。如果该子网曾经被执行过扫描，则删除子网暂时不清除数据库中的扫描信息日志。

◆　查看子网，子网处于启动扫描、轮询或者停止扫描状态，都可以进行查看子网。查看子网信息，在子网列表中选择要查看的子网，通过右键菜单选择“子网属性”选项或者双击查看选中的子网，只能进行子网信息查看，不能编辑。

6.2 配置参数

单击“配置参数”菜单项，进入配置参数界面，如图 6-6 所示。参数配置包括两部分：基本参数配置和阻断参数配置。

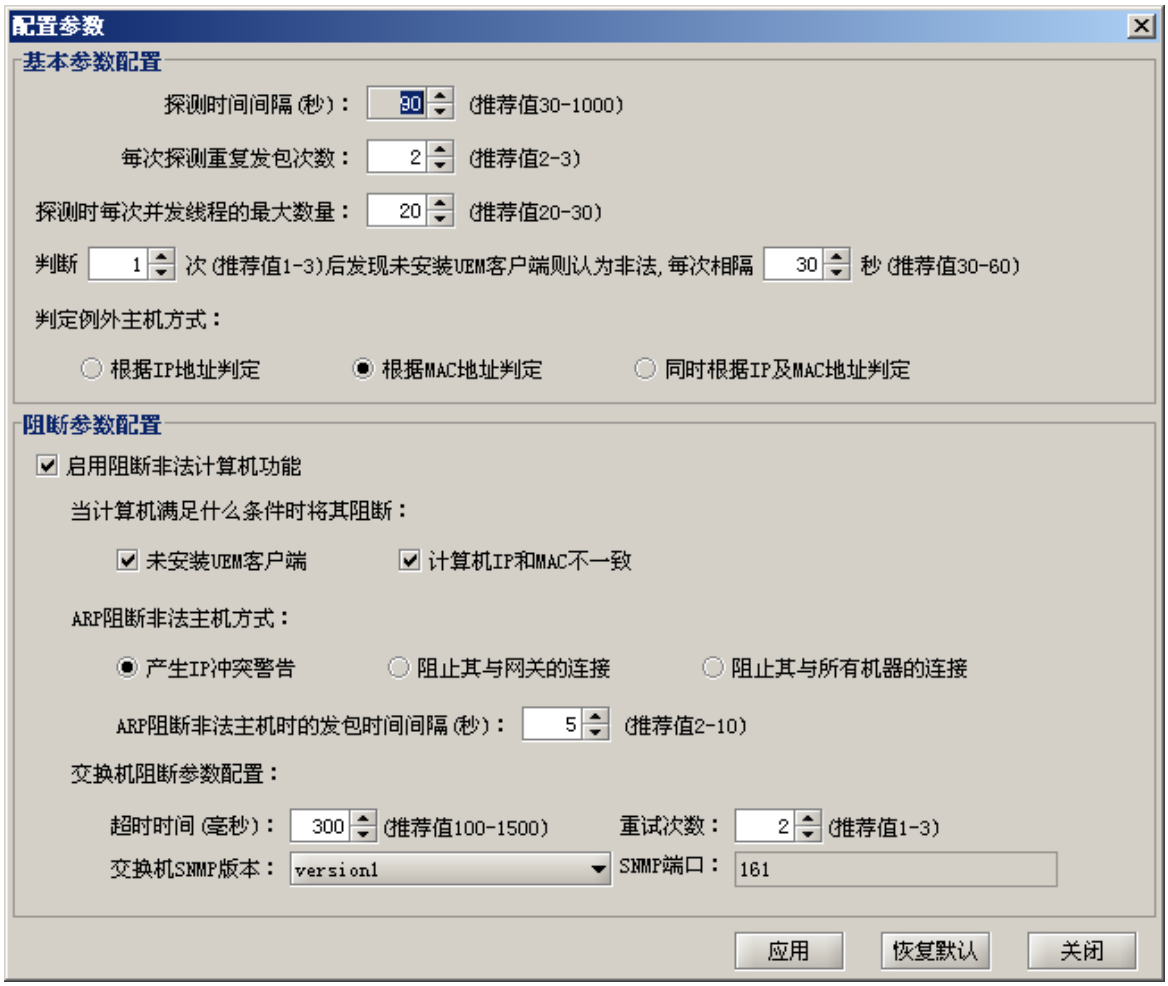


图 6-6　配置参数界面

6.2.1　基本参数配置

探测时间间隔：扫描时间间隔不要过短，否则本机的资源消耗将提高，默认为 90 秒，推荐值（30-1000）秒。

重复发包次数：推荐值（2-3），接受默认值即可。

最大并发线程数：为允许该进程启动的最大线程数量，当代理启用线程数过多时，会影响代理主机的性能，推荐值（20-30）。

判断次数和时间间隔：设置判断几次（推荐值 1-3）后，发现未安装 UEM 客户端则认为非法，每次相隔多少秒（推存值 30-60 秒）。

判定例外主机方式：有三种方式（根据 IP 地址判定、根据 MAC 地址判定，或者同时根据 IP 地址和 MAC 地址判定），任选其一。

6.2.2　阻断参数配置

如果要启用网络阻断功能，首先要选择“启用阻断非法计算机功能”复选框，然后进行下面的参数设置，设置完成后单击“应用”按钮。

（1）阻断条件

◆　选中“未安装 UEM 客户端”，则当发现某计算机未安装 UEM 客户端时将其阻断。

◆　选择“计算机 IP 和 MAC 不一致”，当存在于数据库中的某主机修改 IP 地址时，如果客户端未将其新的 IP 地址上传至服务器，则系统将其阻断。

上述两种阻断条件是“或者”的关系，即如果同时选中这两个条件，只要某计算机满足一项条件，就会对其进行阻断。

若启用阻断功能，还需要在“子网设置”中选中“启用交换机阻断功能”或者“启用 ARP 欺骗阻断功能”复选框。

（2）ARP 阻断参数配置

◆　选择“产生 IP 冲突警告”，则非法主机被成功阻断后，将会收到网络上有重复的 IP 地址的警告，但不会影响其网络的连接。如果客户端为 Vista 系统，发生 IP 冲突时，会自动将网络断掉。

◆　选择“阻止与其网关的连接”，则非法主机被成功阻断后，将会失去与网关的连接。

◆　选择“阻止与所有机器的连接”，则非法主机被成功阻断后，将会失去与其他所有主机的连接。

◆　“发包时间间隔”表示，当对某计算机发送 ARP 欺骗包时的时间间隔。默认的时间间隔为 5 秒，推荐值（2-10）。

（3）交换机阻断参数配置

◆　输入“超时时间”和“重试次数”。超时时间范围为：100-1500 毫秒，重试次数为：1-3。这两个参数关系到阻断成功与否，如无特殊需要采用默认参数即可。

◆　选择交换机 SNMP 版本，SNMP 端口号按默认值。

6.3 执行扫描

在配置完各子网信息和扫描参数后，即可进行扫描操作。

首先选择需要扫描的子网，用鼠标单击左侧网络结构中的“全局网络”或其分支子网项，确定扫描范围。如果选择“全局网络”，系统将对全部子网进行扫描。

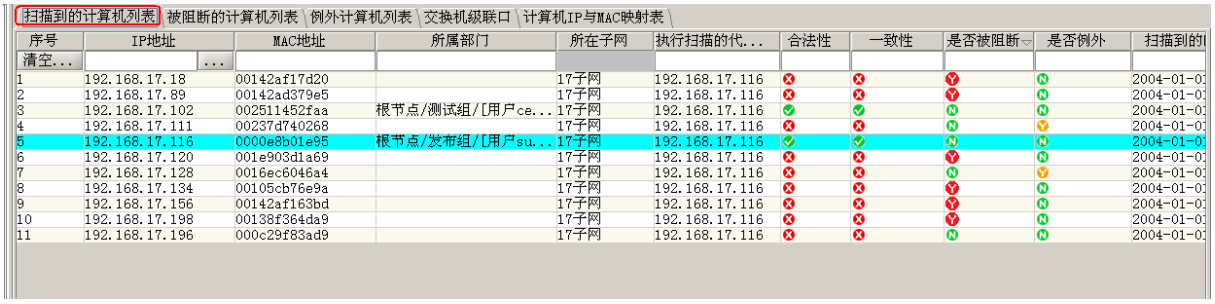
单击工具菜单栏中“启动扫描”按钮，或者在选中的子网项上单击右键菜单，选中“启动扫描”，开始扫描操作。扫描结果将显示在右侧的扫描信息列表中，单击“扫描到的计算机列表”标签页查看。若要停止该网段计算机扫描，点击“停止扫描”按钮，或者在该子网选项上单击右键菜单，选中“停止扫描”，结束扫描操作。内网安全扫描可单独控制某一个子网的启动和停止扫描操作，而其他网段的扫描状态不受影响。

提示：开始执行子网扫描时，UEM 服务器首先根据代理主机列表的优先级设置启动扫描代理，如果代理成功启动，则进行正常的扫描工作，并且在控制台左侧的网络结构中，该子网的图标上将出现绿色箭头。如果该子网代理列表中的所有代理均处于离线状态，则服务器将进行轮询检查，直至有代理主机上线为止，在此期间，该子网的图标上箭头将为黄色，如图 6-7 所示。

图 6-7　子网状态显示

6.3.1　扫描到的计算机列表

在扫描到的计算机列表中，显示计算机 IP 地址、MAC 地址、所属部门、所在的子网、执行扫描的代理地址、合法性、一致性、是否被阻断、是否例外主机、扫描到的时间和备注等信息，如图 6-8 所示。正在执行扫描的代理主机以高亮条显示出来，例如：图中 IP 地址为 192.168.17.116 的主机，就是正在执行扫描的代理主机。



序号	IP地址	MAC地址	所属部门	所在子网	执行扫描的代...	合法性	一致性	是否被阻断	是否例外	扫描到的
清空...	...									
1	192.168.17.18	00142af17d20		17子网	192.168.17.116			Y	N	2004-01-0
2	192.168.17.89	00142ad379e5		17子网	192.168.17.116			Y	N	2004-01-0
3	192.168.17.102	002511452faa	根节点/测试组/[用户ce...	17子网	192.168.17.116			N	N	2004-01-0
4	192.168.17.111	00237d740268		17子网	192.168.17.116			N	Y	2004-01-0
5	192.168.17.116	0000e8b01e95	根节点/发布组/[用户su...	17子网	192.168.17.116			N	N	2004-01-0
6	192.168.17.120	001e903d1a69		17子网	192.168.17.116			Y	N	2004-01-0
7	192.168.17.128	0016ec6046a4		17子网	192.168.17.116			N	Y	2004-01-0
8	192.168.17.134	00105cb76e9a		17子网	192.168.17.116			Y	N	2004-01-0
9	192.168.17.156	00142af163bd		17子网	192.168.17.116			Y	N	2004-01-0
10	192.168.17.198	00138f364da9		17子网	192.168.17.116			Y	N	2004-01-0
11	192.168.17.196	000c29f83ad9		17子网	192.168.17.116			N	N	2004-01-0

图 6-8　扫描到的计算机列表

IP 地址：显示主机的 IP 地址；

MAC 地址：显示主机的 MAC 地址；

所属部门：如果主机为合法主机，则显示其所属部门的名称和该部门所有上级部门的名称，以及该主机用户的名称，如果某主机上注册了多个用户，则会显示多个用户名；

所在子网：显示主机所在网段的子网名；

执行扫描的代理地址：显示执行本次扫描的代理主机的 IP 地址。在扫描到的主机列表中，执行本次扫描的代理主机记录将会进行高亮显示；

合法性：表示主机是否安装了客户端，如果安装显示为，否则显示为。

一致性：表示主机的 IP 和 MAC 地址是否与地址映射列表的一致，一致显示为，不一致显示为。

是否被阻断：表示该主机是否被交换机或 ARP 阻断了。如果被阻断显示为，否则显示为。

是否例外：如果是例外主机，符合阻断条件也不阻断。

扫描到的时间：显示主机被代理主机扫描到的时间；

备　注：显示该主机是否为合法主机，并对主机的合法性进行具体描述。主机的合法性判断主要采取检查 IP 和 MAC 地址，以 MAC 地址为主的原则来进行。以下为判断规则：

1、如果 MAC 地址不在注册计算机之列，列为非法主机。IP 与 MAC 地址未知，备注中显示“计算机未注册 UEM 客户端”；

2、如果 MAC 地址在注册计算机之列，但 IP 地址不符，此时主机不在线，列为非法主机，IP 与 MAC 不一致，备注信息显示“该计算机可能假冒合法计算机”;

3、如果 MAC 地址在注册计算机之列，但 IP 地址不符，此时主机在线，列为合法主机，IP 与 MAC 不一致，备注信息显示“用户更改了主机的 IP 地址”;

4、如果 MAC 地址在注册计算机之列，且 IP 地址相同，但主机不在线，列为非法主机，IP 与 MAC 一致，备注中提示“客户端可能已经卸载或者第二操作系统登录“;

5、如果 MAC 地址在注册计算机之列，IP 地址相同，且主机在线，列为合法主机。

在扫描到的计算机列表中，对于那些认为无需进行检测的主机，如：交换机、网关、UEM 服务器等，可将它们添加至例外主机列表中，具体操作为：在列表中选中不进行扫描的主机项，右键菜单，单击“加入到例外主机列表”，可将该主机添加至例外主机列表中。

在进行某网段扫描的过程中，可以进行更换扫描代理的操作。要完成该项操作，首先从扫描到的计算机列表中选择新的代理主机，它必须具有合法性，且不局限于代理列表中的主机。然后右键该主机项，单击“启动为客户端代理”即可。更换成功后，新的代理主机将会高亮显示。如果需停止现有代理主机的扫描时，只需点击右键菜单中的“停止客户端代理”即会完成停止代理的操作。

在进行新的扫描前，可以从已有的扫描到的计算机列表中任选一条记录，单击鼠标右键菜单，选择“清空列表”，从而对上一次扫描到的计算机列表进行清空，该操作需要在扫描停止后进行。

在扫描到的计算机列表中，任选一条记录，单击鼠标右键菜单，选择“导出数据”，可以将该列表导出为*.xls 文件保存。如果选择“主机属性”，可以查看该主机的详细信息，并可通过点击“上一条”和“下一条”按钮来查看列表中相邻主机的信息，如图 6-9 所示。

图 6-9　被扫描到主机的详细信息

6.3.2　被阻断的计算机列表

设置好阻断条件，并在子网设置中启用交换机阻断或 ARP 阻断，可阻断非法主机。当阻断主机后，被阻断的主机信息将显示在阻断列表中，单击“被阻断的计算机列表”标签页查看，如图 6-10 所示。如果是被 ARP 阻断，不是被交换机阻断，“是否被交换机阻断”一项显示 N。如果主机是被 ARP 阻断，则“交换机/代理 IP 地址”一项显示的代理主机的 IP 地址；若主机是被交换机阻断，则该项显示的是交换机的 IP 地址。

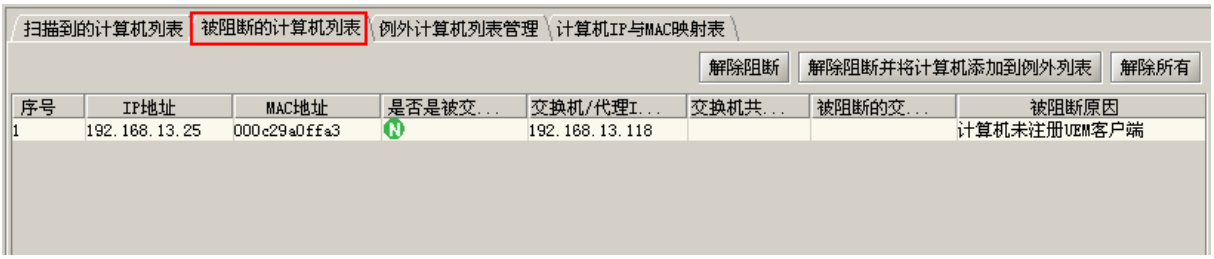


图 6-10　被阻断的计算机列表

点击“解除阻断”按钮，可解除被阻断主机。点击“解除所有”按钮，将解除所有被阻断主机。解除某主机的阻断后，如果系统扫描到该主机仍然满足阻断条件，则仍会继续阻断该主机。

当点击“解除阻断并添加到例外计算机列表”后，被阻断主机将被解除阻断，并被添加到例外主机列表中。此后，当再次扫描到该主机后，其将不会被阻断。

6.3.3　例外计算机列表

在扫描信息列表中，选中网关、UEM 服务器或者其他不需要执行阻断的主机，单击鼠标右键菜单，选择“加入到例外主机列表”，将该主机加入到例外主机列表中。

单击“例外主机列表”选项卡，查看例外列表信息，在此可以添加、删除例外主机或者清空列表，如图 6-11 所示。

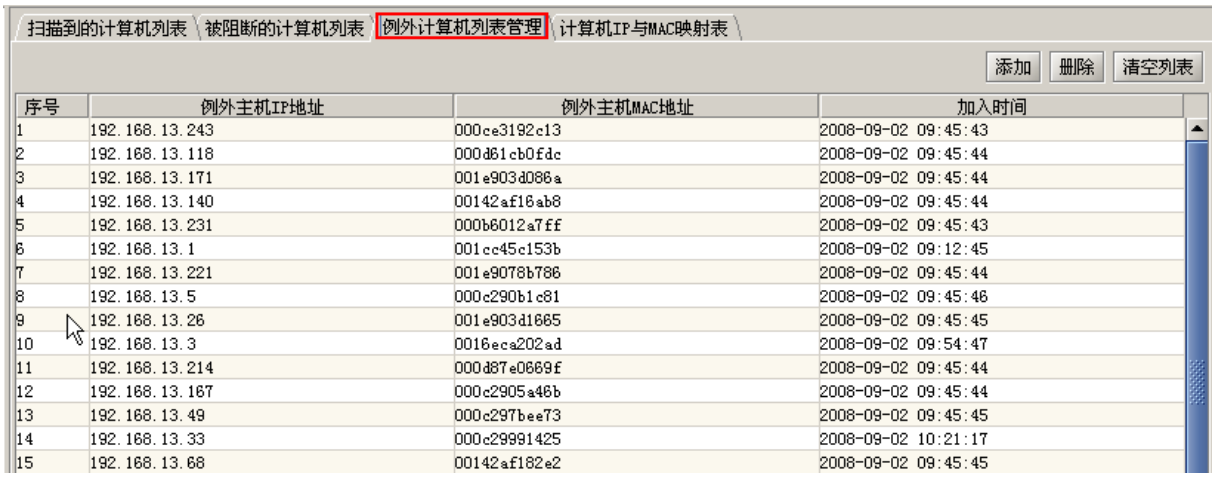


图 6-11　例外计算机列表

提示：在点击“添加”按钮进行添加例外主机操作时，主机的 IP 地址和 MAC 地址均不能为空，且必须保证两者的格式正确无误。

6.3.4　交换机级联口

UEMR7 的内网安全扫描，新增交换机的级联口管理功能。在该列表中可以配置交换机的 IP 地址、级联口、交换机型号信息。当进行内网扫描时，如果启用了交换机阻断功能，在阻断某台非法主机过程中，要首先判断欲被阻断的交换机端口，是否为“交换机级联口列表”中的某台交换机端口。如果是级联口，则打出日志信息说明被阻断端口为交换机的级联口，并且放弃阻断该端口；如果不是级联口，则阻断该端口。

单击“交换机级联口”选项卡，弹出交换机级联口界面。单击“添加”按钮，输入交换机 IP 地址、级联端口、交换机类型，将此信息添加到级联口列表中，如图 6-12 所示。选择列表中某条信息，单击右上角“删除”按钮，可以将其删除。

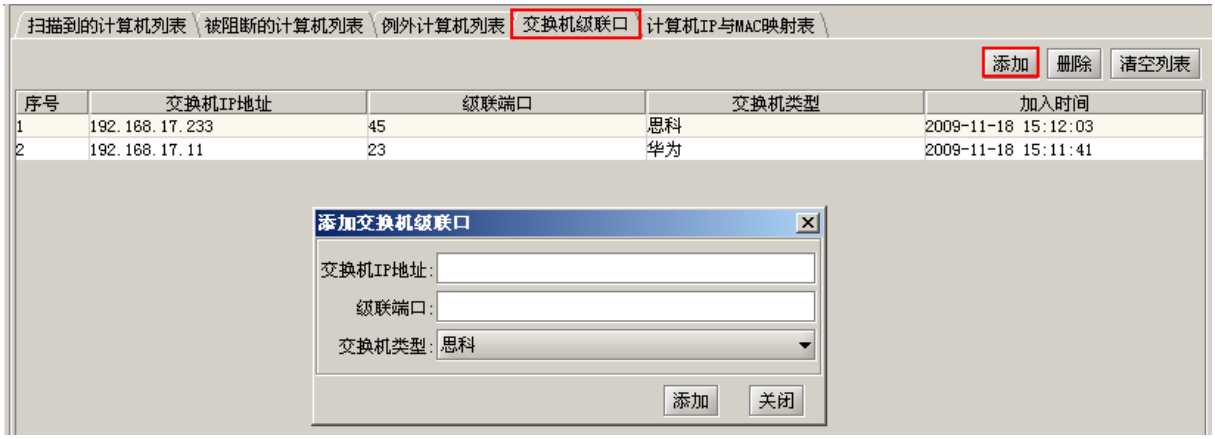


图 6-12　交换机级联口

6.3.5　计算机 IP 与 MAC 映射表

单击“计算机 IP 与 MAC 映射表”标签项，查看 IP 与 MAC 映射关系信息，如图 6-13 所示。该表中的主机 IP 地址和 MAC 地址映射关系是从 UEM 系统组织结构中所获取，故不能编辑和删除该列表。点击右键菜单，可以将该列表导出为*.xls 文件保存。

图 6-13　计算机 IP 与 MAC 映射列表

6.4　补充说明

交换机第二层的端口状态有两种，即 Enable 和 Disable。某一时刻，交换机端口要么处于 Enable 状态，要么处于 Disable 状态。内网安全扫描是通过直接控制二层交换机或三层交换机第二层的端口状态来实现阻断的。

在进行以下步骤之前，请准备好交换机的管理 IP 地址、交换机密码、交换机特权模式密码。

6.4.1　判断交换机的种类

该系统将交换机分为以下三类：

1. CSICO 交换机
   - 操作系统为 IOS 的交换机；
   - 操作系统为 CatOS 的交换机；

注：登录到交换机后，使用“show version”命令可显示交换机操作系统信息。若有“IOS”字样显示则表明交换机为 IOS 系统，其余为 CatOS 系统。

2. 华为交换机
3. 其它交换机。

判断交换机的方法非常简单，机箱的前面板或后面板有明显的厂商标志。如果你的交换机不是前两种，即既不是 CSICO、也不是华为交换机，请与我们联系（联系方式附后），我们将提供及时指导和服务。

6.4.2　远程登录到交换机

（1）打开 Windows 的“命令提示符”对话框。鼠标点击 Windows 屏幕左下方的“开始”菜单，然后依次点击“程序”、“附件”和“命令提示符”。

（2）在命令提示符对话框中输入下列命令

```
telnet 192.168.13.1[回车]
```

此处 192.168.13.1 是用户输入的交换机管理 IP 地址。当系统提示你输入交换机密码时，输入交换机密码并回车，登录到交换机配置模式时还需输入交换机的特权密码。

6.4.3　开启交换机的 SNMP 服务

1．对于操作系统为 IOS 的交换机

这类交换机是 CISCO 的低端型号交换机。下面以 CSICO 2950 为例说明如何开启 SNMP 服务。

(1) 进入特权模式

输入下列命令：

```
Switch>enable[回车]
```

“Switch>”是系统自动出现的提示符，不是用户输入的字符串。当系统提示输入交换机特权密码时，输入交换机特权密码并回车。此时交换机的提示符自动变为“Switch#”。

(2)　进入全局配置模式

在交换机提示符后，键入下列命令：

```
Switch#configure terminal[回车]
```

此时交换机的提示符自动变为“Switch(config)#”。

(3) 配置交换机的读写共同体名

在交换机提示符后键入如下命令，将读写共同名设置为 private:

```
Switch(config)#snmp-server community private rw[回车]
```

“Switch(config)#”是交换机自动给出的提示符，不是用户输入的字符串。“private”是读写共同体名。详细信息如图 6-14 所示。

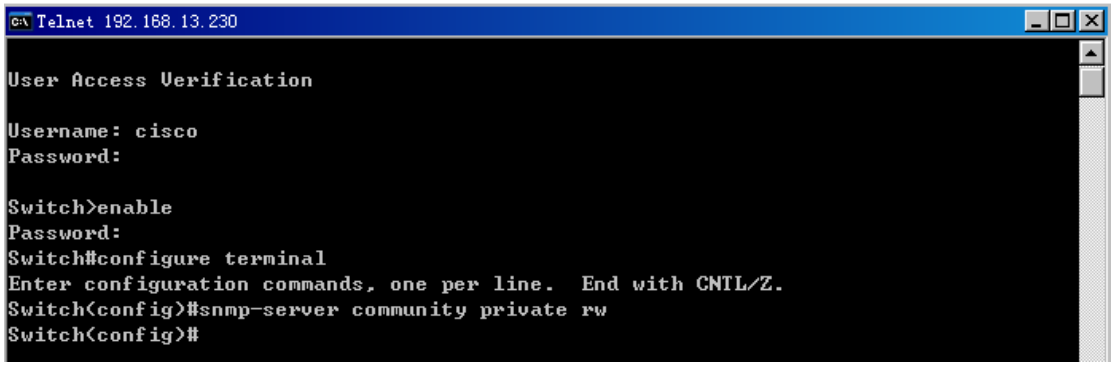


图 6-14　配置 cisco2950 的读写共同体名

2. 对于操作系统为 CatOS 的交换机

这类交换机是 CISCO 的高端型号交换机，下面以 CISCO6509 为例说明如何开启 SNMP 服务。

(1) 进入特权模式

输入下列命令：

```
Switch>enable[回车]
```

“Switch>”是系统自动出现的提示符，不是用户输入的字符串。当系统提示输入交换机特权密码时，输入交换机特权密码并回车。此时交换机的提示符自动变为“Switch<enable>”。

(2) 配置交换机的读写共同体名

在交换机提示符后键入如下命令，将读写共同名设置为 private:

```
Switch> <enable> set snmp community read-write-all private[回车]
```

“Switch> <enable>”是交换机自动给出的提示符，不是用户输入的字符串。“private”是读写共同体名。详细信息如图 6-15 所示。

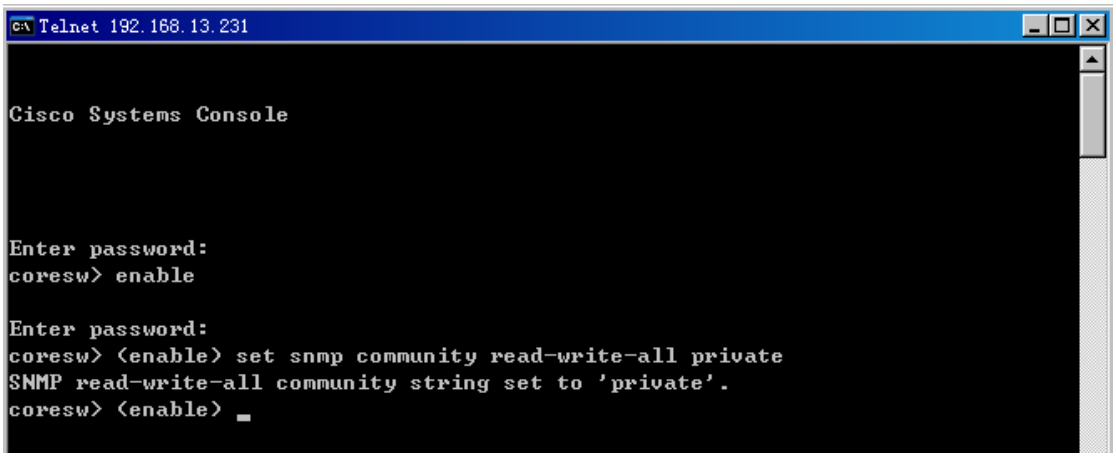


图 6-15　配置 cisco6509 的读写共同体名

3. 对于华为的交换机

下面以华为的 Quidway S2403H-EI 为例，说明如何开启 SNMP 服务。

(1) 进入特权模式

输入下列命令：

```
<Quidway>super[回车]
```

“<Quidway>”是系统自动出现的提示符，不是用户输入的字符串。当系统提示你输入交换机特权密码时，输入交换机特权密码并回车。

(2) 进入系统视图

输入下列命令：

```
<Quidway>system-view[回车]
```

此时交换机的提示符自动变为“[Quidway]”。

(3) 配置本交换机的写共同体名

在交换机提示符后键入如下命令，将读写共同名设置为 private:

```
[Quidway] snmp-agent community write private[回车]
```

“[Quidway]”是交换机自动给出的提示符，不是用户输入的字符串。“private”是读写共同体名。

(4) 配置交换机 snmp 版本

需将访问交换机的 snmp 版本跟内网安全扫描中配置的参数一致。如系统中配置的交换机版本为 v1，则应在交换机提示符后键入如下命令，将交换机 snmp 版本号设置为 v1:

```
[Quidway] snmp-agent sys-info version v1[回车]
```

注： 内网安全扫描中交换机 SNMP 版本号配置选项在参数设置对话框中，其版本默认为 v1。

(5) 如果是 3900 交换机，配置方式稍有不同，具体命令如下所示。

进入配置模式，并进入命令 snmp 然后配置。

(6) 配置本交换机的读写共同体名为 private

```
community read-write private[回车]
```

(7) 将交换机的 snmp 信息配置为允许写

```
writedisable off[回车]
```

详细信息如图 6-16 所示。

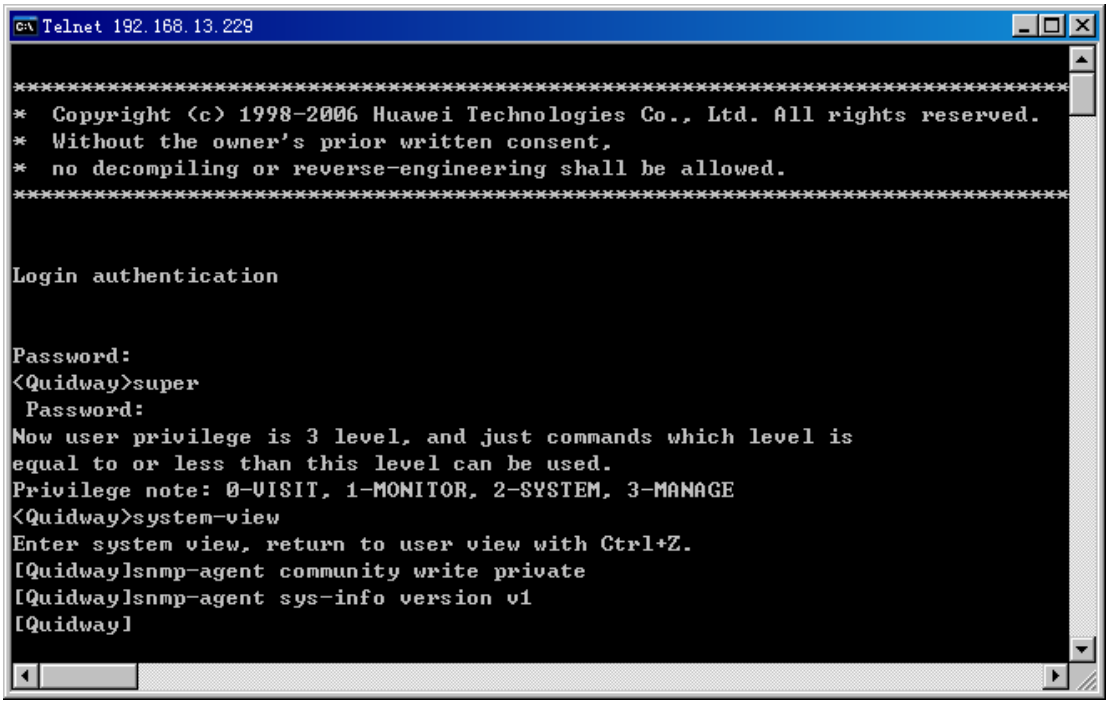


图 6-16　配置 Quidway S2403 的读写共同体名

第七章　响应与知识库管理

根据策略设置，把客户端产生的违规行为，按照危害程度的高低划分五个等级。从低到高，一级报警为一般警报，威胁程度最低；五级报警为严峻警报，威胁程度最高。可以设置警报归并方式，按时间间隔或累计数量报警一次。也可以设置警报处理方式，邮件报警、短信报警或声音报警。

7.1 知识库管理

7.1.1 报警类型定义

1. 单击“响应与知识库”，进入“知识库管理”界面，如图 7-1 所示。在左边的警报类型中，任选一项设置报警。例如：点选“失泄密防护”→“应用层”→“FTP”，单击右下方的“编辑”按钮，进入编辑页面。

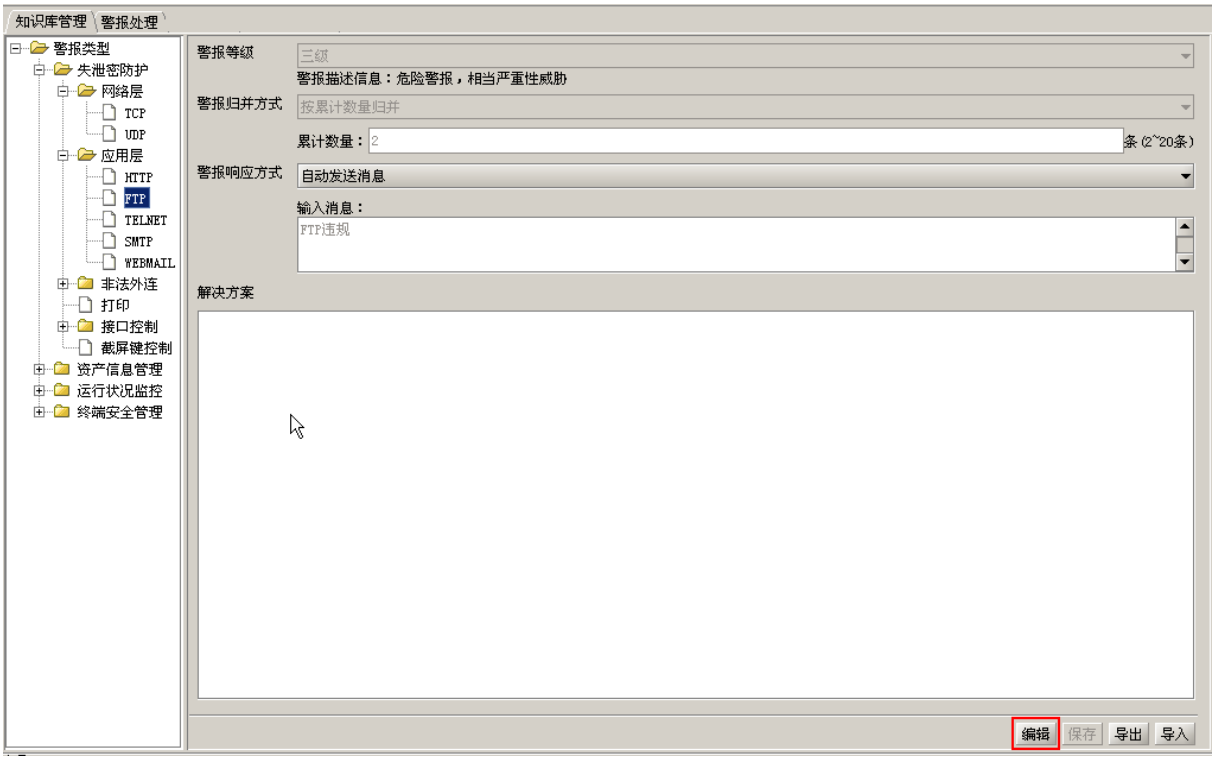


图 7-1　警报处理知识库管理

2. 在如图 7-2 所示“知识库管理”页面中，单击“警报等级”下拉框，根据危害程度选择报警等级（一级~五级）；单击“警报归并方式”下拉框，根据需要设置归并方式。如果选择“按时间间隔归并”或“按累计数量归并”，还要输入间隔时间和累计数量；单击“警报响应方式”下拉框，如果选择“自动发送消息”，就要在下面框中输入消息具体内容；在解决方案中，输入具体措施、方法。

全部输入完成后，单击右下方的“保存”按钮保存。也可以将知识库导出为*.xml 文件保存，需要时再导入进来。

设置说明见下表:

报警等级	一级	一般警报，最低程度性威胁。
	二级	警戒警报，一般性威胁。
	三级	危险警报，相当严重性威胁。
	四级	危机警报，对重要安全设备，安全信息已构成严重威胁。
	五级	严峻警报，为最高级别警报。对绝密信息已构成严重威胁，或对重要安全设备、安全信息威胁已发生。
归并方式	未定义	对报警不进行归并，全部发送给服务器。
	全部忽略	对所有报警均忽略不报。
	按时间间隔归并	对报警信息进行归并，按照设置时间，多长时间报警一次(1 分钟～60 分钟)。
	按累计数量归并	对报警信息进行归并，按照累计数量，达到多少条报警一次(2～20 条)。
响应方式	未定义	向服务器发送报警信息。
	自动发送消息	自动向控制台发送报警信息。

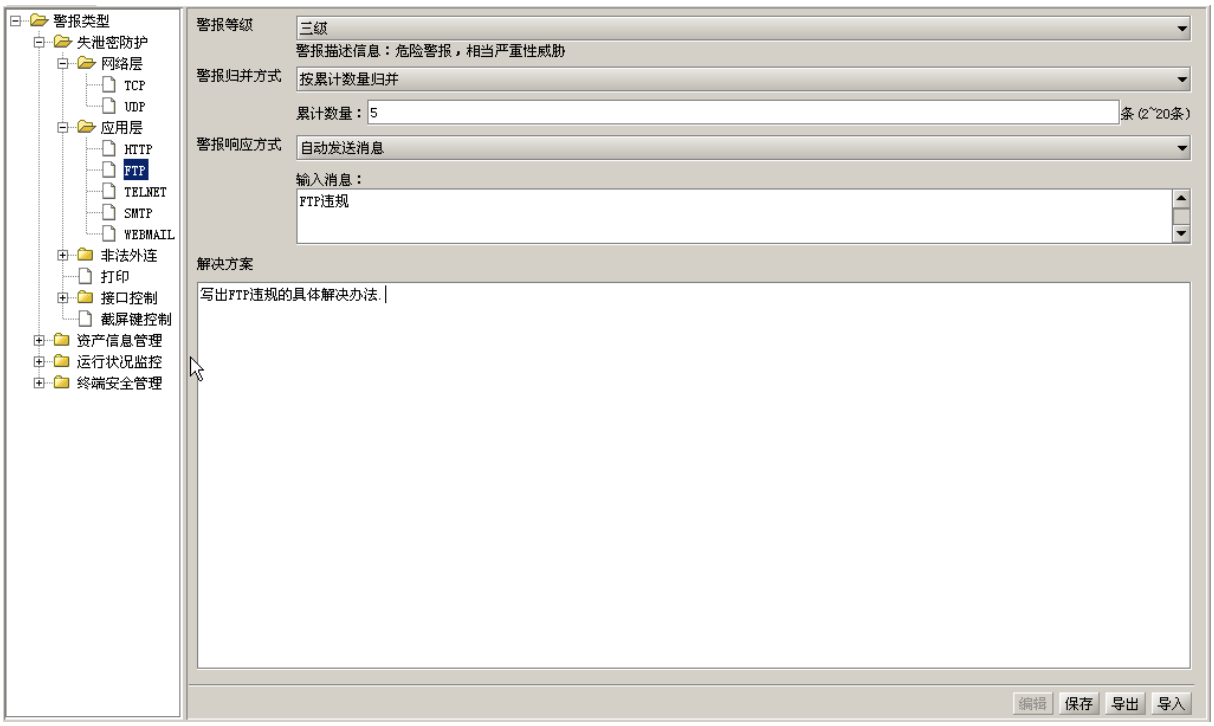


图 7-2　设置报警方式

提示：警报类型中其它各子项设置，与上面 FTP 报警设置相同，这里不再一一详述。

7.1.2 配置信息定义

7.1.2.1 订阅邮件报警

订阅邮件报警需要以下三个方面的设置：

（1）配置 SMTP 服务器

以系统管理员用户（默认 admin）登录控制台，单击“系统参数设置”→“服务器端参数配置”→“SMTP 服务器配置”，进入 SMTP 服务器配置界面，如图 7-3 所示。

在“SMTP 邮箱配置”中配置 SMTP 服务器地址以及账户信息，并检查输入的有效性。在“SMTP 邮箱测试”中，用户可以输入一个保证能收到邮件的地址以及邮件内容，测试是否能收到 SMTP 服务器发送的测试邮件，检测配置是否成功。系统会给出检测成功与否的提示。

图 7-3　配置 SMTP 服务器

（2）修改个人信息

单击控制台菜单“设置”→“修改个人信息”，或者按“Ctrl+Alt-u”快捷键，出现修改个人信息界面，如图 7-4 所示。输入邮箱地址和手机号，测试通过后，服务器会按警报设置类型，向这里设置的邮箱地址或者手机号码，发送测试邮件或者短信。

图 7-4　修改个人信息

（3）订阅邮件报警

以系统操作员身份登录控制台，单击“响应与知识库”→“知识库管理”→“配置信息定义”→“订阅邮件报警”，进入邮件报警类型设置界面，如图 7-5 所示。选择要订阅的邮件警报类型和等级，并设置邮件发送频率，最后，单击“应用”按钮。

“**设置邮件发送频率**”，有三种形式：

实时发送：每产生一条警报就发送一封邮件。

按时间间隔发送：设置时间间隔发送所有订阅的未处理警报的汇总信息，另外，用户还可以通过勾选下方的复选框来设置发送警报的明细信息。

每日定时发送：设置每日固定时间发送所有订阅的未处理警报的汇总信息，另外，用户还可以通过勾选下方的复选框来设置发送警报的明细信息。

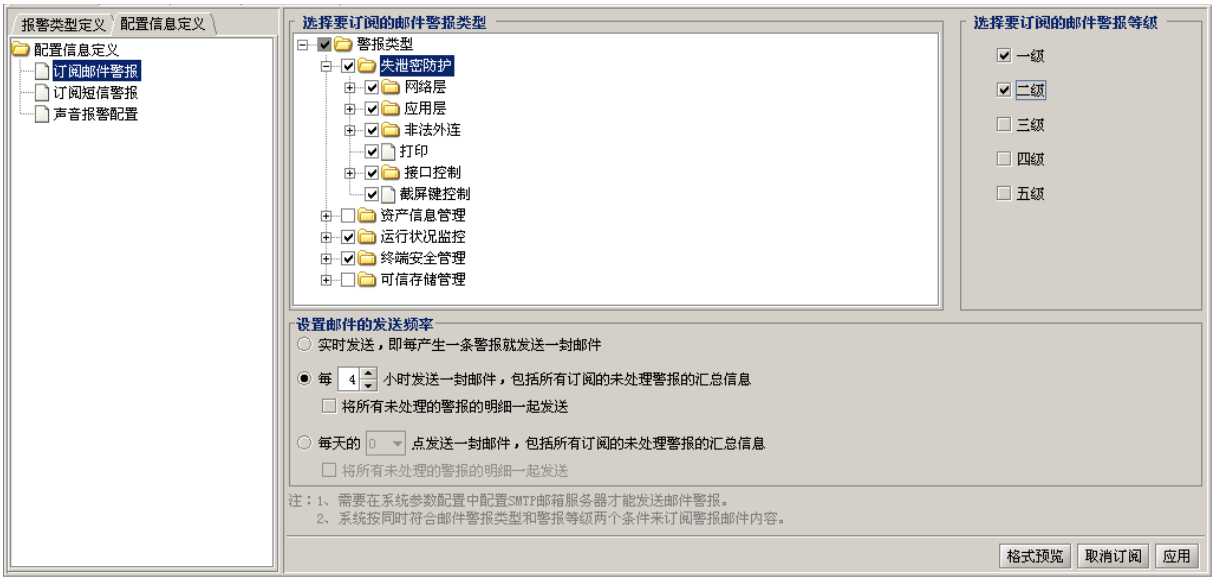


图 7-5　选择要订阅的邮件警报类型

7.1.2.2 订阅短信报警

订阅短信报警需要以下三个方面的设置：

（1）短信网关配置

以系统管理员用户（默认 admin）登录控制台，单击“系统参数设置”→“服务器端参数配置”→“短信网关配置”，进入短信网关配置界面，如图 7-6 所示。

在“短信网关配置”中输入短信中心号码，并通过下拉框选择串口。在“短信网关测试”中，用户可以输入一个保证能收到短信的号码及短信内容，测试是否能收到短信中心发送的短信，检测配置是否成功。系统给出检测成功与否的提示。

提示：输入短信中心号码时，需要咨询本地通信运营商，各地的号码可能不一样。北京移动的是 13800100500，北京联通的是 13010112500。

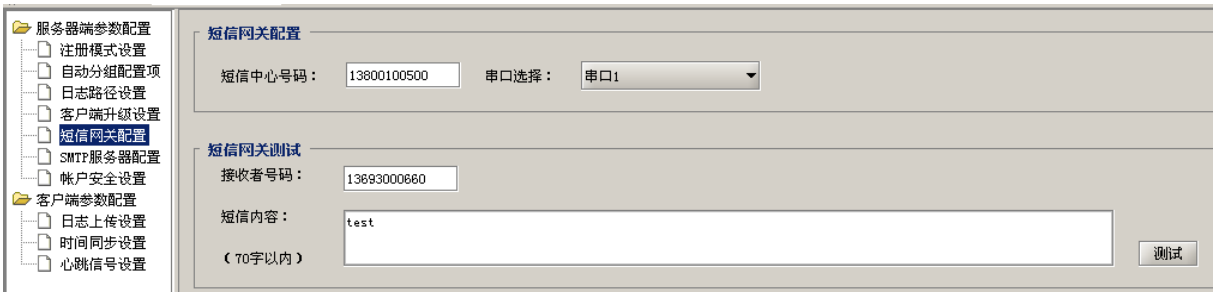


图 7-6　配置 SMTP 服务器

（2）修改个人信息

请参考前面修改个人信息操作。

（3）订阅短信报警

以系统操作员身份登录控制台，单击“响应与知识库”→“知识库管理”→“配置信息定义”→“订阅短信报警”，进入短信报警类型设置界面，如图 7-7 所示。选择要订阅的短信警报类型和等级，并设置短信发送频率，最后，单击“应用”按钮。

“**设置短信发送频率**”，有三种形式：

实时发送：每产生一条警报就发送一条短信。

按时间间隔发送：设置时间间隔发送所有订阅的未处理警报的汇总信息，另外，用户还可以通过勾选下方的复选框来设置发送警报的明细信息。

每日定时发送：设置每日固定时间发送所有订阅的未处理警报的汇总信息，另外，用户还可以通过勾选下方的复选框来设置发送警报的明细信息。

“**短信格式预览**”：当左侧“设置邮件的发送频率”的选择变化时，短信内容的格式也随之变化。

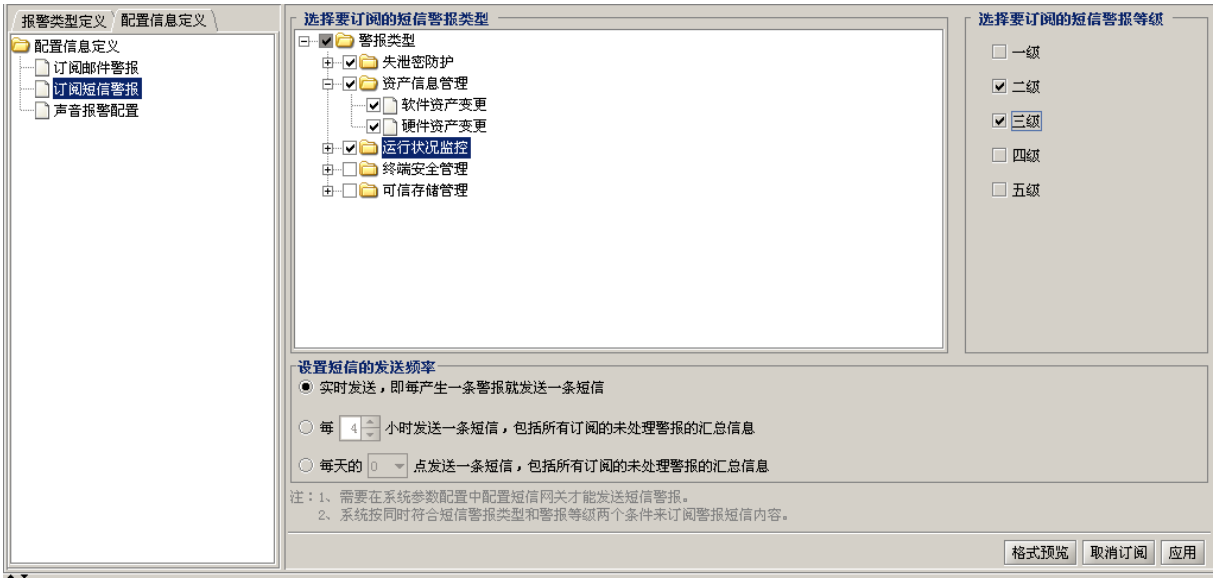


图 7-7　选择短信报警类型

7.1.2.3 订阅声音报警

以系统操作员身份登录控制台，单击“响应与知识库”→“知识库管理”→“配置信息定义”→“订阅声音报警”，进入声音报警配置界面，如图 7-8 所示。

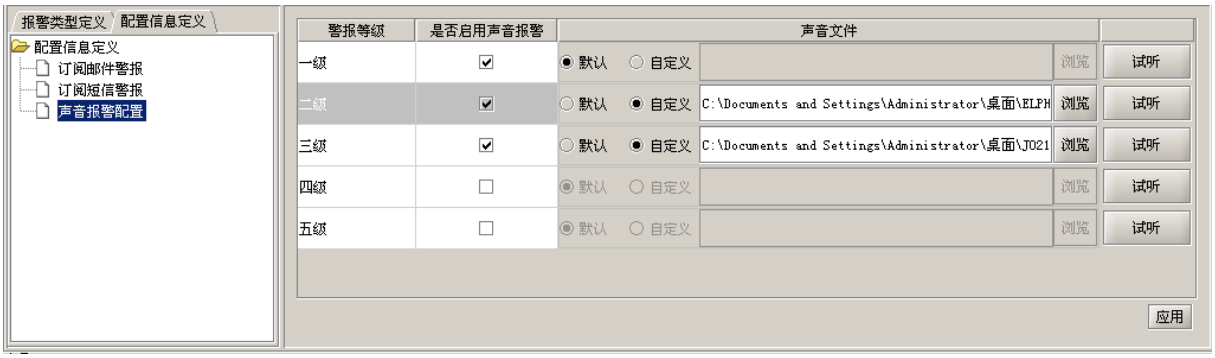


图 7-8　声音报警配置

“警报等级”列表示警报的五个级别；用户可勾选“是否启用声音报警”来订阅声音报警。勾选“是否启用声音警报”列，则“声音文件”列可供编辑，否则禁止用户编辑。

启用声音报警的情况下，有两种配置声音报警的方式：默认和自定义。用户可以单击“浏览”按钮，导入本地*.wav 文件，作为自定义声音文件。

最后，单击“应用”按钮，将配置信息保存至..\conf\AlarmSound.xml 文件。如果发生报警时，无意将本地自定义的声音文件删除，系统会做出判断，播放系统默认的声音。

7.2 警报处理

1．在响应与知识库管理界面，单击“警报处理”选项卡，或者双击控制台下面的小图标警报，都可以进入警报处理界面。根据用户需要设置查询条件，单示刷新查询结果列表，如图 7-9 所示。

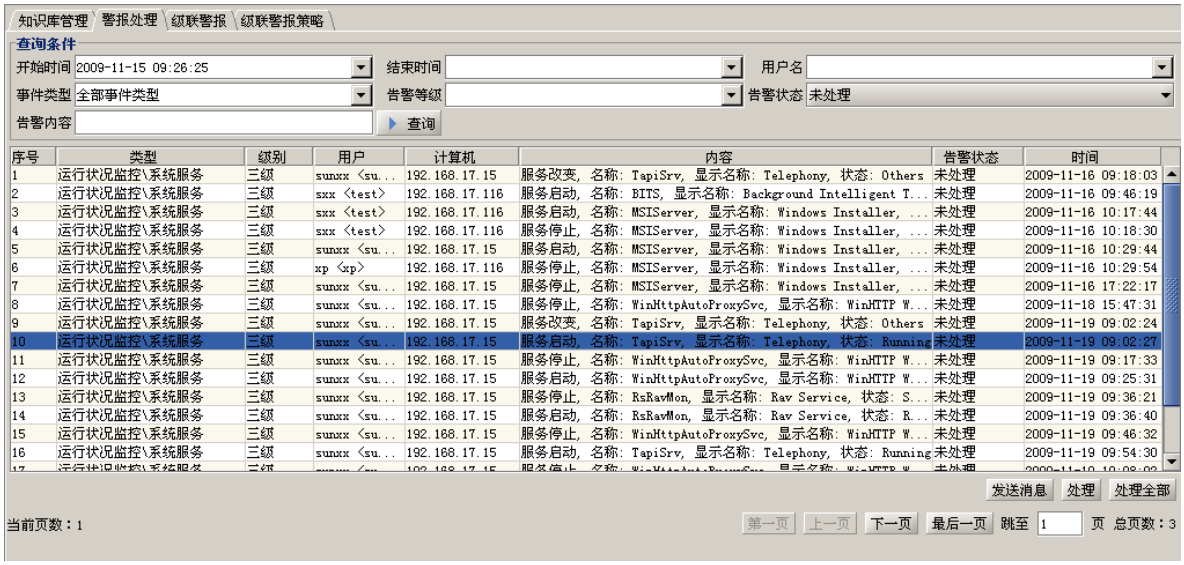


图 7-9　未处理报警信息列表

2．在报警信息列表中，任选一条“未处理”报警，单击“处理”按钮，即可将该类“未处理”警报全部变成“已处理”状态，如图 7-10 所示。

提示：选取某条信息做处理时，将对字段值（用户、计算机、类型、内容、告警状态）相同的报警一起处理，方便用户处理大量的相同报警。

序号	类型	级别	用户	计算机	内容	告警状态	时间
1	运行状况监控\系统服务	三级	sxx <test>	192.168.17.116	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-16 09:17:50
2	运行状况监控\系统服务	三级	sunxx <su...	192.168.17.15	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-16 09:18:05
3	运行状况监控\系统服务	三级	sunxx <su...	192.168.17.15	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-17 08:55:29
4	运行状况监控\系统服务	三级	sxx <test>	192.168.17.116	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-18 08:54:03
5	运行状况监控\系统服务	三级	sunxx <su...	192.168.17.15	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-18 08:54:15
6	运行状况监控\系统服务	三级	sunxx <su...	192.168.17.15	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-19 09:02:27
7	运行状况监控\系统服务	三级	sunxx <su...	192.168.17.15	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-19 09:54:30
8	运行状况监控\系统服务	三级	sunxx <su...	192.168.17.15	服务启动, 名称: TapiSrv, 显示名称: Telephony, 状态: Running	已处理	2009-11-20 14:27:11

图 7-10　已处理报警信息列表

3．在报警信息列表中，任选一项双击，进入报警信息处理界面，如图 7-11 所示。用户可以单击“处理”按钮，处理当前的报警信息。该条信息被处理后变成“已处理”状态；用户也可以单击“编辑”按钮，设置警报处理方式。设置完成后，单击“保存”按钮保存。

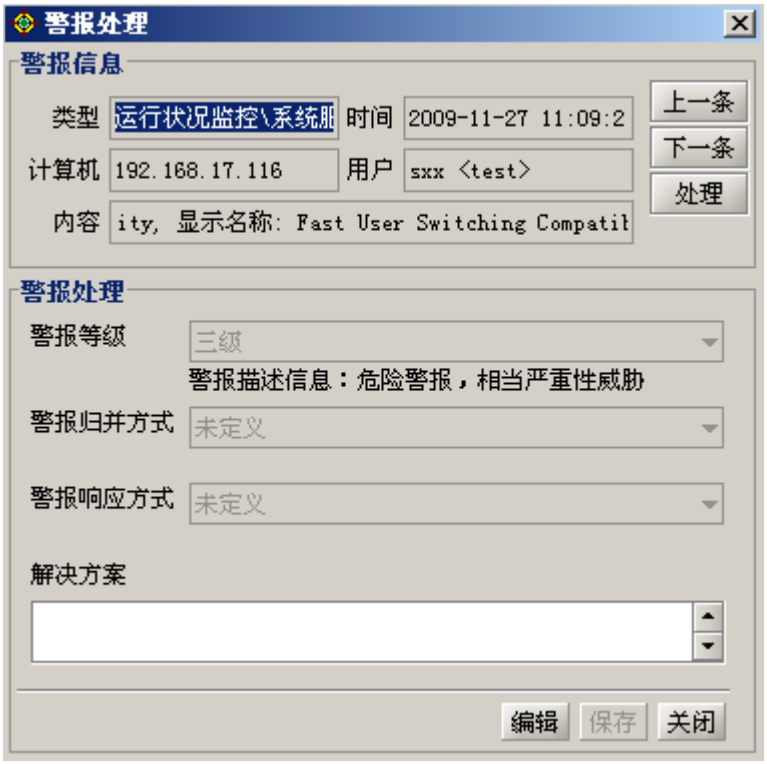


图 7-11　报警处理

3．在报警信息列表中任选一项，单击“发送消息”按钮，进入远程消息页面，如图 7-12 所示。输入信息后，单击“发送”按钮，即可发送给客户端。


远程消息
计算机SUPERSTAR[192.168.13.68]-[WD-WMAM9P8...
使用者feigj [feigj]
在此输入消息内容
发送
关闭

图 7-12　远程消息

第八章　统计审计分析

统计审计分析是对报警信息、客户端日志信息、软硬件资产信息、安全文档、可信移动介质和策略使用情况进行统计审计，支持按时间、用户名、类型等条件查询，也可根据用户需要设置过滤条件、选择要显示的某些列，以及对某些项进行具体分析等。

各个模块的使用方法一样，下面以告警信息统计为例，来说明使用方法。因为我们查询的数据量比较小，在“偏好设置”中不勾选“点击查询按钮才开始查询操作”，这样用户在左侧目录树中选择要查询的日志项，右侧将直接展示查询结果。参见偏好设置章节。

8.1　一般查询方法

1. 以审计员角色用户登录控制台，单击“统计审计分析”，进入统计审计分析界面。在左边的功能选择树中，选择“告警信息统计”，可以看到所有告警信息的列表，如图 8-1 所示。

告警事件详细记录了用户所属组织、用户名、计算机所属组织、计算机名、计算机 IP、警报类型、警报等级、发生时间、是否处理、具体内容等，请用户注意查看。

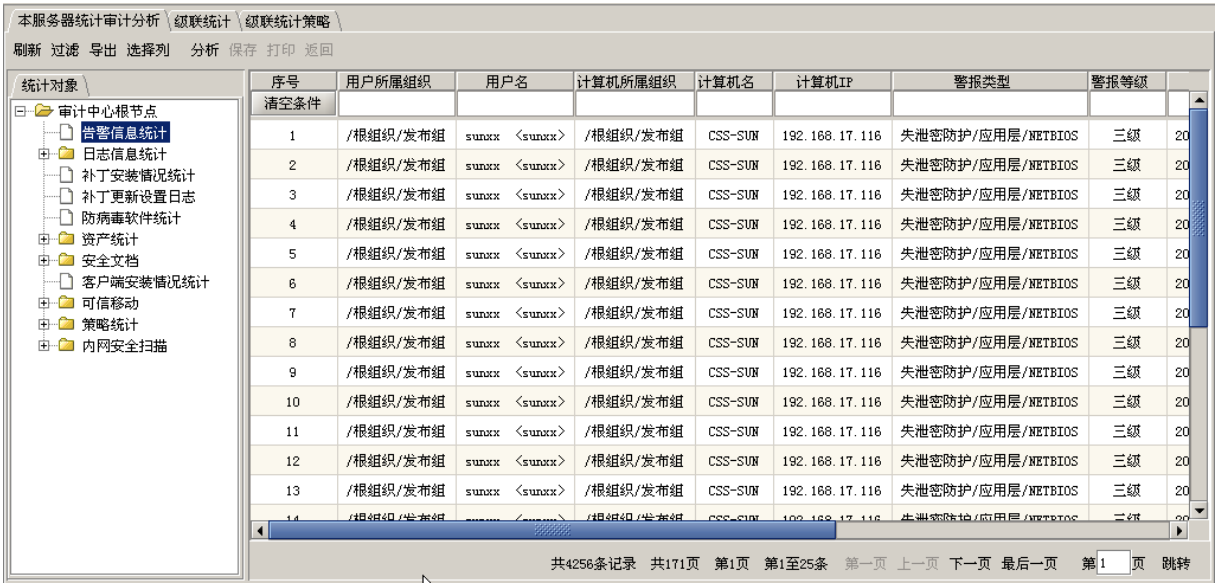


图 8-1　告警信息列表

提示：默认列表为所有告警事件。如果列表项下面为空白框，点击空白框中的浏览按钮，可以有条件筛选告警信息；如果列表项下面选择框被灰掉，表示不可选，即不能按该条件过滤告警信息。

2. 单击“用户名”下面的空白框，再单击空白框中的浏览按钮，弹出设置“用户名”条件框。根据需要勾选要查看的用户，单击“确定”按钮后，列表中只显示选定用户的告警事件，如图 8-2 所示。

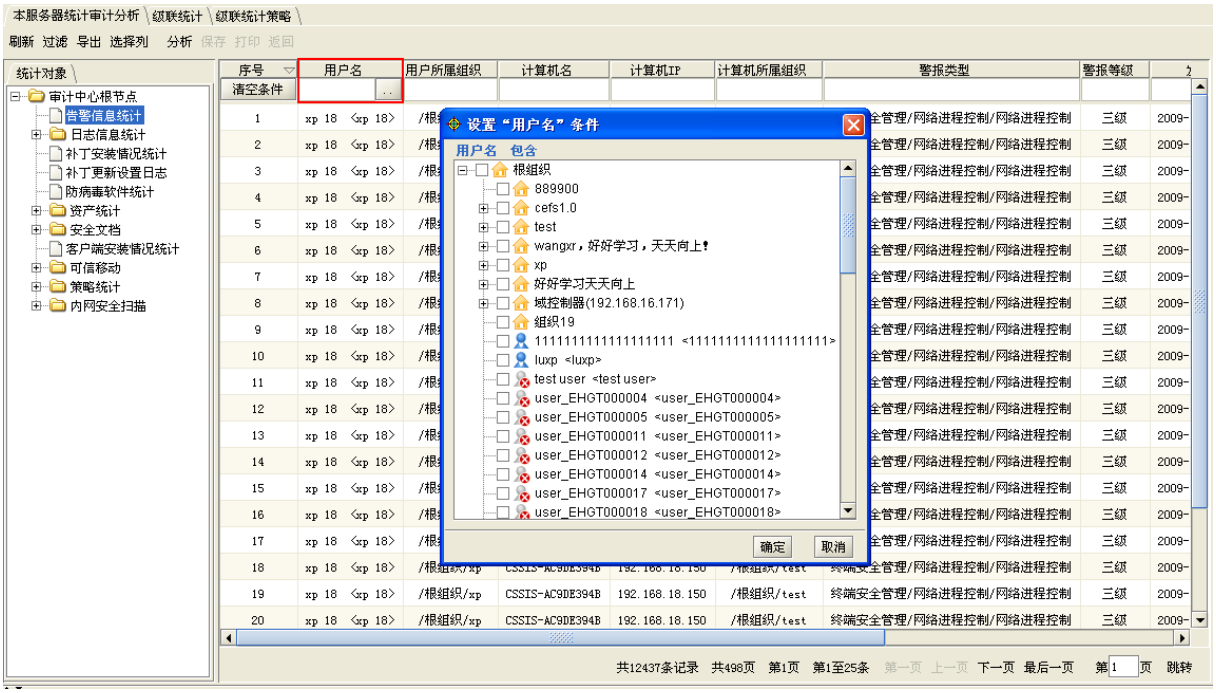


图 8-2　选择告警事件“用户名”

3. 单击“计算机 IP”下面的空白框，再单击空白框中的浏览按钮，弹出设置“计算机 IP”条件框。根据需要选择要查看的 IP 地址范围，单击“确定”按钮后，列表中只显示选定计算机 IP 范围内的告警事件，如图 8-3 所示。

图 8-3　选择告警事件“计算机 IP”

4. 单击“警报类型”下面的空白框，再单击空白框中的浏览按钮，弹出设置“警报类型”条件框。根据需要选择要查看的警报类型，单击“确定”按钮后，列表中只显示选定警报类型的的告警事件，如图 8-4 所示。

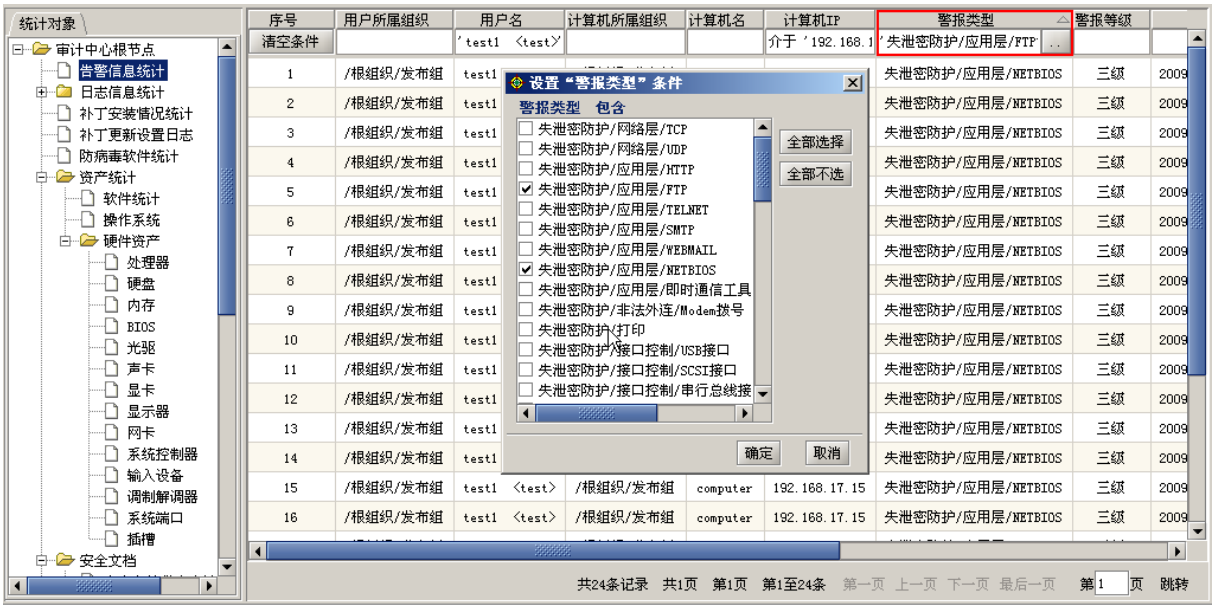


图 8-4　选择告警事件“警报类型”

5. 单击“警报等级”下面的空白框，再单击空白框中的浏览按钮，弹出报警等级选择框。根据需要选择要查看的告警等级（如三级），单击“确定”按钮后，列表中只显示告警等级为三级的告警事件，如图 8-5 所示。

图 8-5　选择告警等级

6. 单击“发生时间”下面的空白框，再单击空白框中的浏览按钮，弹出时间选择框。选择起止时间后，单击“确定”按钮，列表中将只显示选定时间段内的告警事件，如图 8-6 所示。

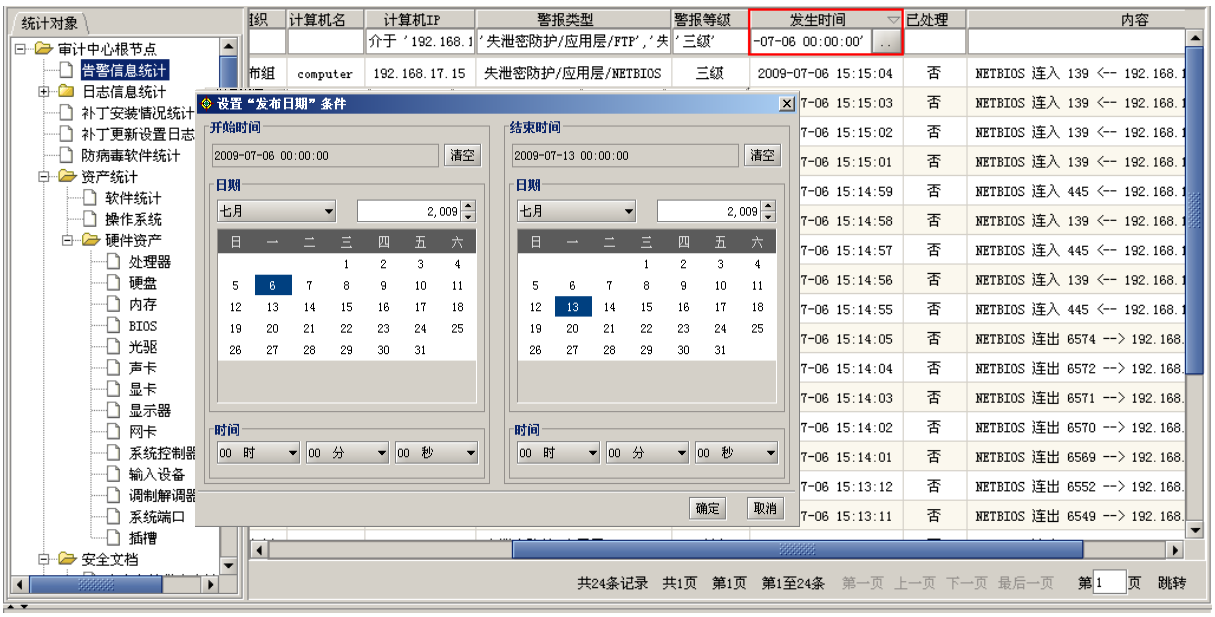


图 8-6　选择时间范围

7. 单击“已处理”下面的空白框，再单击空白框中的浏览按钮，弹出告警状态选择框。根据需要选择要查看的告警状态（如“否”），单击“确定”按钮后，列表中将只显示告警状态为“否”的告警事件，如图 8-7 所示。

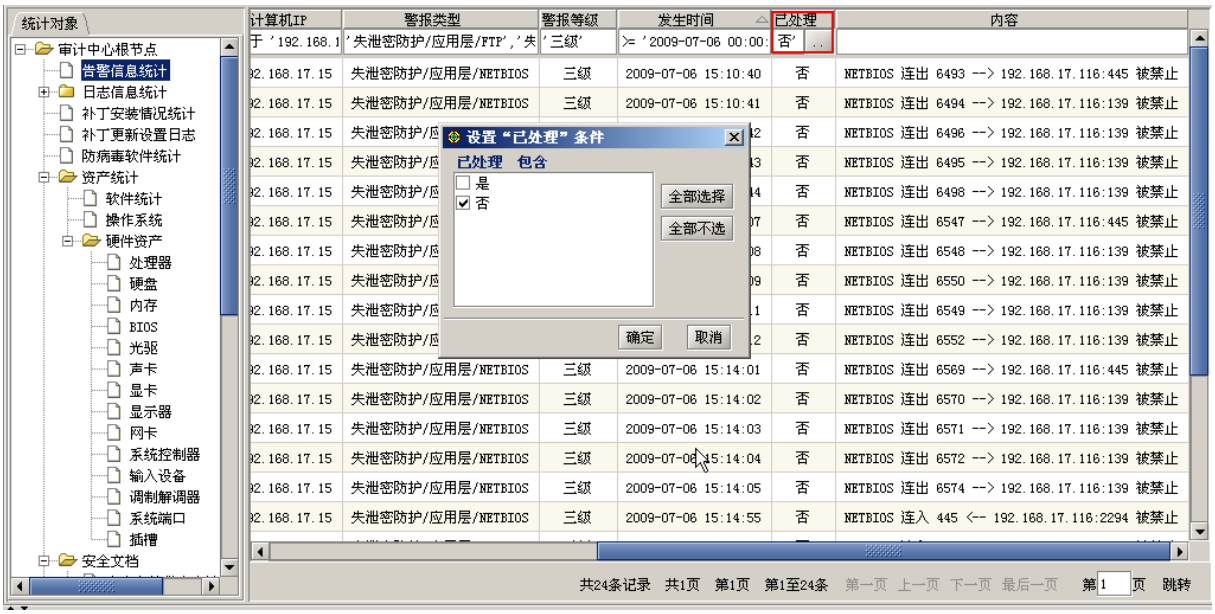


图 8-7　选择告警状态

8. 告警信息支持按内容查找。单击“内容”下面的空白框，再单击空白框中的浏览按钮，弹出内容输入框。如果我们输入“被禁止”三个字，单击“确定”按钮后，列表中将显示所有包含“被禁止”三个字的告警事件，如图 8-8 所示。

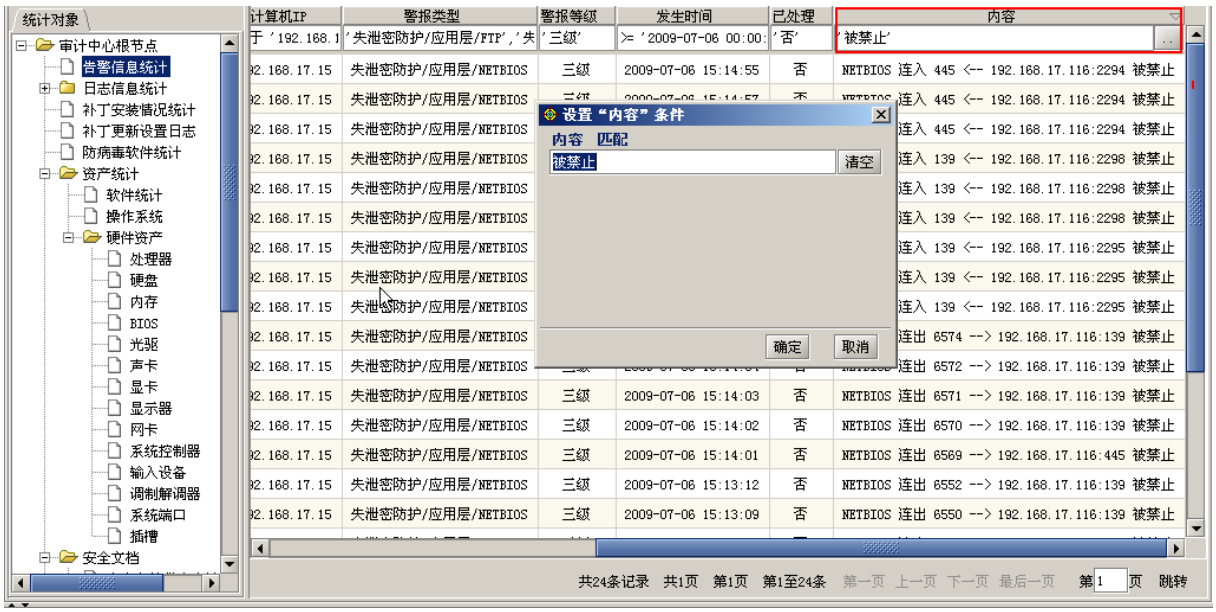


图 8-8　　选择告警内容

9. 我们可以同时设置几个查询条件，他们之间是“与”的关系。在告警事件列表中，单击下面的“上一页”、“下一页”或“跳到某页”，可以逐页查看。任选一列表项双击，可以查看详细信息，单击“上一条”，“下一条”，可以逐条查看，如图 8-9 所示。

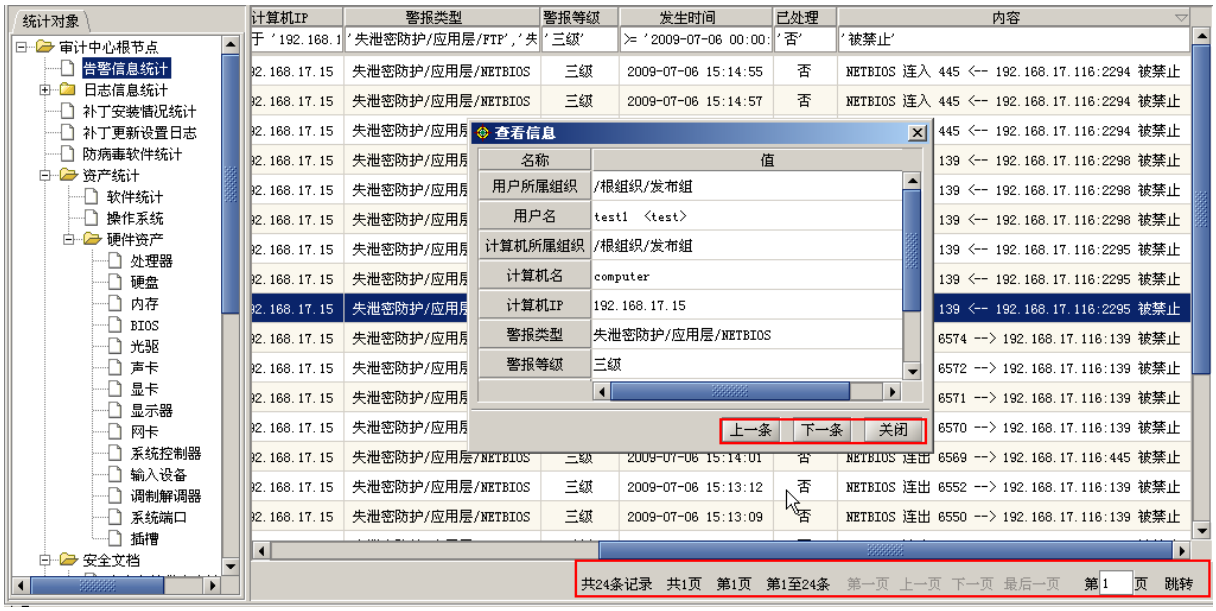


图 8-9　　告警事件详细信息

8.2　高级使用方法

“统计审计分析”界面中有一些功能项：过滤、选择列、导出、分析等，利用它可以方便用户操作，对统计数据做深入分析，如图 8-10 所示。

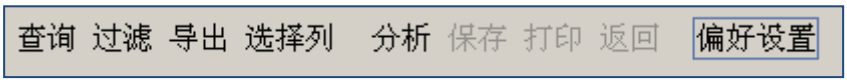


图 8-10　统计审计功能项

8.2.1　过滤

用户在查询过程中，可以根据自身的需要设置较复杂的查询条件，并将这些查询条件保存起来，便于下次查询。

（1）单击“过滤”按钮，出现过滤条件管理界面，如图 8-11 所示。单击过滤条件各选项后面的空白框，出现浏览按钮 ...，再单击浏览按钮选择查询条件。

图 8-11　选择过滤条件

（2）单击“确定”按钮，弹出按过滤条件筛选的列表信息，如图 8-12 所示。过滤条件可以自动保存。下次查询时，自动显示上次过滤条件的查询结果。

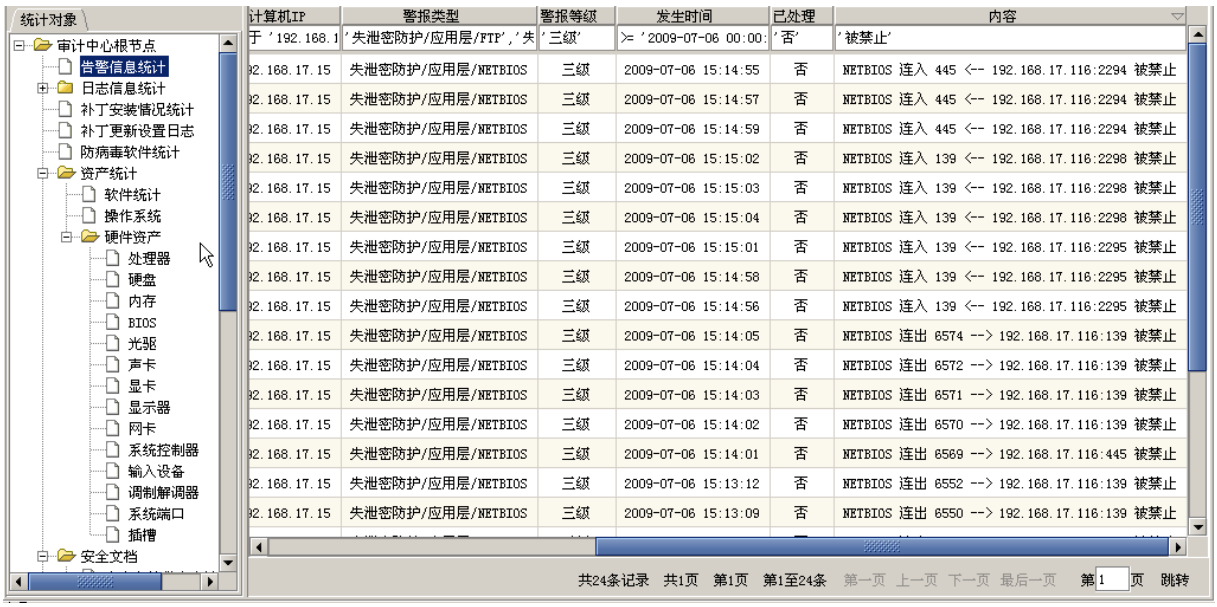


图 8-12　按过滤条件显示的列表信息

8.2.2　选择列

用户在查询结果显示窗中，可以自定义要显示的列表项，不必按系统提供的默认列显示。

例如：在上面的告警信息统计界面中，单击“选择列”按钮，出现选择列界面，如图 8-13 所示。勾选要显示的列，单击“确定”按钮退出。

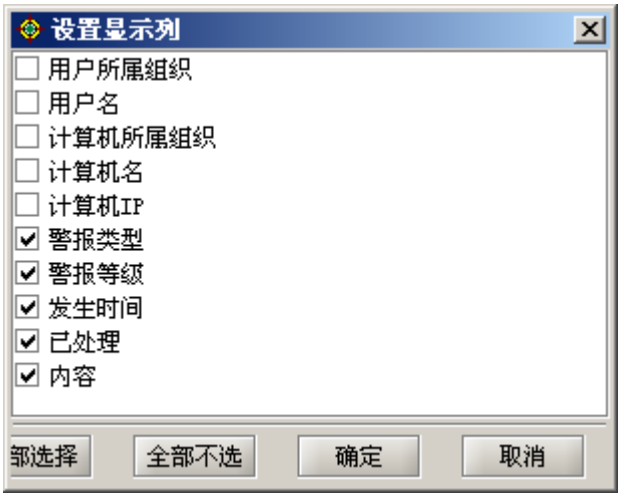


图 8-13　选定列界面

重回到告警信息统计界面中，可看到没有勾选的列不再显示，列表中只显示选定的列，如图 8-14 所示。“选择列”也有自动保存功能，下次再查询告警信息统计时，自动显示上次选择列内容。

图 8-14　列表中只显示选定列

8.2.3　导出

单击“导出”按钮，可以将当前节点下的所有数据导出为*.XLS、*.HTML、*.PDF 格式的文件，方便用户带出使用，如图 8-15 所示。如果日志数据量比较大（超过 5000 条），系统会自动分多个文件导出。

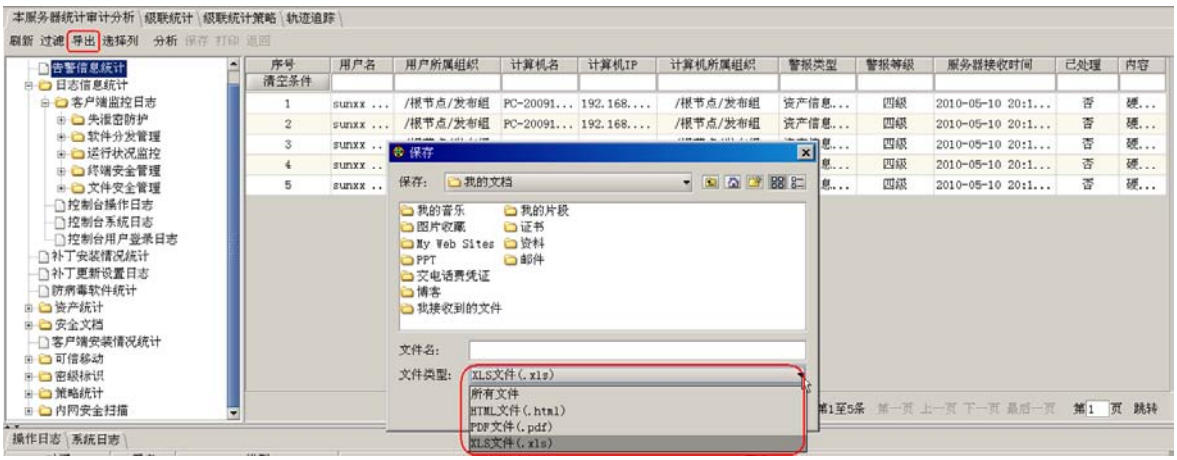


图 8-15　导出 XLS 文件

8.2.4　分析

（1）在告警信息统计页面中，单击“分析”按钮，进入分析界面，如图 8-16 所示。分析页面有五种视图显示方式：汇总表、对比图、排序图、趋势图和频率图，用户根据需要选择。

图 8-16　告警信息分析——汇总表

（2）单击表格中的蓝色数字（如：125），可以查看详细信息，如图 8-17 所示。

图 8-17　告警信息分析——详细信息

（3）单击“X 轴”和“分组”下拉框，选择警报类型、用户名、计算机名、警报等级、计算机 IP 等，可以得到不同类型的汇总表。在不同的统计审计模块中，“X 轴”和“分组”选项不同，如图 8-18 所示。

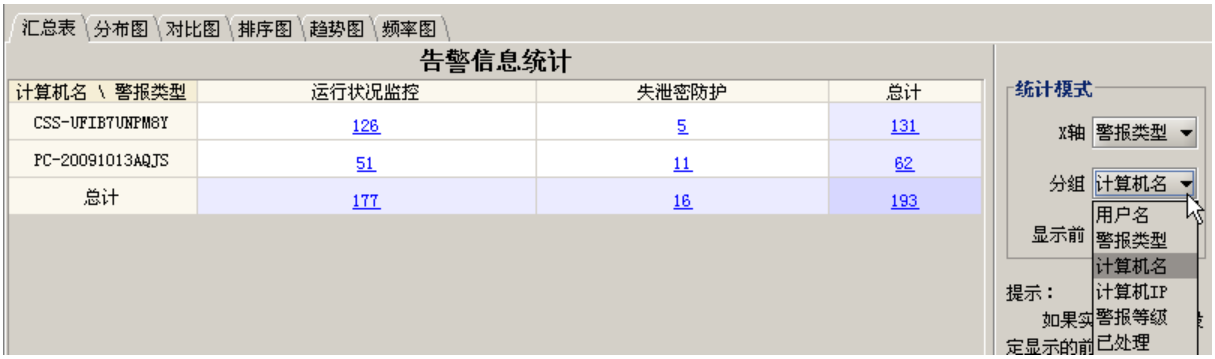


图 8-18　选择 X 轴和分组

（4）单击“分布图”标签页，进入分布图显示页面，如图 8-19 所示。此分布图是按警报类型构成的，不同的颜色代表不同的警报类型。单击“X 轴”下拉框，选择不同的选项，可以得到不同的分布图。单击不同的颜色部分，也可以进入不同的详细信息列表。

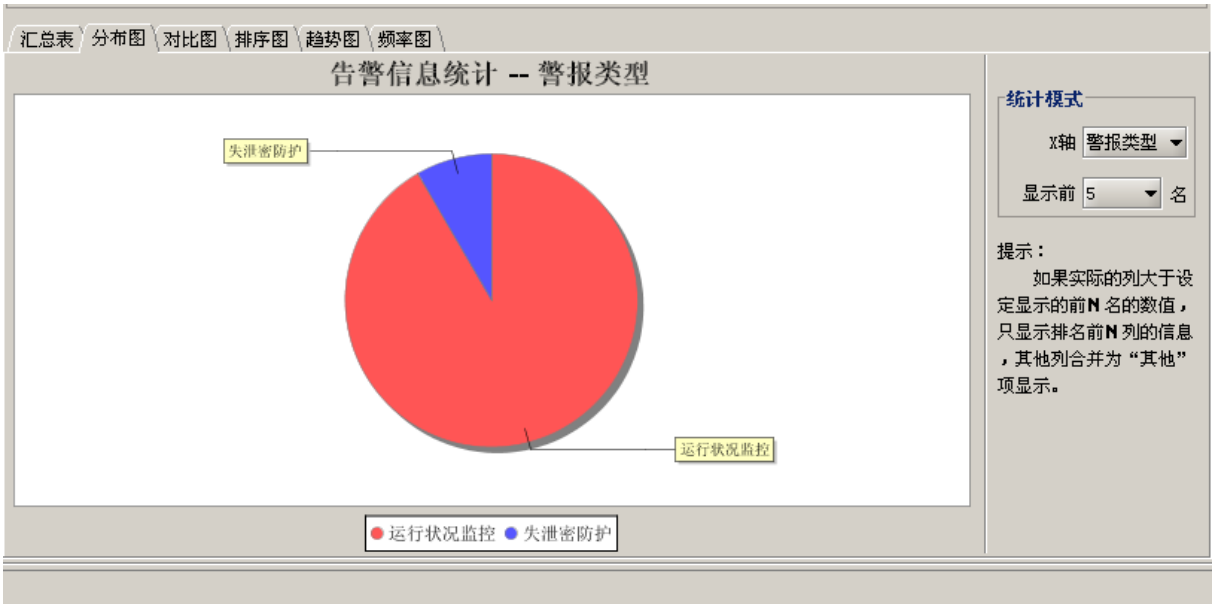


图 8-19　告警信息分析——分布图

（5）单击“打印”选项，可以将饼图打印输出。单击“保存”选项，可以将饼图保存成 PNG 格式的图像，存放在本地，如图 8-20 所示。

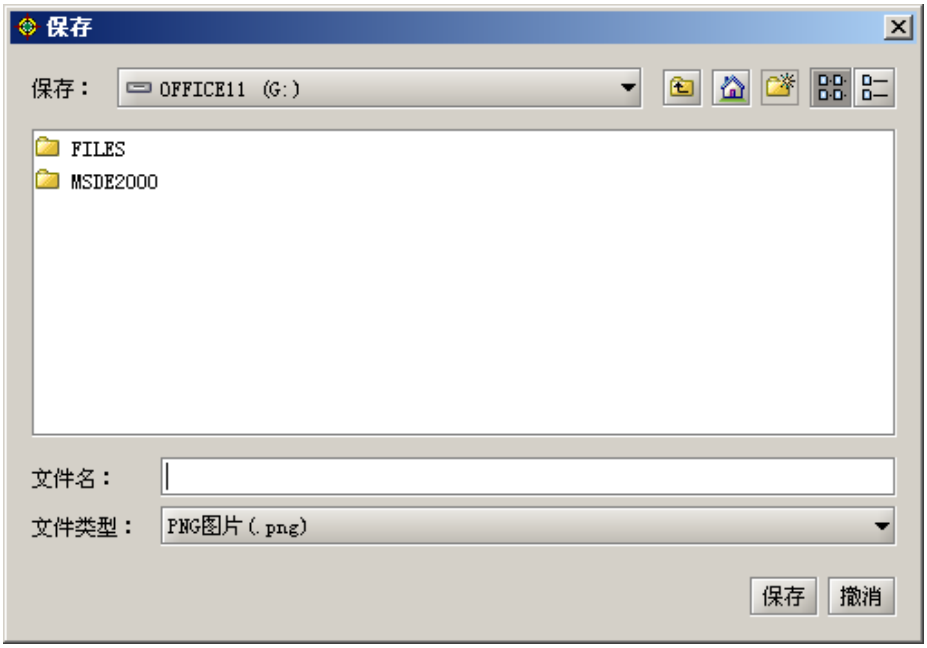


图 8-20　保存成 PNG 格式图片

（6）单击“对比图”标签页，进入对比图显示页面，如图 8-21 所示。可以按照用户需要生成不同的对比图，也可以打印或保存该对比图。

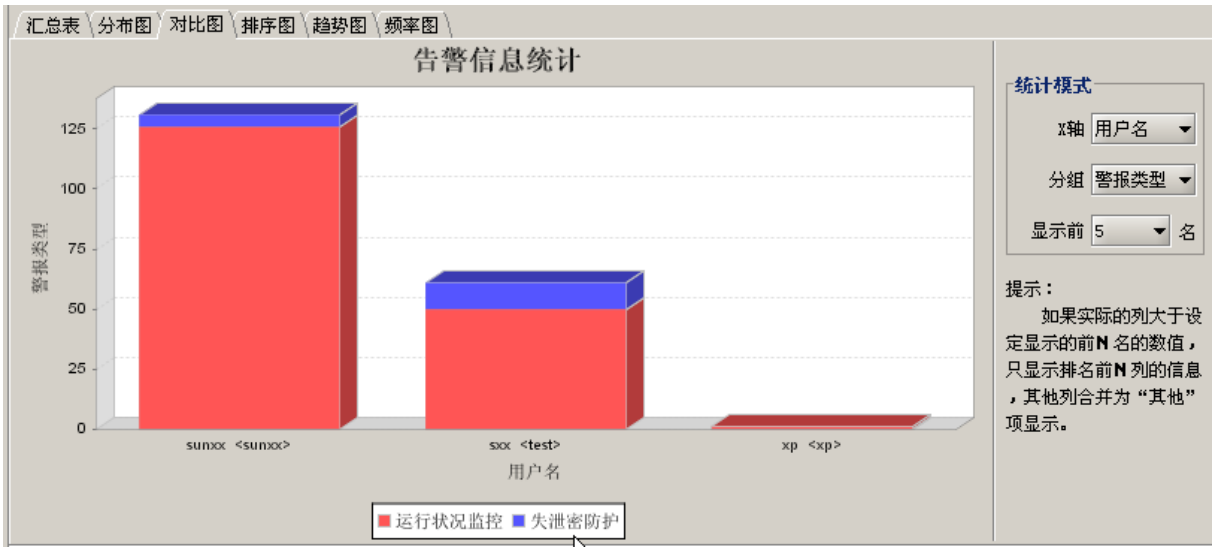


图 8-21　告警信息分析——对比图

（7）单击“排序图”标签页，进入排序图显示页面，如图 8-22 所示。

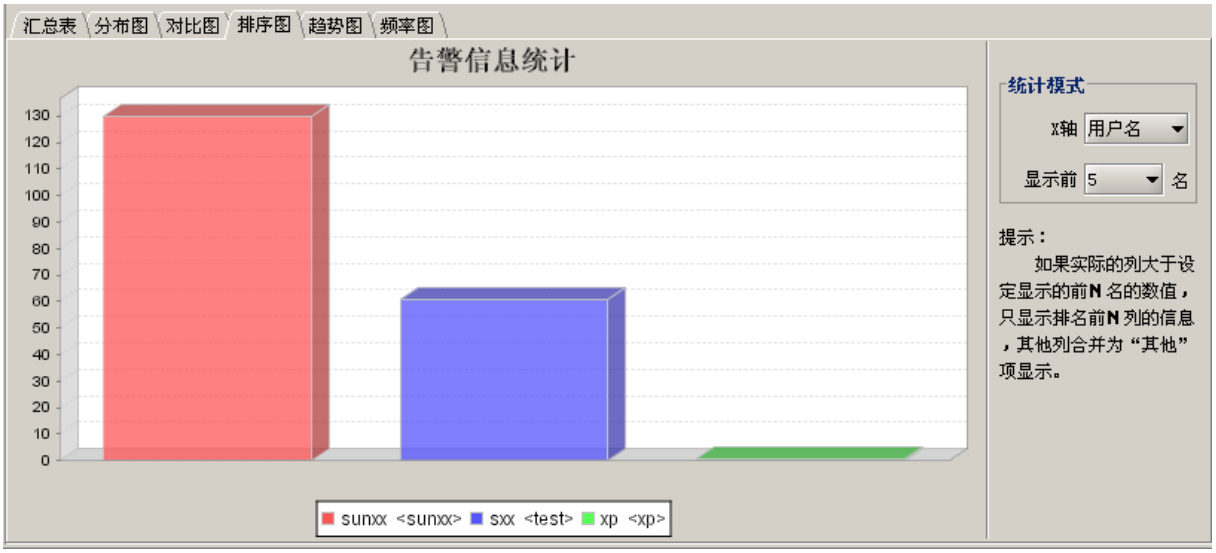


图 8-22　告警信息分析——排序图

（8）单击“趋势图”标签页，进入趋势图显示页面，如图 8-23 所示。

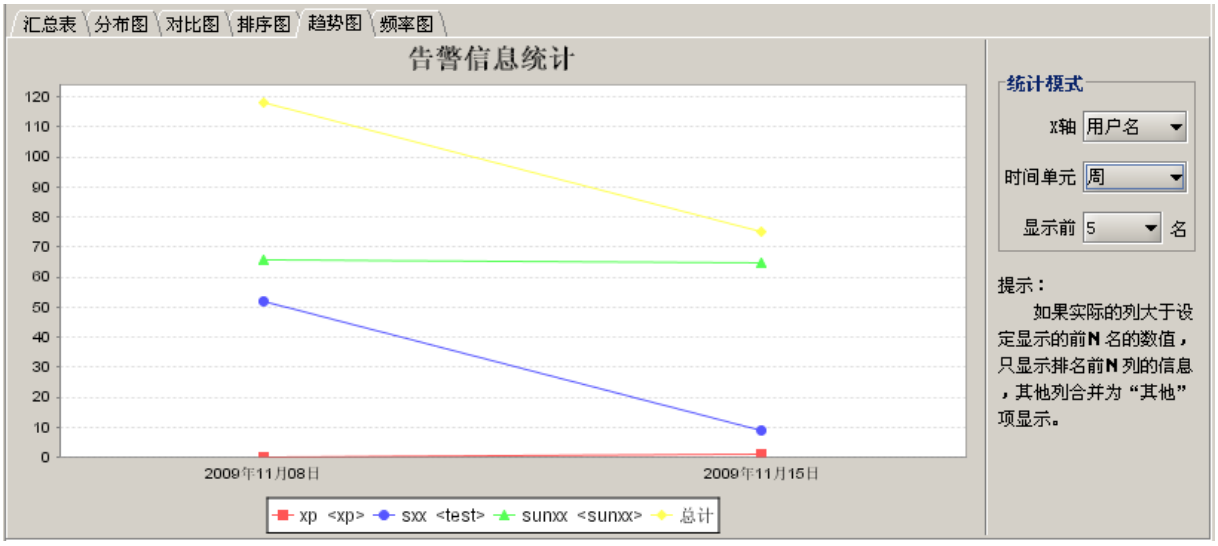


图 8-23　告警信息分析——趋势图

（9）单击“频率图”标签页，进入频率图显示页面，如图 8-24 所示

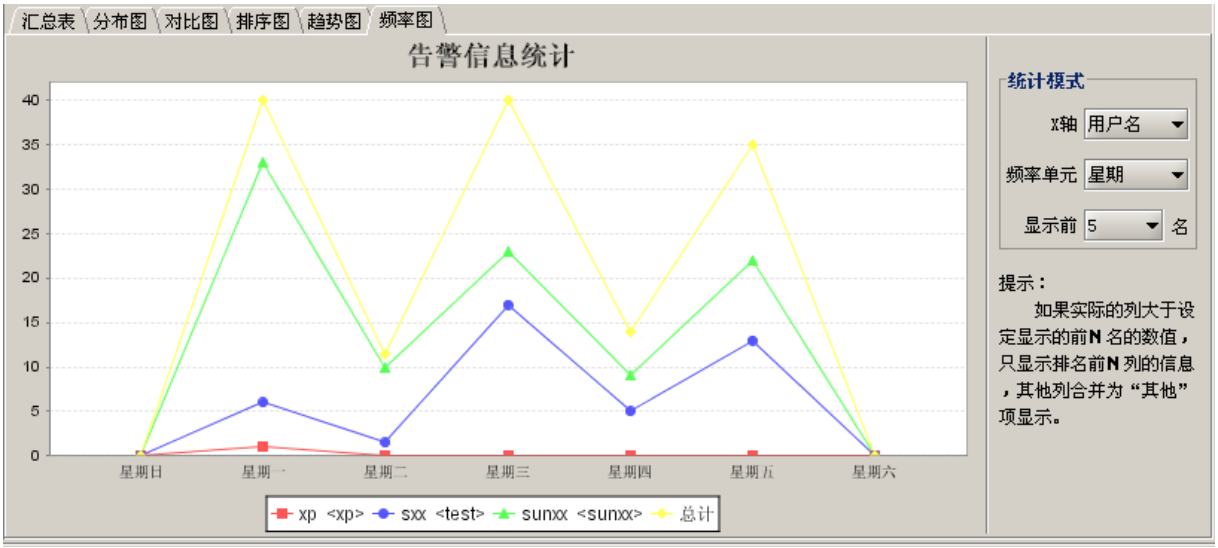


图 8-24　告警信息分析——频率图

8.2.5　偏好设置

点击“偏好设置”按钮，用户可以按自己的爱好设置查询方式，如图 8-25 所示。在统计审计分析中，如果在左侧目录树中选择要查询的日志项，右侧直接展示查询结果，这种查询方式在数据量达到千万级时容易出问题。所以，建议用户在数据量特大时勾选“点击查询按钮后才开始查询操作”，也就是说在左侧目录树中选定要查询的日志项，设置查询条件，点击“查询”按钮后，才在右侧展示查询结果。另外，也可以设置“记忆输入的查询条件”，下次查询相同的日志项时，不需要输入查询条件，自动显示上次的查询条件和查询结果。

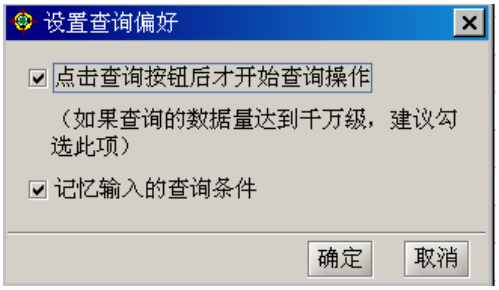


图 8-25　设置查询偏好

8.3　日志统计内容

8.3.1　日志信息统计

日志信息统计和告警信息统计的使用方法一样，这里不再详述。不同的地方在于：如果日志记录中有备份文件，点击右键可以下载。

根据用户下发的策略，会产生不同的日志信息，详细记录用户行为，供事后审计。在日志信息统计中，各日志项记录的内容不同，如下表：

分类		日志信息项	日志记录内容	备　注
失泄密防护日志	网络层	TCP 控制 UDP 控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、本地端口、远程 IP 地址、远程端口、方向、进程名。	
	应用层	HTTP 控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、远程 URL 地址、进程名称。	
		FTP 控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、FTP 服务器 IP、上传文件名、记录方式、备份文件路径。	如果有备份文件，单击右键可以下载。
		TELNET 控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、TELENT 目标 IP、进程名称。	
		SMTP 控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、发件人地址、收件人地址、邮件标题、进程名、备份文件路径。	如果有备份文件，单击右键可以下载。
		WEBMAIL 控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、进程名称。	
		NETBIOS	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、 发生时间、操作类型、文件名、进程名。	
		即时通信	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、通信工具类型、日志类型、附件名称列表。	

失泄密防护日志	非法外连	MODEM 拨号	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、拨号号码、事件类型、电话簿、提供商、进程名。	
	打印机	打印机	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、打印文件名、打印份数、打印页数、共享打印机、标题、打印机名称、打印机服务名称、打印端口、Windows 用户名、进程名、打印机类型。	如果有备份文件，单击右键可以下载。
		打印审批	申请者、申请者所在计算机、申请者所在计算机 IP、申请时间、审批员、审批员所在的计算机、审批员所在计算机 IP、审批时间、审批终止、审批通过、审批文件文件名、申请打印份数、剩余份数、有效打印开始时间、有效打印结束时间、是否有打印日志。	
	媒体介质	加密带出	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、操作类型、源文件名、目的文件名、控制类型、介质类型、进程 ID、进程名。	用户策略中对普通移动盘下发策略产生的日志
		记录带出	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、操作类型、源文件名、目的文件名、控制类型、介质类型、进程 ID、进程名、备份文件路径。	
		复制审批	审批单类型、申请者、申请者所在计算机、申请者所在计算机 IP、申请时间、申请原因、申请文件、介质、审批员、审批员所在的计算机、审批员所在计算机 IP、审批时间、审批完成、审批通过。	
软件分发管理		环境检测	任务名称、软件包名称、发生时间、计算机名、计算机 IP、计算机所属组织、操作系统、系统补丁、系统语言、IE 版本号、内存大小、缓冲区大小、环境监测结果。	
		软件包下载	任务名称、软件包名称、发生时间、计算机名、计算机 IP、计算机所属组织、下载结果。	
		软件包安装	任务名称、软件包名称、发生时间、计算机名、计算机 IP、计算机所属组织、安装结果。	
		软件分发任务审计	管理员名称、下发时间、计算机名、计算机所属组织、任务名称、软件包名称、计算机操作系统、软件包语言、软件包描述、软件包类型、环境检测结果、下载优先级、下载时间类型、下载开始时间、下载结果、安装类型、安装时间类型、安装开始时间、安装结果。	
运行状况监控		共享文件夹监控	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、变化类型、共享名、共享路径、共享描述。	
		文件操作	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、介质类型、操作类型、文件名、进程名。	因 Windows 驱动技术限制，文件操作日志记录可能不准确，有重复现象。

	用户变化	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、操作类型、Windows 用户名称、Windows 用户全名、Windows 用户描述。	
	组变化	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、操作类型、Windows 组名称、Windows 组描述。	
	系统服务	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、操作类型、服务名称、服务状态、显示名称。	
	客户端系统日志	计算机名、计算机 IP、计算机所属组织、事件 ID、日志源类型、日志类型、事件源、产生时间、写入时间。	
终端安全管理	客户端登录日志	计算机名、计算机 IP、计算机所属的组织、用户名、用户所属的组织、系统用户名、组名、事件类型、发生时间。	
	用户身份认证	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、登录时间、系统用户名、组名、日志发生时间。	
	网络进程控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、远程 IP 地址、远程端口、进程名。	
	网络服务控制	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、日志记录类型、监听端口、进程名。	
文件安全管理	文件加密 文件解密	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、共享模式、源文件名、目的文件名、文件后缀。	通过“安全文件加解密”产生的日志
	解密带出	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、发生时间、共享模式、源文件名、目的文件名、备份文件。	解密到移动介质产生的
	文件传输	文件名、文件路径、文件大小、发送用户、发送计算机、接收用户、接收计算机、任务开始时间、任务结束时间、任务状态。	客户端安全文件传输产生的日志
客户端健康检查	检查日志	计算机名、计算机 IP、计算机所属组织、检查结果、检查内容、结果描述、检查时间。	
	修复日志	计算机名、计算机 IP、计算机所属组织、修复结果、修复内容、结果描述。	
控制台操作日志		系统用户、日志时间、日志类型、日志描述。	
控制台系统日志		用户名/计算机名、日志时间、计算机 IP、策略名、策略状态。	
控制台用户登录日志		系统用户、用户名、登录类型、登录时间。	
补丁安装情况统计		计算机名、计算机所属组织、计算机 IP、补丁名称、安全级别、补丁大小、安装状态、发布日期。	
补丁更新设置日志		用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、更新设置、更新方式、更新日期、更新时间、是否重启、是否立即安装、发生时间、接收时间。	

防病毒软件统计		计算机名、计算机 IP、计算机所属的组织、防病毒软件名称、厂商、版本、病毒库版本、安装路径、更新时间、病毒库更新状态、服务器接收时间。	如果记录项显示为“未知”，表示系统未获取到信息。
客户端安装情况统计		计算机名、计算机 IP、计算机所属的组织、客户端版本、用户是否注册、计算机密级等级、安装时间、计算机最后在线时间、注册用户数。	

8.3.2　资产统计

资产统计是对客户端的软件资产和硬件资产进行统计，操作方法同上，具体统计内容见下表：

分类	统计项	统计内容	备　注
软件统计		计算机名、计算机 IP、计算机所属组织、软件名称、软件类型、版本、厂商、安装时间。（软件名称包括系统软件和应用软件）	安装时间未知时,默认为 1970-01-01，便于用户按时间条件查询。
操作系统		计算机名、计算机 IP、计算机所属组织、名称、版本、安装路径、安装时间、注册用户、注册公司、系列号、虚拟内存、上次启动时间。	
硬　件资产		计算机名、计算机 IP、计算机所属组织、计算机购入时间、操作系统、主板、处理器数量、处理器总频率、处理器频率信息、内存总容量、内存容量信息、内存类型信息、内存数量、硬盘数量、硬盘总容量、硬盘容量信息、端口数量、插槽数量、显示器、显卡数量、输入设备数量、声卡数量、控制器数量、光驱数量、网卡数量、调制解调器数量。	
	处理器	计算机名、计算机 IP、计算机所属的组织、名称、类型、主频、制造商。	
	内存	计算机名、计算机 IP、计算机所属的组织、容量、类型、插槽。	
	硬盘	计算机名、计算机 IP、计算机所属的组织、容量、制造商、速度、类型、描述。	
	BIOS	计算机名、计算机 IP、计算机所属的组织、序列号、制造商、版本、出厂时间。	
	光驱	计算机名、计算机 IP、计算机所属的组织、名称、类型、制造商。	
	声卡	计算机名、计算机 IP、计算机所属的组织、名称、制造商。	
	显卡	计算机名、计算机 IP、计算机所属的组织、名称、制造商、芯片组、显存大小。	
	显示器	计算机名、计算机 IP、计算机所属的组织、型号。	
	网卡	计算机名、计算机 IP、计算机所属的组织、名称、MAC 地址、类型、速度、制造商。	
	系统控制器	计算机名、计算机 IP、计算机所属的组织、名称、类型、制造商。	

	输入设备	计算机名、计算机 IP、计算机所属的组织、接口、类型、制造商、描述。	
	调制解调器	计算机名、计算机 IP、计算机所属的组织、名称、速度、模型、类型、制造商、接口类型、描述。	
	系统端口	计算机名、计算机 IP、计算机所属的组织、名称。	
	插槽	计算机名、计算机 IP、计算机所属的组织、设计、状态、共享。	

8.3.3　安全文档

统计审计分析中，安全文档部分记录了用户的带出申请日志、带出审批日志和自解密日志。具体内容见下表：（**注：**如果服务器没有授权这个功能模块，就不会产生这些日志信息。）

日志项	日志记录内容	备　注
带出申请日志	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、审批包名称、带出文件（夹）路径、带出文件名称列表、接收时间。	审批包名称是指用户制作的审批请求包名称，是一个压缩包，里面存有要审批的文档。
带出审批日志	使用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、审批包名称、带出文件（夹）路径、接收时间。	
自解密日志	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、文档名称、文档路径、接收时间。	
客户端扫描状态统计	计算机名、IP 地址、在线状态、最近一次扫描完成时间、扫描加密当前状态、客户端版本、所属部门。	
客户端扫描历史信息统计	计算机名、IP 地址、开始时间、完成时间、执行结果、扫描文件个数、加密文件个数、扫描文件类型、备注等。	

8.3.4 主动授权文件使用日志

日志项	日志记录内容	备　注
主动授权文件使用日志	文件名、部门、用户、使用结果、是否可访问、是否可读、是否可修改、是否可打印、是否可拷贝、是否可截屏、是否控制时间、时间控制的开始时间、时间控制的结束时间、是否可再授权、使用时间。	

8.3.5　可信移动存储介质

使用可信移动存储介质时，系统能够记录用户的使用台帐、锁定与自毁日志、文件操作日志、违规使用日志和口令更改日志等，具体内容见下表：

日志项	日志记录内容	备　注
可信磁盘授权日志	授权中心、授权编号、磁盘编号、控制台授权人、授权时间、责任人、主管部门、安全级别、商旅模式、处理方式（密码）、处理方式（到期）、已回收、文件系统。	
可信磁盘授权审批日志	申请者、申请者所在的计算机、申请者所在计算机 IP、申请时间、申请理由、审批员、审批员所在计算机、审批员所在计算机 IP、审批时间、审批完成、审批状态、审批描述。	
可信移动使用台帐	磁盘编号、用户名、用户所属的组织、计算机 IP、计算机名、计算机所属的组织、授权中心 ID、授权编号、操作时间、操作类型、剩余次数、使用状态。	
可信移动文件操作日志	磁盘编号、服务器 ID、用户名、用户所属的组织、计算机 IP、计算机名、计算机所属的组织、授权中心 ID、授权编号、操作时间、操作类型、文件名、进程名、是否跨服务器。	
可信移动锁定与自毁日志	磁盘编号、服务器 ID、用户名、用户所属的组织、计算机 IP、计算机名、计算机所属的组织、授权中心 ID、授权编号、锁定与自毁原因、操作时间、是否跨服务器。	
可信磁盘解锁日志	授权中心 ID、授权编号、磁盘编号、解锁时间、解锁人。	
商旅磁盘激活与反激活日志	授权中心、授权编号、磁盘编号、操作类型、操作时间、是否客户端激活、操作人、用户名、用户所属的组织、计算机 IP、计算机名、计算机所属的组织。	
跨服务器使用日志	磁盘编号、授权中心、授权编号、磁盘使用服务器、磁盘使用计算机、用户、事件类型、操作时间。	如果服务器没有授权服务器级联功能，就没有这些日志。
启用跨服务器日志	磁盘编号、授权中心 ID、授权编号、操作时间、操作员。	
关闭跨服务器日志	磁盘编号、授权中心 ID、授权编号、操作时间、操作员。	
可信移动口令更改日志	磁盘编号、服务器 ID、用户名、用户所属组织、计算机 IP、计算机名、计算机所属组织、授权中心 ID、授权编号、操作时间。	
可信移动违规使用日志	磁盘编号、服务器编号、用户名、用户所属组织、计算机 IP、计算机名、计算机所属组织、授权中心、授权编号、使用时间、原因、跨服务器使用状态。	
普通移动磁盘接入日志	用户名、用户所属的组织、计算机名、计算机 IP、计算机所属的组织、磁盘类型、磁盘名称、接入时间、磁盘大小。	

8.3.6　策略统计

策略统计按分类统计了失泄密策略、主机安全策略、可信策略、安全文档策略和密级文件策略，详细内容见下表。

日志项	日志记录内容	备　注
失泄密防护策略	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、策略项、策略名、策略控制内容、当前策略、策略启用时间、策略结束时间、管理员。	
主机安全策略	主机名、IP 地址、管理员、策略启用时间、策略结束时间、当前策略、软件和硬件管理策略、硬件基线设置、计算机名控制、CPU 监测、内存监测等。	
可信策略	计算机名、计算机所属的组织、计算机 IP、文件的创建、读取、写、重命名、删除等操作监控。	
安全文档策略	用户名、用户所属的组织、加密进程、自解密、审批权限等控制，以及策略启用和结束时间	
密级文件策略	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、访问控制规则、指定范围访问控制、违规报警控制、访问高密级文件控制、当前策略、策略启用时间、策略结束时间、管理员。	

8.3.7　密级标识

日志项	日志记录内容	备　注
密级文件审批日志	审批文件名称、审批单类型、申请者、申请者所在计算机、申请者所在计算机 IP、申请时间、审批员、审批员所在计算机、审批员所在计算机 IP、审批时间、审批完成、审批通过。	

8.3.8　内网安全扫描

内网安全扫描的过程中,系统详细记录执行扫描的代理日志和扫描到的主机日志,具体内容见下表。

日志项	日志记录内容	备　注
主机日志	MAC 地址、IP 地址、事件类型、发生时间、合法性、一致性、是否例外计算机。	
代理日志	MAC 地址、IP 地址、事件类型、发生时间。	

8.3.9　可信计算

可信计算记录了进程运行状况日志和核心文件检查结果日志，具体内容如下：

日志项	日志记录内容	备　注
进程运行状况日志	用户所属组织、计算机名、计算机 IP、计算机所属组织、控制类型、父进程名、父进程 ID、被操作的进程名、被操作的进程 ID、进程运行时间、服务器接收时间。	
核心文件检查结果日志	用户名、用户所属组织、计算机名、计算机 IP、计算机所属组织、检查时间、文件名称、文件路径、文件版本、发布公司、操作系统、文件 hash 值、文件大小、检查结果。	

8.4　轨迹追踪

密级文件在创建过程中，如果启用了轨迹追踪，那么客户端用户每次打开密级文件时，系统都会检查密级文件附加属性中的计算机属性与路径属性，当发现与实际的属性不一致时，自动向服务器发送信息，记录密级文件的位置发生了变化。用户可通过轨迹追踪，查看密级文件在不同路径、不同计算机上的运行轨迹，并正向或逆向追踪密级文件的来龙去脉。

8.4.1　文件列表

1. 以审计员身份登录控制台，单击“统计审计分析→轨迹追踪”，进入轨迹追踪的文件列表界面，如图 8-26 所示。

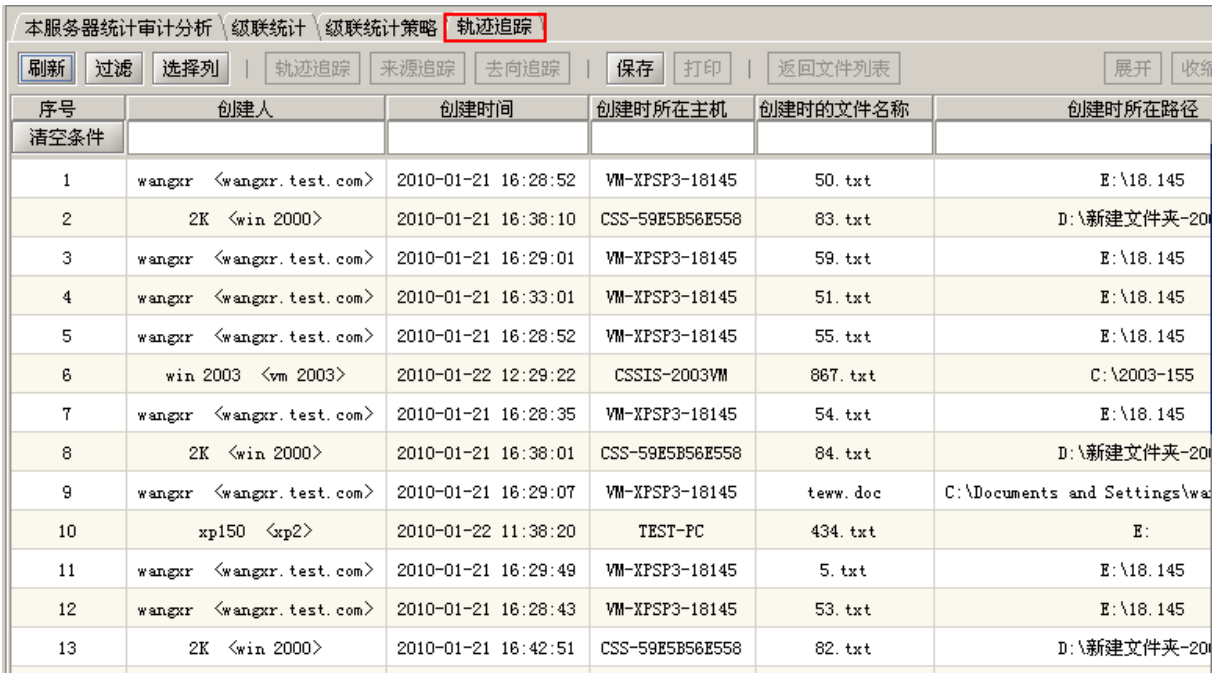


图 8-26　轨迹追踪文件列表

2. 单击“过滤”按钮，设置全部查询条件；或者单击表头下方的空白框，设置单项查询条件，确定后，即可按过滤条件显示文件列表。例如：我们想查看轨迹追踪图，就先要把所有记录轨迹的密级文件过滤出来，如图 8-27 所示。

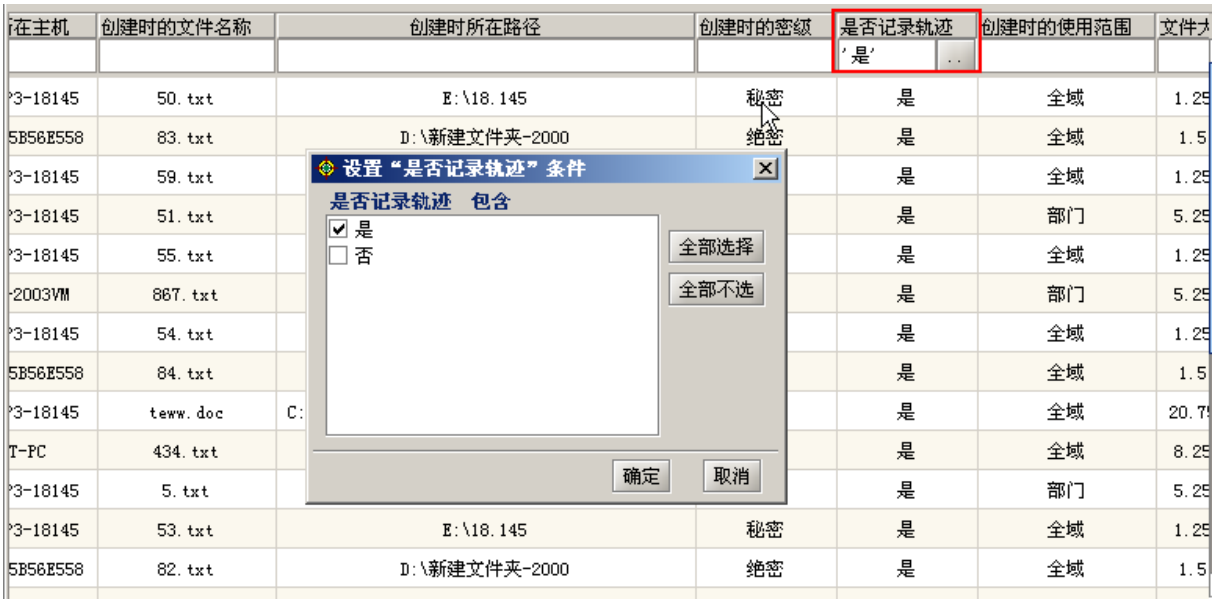


图 8-27　查询文件列表

3. 单击“选择列”按钮，出现设置显示列界面，如图 8-28 所示。用户可自行勾选要显示的列表项，不必按系统提供的默认列显示。确定后，可看到没有勾选的列不再显示，列表中只显示选定的列。

图 8-28　设置显示列

4. 在文件列表中，选择某一轨迹文件的记录，如图 8-29 所示。单击“轨迹追踪”按钮，或双击该文件记录，都可进入文件轨迹追踪界面。

时所在主机	创建时的文件名称	创建时所在路径	创建时的密级	是否记录轨迹	创建时的使用范围	文件大小
				'是'		
XPSP3-18145	teww.doc	C:\Documents and Settings\wangx...	普通	是	全域	20.75 KB
SIS-2003VM	aa.txt	C:\2003-155	机密	是	部门	2 KB
SIS-2003VM	867.txt	C:\2003-155	绝密	是	部门	5.25 KB
-59E5B56E558	84.txt	D:\新建文件夹-2000	绝密	是	全域	1.5 KB
-59E5B56E558	83.txt	D:\新建文件夹-2000	绝密	是	全域	1.5 KB
-59E5B56E558	82.txt	D:\新建文件夹-2000	绝密	是	全域	1.5 KB
-59E5B56E558	81.txt	D:\新建文件夹-2000	绝密	是	全域	1.5 KB
XPSP3-18145	77.txt	C:\Documents and Settings\wangx...	普通	是	部门	5.75 KB
TEST-PC	678.txt	C:	机密	是	全域	1.25 KB
XPSP3-18145	66.txt	C:\Documents and Settings\wangx...	秘密	是	全域	1.25 KB
XPSP3-18145	60.txt	E:\18.145	普通	是	部门	1.5 KB
XPSP3-18145	59.txt	E:\18.145	秘密	是	全域	1.25 KB
XPSP3-18145	58.txt	E:\18.145	秘密	是	全域	1.25 KB

图 8-29　选择文件进行轨迹追踪

8.4.2　轨迹追踪

在轨迹追踪界面，左侧显示文件详情和导航区信息，右侧显示轨迹图和表格图，如图 8-30 所示。从轨迹图可以看出该密级文件在不同组织（部门）、计算机和同一机器不同路径的流转情况。每个流转轨迹从上到下按时间顺序排列，从左到右按不同组织（部门）和计算机排列。

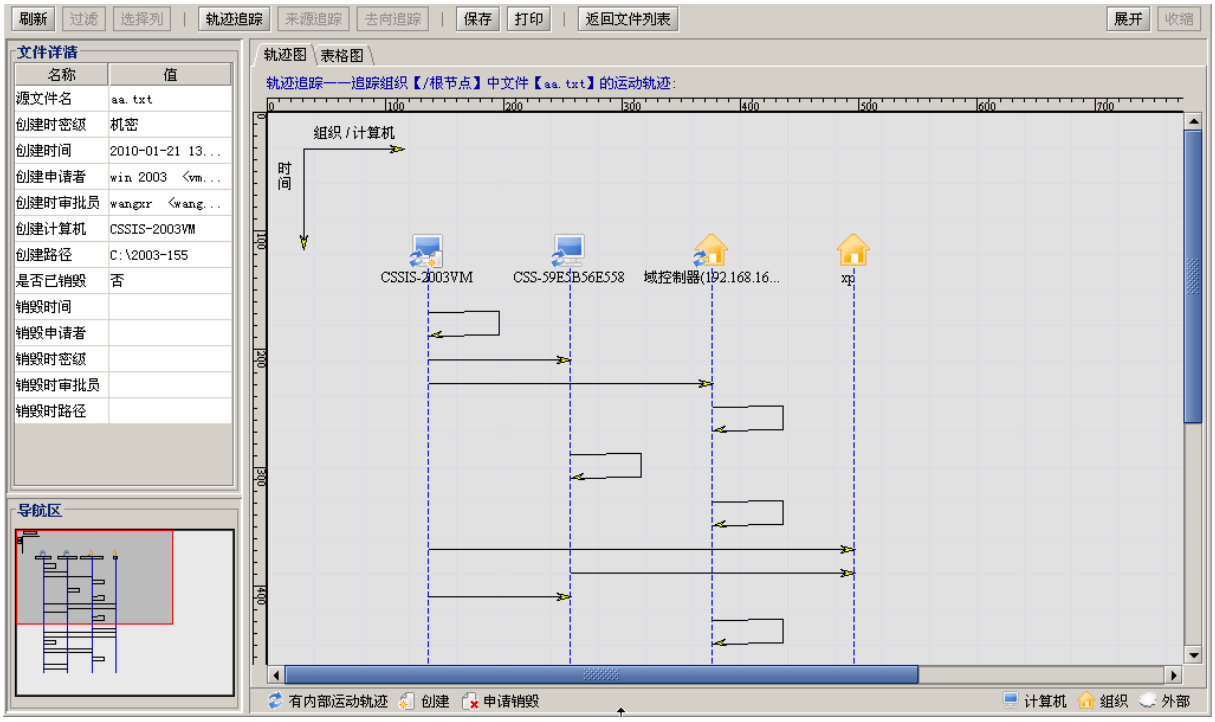


图 8-30　密级文件轨迹图

1. 如果轨迹追踪图中，有不同的组织（部门）。单击“展开”按钮，显示密级文件在所有计算机上的流转轨迹，如图 8-31 所示。直线表示不同机器上的流转轨迹，弯线表示同一机器不同路径下的流转轨迹。另外，不同的图标含义也不同，下面有图示，请用户查看。

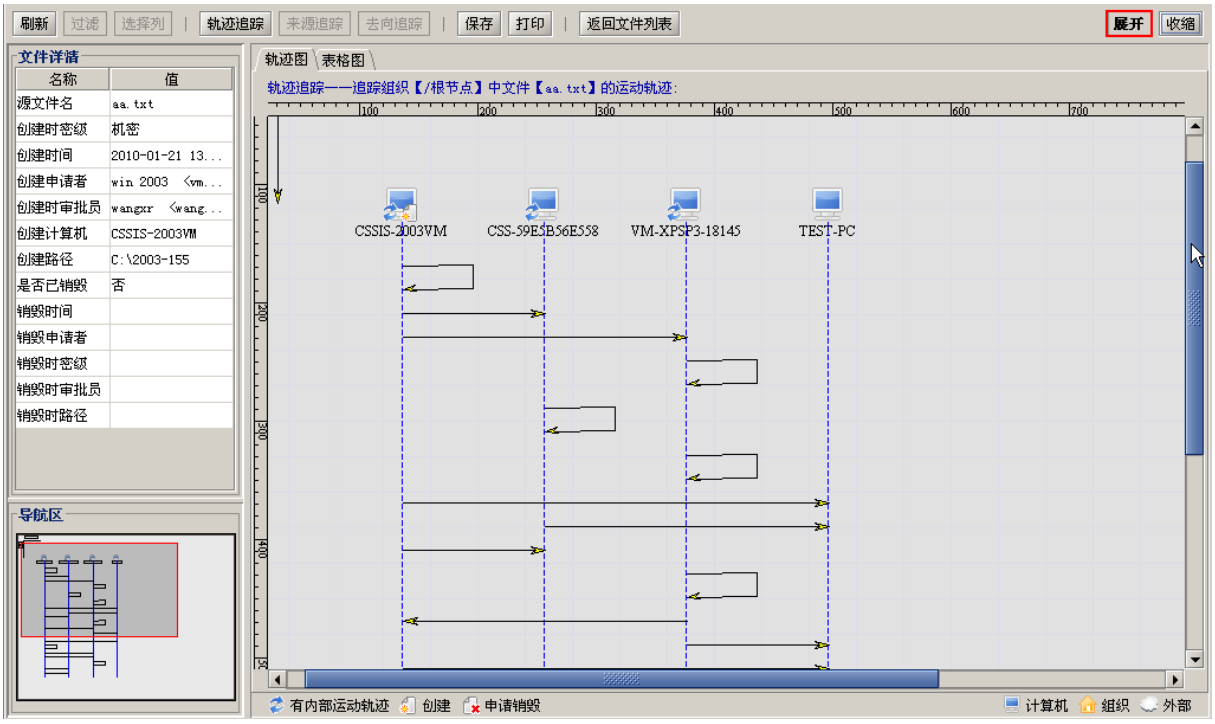


图 8-31　查看密级文件在计算机上流转轨迹

2. 双击某直线或弯线轨迹图，显示该轨迹的详细信息列表。其中包括：文件名、密级、源文件所在路径、目的文件所在的路径等，如图 8-32 所示。查看完毕后，单击“收缩”按钮，或者单击“轨迹追踪”按钮，回到原来默认的轨迹追踪界面。

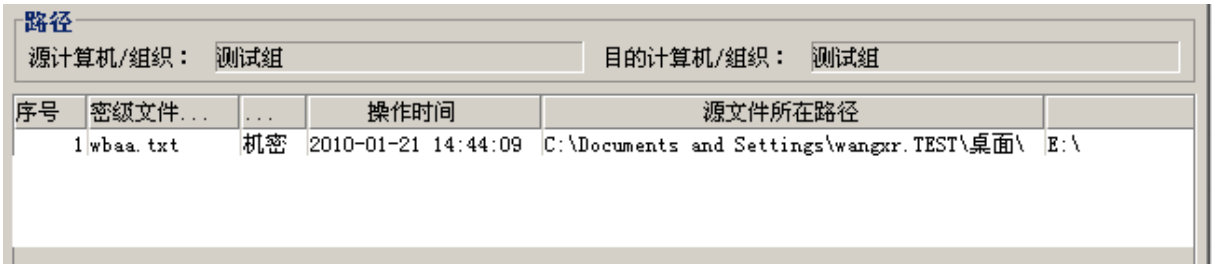


图 8-32　单个轨迹的详细信息列表

3. 在轨迹追踪界面，双击某组织（部门）→子部门，显示该部门下的计算机，以及密级文件在部门内部计算机上的流转轨迹，如图 8-33 所示。双击某计算机，显示密级文件在该机上所有的流转信息列表，包括来源信息和去向信息。该表详细记录了密级文件名称、密级、源计算机、目的计算机、源文件所在路径和目的文件所在路径等，如图 8-34 所示。

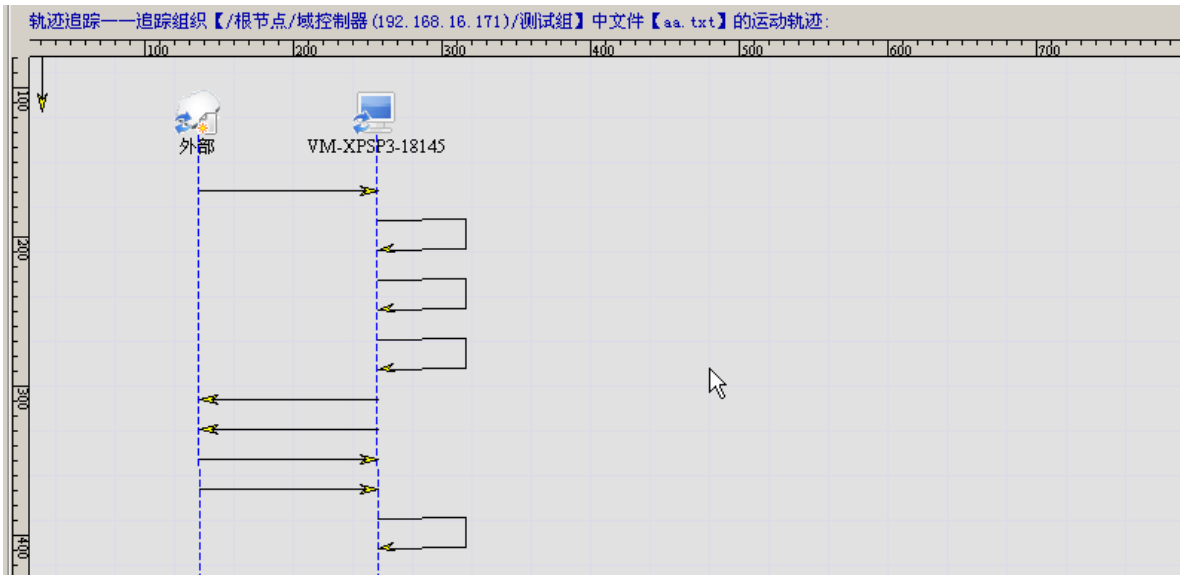


图 8-33　密级文件在部门内部的流转轨迹

查看密级文件【aa.txt】在计算机【VM-XPSP3-18145】中流转的信息：

序号	密级文件名称	密级	操作时间	源计算机	源计算机所属组织	目的计算机	目的计算机所属...
1	aa.txt	机密	2010-01-21 14:43:56	CSSIS-2003VM< 19...	根节点	VM-XPSP3-18145< ...	测试组
2	wbaa.txt	机密	2010-01-21 14:44:09	VM-XPSP3-18145< ...	测试组	VM-XPSP3-18145< ...	测试组
3	wbaa.txt	机密	2010-01-21 14:48:45	VM-XPSP3-18145< ...	测试组	VM-XPSP3-18145< ...	测试组
4	wbaa.txt	机密	2010-01-21 16:25:08	VM-XPSP3-18145< ...	测试组	VM-XPSP3-18145< ...	测试组
5	wbaa.txt	机密	2010-01-21 16:43:04	VM-XPSP3-18145< ...	测试组	CSSIS-2003VM< 19...	根节点
6	wbaa.txt	机密	2010-01-21 16:43:56	VM-XPSP3-18145< ...	测试组	TEST-PC< 192.168...	xp
7	aab.txt	机密	2010-01-21 16:54:30	CSSIS-2003VM< 19...	根节点	VM-XPSP3-18145< ...	测试组
8	aaxp.txt	机密	2010-01-21 16:54:35	CSSIS-2003VM< 19...	根节点	VM-XPSP3-18145< ...	测试组
9	wbaa.txt	机密	2010-01-21 16:54:36	VM-XPSP3-18145< ...	测试组	VM-XPSP3-18145< ...	测试组

图 8-34　密级文件在计算机上所有流转信息列表

4．选择某计算机，单击“来源追踪”按钮，显示该机上密级文件的来源视图，如图 8-35 所示。来源追踪图中用虚线表示密级文件的来源轨迹。双击某条虚线，显示该轨迹的所有来源信息列表，如图 8-36 所示。

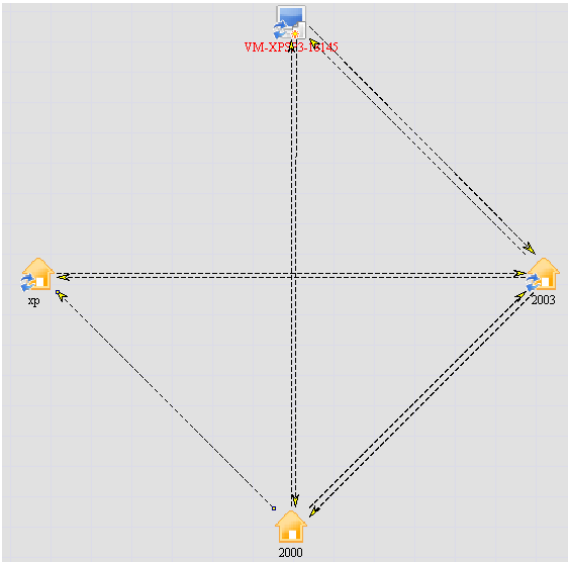


图 8-35　密级文件来源轨迹追踪图

路径

源计算机/部门：2003　　目的计算机/部门：xp

...	密级文件名称	...	操作时间	源文件所在...	目的文
1	测试-00.doc	秘密	2010-02-02 11:37:01	C:\test-2003\	C:\Documents and Se
2	测试-2003.doc	绝密	2010-02-02 11:37:05	C:\test-2003\	C:\Documents and Se
3	测试-00.doc	秘密	2010-02-02 11:41:09	C:\test-2003\	C:\Documents and Se

图 8-36　密级文件来源详细信息列表

5. 选择某计算机，单击“去向追踪”按钮，显示该机上密级文件的去向视图，如图 8-37 所示。去向追踪图中用实线表示密级文件的去向轨迹。双击某条实线，显示该轨迹的所有去向信息列表，如图 8-38 所示。

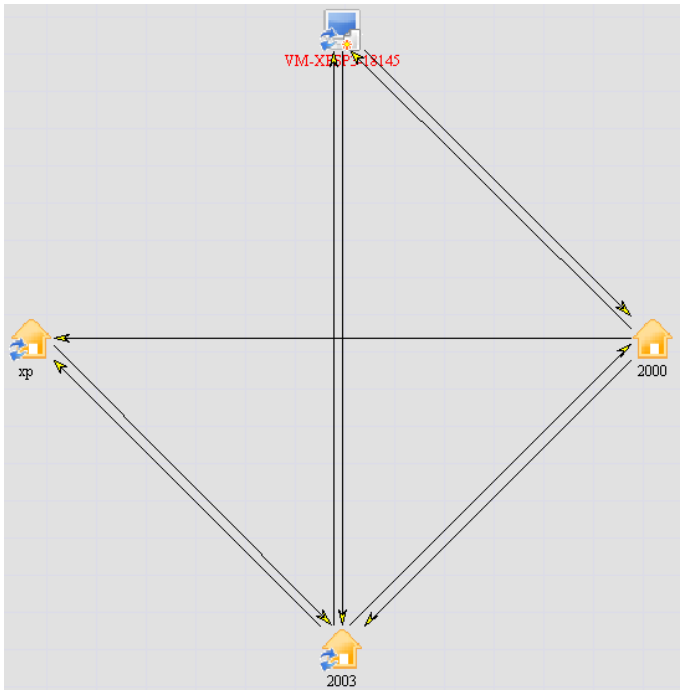


图 8-37　密级文件去向轨迹追踪图

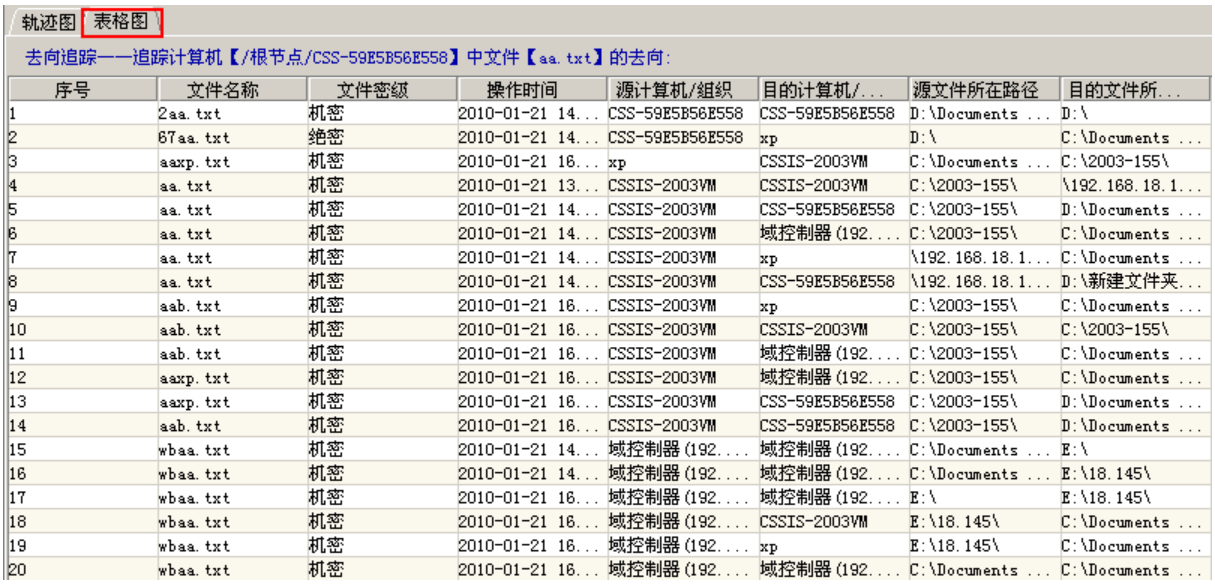
路径

源计算机/部门：2003　　目的计算机/部门：VM-XPSP3-18145

...	密级文件名称	...	操作时间	源文件所在...	目的文件所在路
1	测试-2003.doc	绝密	2010-02-02 11:38:50	C:\test-2003\	E:\新建文件夹\
2	测试-00.doc	秘密	2010-02-02 11:38:53	C:\test-2003\	E:\新建文件夹\
3	测试-01.doc	秘密	2010-02-02 11:44:28	C:\test-2003\	\\192.168.18.155\tes

图 8-38　密级文件去向详细信息列表

6. 在“轨迹追踪”视图下，单击“表格图”标签页，显示密级文件流转轨迹详细信息列表，如图 8-39 所示。“表格图”和“轨迹图”表示方式不一样，但表达内容完全一样，一一对应。“轨迹图”是“表格图”的最好图示，“表格图”是“轨迹图”的详细信息列表。



轨迹图 | 表格图

去向追踪——追踪计算机【/根节点/CSS-59E5B56E558】中文件【aa.txt】的去向：

序号	文件名称	文件密级	操作时间	源计算机/组织	目的计算机/...	源文件所在路径	目的文件所...
1	2aa.txt	机密	2010-01-21 14...	CSS-59E5B56E558	CSS-59E5B56E558	D:\Documents ...	D:\
2	67aa.txt	绝密	2010-01-21 14...	CSS-59E5B56E558	xp	D:\	C:\Documents ...
3	aaxp.txt	机密	2010-01-21 16...	xp	CSSIS-2003VM	C:\Documents ...	C:\2003-155\
4	aa.txt	机密	2010-01-21 13...	CSSIS-2003VM	CSSIS-2003VM	C:\2003-155\	\192.168.18.1...
5	aa.txt	机密	2010-01-21 14...	CSSIS-2003VM	CSS-59E5B56E558	C:\2003-155\	D:\Documents ...
6	aa.txt	机密	2010-01-21 14...	CSSIS-2003VM	域控制器(192....	C:\2003-155\	C:\Documents ...
7	aa.txt	机密	2010-01-21 14...	CSSIS-2003VM	xp	\192.168.18.1...	C:\Documents ...
8	aa.txt	机密	2010-01-21 14...	CSSIS-2003VM	CSS-59E5B56E558	\192.168.18.1...	D:\新建文件夹...
9	aab.txt	机密	2010-01-21 16...	CSSIS-2003VM	xp	C:\2003-155\	C:\Documents ...
10	aab.txt	机密	2010-01-21 16...	CSSIS-2003VM	CSSIS-2003VM	C:\2003-155\	C:\2003-155\
11	aab.txt	机密	2010-01-21 16...	CSSIS-2003VM	域控制器(192....	C:\2003-155\	C:\Documents ...
12	aaxp.txt	机密	2010-01-21 16...	CSSIS-2003VM	域控制器(192....	C:\2003-155\	C:\Documents ...
13	aaxp.txt	机密	2010-01-21 16...	CSSIS-2003VM	CSS-59E5B56E558	C:\2003-155\	D:\Documents ...
14	aab.txt	机密	2010-01-21 16...	CSSIS-2003VM	CSS-59E5B56E558	C:\2003-155\	D:\Documents ...
15	wbaa.txt	机密	2010-01-21 14...	域控制器(192....	域控制器(192....	C:\Documents ...	E:\
16	wbaa.txt	机密	2010-01-21 14...	域控制器(192....	域控制器(192....	C:\Documents ...	E:\18.145\
17	wbaa.txt	机密	2010-01-21 16...	域控制器(192....	域控制器(192....	E:\	E:\18.145\
18	wbaa.txt	机密	2010-01-21 16...	域控制器(192....	CSSIS-2003VM	E:\18.145\	C:\Documents ...
19	wbaa.txt	机密	2010-01-21 16...	域控制器(192....	xp	E:\18.145\	C:\Documents ...
20	wbaa.txt	机密	2010-01-21 16...	域控制器(192....	域控制器(192....	C:\Documents ...	C:\Documents ...

图 8-39　密级文件流转轨迹列表

7. 在“轨迹图”和“表格图”视图中，单击“保存”按钮，能将轨迹图保存为*.png 格式，表格图保存为*.xls 格式。另外，“轨迹图”可以打印，“表格图”不能打印。

提示：

1. 在任何轨迹图中，单击“轨迹追踪”按钮，都可回到“轨迹追踪”原始界面；在任何轨迹图中，单击“返回文件列表”按钮，都可返回到密级文件列表视图。

2. 在密级文件列表视图中，选择有轨迹记录的文件，单击“轨迹追踪”按钮或者双击该文件记录，都可进入轨迹追踪视图。

第九章　系统参数设置

以系统管理员身份（默认 admin）登录控制台进行系统参数设置，包括：服务器端参数配置和客户端参数配置。

9.1 服务器端参数配置

9.1.1 注册模式设置

客户端注册模式可以设置为“认证模式”或“自由模式”，如图 9-1 所示。

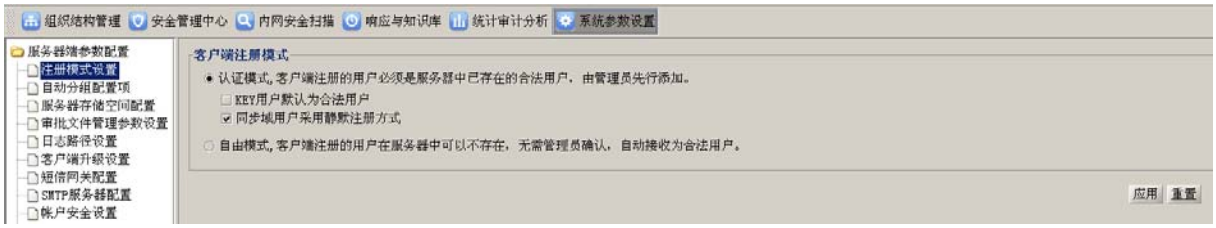


图 9-1　客户端注册模式

认证模式是指客户端注册的用户必须是服务器中已存在的合法用户（管理员添加），或者 KEY 用户、域帐户。

KEY 用户默认为合法用户：为 KEY 用户安装客户端，事先在控制台成功导入 KEY 用户信息，那么系统就会默认该 KEY 用户为合法用户，不必选择 “KEY 用户默认为合法用户”，就可以注册成功；如果没有在控制台导入 KEY 用户信息，就必须选择 “KEY 用户默认为合法用户”，否则注册不成功。

同步域用户采用静默注册方式：域用户安装客户端，可以在控制台进行同步域账户，在这里选择域用户静默安装方式。然后，以域帐户登录域，安装客户端完成后自动注册。

自由模式：客户端注册的用户在服务器中可以不存在，无需管理员确认，自动接收为合法用户。

客户端以自由模式注册时，使用的用户名是数据库中已经存在的，那么密码必须和数据库中保存的一致才能注册上。如果客户端安装时启用“网络接入认证”，那么不能采用自由模式注册。

9.1.2 自动分组配置项

将主机的 IP 地址和组织结构之间建立一个映射表。单击“添加”按钮，将组织名称和 IP 地址段一一对应起来，如图 9-2 所示。该策略应用下发后，客户端注册时系统能根据主机 IP 地址，自动将其分配到相应的组织中。如果根据主机的 IP 找不到对应的组织名称，或者组织名称在组织结构中已经删除，那么系统自动将其分配到组织结构的根目录中。

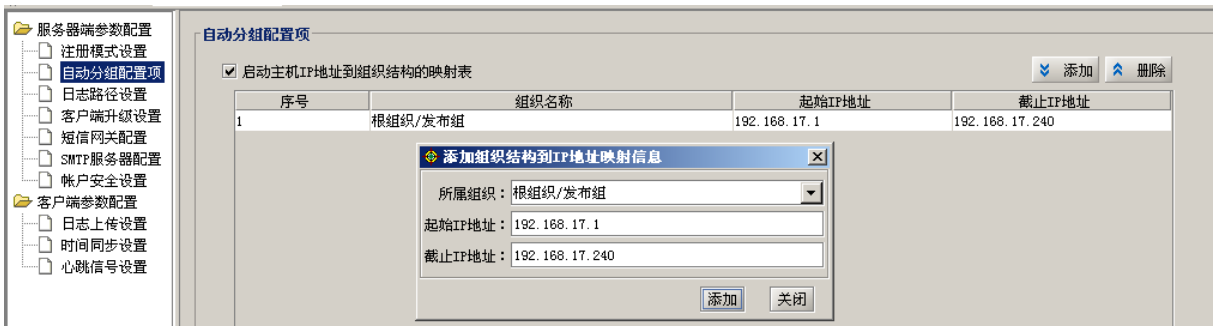


图 9-2　自动分组配置项

9.1.3　服务器存储空间配置

客户端上传给服务器的文件，默认存放在“C:\Program Files\CSS\UEM\WBServer\filestore”下，当存储空间将满时，用户可以添加存储位置，如图 9-3 所示。新添加的存储位置，统一在指定盘符的 UemDataFiles 目录下，空间编号会自动生成，当它显示是红色时，表示已经存储了文件，不能删除。

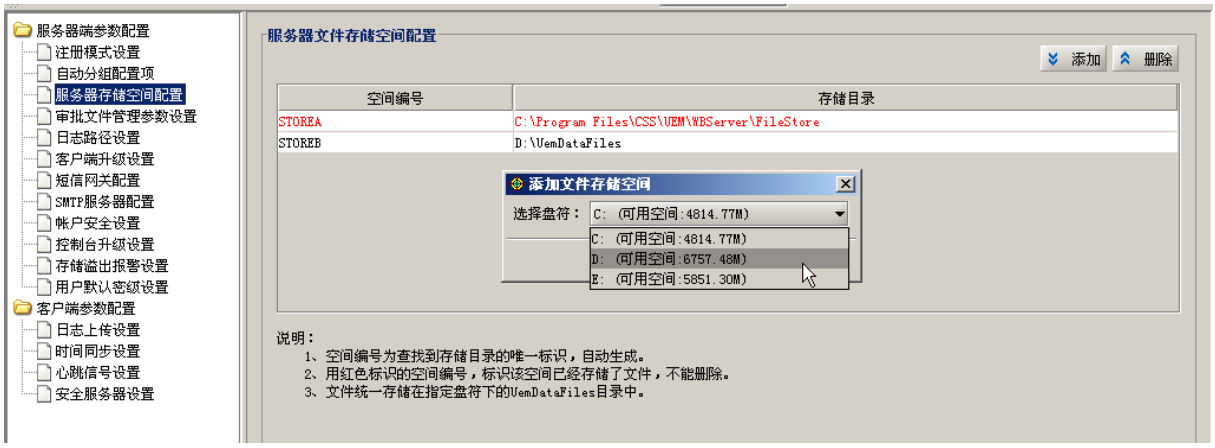


图 9-3　服务器存储空间配置

9.1.4　审批文件管理参数设置

客户端上传给服务器的待审批文件，自动存放在“服务器文件存储空间”中指定的位置，原始默认位置在“C:\Program Files\CSS\UEM\WBServer\filestore”。审批过程完成后，客户端执行相关操作后，一些审批备份文件已无任何用途，徒占服务器存储空间。这时，管理员可以单击“立刻清理”按钮，一次性清理无用的审批备份文件，也可勾选“审批完成后自动清理存放在服务器的审批备份文件”，将策略“应用”后，由服务器自动清理无用的审批备份文件，如图 9-4 所示。

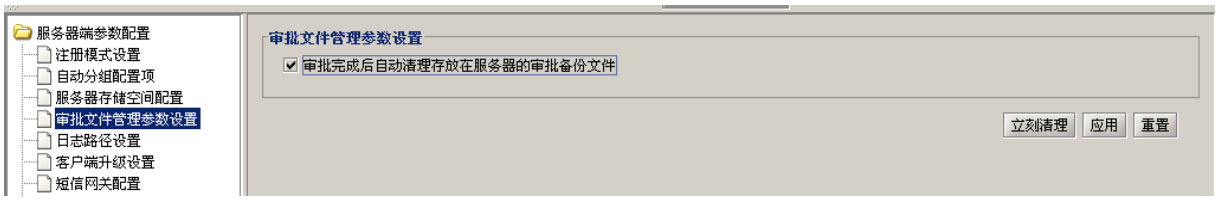


图 9-4　审批文件管理参数设置

9.1.5　日志路径设置

服务器日志默认存放在“C:\Program Files\CSS\UEM\WBServer\files\log”下，在这里可以任意更改客户端上传数据日志的存放路径，如图 9-5 所示。更改完成后，请在停止服务的情况下，手工将原日志路径下的文件备份到新日志路径下。

当服务器所在磁盘空间小于 500M 时，默认每隔 5 分钟会向控制台报警。

图 9-5　服务器日志路径设置

9.1.6　客户端升级设置

客户端可以自动升级，在这里进行升级设置，如图 9-6 所示。

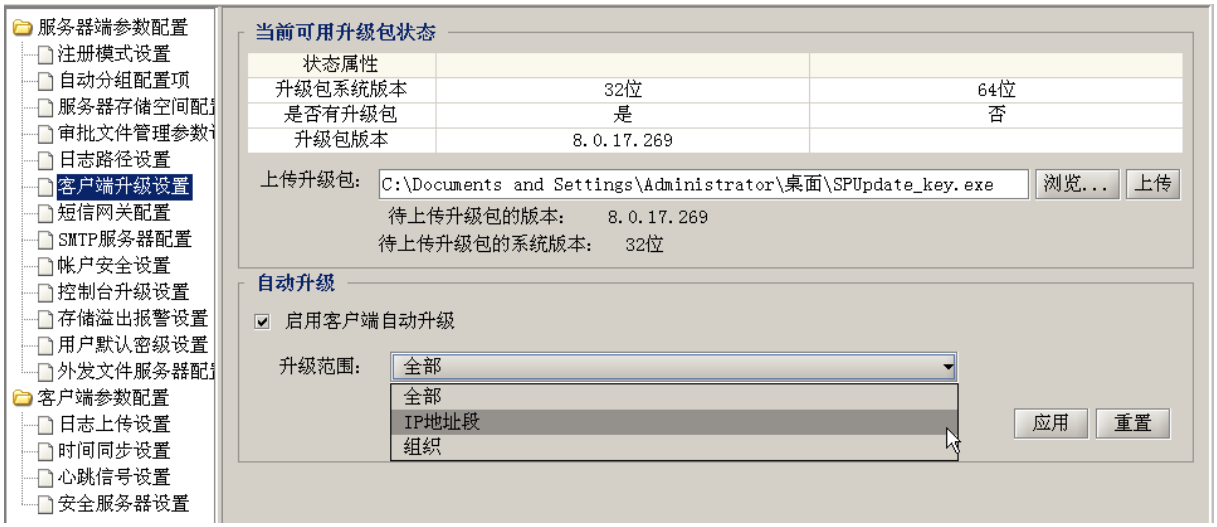


图 9-6　客户端升级设置

在上面的“当前可用升级包状态”栏中，查看服务器上是否有升级包，版本是不是最新的，是 64 位还是 32 位。如果没有升级包，或者版本比较早，那么单击“浏览”按钮，选择新的升级包，上传至服务器。在下面的“自动升级”框中，启用客户端自动升级，通过下拉框选择升级范围。如果选择的是 IP 地址段，需要添加具体的 IP 地址；如果选择的是组织，需要勾选具体的组织。最后，单击“应用”按钮，在升级范围内的客户端重启时都将自动升级。

提示：如果不启用客户端自动升级设置，需要在组织结构管理→计算机管理中，选择某些计算机，通过下发“升级客户端”命名，对选中的主机进行客户端升级。参见 4.2.2.1 升级客户端.

9.1.7　短信网关配置

在“短信网关配置”中输入短信中心号码，并通过下拉框选择串口，如图 9-7 所示。在“短信网关测试”中，用户可以输入一个保证能收到短信的号码及短信内容，测试是否能收到短信中心发送的短信，检测配置是否成功。系统给出检测成功与否的提示。

提示：输入短信中心号码时，需要咨询本地通信运营商，各地的号码可能不一样。北京移动的是 13800100500，北京联通的是 13010112500。

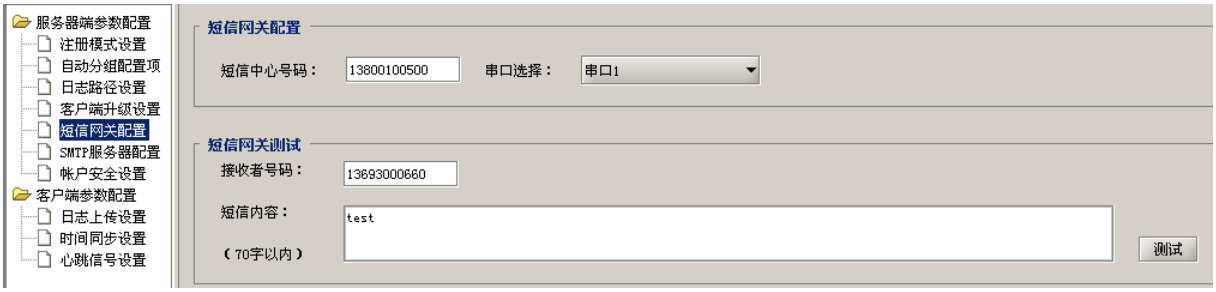


图 9-7　配置 SMTP 服务器

9.1.8　SMTP 服务器配置

在“SMTP 邮箱配置”中，配置 SMTP 服务器地址以及账户信息，并检查输入的有效性，如图 9-8 所示。在“SMTP 邮箱测试”中，用户可以输入一个保证能收到邮件的地址以及邮件内容，测试是否能收到 SMTP 服务器发送的测试邮件，检测配置是否成功。系统会给出检测成功与否的提示。

图 9-8　配置 SMTP 服务器

9.1.9　帐户安全设置

在“帐户安全设置”中，设置管理员帐号密码的最小长度、连续尝试登录次数、清零时间间隔和锁定时间，清零时间间隔一定要小于锁定时间，如图 9-9 所示。

当管理员登录控制台时（非 KEY 用户），如果密码连续尝试次数超过了最大次数将被锁定，可请求系统管理员（默认 admin）解锁，或者到了锁定时间自动解锁；当管理员在指定的时间间隔内不操作控制台则自动锁定，需要重新输入密码才能再次登录控制台，继续原来的操作。参见控制台登录控制。

图 9-9　　帐户安全设置

9.1.10　控制台升级设置

控制台也可以自动升级，在这里进行升级设置，如图 9-10 所示。

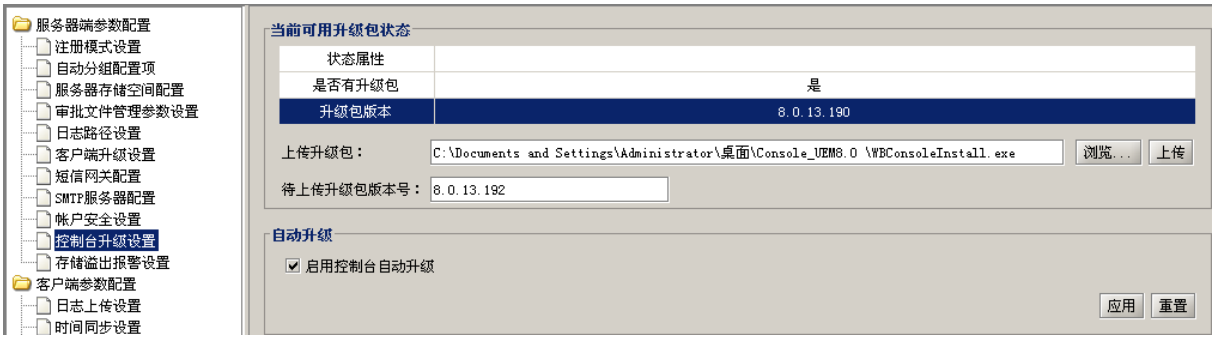


图 9-10　　控制台升级设置

在上面的“当前可用升级包状态”栏中，查看服务器上是否有升级包，版本是不是最新的。如果没有升级包，或者版本比较早，那么单击“浏览”按钮，选择新的升级包、输入版本号，上传至服务器。在下面的“自动升级”框中，启用控制台自动升级。最后，单击“应用”按钮，那么控制台系统管理员登录控制台时，发现控制台版本过低且有可用的新版本，可用提示用户进行升级。

9.1.11　存储溢出报警设置

在“存储溢出报警设置”中，可配置是否启用报警。当服务器空间小于阀值时，产生报警信息，同时也支持短信报警，如图 9-11 所示。服务器存储空间不足时，通过配置能够停止对客户端日志的接收，以保障服务器的正常运行。

提示：接收短信的手机号码最多可输入 5 个，各个手机号之间用“|”隔开。这些手机号需在短信网关配置中测试通过，保证能够收到报警短信。

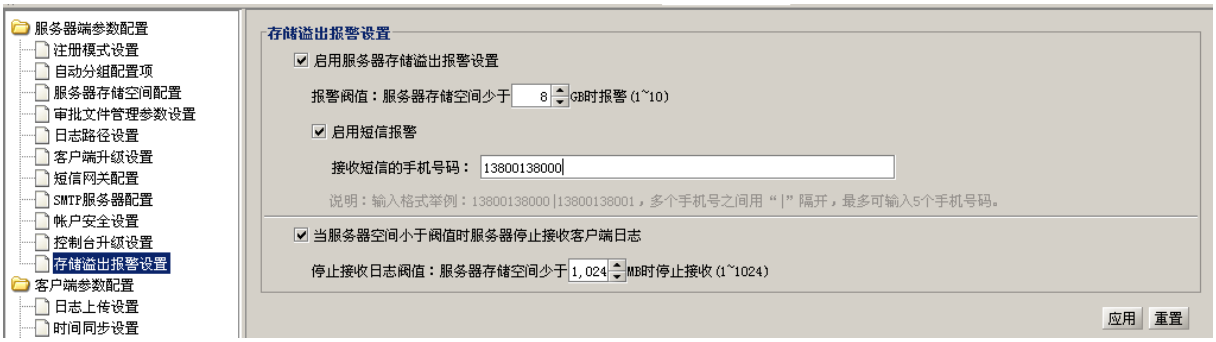
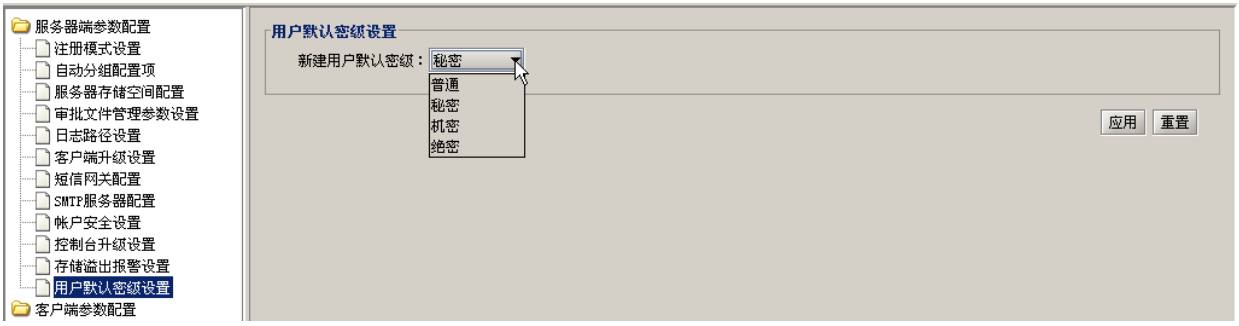


图 9-11　存储溢出报警设置

9.1.12　用户默认密级设置

在“用户默认密级设置”中，可设置新建用户的默认密级，并将配置信息保存到服务器上，如图 9-12 所示。当系统添加新用户时，首先赋予用户这个默认密级，也可根据需要更改；当客户端用户采用自动方式注册时，因为没有预设的密级，需要从服务器获取用户默认密级；另外，当客户端由老版本升级到新版本时，如果客户端用户无密级属性，则在升级过程中，也需要从服务器获取用户默认密级。



.图 9-12　用户默认密级设置

9.1.13 审批平台服务器配置

在“审批平台服务器配置”中，可设置审批平台服务器的 IP 地址和端口号，客户端申请在线授权审批时，会自动连接到审批平台服务器，如图 9-13 所示。

图 9-13　审批平台服务器配置

9.1.14 客户端更换证书配置

服务器通过备份与恢复工具的“证书恢复”改变了服务器的证书，客户端需要更换证书配置，如图 9-14 所示。如果设置成“允许客户端更换证书”，客户端会自动从服务器获取新的证书，并使用新证书通信；如果设置成“禁止客户端更换证书”，客户端将不能获取新的证书，无法与服务器进行通信。

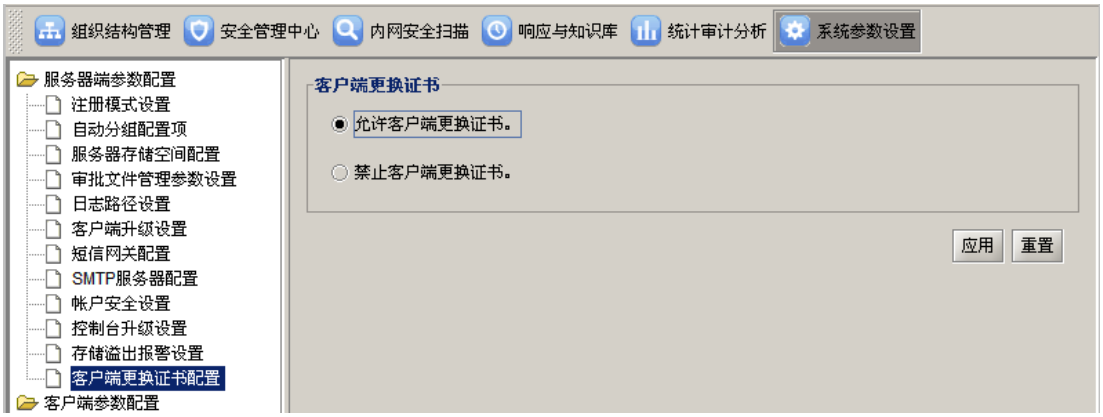


图 9-14　客户端更换证书配置

9.2　客户端参数配置

客户端参数配置：包括设置客户端的日志上传模式，时间同步的误差和频率，以及心跳信号的时间间隔。

9.2.1　上传日志设置

在“日志上传设置”页面中，可以选择实时上传、定时上传、按日志文件的大小或行数上传，如图 9-15 所示。该上传的日志是指 UEM 客户端监控日志。

提示：

（1）定时上传，上传频率在 1 小时～64 小时之间；

（2）根据日志文件大小上传，上传的日志大小在 1 兆～500 兆之间；

（3）根据日志文件行数上传，上传的日志行数在 1 行～400000 行之间。

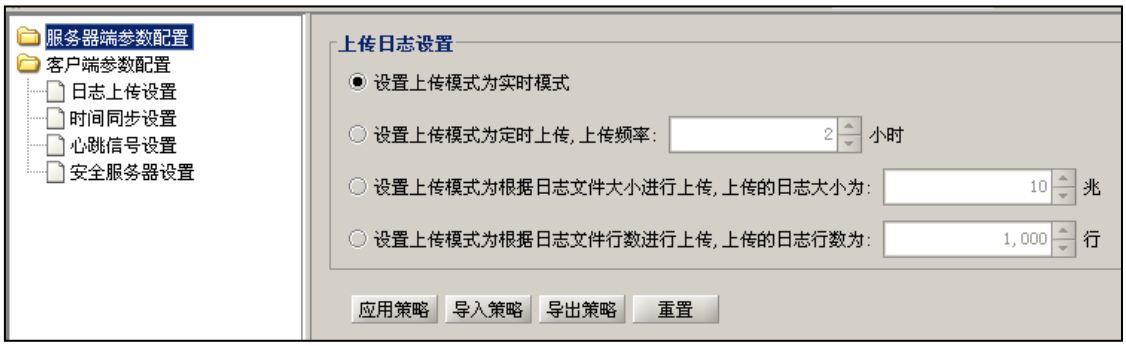


图 9-15　日志上传设置

9.2.2　时间同步设置

在“时间同步设置”页面中，可以进行客户端和服务器的时间同步设置。启用时间同步后，根据用户需要设置允许的误差范围（10 秒～60 秒）和时间同步的频率（大于 5 秒），也可以启用日期同步，如图 9-16 所示。

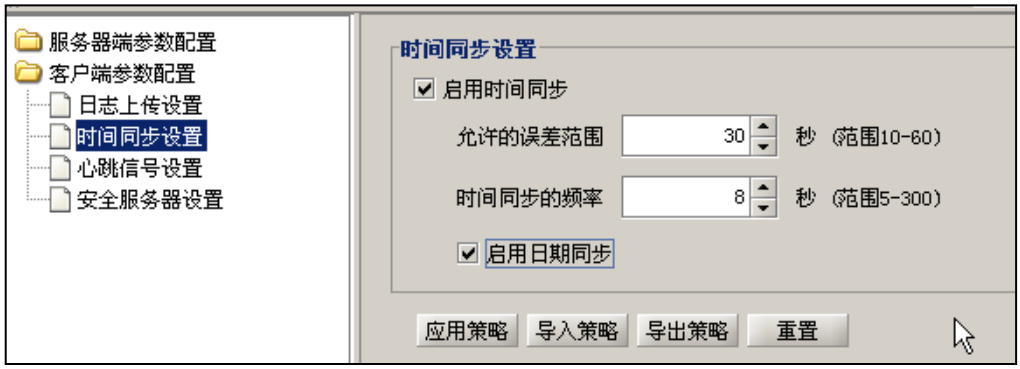


图 9-16　时间同步设置

9.2.3　心跳信号设置

在“心跳信号设置”页面中，可以设置心跳时间间隔（4 秒～32 秒），如图 9-17 所示。客户端在设定的时间内与服务器进行通讯连接，服务器在特定的时间内判断客户端是否离线。

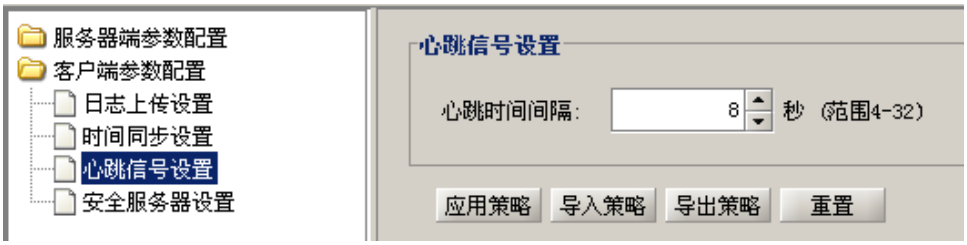


图 9-17　心跳信号设置

9.2.4　安全服务器设置

在“安全服务器设置”中，单击“添加”按钮，将一些特定的安全服务器，如“防病毒软件服务器”、“Windows 补丁服务器”、“软件服务器”等，添加到安全服务器列表中，如图 9-18 所示。这样将策略下发，客户端运行终端安全检查时，由于不满足检查项而被设置成安全模式后，仍然能访问列表中的安全服务器。

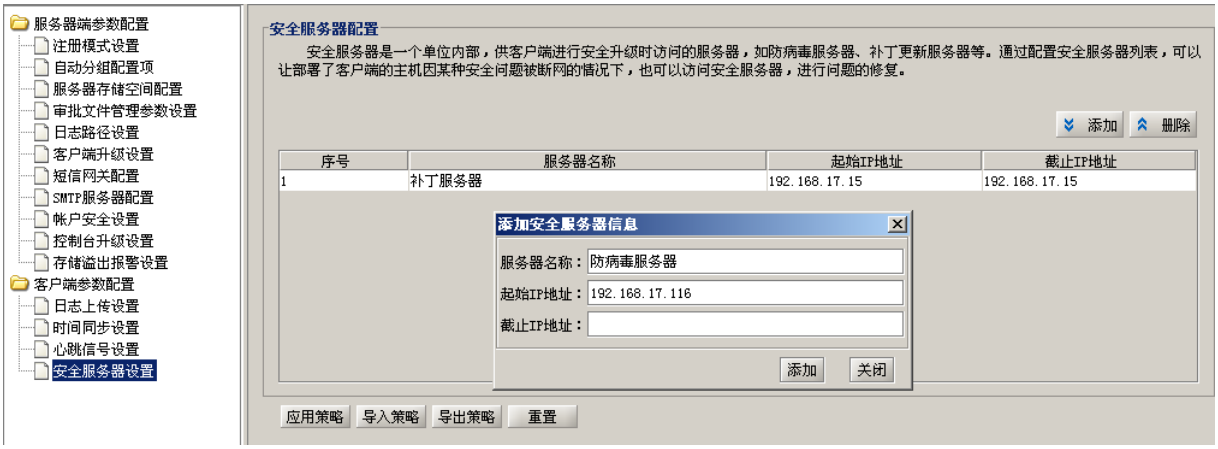


图 9-18　安全服务器设置

第十章　服务器操作指南

10.1 备份与恢复工具

“备份与恢复工具”是将服务器上的组织结构、策略、警报信息、日志信息以及日志文件备份到安全的地方，需要的时候再恢复过来。既可以将备份数据恢复到新建的服务器上，保留原来服务器的组织结构、基本表、日志、数据和文件等，也可以将备份数据导入到审计系统中，实现离线审计。同时，“备份与恢复工具”还可实现服务器证书的备份和恢复操作。

10.1.1 数据导出

1. 在服务器桌面上找到“备份与恢复工具”图标，双击进入“备份与恢复工具”界面，如图 10-1 所示。或者单击“开始”→“程序”→“CSS”→“服务器”→“备份与恢复工具”，也可以进入该界面。

图 10-1　备份与恢复工具图标

2. 在备份与恢复界面，单击“数据导出”功能按钮，进行导出设置，如图 10-2 所示。单击“选择”按钮，选择输出目录路径。通过数据规模右侧的下拉框，选择导出数据类型（核心数据、常用数据、所有数据）。为了导出数据的安全性，可以输入密码保护。

提示

1. 导出数据前，先估算一下所需磁盘空间，以便选择输出路径。

2. 导出数据时，最好先停止应用服务器，也就是停止 UEM Security Patron Service，保证导出数据的完整性。

3. 导出数据时，有一定的压缩比。如果数据库文件大小为 1G，导出后为 30M。如果日志文件大小为 1G～2G，压缩后为 1G。

4. 导入数据时，也要按照压缩文件大小与实际的文件大小的大致比例，估算一下导入文件时数据库与日志文件所需要的空间，以免导入失败。

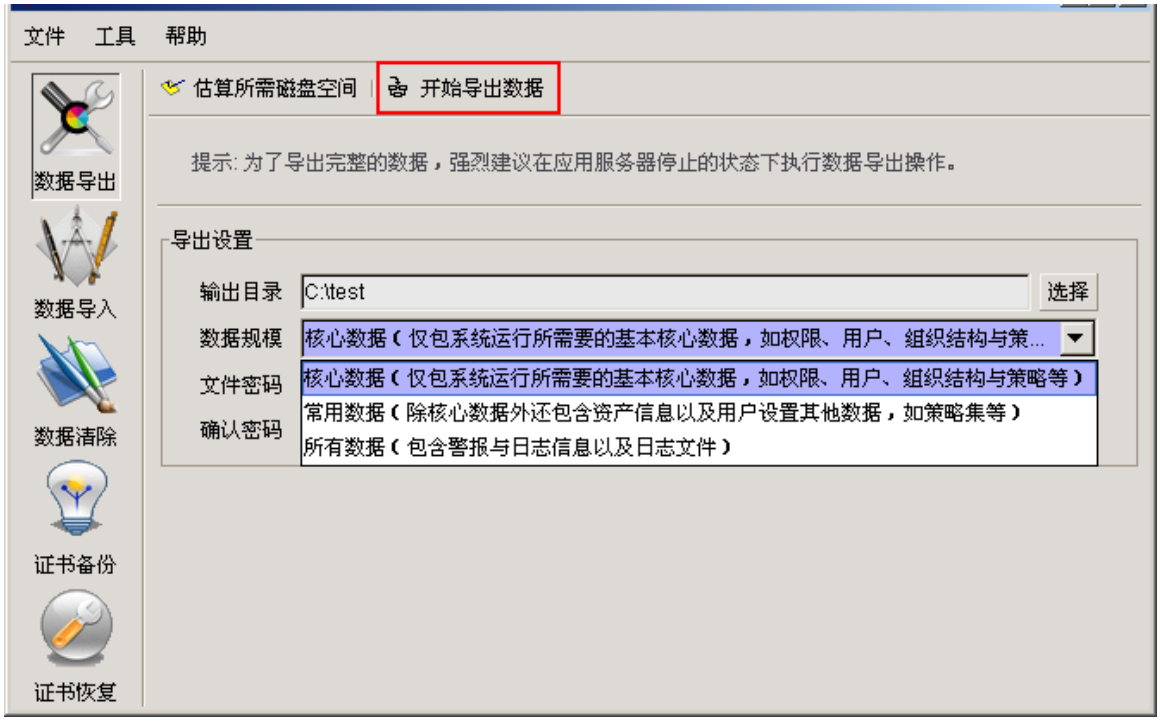


图 10-2　服务器数据导出

3. 单击“开始导出数据”，进行数据导出操作。导出完成后，会有数据导出报告，用户可以查看导出结果，如图 10-3 所示。也可以单击“保存”按钮，将此报告保存起来。

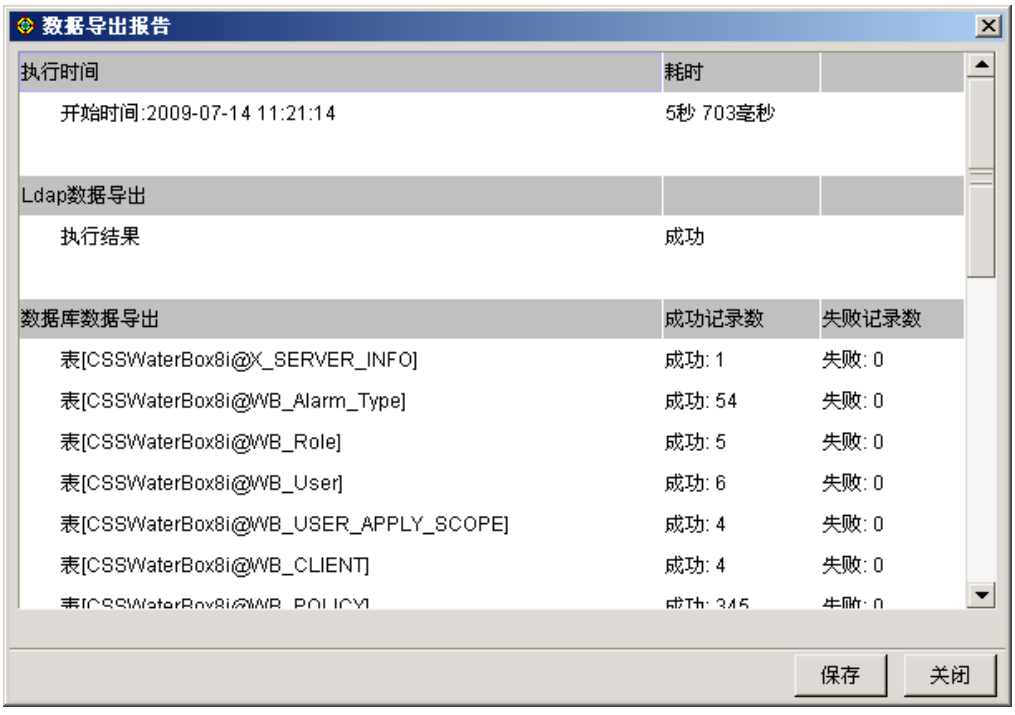


图 10-3　数据导出报告

10.1.2　数据导入

1. 在备份与恢复界面，单击“数据导入”功能按钮，进行导入设置，如图 10-4 所示。单击“选择”按钮，选择输入文件 index.idx。如果数据备份时有密码，在这里需要输入文件密码。

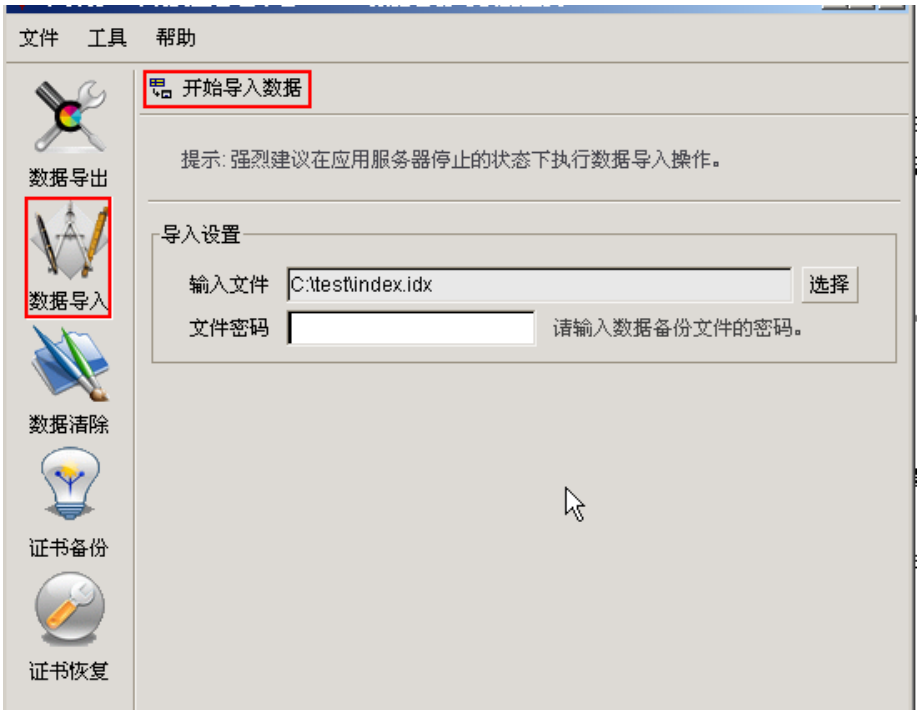


图 10-4　服务器数据导入

2. 单击“开始导入数据”，确认后进行数据导入操作。导入完成后，会有数据导入报告，用户可以查看导入结果，如图 10-5 所示。也可以单击“保存”按钮，将此报告保存起来。

图 10-5　数据导入报告

10.1.3　数据清除

1．单击“数据清除”功能按钮，进行清除数据项和时间段设置，如图 10-6 所示。在列表框中勾选要清除的数据项；单击开始时间和结束时间右边下拉框，选择时间段。

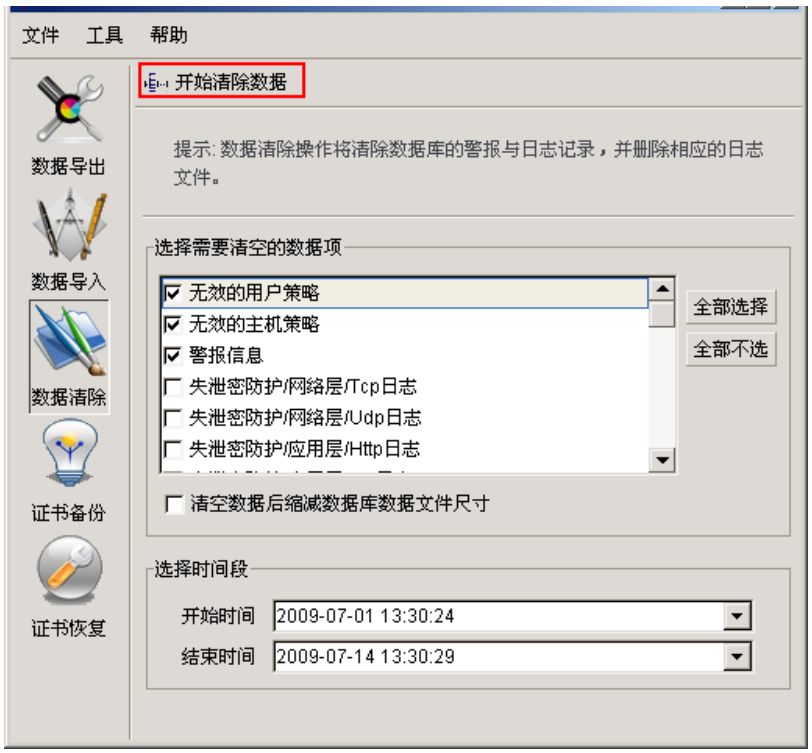


图 10-6　数据清除设置

2．单击“开始清除数据”命令，出现确认提示框，单击“确定”按钮后，开始数据清除操作。清空数据完成后，会有数据清空报告，如图 10-7 所示。清空数据后不能再恢复，操作时一定要谨慎。

图 10-7　清空数据报告

10.1.4　证书的备份

1．单击操作选项区中的“证书备份”，进入证书备份界面，如图 10-8 所示。单击“选择”按钮，选择输出备份文件路径。在服务器安装目录中，输入正确路径。

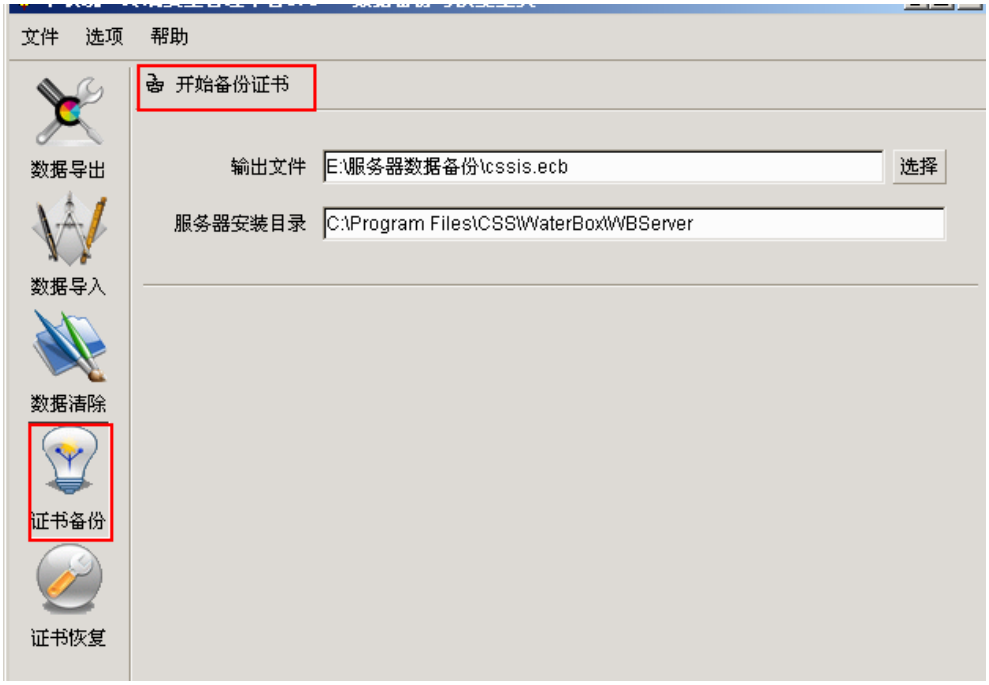


图 10-8　服务器证书备份

2．单击上面“开始备份证书”，开始备份操作。备份完成后，有成功提示框，如图 10-9 所示。

图 10-9　证书备份成功

10.1.5　证书的恢复

1．单击操作选项区中的“证书恢复”，进入证书恢复界面，如图 10-10 所示。单击“选择”按钮，选择输入备份文件路径。在服务器安装目录中，输入正确路径

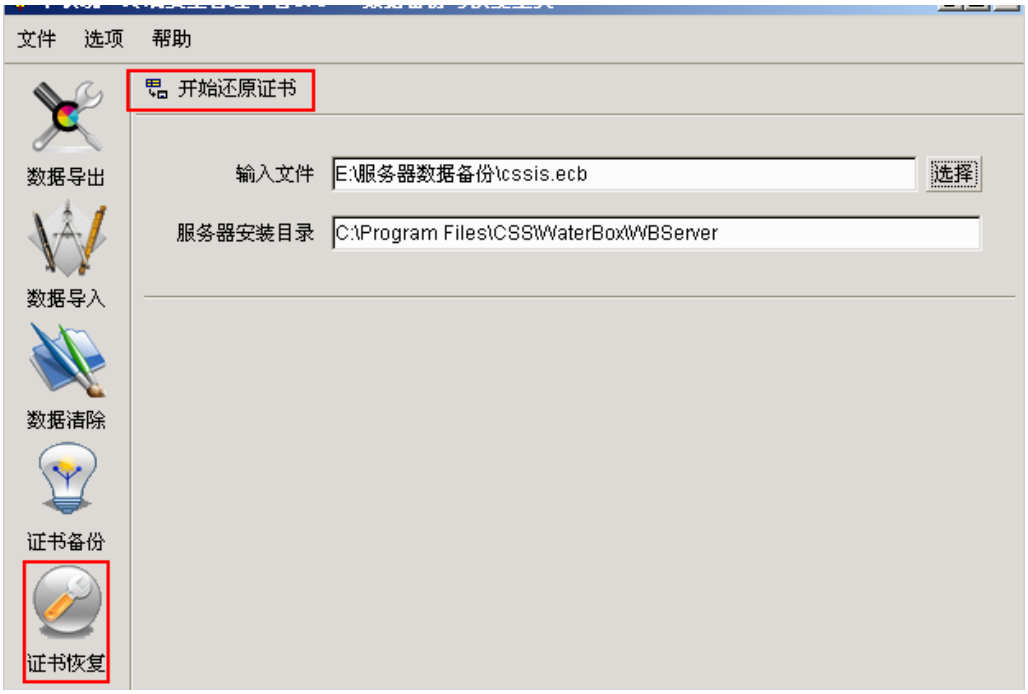


图 10-10　服务器证书的恢复

2．单击上面“开始还原证书”，开始还原操作。还原完成后，有成功提示框，如图 10-11 所示。

图 10-11　证书还原成功

10.1.6　定时备份

1．单击菜单项“配置”—“数据定时备份配置”，出现定时备份设置界面，如图 10-12 所示。

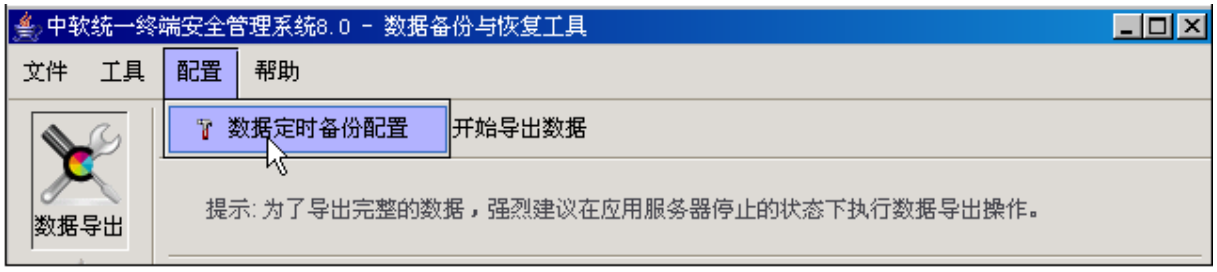


图 10-12　数据定时备份配置菜单项

2．在“数据定时备份配置”界面中，启用定时备份功能，设置备份周期、备份时间、备份数据规模、备份目录等，如图 10-13 所示。系统支持多任务，允许不同的时间点自动备份数据库内容，不同时间的备份文件自动以时间-日期命名。

系统将每次备份的详情汇总为一个报告文件（.txt 文件），同数据备份文件一同保存在同一个目录下。备份的最终结果能以邮件形式发送到指定邮箱，邮箱配置参见 SMTP 服务器配置。

提示：如果是设定的时间点，服务器意外离线了，那么等服务器上线后，会自动执行未备份的任务。

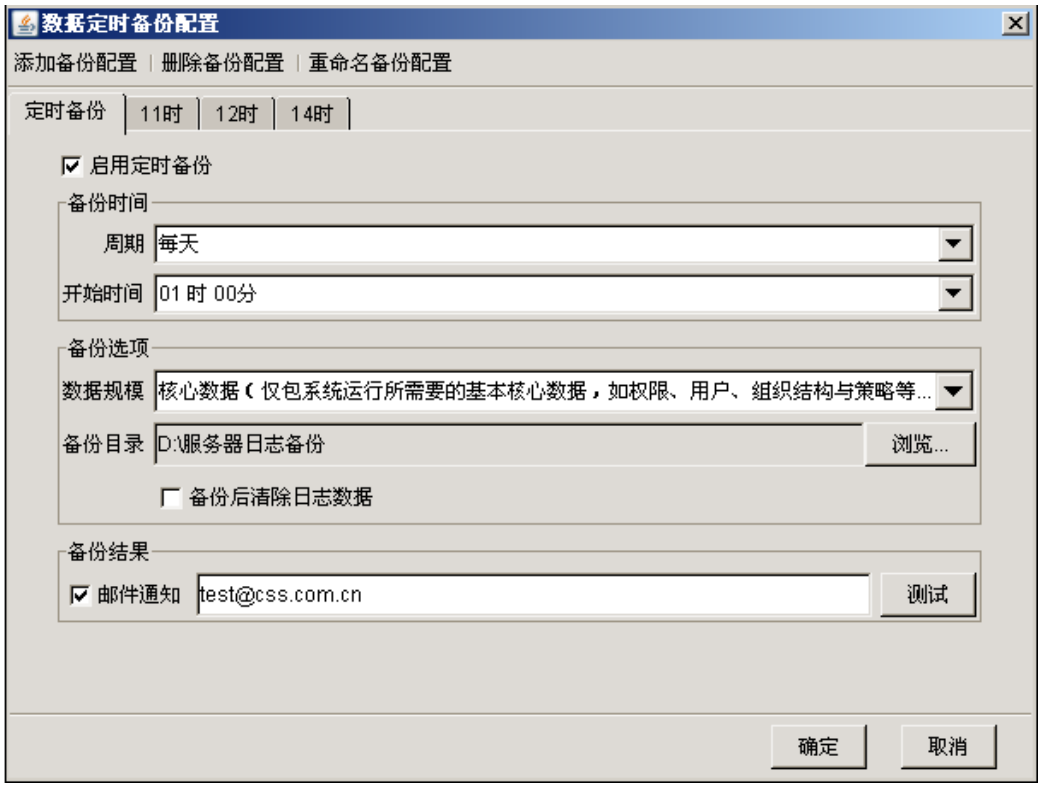


图 10-13　数据定时备份配置

10.1 手动备份与恢复指南

用户在使用过程中，某些情况下服务器出现故障，不能运行备份与恢复工具，这时需要进行手动备份与恢复，具体操作步骤如下：

一、备份过程

1、 备份数据库，通过 SQLServer 提供的备份工具备份数据库。也可将数据库分离到某个地方，然后将数据库备份。

2、 LDAP 备份（需停止 wbldap 服务），直接拷贝指定路径下的所有目录和文件即可，路径：服务器安装路径（例如 c:\program files）\CSS\UEM\WBLDAP\data

3、 服务器证书备份

服务器证书库（Server.keystore）：服务器安装路径（例如 c:\program files）\css\UEM\wbserver\server\default\conf

服务器证书（Wbserver.cer）：服务器安装路径（例如 c:\program files）\css\UEM\wbserver\server\default\conf

4、 配置文件

Jboss-service.xml ： 服 务 器 安 装 路 径 （ 例 如 c:\program files ） \css\UEM \wbserver\server\default\conf

Server.xml ： 服 务 器 安 装 路 径 （ 例 如 c:\program files ） \css\UEM \wbserver\server\default\deploy\jbossweb-tomcat55.sar

Adconfig.xml：服务器安装路径（例如 c:\program files）\css\UEM \wbserver\conf\adconfig.xml 只有同步域帐户后，才有此文件。

二、恢复过程

卸载服务器，手工删除数据库和 LDAP 数据

1、 重新安装服务器(参见安装手册) 。

2、 数据库恢复，通过 SQLServer 提供的恢复工具恢复。如果进行了数据库分离操作，需要附加数据库完成恢复。

3、 LDAP 恢复（需停止 LDAP 服务），将备份的数据拷贝到原相应路径下。

4、 证书库、证书和配置文件的恢复（需停止 wbserver 服务），将备份的文件分别拷贝到原相应路径下。

5、 启动 wbserver 和 wbldap 服务。

第十一章　服务器级联

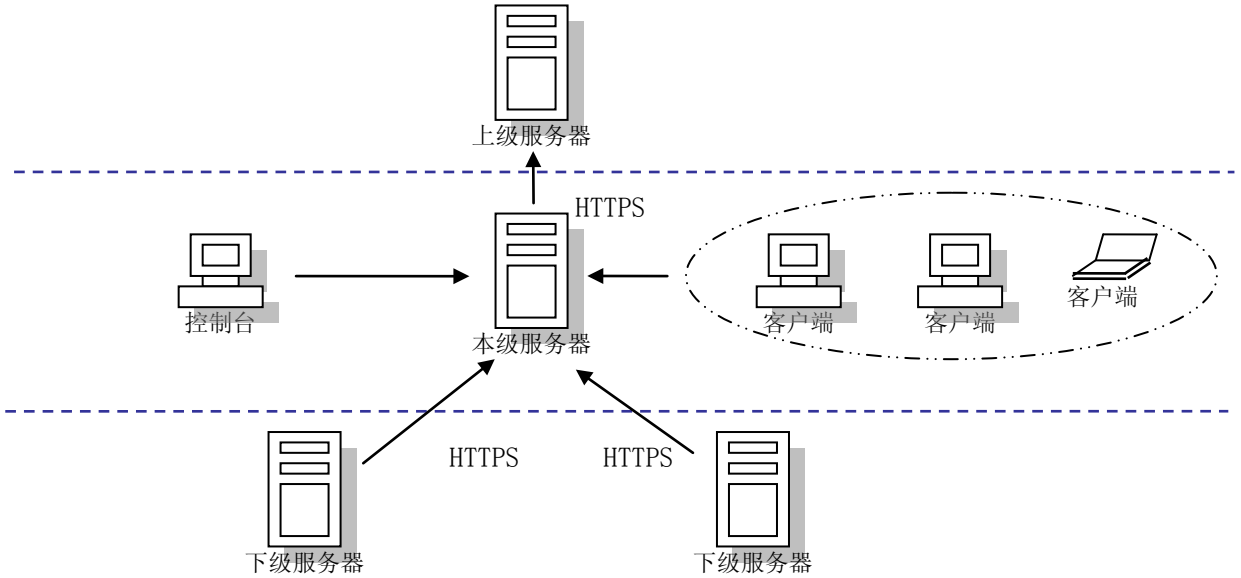
11.1 概述

随着 UEM 系统的推广，在一些规模较大的企业里，组织内的客户端超过一定数量时，单个服务器由于自身的运算速度和能力的限制，需要采用多个服务器进行负载分流。各个服务器之间根据树型结构组成一个服务器群，上级服务器向下级服务器发送策略，下级服务器根据上级要求传输相关数据。这样，上级服务器能够管理以自己为顶点的所有下级服务器以及他们所辖的终端主机情况，上、下多个服务器之间形成了级联关系，这就是我们所谓的“服务器级联”。

服务器级联是一个独立的功能模块，需要授权才可使用。在使用过程中，每级服务器通过控制台申请注册到上级服务器，上级服务器审核通过后，即可形成上、下服务器的级联关系。服务器级联不限于两层，在一个规模较大的单位里，可能存在多层级联关系。每层服务器都可以拥有自己的终端主机，且每层服务器与自己所带的客户端、控制台都是一个独立的系统。在服务器没有注册到上级服务器和没有自己的下级服务器时，整个系统和无级联时一样，服务器级联功能并不启动。

11.2 系统部署

在服务器级联系统中，每个服务器都是一个单独的子系统，包括本级服务器、控制台、客户端，以及上级服务器和下级服务器。本级服务器即可作为客户端访问上级服务器，也可作为服务器给控制台、客户端、以及下级服务器提供服务。其部署结构如下：



11.3 通信方式

上下级服务器之间采用 HTTPS 协议进行通信。下级服务器作为客户端单向访问上级服务器，上级服务器开设一组专门的 HTTPS 服务用来处理下级服务器的请求。

下级服务器以固定的频率访问上级服务器，从上级服务器的信号队列中获取与自己相关的命令，信号获取成功后，便返回一个销毁信号应答上级服务器，以便上级服务器从相应的信号队列销毁信号。然后解析命令并根据命令执行相关任务，当任务执行成功后，再向上级服务器回复相关应答，使上级服务器知道下达给下级服务器的命令所对应的任务已经成功执行，可以进行相应的处理。

11.4 使用方法

在使用服务器级联功能时，首先要进行下级服务器的注册，注册成功后能够实现组织结构上传、实时警报上传、警报统计和资产统计。具体操作过程如下所述：

11.4.1　注册

在下级服务器注册到上级服务器成为上级服务器的子服务器，是整个服务器级联系统中的最基本也是最关键的一步，通过这个步骤，多个服务器才能组合成一个级联系统。

◆　**导入证书**

通信证书是用来保证上、下级服务器之间进行信任通信的依据。下级服务器的管理员必须将上级服务器的通信证书，正确导入到本服务器后，才能实现上、下级服务器之间的正常通讯。

（1）点击“导入证书”，进入“导入证书”界面，如图 11-1 所示。将上级服务器证书拷贝到本级服务器，输入上级服务器证书所在的路径。然后输入上级服务器地址、端口号，检测本服务器是否能连接到上级服务器。

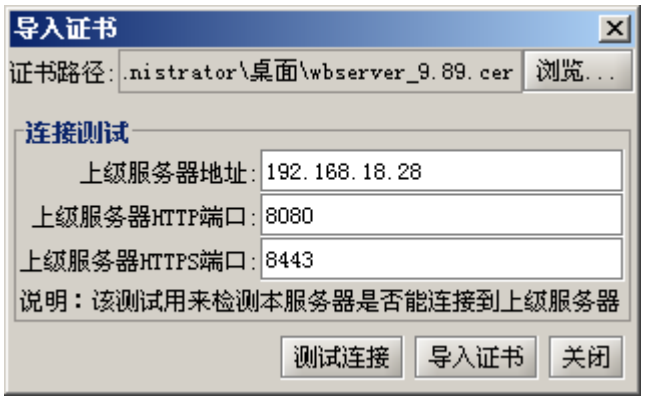


图 11-1　注册后本服务器

（2）单击“测试连接”按钮，测试本服务器是否能连接到上级服务器。如果能正常通信，再单击“导入证书”按钮，证书导入成功后出现提示框，确定即可，如图 11-2 所示。

图 11-2　导入证书成功

◆ **注册到上级服务器**

（1）登录控制台，点击组织结构管理→服务器级联→本服务器，进入本服务器页面，如图 11-3 所示。在这里可以看到本服务器的属性，包括：名称、当前路径、是否注册等。

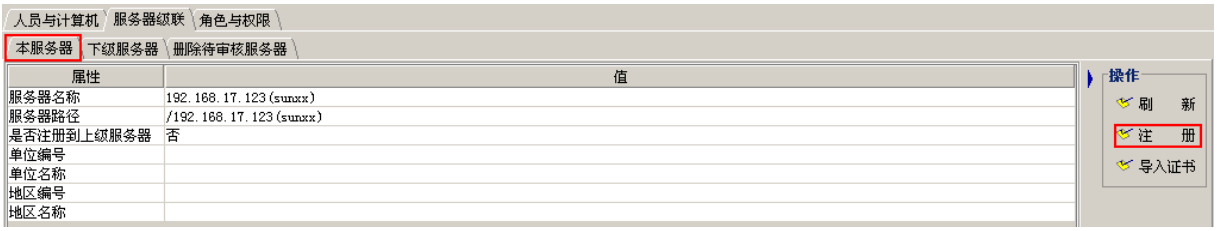


图 11-3　本服务器属性

（2）点击“注册”，进入注册界面，如图 11-4 所示。输入要注册到的上级服务器地址、HTTP 端口和 HTTPS 端口。另外，再给本服务器加一个好记的名称（不能含有字符“/”），以区分其它的服务器。

图 11-4　注册到上级服务器

（3）单击“确定”按钮，提示注册成功，如图 11-5 所示。注册成功后，可以在本服务器属性中查看该服务器的名称（别名）、级联路径、是否注册到上级服务器、注册时间、是否通过上级服务器审核，以及上级服务器的地址、端口号等，如图 11-6 所示。

图 11-5　注册成功

图 11-6　注册后本服务器属性

◆ 审核

下级服务器注册成功后，上级服务器会自动产生一个未通过审批的下级服务器。上级服务器的管理员根据情况审核下级服务器的注册。下级服务器被上级服务器审核通过后，才能向上级服务器上传数据。

（1）以有审核权限的用户登录控制台，点击组织结构管理→服务器级联→下级服务器，进入下级服务器页面，可以看到上面注册未审核通过的服务器，如图 11-7 所示。

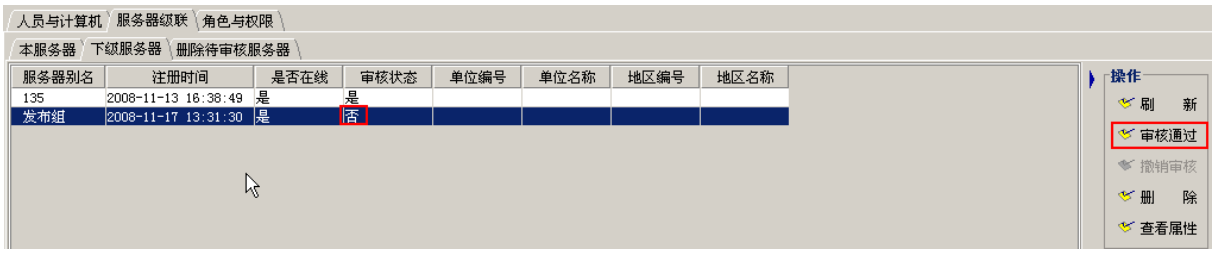


图 11-7　未审核通过的下级服务器

（2）选择未审核通过的下级服务器，点击右边的“审核通过”菜单项，可以看到审核状态由“否”变为“是”，如图 11-8 所示。

审核通过后，上、下级服务器之间形成了级联关系，可以正常通信，上级向下级传达信号命令，下级向上级传送数据。

图 11-8　审核通过的下级服务器

◆ 删除下级服务器

上级服务器的管理员有权删除自己的下级服务器，待删除的服务器被审核通过后，正式从上级服务器删除，清空与该服务器相关的数据，并向被删除的下级服务器发送删除信号。下级服务器接到自己被删除的信号，中断所有与上级服务器的通信，清空与上级服务器相关的数据，不再接收上级服务器要求上传的数据，并更改自己的路径，也通知自己的下级服务器更改路径；如审核不通过，下级服务器还原到原来的状态，继续与上级服务器保持通信。

（1）在上级服务器控制台中，选中要删除的下级服务器，如图 11-9 所示。

图 11-9　选择要删除的下级服务器

（2）单击右边的“删除”菜单项，出现确认框，如图 11-10 所示。确定后，此服务器被标记为删除待审核服务器，需通过审核后才能被彻底删除。

图 11-10　删除下级服务器确认框

（3）以有审核权限的用户登录控制台，点击组织结构管理→服务器级联→删除待审核的服务器，选定待审核的下级服务器，如图 11-11 所示。单击右边“审核通过”菜单项，出现一个提示框，确认删除后，该下级服务器被彻底删除。如果单击“审核拒绝”菜单，该下级服务器不被删除，恢复到原来状态。

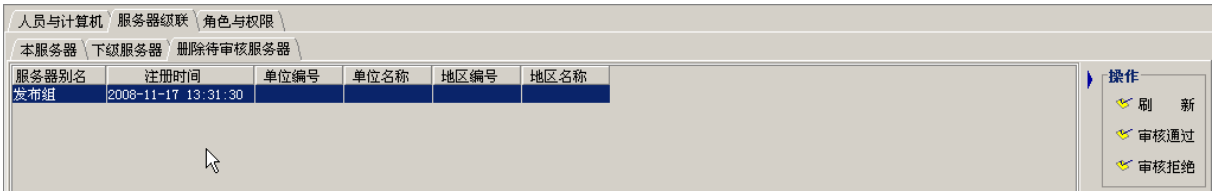


图 11-11　审核待删除的下级服务器

11.4.2　组织结构上传

服务器注册成功后，依次（部门、人员、计算机、客户端）读取本服务器的组织结构信息，向上级服务器上传。同时，实时监听本级服务器的组织结构变化，并把相应的操作与信息上传给上级服务器，以便上级服务器做相应修改。另外，本级服务器还能将下级服务器上传来的组织结构信息上传到上上级服务器。

（1）以管理员身份登录上级服务器控制台，点击组织结构→人员管理，可以看到下级服务器上传的组织结构信息，如图 11-12 所示。

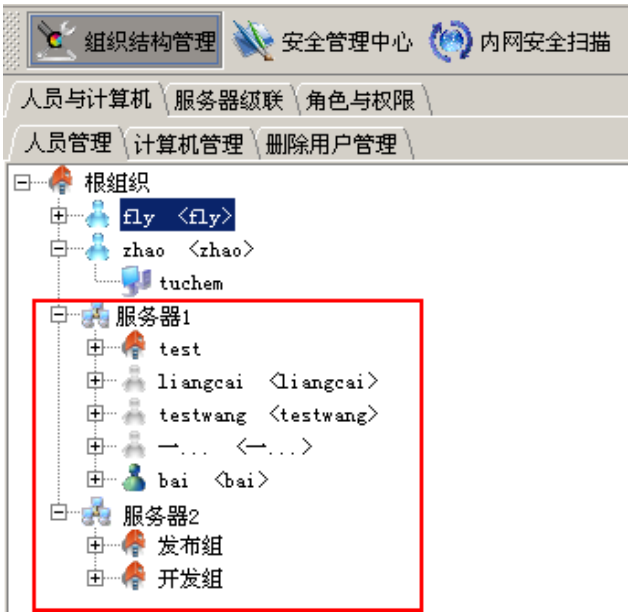


图 11-12　组织结构上传信息

（2）上级管理员只能查看下级服务器上传的组织结构信息，不能对下级服务器的组织结构进行管理。

提示：组织结构管理的其它部分操作请参阅“组织结构管理”

11.4.3　报警上传

上级服务器向下级服务器下发报警策略，定义下级服务器上传的报警日志类型，下级服务器会根据上级的要求，及时上传报警日志。这样一级一级往上传，可以把报警日志上传到顶级服务器。

◆ **级联警报策略**

（1）登录控制台，点击响应与知识库→级联警报策略，进入级联警报策略设置界面，如图 11-13 所示。

警报类型	上级服务器要求上传类型	本服务器要求上传类型	下级服务器实际要上传类型	本服务器警报等级
⊟ 失泄密防护	0	0	0	
⊞ 网络层	0	0	0	
⊞ 应用层	0	0	0	
⊞ 非法外连	0	0	0	
打印	☐	☐	☐	三级
⊞ 接口控制	0	0	0	
截屏键控制	☐	☐	☐	三级
⊞ 资产信息管理	0	0	0	
⊞ 运行状况监控	0	0	0	
⊞ 终端安全管理	0	0	0	
⊞ 可信存储管理	0	0	0	
汇　总	0	0	0	

图 11-13　级联警报策略设置

（2）单击“⊞”展开警报类型，单击“⊟”收缩警报类型。选择☑本服务器要求上传的日志类型，点击“应用”按钮，将策略下发。

提示：

1. 如果上级服务器要求上传 TCP 报警日志，那么本级服务器和下级服务器都要将 TCP 报警日志上传给上级服务器。下级服务器首先将报警日志上传给本级服务器，然后通过本级服务器将日志上传给上级服务器。

2. 如果上级服务器要求上传 TCP 报警日志，本级服务器没有选择 TCP 报警日志，那么本级服务器也要将自己的 TCP 报警日志和下级服务器的 TCP 报警日志一并上传给上级服务器。

3. 如果上级服务器没有要求上传 TCP 报警日志，但上上级服务器要求上传 TCP 报警日志，那

么本级服务器也要将自己的 TCP 报警上传给上级服务器，通过上级服务器上传给上上级服务器。

4．如果上级服务器不要求上传，本级服务器要求上传的数据，下级服务器和下级服务器就将数据上传到本级服务器为止。

5．上级服务器也指所有的上级服务器，只要有一个下发上传报警日志的策略，它以下的所有下级服务器都要按照这个策略将报警日志上传给它为止。当然下级服务器也指所有的下级服务器，当上级服务器下发某个策略时，它以下的所有下级服务器都要按照这个策略去执行。

◆ 级联警报

（1）点击响应与知识库→级联警报，进入级联警报界面，如图 11-14 所示。根据级联警报策略设置，在这里查看下级服务器的报警日志。

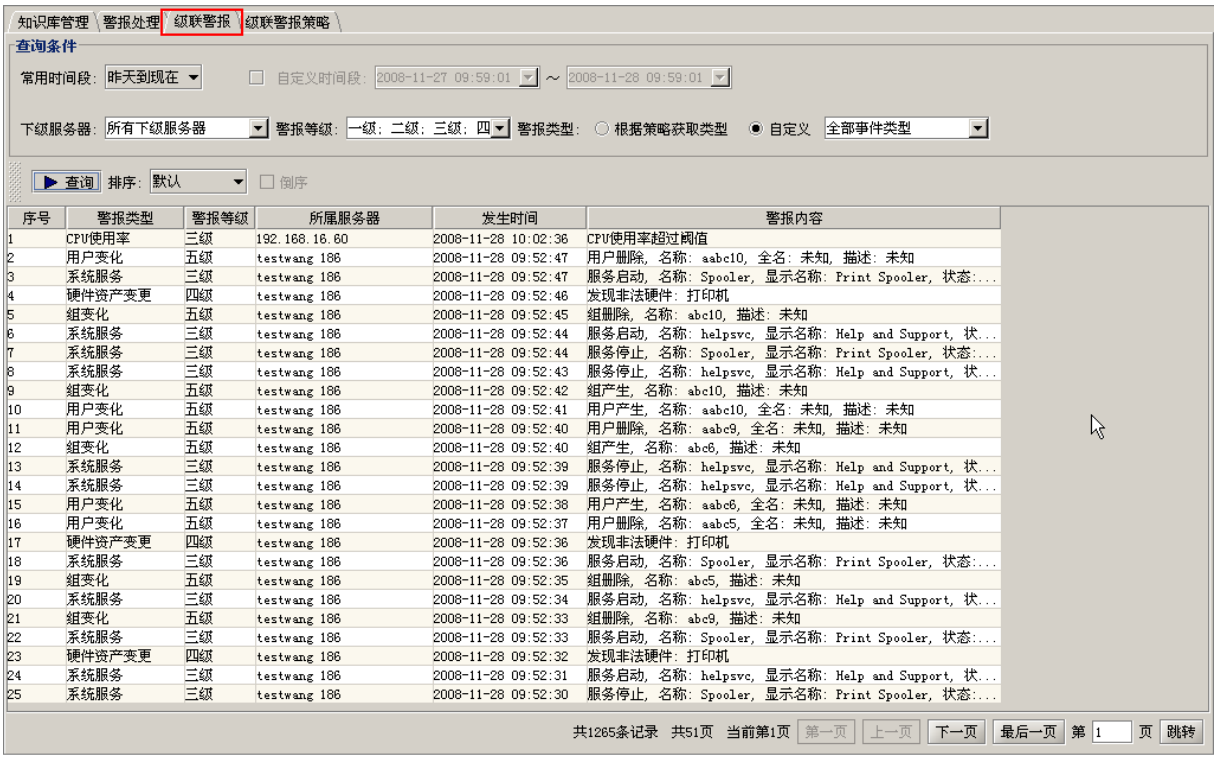


图 11-14　级联警报信息

（2）用户可以选择时间段、所属的下级服务器、警报等级、警报类型等条件查询，查询结果也可以按选项排序，方便用户使用。

提示：

1．“级联警报”显示的日志信息是根据“级联警报策略”设置实时上传的日志信息，有告警信息就上报，没有告警信息就不报。“统计与审计分析”中“级联统计”显示的告警信息，是根据“级联统计策略”设置定时上传的日志信息，在规定的时间段内有告警信息或者没有告警信息，在规定的时间点都要上报。

2．响应与知识库管理其它部分操作请参阅第六章“响应与知识库管理”。

11.4.4　日志统计上传

日志统计上传就是将警报信息、软硬件资产信息按设定的时间段定期上传，支持时报、日报、周报、月报、年报和自定义等多种上传方式。

◆ **级联统计策略**

（1）点击统计审计分析→级联统计策略，进入级联统计策略界面，如图 11-15 所示。选择下级服务器，设置具体上报时间。

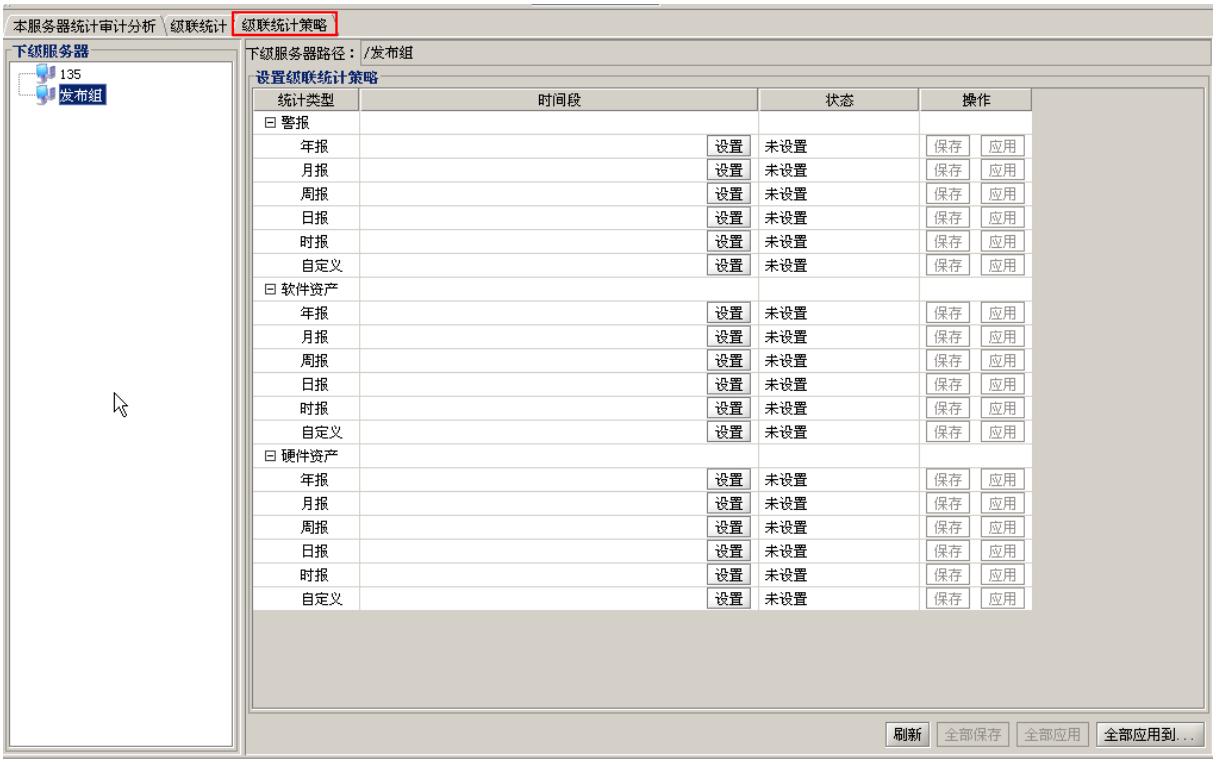


图 11-15　级联统计策略

（2）单击年报、月报、周报、日报、时报后的“设置”按钮，弹出时间设置框，在这里设置开始时间和上报时间点，如图 11-16 所示。

系统默认设置，开始时间就是当前系统时间，年报为每年的 1 月，月报为每月的 1 日，周报为每周的星期日，日报为每天的 1 点，时报为每个小时的第 1 分钟。如果选择自定义，可以按照用户需要自由设置。

例如：我们设置 2008-01-01 开始，每周的星期日进行报表统计（周报）。

图 11-16　　设置时间框

（3）设置完成后，单击“保存”、“应用”，可以单个保存应用，也可以全部保存应用。策略下发给选择的下级服务器后，下级服务器将以设置的方式上传数据。

◆ 级联统计

（1）单击“统计审计分析”→“级联统计”，查看下级服务器上传的数据信息。选择下级服务器和报表类型，可以看到详细信息。

例如：我们根据上面设置的周报策略（2008-01-01 开始，每周的星期日进行报表统计），查看 2007-10-01～2008-11-01 的周报。因为我们设置的开始统计时间是 2008-01-01，那么我们要查询的 2007-10-01～2008-01-01 这个时间段不存在周报的，不会显示出来，只能显示 2008-01-01～2008-11-01 这个时间段的周报信息，如图 11-17 所示。

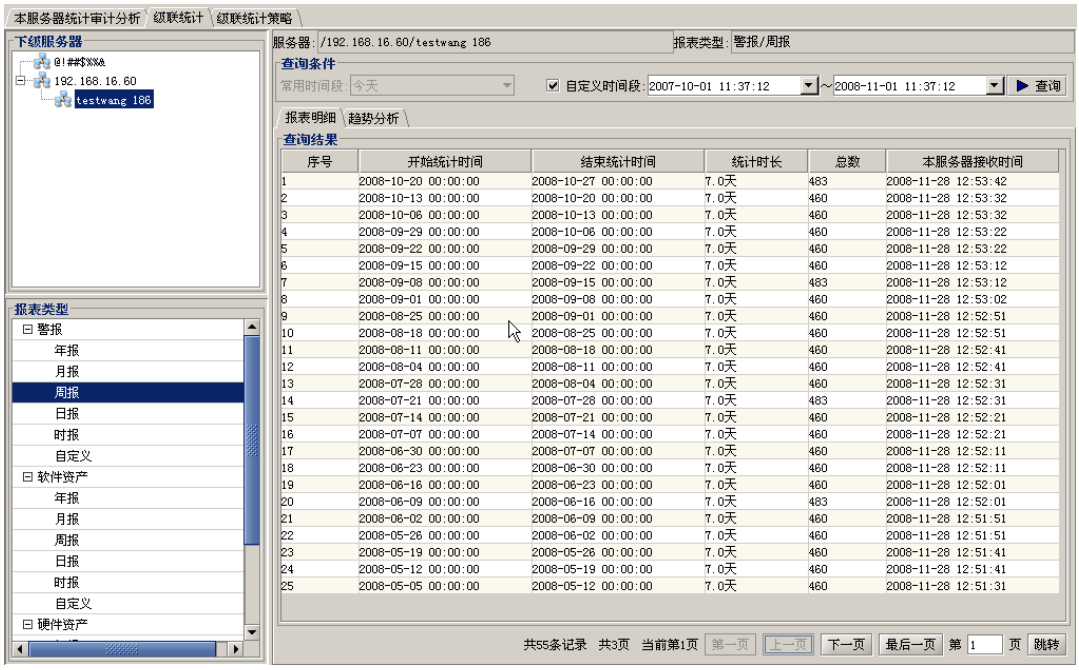


图 11-17　　级联统计界面

提示：

1. 若报表类型选择“时报”，常用时间段选择“本周”可以看到本周下级服务器上传的时报；若报表类型选择“时报”，常用时间段选择“本月”将看到本月下级服务器上传的时报。时报列表随着时间段变化。

2. 若选择年报、月报，常用时间段内（“本周”、“最近一天”、“今天”、“昨天到现在”）没有上传的年报和月报信息，将显示为空。

3. 如果统计策略设置自定义方式，统计时间段为 2007-01-01 至 2007-12-30，那么你在 2007-12-30 之前是看不到统计结果的，必须在 2007-12-30 之后才能看到统计报表。

（2）在列表中选择某一行，双击进入查看统计数据，如图 11-18 所示。不同的统计模式显示不同的统计结果。

	一级	二级	三级	四级	五级	合计
失泄密防护	0	0	180	0	0	180
资产信息管理	0	0	20	20	0	40
运行状况监控	0	0	140	0	20	160
终端安全管理	0	0	80	0	0	80
合计	0	0	420	20	20	460

x轴	分组
警报等级	类型
警报等级	状态
类型	警报等级
类型	状态
状态	警报等级
状态	类型

图 11-18　查看统计数据

（3）单击“趋势分析”，显示汇总表，如图 11-19 所示。选择右边的“分组方式”和“时间设置”，显示不同的列表。

图 11-19　趋势分析汇总表

（4）单击“趋势分析”，显示曲线图，如图 11-20 所示。选择右边的“分组方式”和“时间设置”，曲线图随着变化。不同的颜色有不同的含义，注意观察。

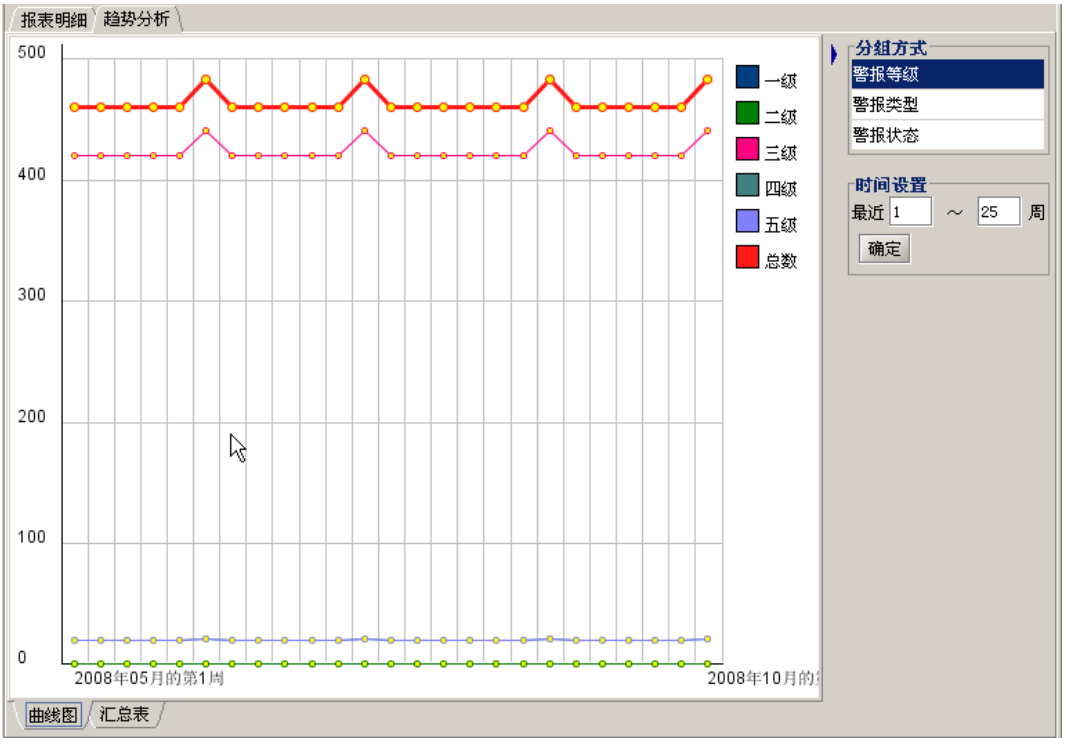


图 11-20　趋势分析曲线图

提示：统计审计分析的其它部分操作请参阅第七章“统计审计分析”。

第十二章　客户端操作指南

中软统一终端安全管理系统 8.0 客户端（简称客户端）能将用户的重要文件和敏感信息进行加密保护，还能将加密文件解密到指定的路径，方便带出使用。另外，客户端能和控制台即时通讯，向控制台发送即时消息，同时也能接收控制台发送过来的消息。

12.1 我的加密文件夹

1．客户端安装成功后，桌面上出现“我的加密文件夹”图标，如图 12-1 所示。

加密文件夹的目的是为终端用户提供存放敏感文件的安全目录，在该目录下的文件都是加密的，只有该用户自己可以查看。

图 12-1　我的加密文件夹

2．用户只要将文件拖在“我的加密文件夹”中，就变成了加密文件（文件图标有小锁标志），如图 12-2 所示。

图 12-2　加密文件

3．如果要在本地打开加密文件，只需双击自动解密查看，但保存以后还是加密的。如图 12-3 所示。

提示：我的加密文件夹加密属主动加密，用户根据自己的意愿选择是否加密。安全文档加密属被动加密，需要通过控制台下发加密进程策略。

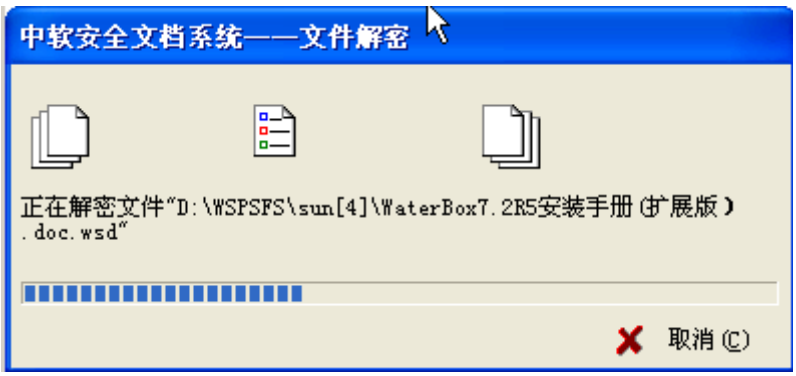


图 12-3　双击自动解密

12.2 安全文件传输

客户端要在 UEM 系统内向其它客户端传输文件时，系统自动用公钥将被传输的文件加密，然后通过网络方式发送到 UEM 服务器。如果接受数据的用户在线，则将加密文件自动发送到接受方，接受方用公钥解密后，再用自己的私钥加密到“我的加密文件夹”中；如果接收用户不在线，加密传输的文件可以在服务器暂时保留七天，七天内用户一旦上线，则自动接收加密传输的文件。

1. 在客户端选择要加密传输的文件，单击右键选择“安全文件传输”菜单项，如图 12-4 所示。

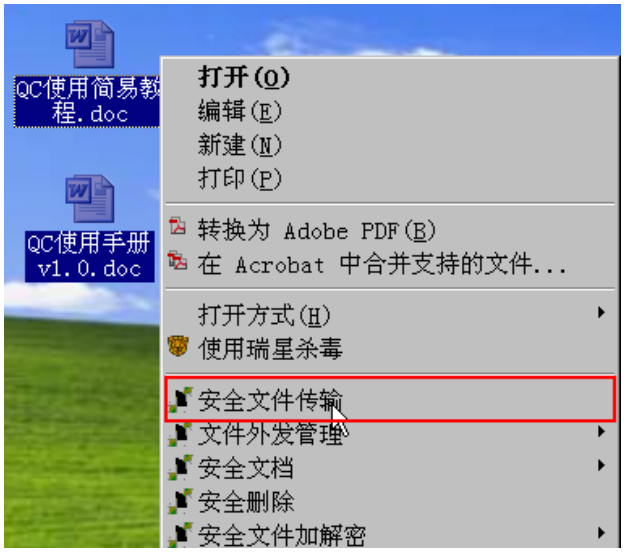


图 12-4　安全文件传输菜单项

2. 在安全文件传输界面中，可以添加要传输的文件，选择接受的用户，如图 12-5 所示。

单击“添加文件”按钮，只能添加“与当前选择传输的文件”同一文件夹下的文件，不同的路径下的文件，不能一同传输。每一次传输时，最多可添加 50 个单文件，并且每个文件的大小不能超过 100M。

人员选择方式有两种：实时搜索和常用列表。刚开始使用时，还没有存储常用用户列表，只好选择实时搜索方式。

如果你准确知道接受方的用户名，可以在“待选人员”下面框中，输入待查找的用户名，系统将按模糊匹配的方式，搜索出所有与之有关的用户，供你选择；如果你不知道接受方的用户名，可以单击“查看组织”按钮，通过筛选组织的方式，逐一选择用户。最后，单击“添加”按钮，将选择的用户，添加到“待传输的人员列表”中。

在“待传输的人员列表”中，最多可添加 100 个用户，也就是说，可同时给 100 个用户传输文件。如果暂时不需要给某个用户传输文件，可以选中该用户将其移除。为方便以后传输文件，可将“待传输的人员列表”存储为常用列表。下次给同样的用户传输文件时，选取“常用列表选取”方式，再选择常用列表名称，省去一个一个选择用户的麻烦。

图 12-5　安全文件传输界面

3. 最后，单击下方的“传输”按钮，将选定的文件传输给指定的用户。传输文件成功后，传输方和接收方的客户端都会弹出提示信息，如图 12-6 所示。

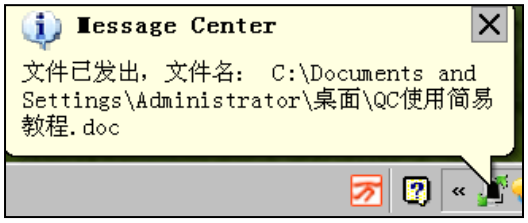


图 12-6　文件传输成功提示信息

12.3 文件传输日志查看

文件安全传输功能还可以通过客户端右键菜单实现，操作过程和上面讲的一样，不再重复。这里只叙述文件传输日志的查看。

1．选中任务栏客户端图标，单击右键选择菜单项“文件传输日志查看”，打开日志信息查看界面，如图 12-7 所示。

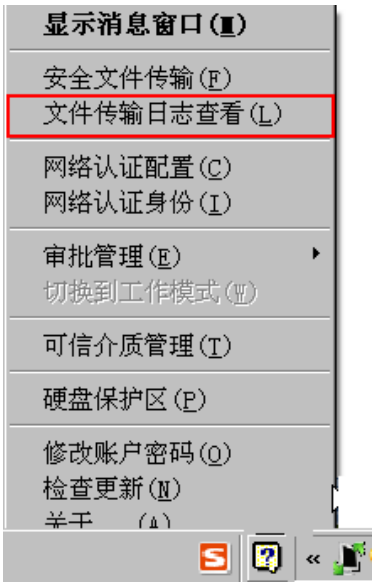


图 12-7　选择“文件传输日志查看”菜单项

2．在“文件传输日志查看”界面，可以看到发送文件的日志信息，包括：发送人名称、发送人计算机、发送人计算机 IP，以及接收人名称、接收人计算机、接收人计算机 IP 和发送结果等等，如图 12-8 所示。

请用户留意“发送结果”列表项，发送和接收成功后，显示“成功”。如果对方的客户端没在线，在“发送结果”中显示“等待中”。如果对方的客户端超过规定时间没在线，那么在“发送结果”中，将显示发送“失败”。

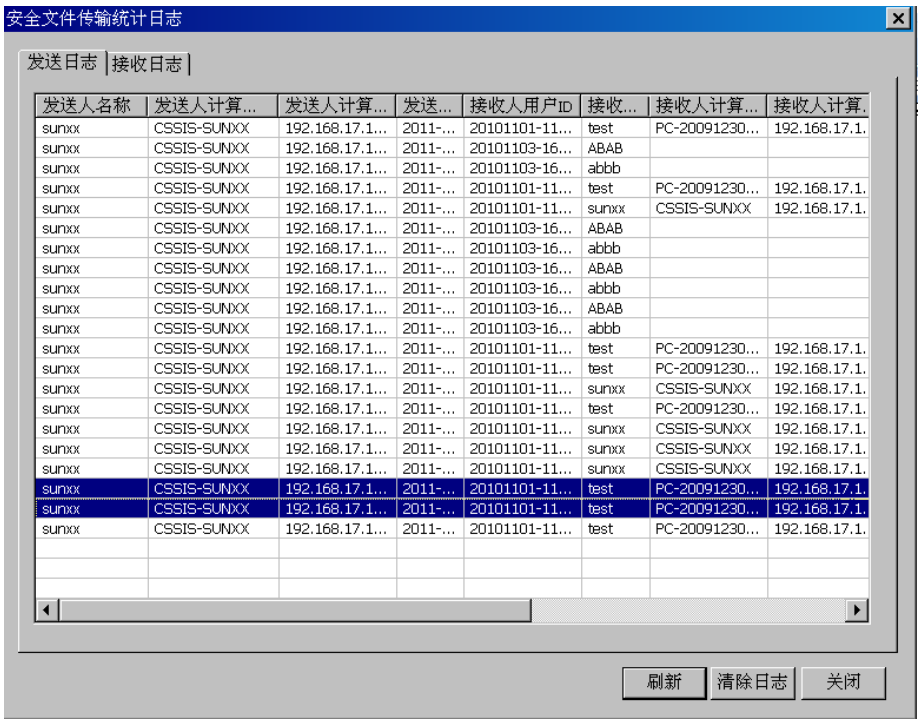


图 12-8　文件传输的发送日志

3．单击“接收日志”标签页，可以看到接收文件的日志信息，包括：发送人名称、发送人计算机、发送人计算机 IP，以及接收人名称、接收人计算机、接收人计算机 IP 和发送结果等等，如图 12-9 所示。

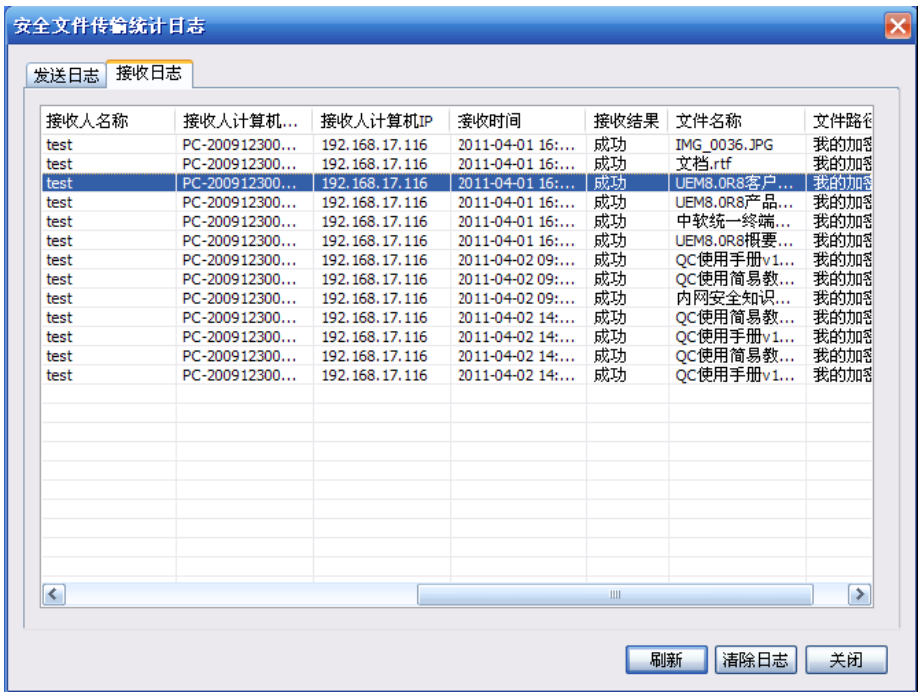


图 12-9　文件传输的接收日志

12.4 安全文件加密

1．安全文件加密也属主动加密范畴。如果用户想将某些文件加密，选定这些文件后单击右键菜单，选择“安全文件加解密”→“加密”、“加密到”或者“加密到我的加密文件夹”，如图 12-10 所示。例如：单击“加密到”菜单项，进入下一界面。

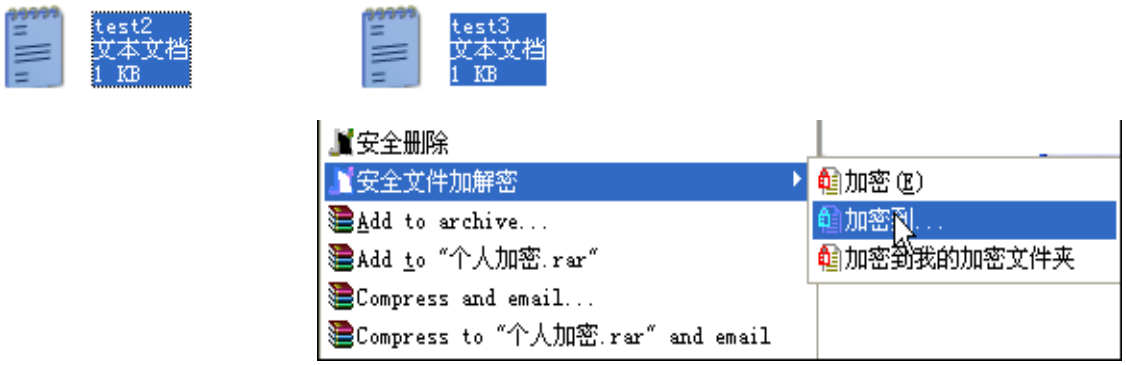


图 12-10　安全文件加解密

选项说明：

“加密”是将选定文件加密保存在原来路径下；

“加密到”是将选定文件加密保存在指定路径下；

“加密到我的加密文件夹”是将选定文件加密保存在“我的加密文件夹”中，这和直接拖进去是一样的。

2．选择加密类型（个人加密、小组用户、公共用户、指定用户），如图 12-11 所示。如果选择加密类型为“指定用户”，则在右侧出现查看组织和添加用户的界面，根据需要指定能查看加密文件的组织和用户。最后，单击“下一步”继续。

个人加密：对个人数据进行加密，以防止其他人员窃取私人信息。

小组用户：将数据文件加密后，仅供同一组织内成员查看，组织成员由控制台决定。

公共用户：经过此类型加密后的数据文件，可供整个安全域内成员查看。

指定用户：采用此种方式加密后的文件，只有指定用户才能解密。

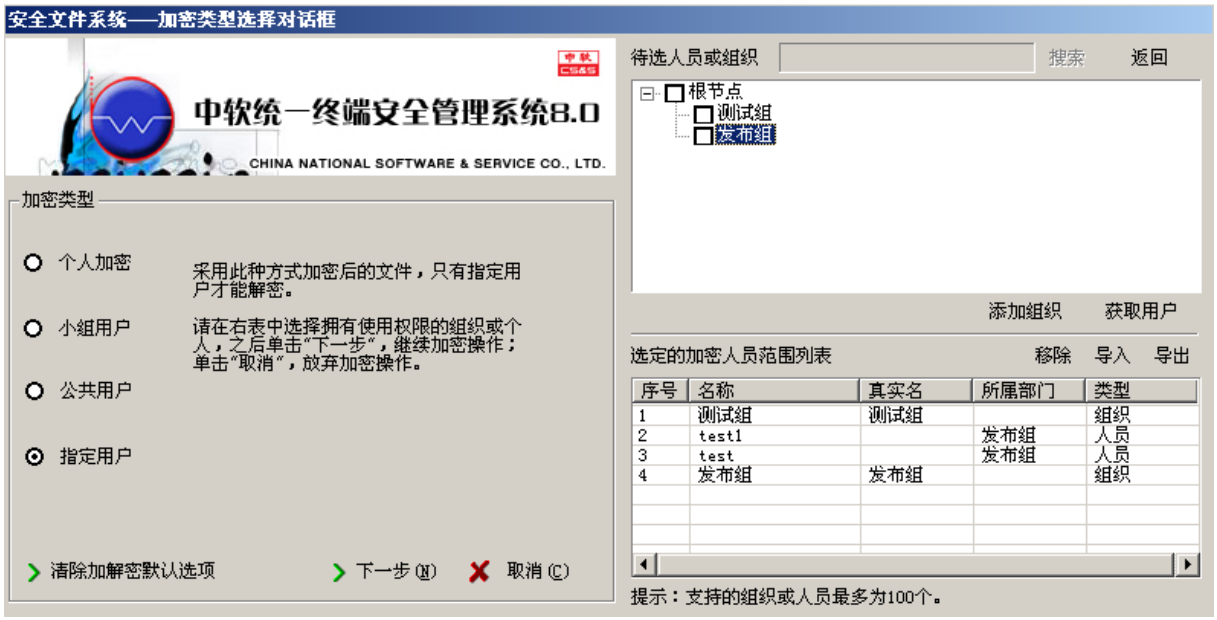


图 12-11　选择加密类型

3．从下拉框中选择加密算法。如果要把选定的加密算法做为以后默认设置，就勾选下面的选项框“以后均按此次选择执行”，如图 12-12 所示。单击“下一步”继续。

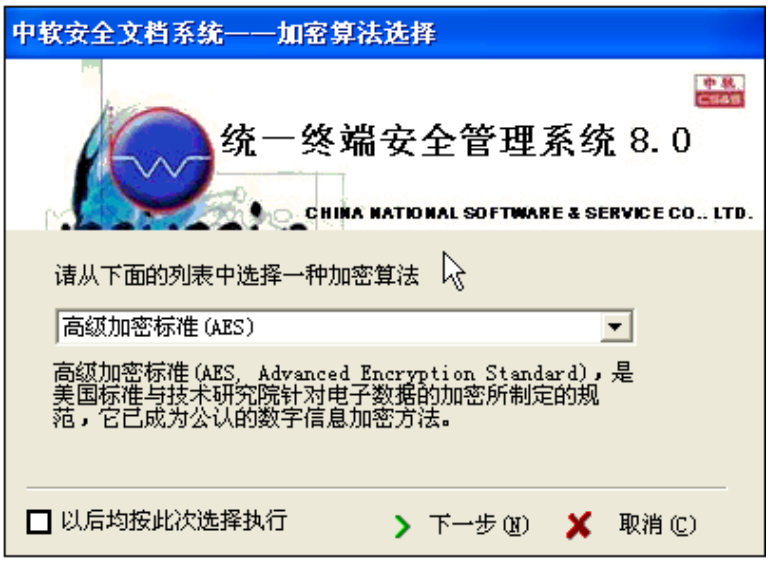


图 12-12　选择加密算法

4．单击浏览按钮“ ”，指定加密文件要存放的路径，然后单击“下一步”继续，如图 12-13 所示。如果单击“ 清除加解密默认选项”，可以清除原来保存的默认设置。

图 12-13　选择加密文件路径

5．如果操作过程中出现相同的文件名，选择你需要的操作方式：直接覆盖重名文件、系统自动指定新文件名、自己指定新文件名，如图 12-14 所示。单击“下一步”继续。

图 12-14　重名时选择

6．选择操作完成后，删除原文件或者保留原文件，如图 12-15 所示。

图 12-15　选择对原文件的处理

7. 加密操作完成后，单击“关闭”退出操作。也可以选择“操作完成后自动关闭”，下次加密操作完成后自动退出，如图 12-16 所示。如果要查看加密日志，单击“显示日志”，即可查看哪些文件被成功加密了，存放在什么地方。

图 12-16　结束加密操作

8. 加密操作结束后，即可在指定的位置看到已加密的文件，被加密的文件图标不一样，上面有一个小锁图标，如图 12-17 所示。

图 12-17　查看加密文件

提示：

（1）个人加密文件为紫色图标，上面有一个字母 S；小组加密文件为绿色图标，上面有一个字母 G；全域加密文件为红色图标，上面有一个字母 D；指定用户加密文件为蓝色图标，上面有一个字母 P。

（2）主动加密后的文件，不要通过属性项更改默认打开方式，否则双击该文件后打开是密文，不再是明文。

12.5 安全文件解密

1．主动加密的文件带出使用时，需要解密。单击右键菜单，选择“安全文件加解密”→“解密到”或者“解密”，如图 12-18 所示。

图 12-18　选择解密文件

2．单击浏览按钮“ ”，选择解密文件的存放路径。可以清除解密默认选项，重新设置。最后，单击“下一步”，继续进行，如图 12-19 所示。

图 12-19　选择解密文件的存放路径

3．如果在操作过程中出现相同的文件名，可以直接覆盖或者指定新文件名，如图 12-20 所示。可以选择“以后均按此次选择执行”，做为默认设置。

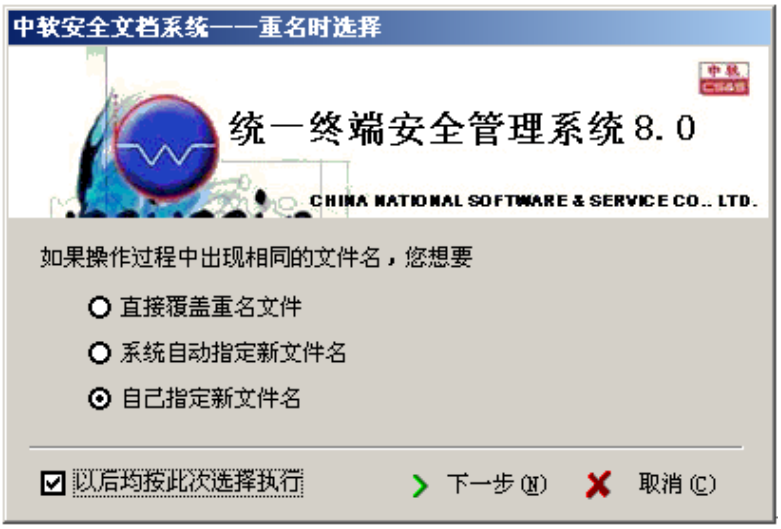


图 12-20　重命名时选择

4．操作完成后，可以删除原文件或者保留原文件，如图 12-21 所示。可以选择“以后均按此次选择执行”，做为默认设置。

图 12-21　选择对原文件的处理

5．正在进行解密操作，选择操作后自动关闭，如图 12-22 所示。

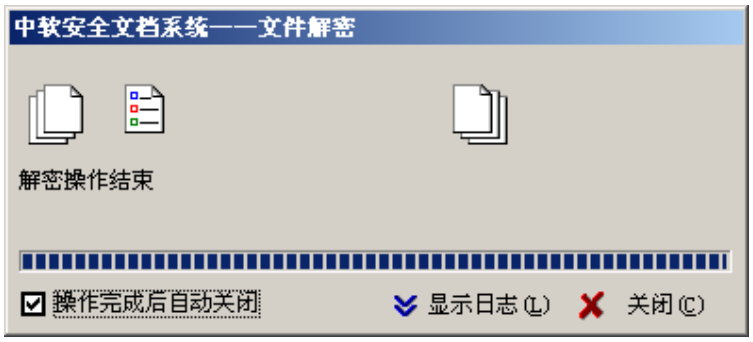


图 12-22　解密操作

注意：解密文件时可能会出现无法同时解密多个加密文件的现象。此时可以把这些文件拷贝到一个文件夹下，对这个文件夹进行解密操作，即可完成对多个文件的解密。

6．解密完成后，能够在指定路径下看到解密文件。

提示：

（1）安全文件解密产生的日志信息，可以在控制台“统计审计分析→日志信息统计→客户端监控日志→文件安全管理→安全文件分发→文件解密”查看。

（2）安全文件解密到可移动存储设备时，产生的日志信息可以在控制台“统计审计分析→日志信息统计→客户端监控日志→文件安全管理→安全文件分发→解密带出”查看。

（3）安全文件加密操作产生的日志信息，可以在控制台“统计审计分析→日志信息统计→客户端监控日志→文件安全管理→安全文件分发→文件加密”查看。

12.6 安全删除文件

Windows 操作系统自带的删除功能，将文件删除后大多还能通过恢复工具还原。如果要将文件彻底删除，就要用到“安全删除文件”功能。

选择要删除的文件，单击右键菜单，选择“安全删除文件”，出现操作提示框，如图 12-23 所示。“确定”后，即可将文件彻底删除。

提示：

（1）客户端彻底删除文件后，不能再恢复。删除快慢与本机的数据回添次数有关，次数越大，删除文件越慢，详见“安全操作配置”章节。另外，安全删除文件时，因日志量过大，系统不记录操作日志。

（2）对于普通文件，或者普通加密文件，采用这种方法删除比较安全。如果是密级文件，则采用销毁将文件彻底删除。

（3）在 win7 系统下，安全删除文件时可能会弹出错误提示信息，这与管理员权限和路径有关。

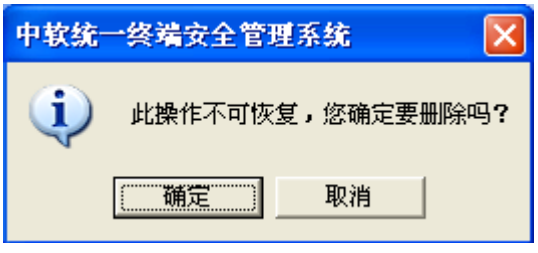


图 12-23　删除文件提示框

12.7 密级文件管理

在控制台给客户端用户下发“启用加密进程策略”，客户端用户启动加密进程后，创建的文件自动变成普通加密文件。根据保密管理的需要，用户可以将普通加密文件申请转化为不同密级的文件，对于密级文件的流转去向，也能进行轨迹追踪。创建、修改、销毁、带出密级文件有一个审批过程，审批规则需在控制台的“审批管理”中创建，在那里设置审批员、审批范围、审批内容等，参见审批管理章节。

普通安全文档，也就是启用加密进程加密的普通加密文件，没有密级之分，一般显示为黄色图标。用户创建的密级文件有四种级别：普通、秘密、机密、绝密，密级依次增高。各种密级文件的图标不一样，请用户注意区分。普通级密级文件为蓝色一个星，秘密级密级文件是黄色两个星，机密级密级文件为橙色三个星，绝密级密级文件为红色四个星，如图 12-24 所示：

图 12-24　显示不同图标的加密文件

提示：（1）用户密级可以通过客户端图标右键菜单“关于”查看。

（2）当用户访问密级文件时，受“密级文件策略”限制，参见密级文件策略章节。

12.7.1 创建密级文件

1. 选择普通加密文件 test1.doc，单击右键菜单“密级文件管理”→“创建”，弹出申请创建密级文件界面，如图 12-25 和 12-26 所示。选择文件密级和使用范围，输入申请理由，勾选是否启用轨迹追踪，最后，单击“提交”按钮。

注意：在文件被审批过程中，请不要移动和修改文件。否则，会导致审批失败。

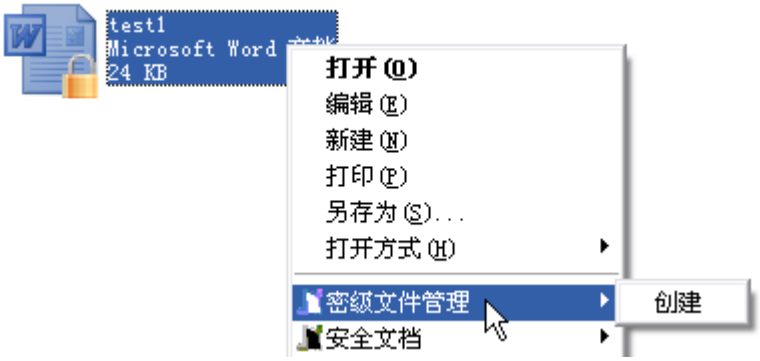


图 12-25　选择创建密级文件菜单

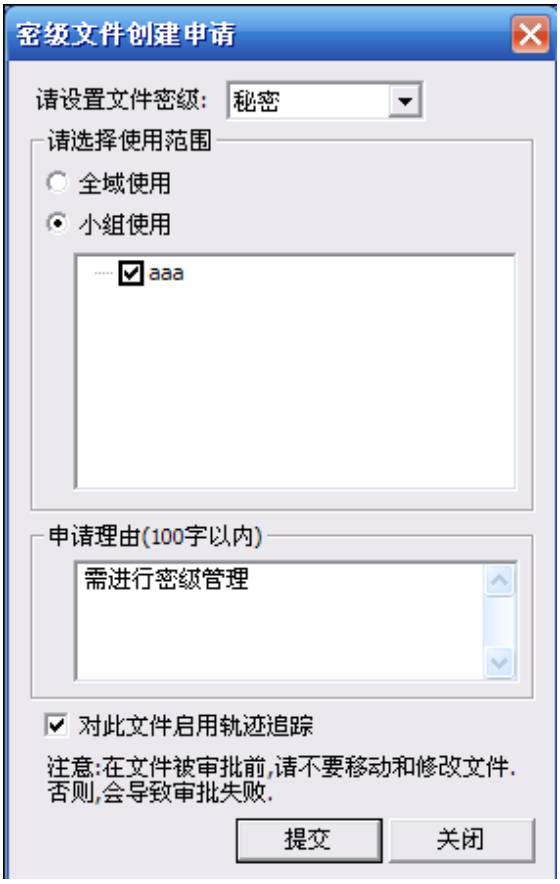


图 12-26　申请创建密级文件

2. 待审批的文件上传服务器成功后，客户端会弹出消息框，如图 12-27 所示。

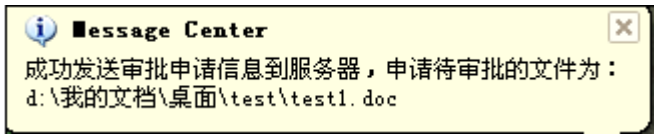


图 12-27　上传审批单成功提示

3. 审批员接到服务器派发的审批请求单，会在任务栏弹出消息框，如图 12-28 所示。

提示：审批员是由审批管理中审批规则确定的。客户端不能自己审批自己的文档。

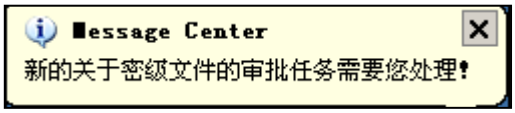


图 12-28　提示审批员有审批任务

4. 审批员单击客户端右键菜单“审批管理”→“密级文件审批管理”，进入“密级文件审批管理”界面，如图 12-29、12-30 所示。单击“刷新”按钮，显示待审批的文件。

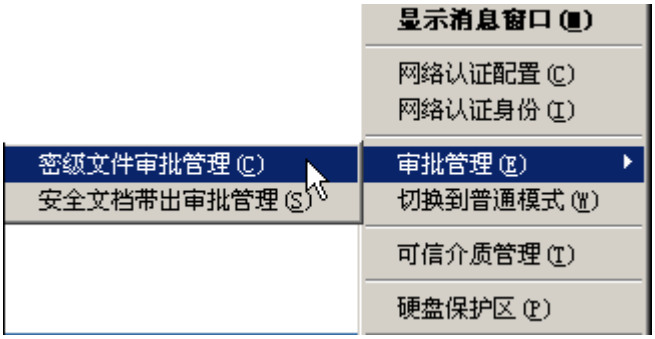


图 12-29　密级文件审批管理菜单

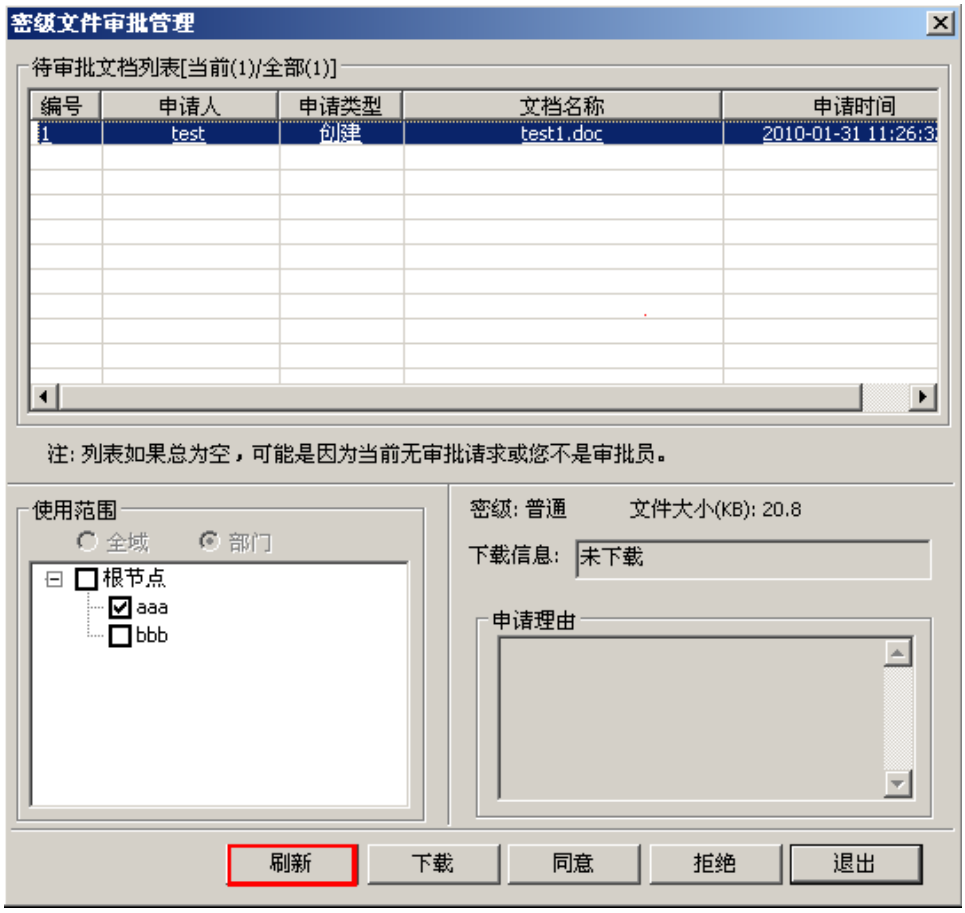


图 12-30　密级文件审批管理界面

5. 单击“下载”按钮，将待审批的文件下载到审批员指定的路径下，如图 12-31 所示。

图 12-31　选择下载路径

6. 如果文件比较大，下载过程可能比较缓慢，请耐心等待，不要关机或重启。下载完成后，弹出消息框，如图 12-32 所示。

图 12-32　下载成功提示框

7. 审批员单击下载的文件，查看具体内容，如图 12-33 所示。

提示：这时的审批员可以打开任何密级的下载文件，不受密级文件策略限制。

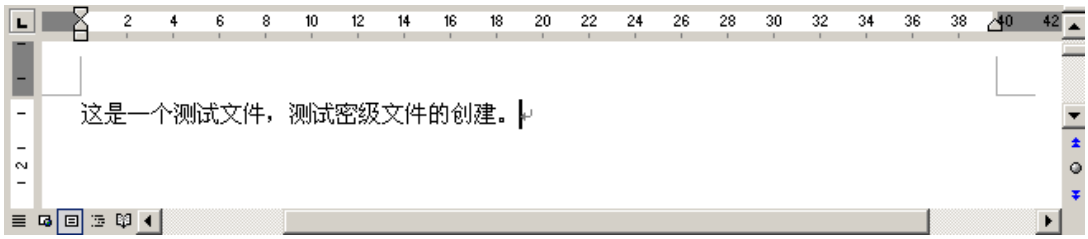


图 12-33　查看待审批文件内容

8. 审批员审核具体内容以后，如果允许创建，就再次返回“密级文件审批管理”界面，如图 12-34 所示。选择同意创建的文件（例如：test1.doc），单击“同意”按钮，系统会弹出提示框，确定后，将审批结果信息发送到服务器，如图 12-35 所示。

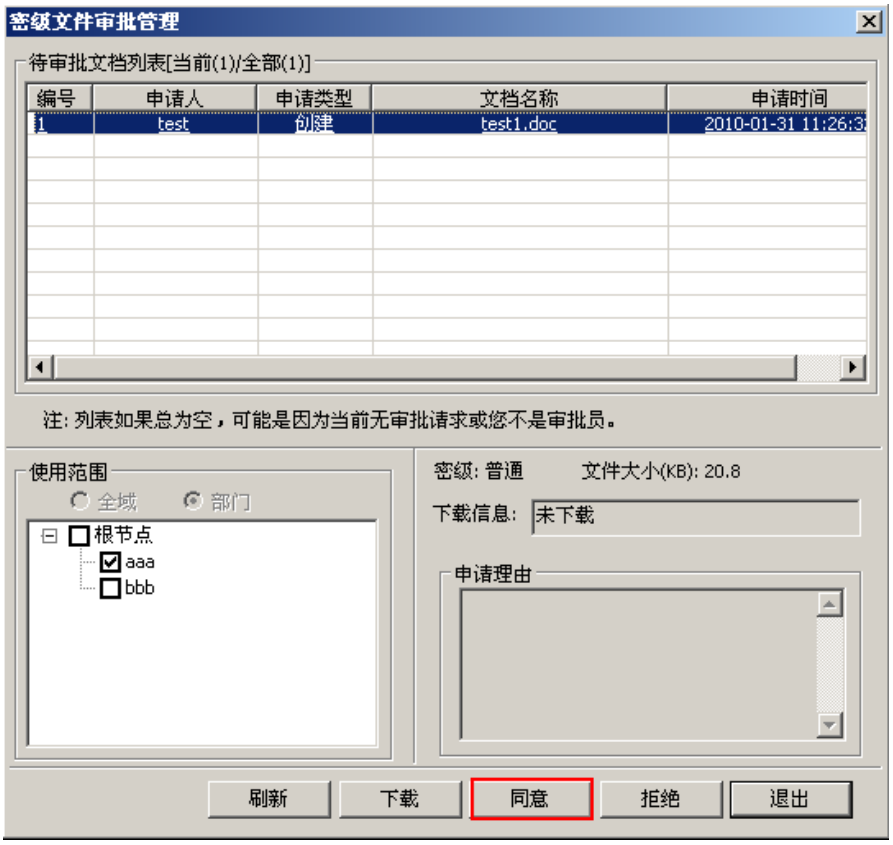


图 12-34　选择同意创建的文件

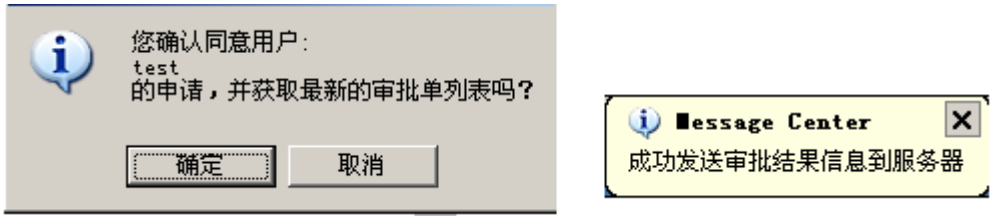


图 12-35　审批成功提示信息

9. 审批通过后，申请人所在的客户端就会弹出消息框，如图 12-36 所示。同时，审批通过的文件也变成既定密级的文件。密级文件一般为只读文件，禁止用户修改内容。

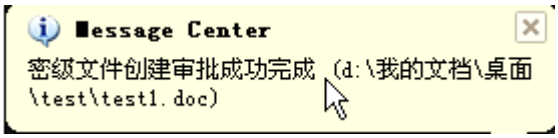


图 12-36　审批通过提示框

10. 还有一种情况，这里也说明一下。如果审批员查看具体内容后，不同意申请人的申请。那么，他就要回到“审批文档列表”界面，如图 12-37 所示。选择拒绝申请的文件（例如：test1.doc），单击“拒绝”按钮，系统会弹出提示框，要求填写拒绝理由，如图 12-38 所示。

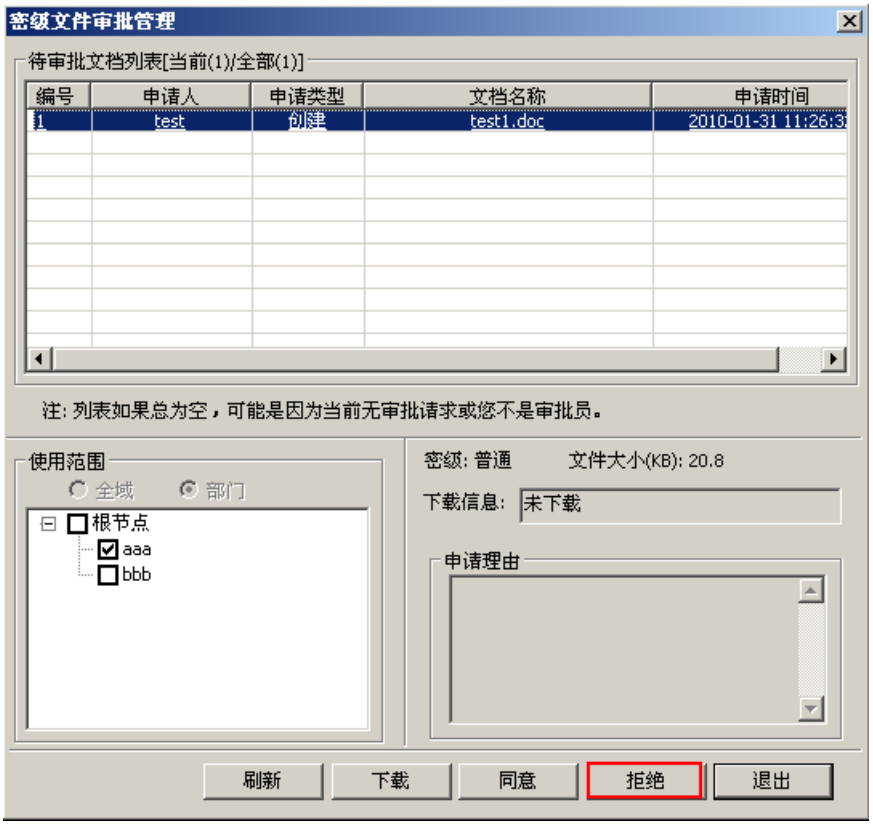


图 12-37　选择拒绝申请的文件

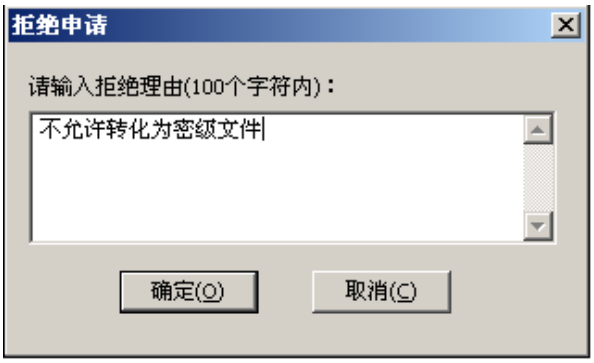


图 12-38　填写拒绝理由

11. 审批员拒绝申请文件后，系统弹出提示框，单击“确定”后，系统将审批结果信息发送到服务器，如图 12-39 所示。

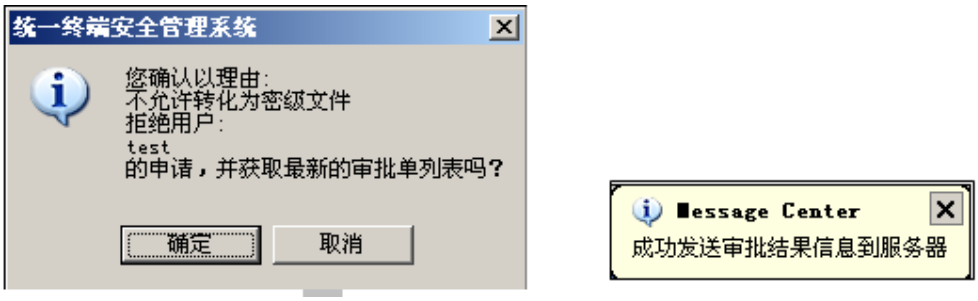


图 12-39　审批拒绝申请人的申请

12. 审批拒绝后，申请人所在的客户端也会弹出消息框，如图 12-40 所示。审批没有通过，申请的文件还是原来的文件，密级没有改变。

图 12-40　申请拒绝提示框

12.7.2　修改密级文件

客户端生成的密级文件，可以通过“修改”菜单，改变文件密级和使用范围，具体操作过程如下：

1. 选择欲改变属性的密级文件 test1.doc，单击右键菜单“密级文件管理”→“修改”，弹出申请修改密级文件界面，如图 12-41 和 12-42 所示。重新选择文件密级和使用范围，输入申请理由，最后单击“提交”按钮。

注意：客户端生成的密级文件一般为只读文件，是禁止用户修改。在修改密级文件过程中，请不要移动文件，否则，会导致审批失败。

图 12-41　选择创建密级文件菜单

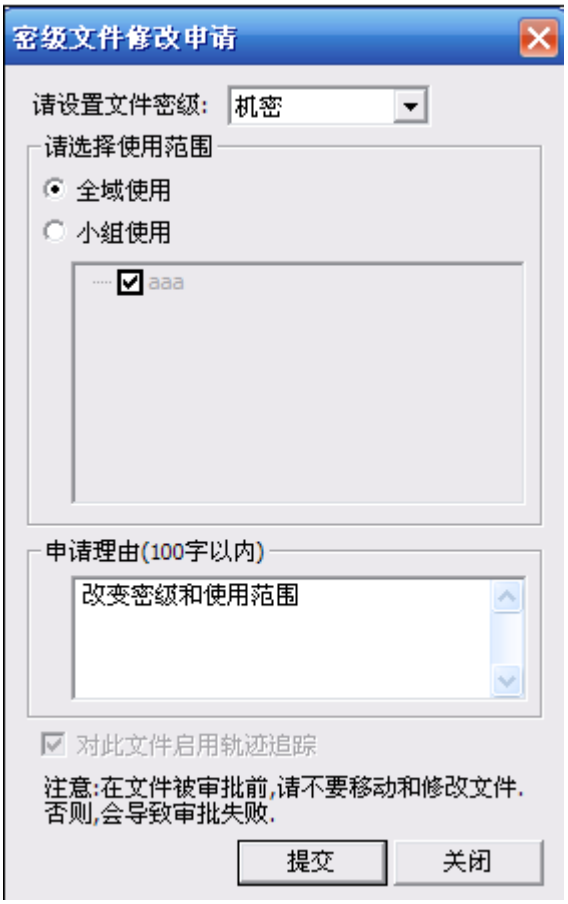


图 12-42　申请修改密级文件

2. 待修改的审批文件上传服务器后，客户端会弹出消息框，如图 12-43 所示。

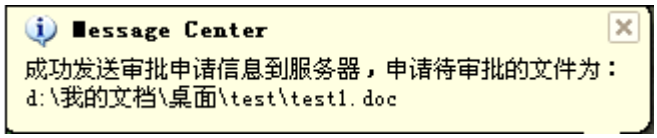


图 12-43　上传审批单成功提示

3. 审批员接到服务器派发的审批请求单，会在任务栏弹出消息框，如图 12-44 所示。

提示：审批员是由审批管理中审批规则确定的。

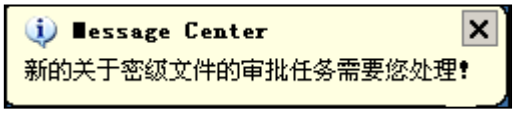


图 12-44　提示审批员有审批任务

4. 审批员单击客户端右键菜单“审批管理”→“密级文件审批管理”，进入“密级文件审批管理”界面，如图 12-45、12-46 所示。单击“刷新”按钮，显示待审批的文件。

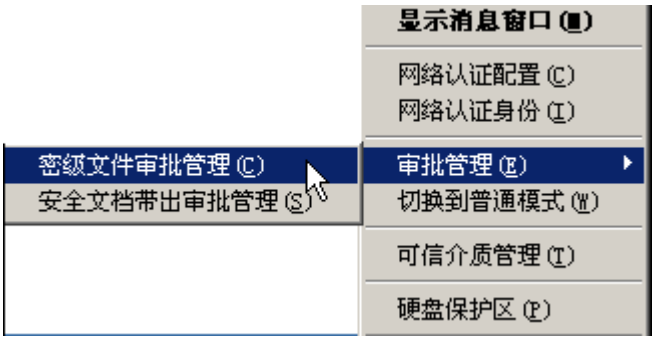


图 12-45　密级文件审批管理菜单

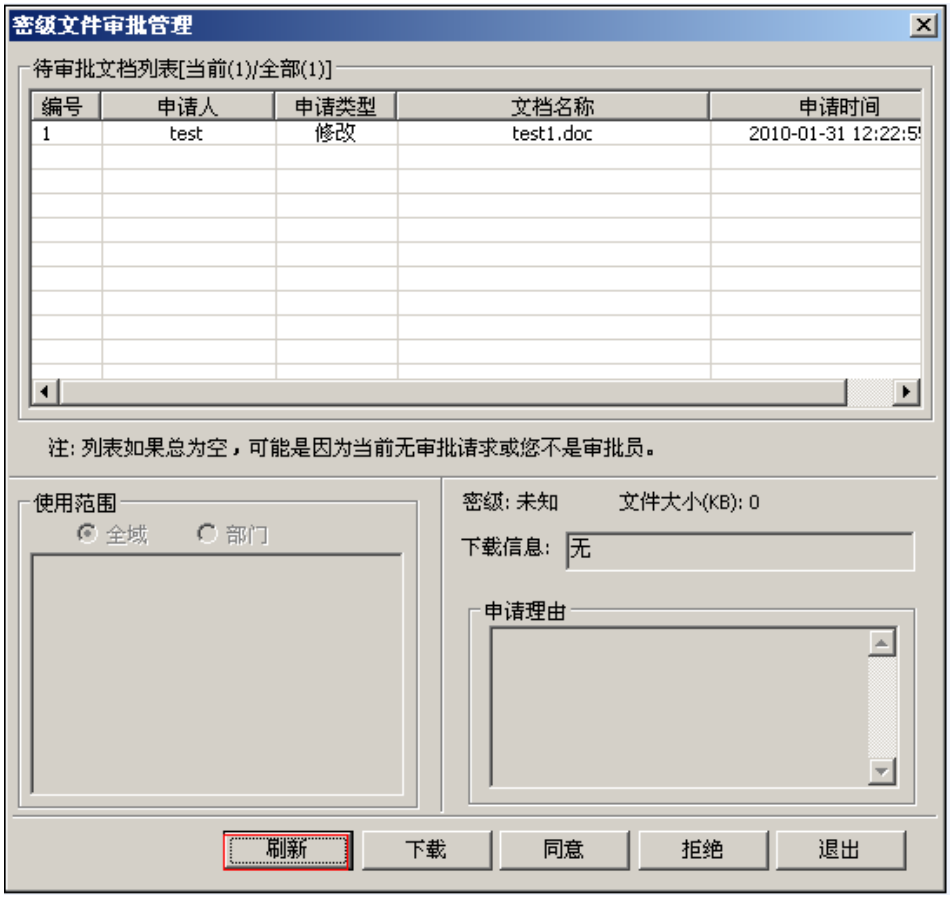


图 12-46　密级文件审批管理界面

5. 单击“下载”按钮，将待审批的文件下载到审批员指定的路径下，如图 12-47 所示。

图 12-47　选择下载路径

6. 如果文件比较大，下载过程可能比较缓慢，请耐心等待，不要关机或重启。下载完成后，弹出消息框，如图 12-48 所示。

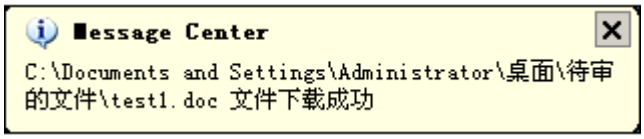


图 12-48　下载成功提示框

7. 审批员单击下载的文件，查看具体内容，如图 12-49 所示。

提示：这时的审批员可以打开任何密级的下载文件，不受密级文件策略限制。

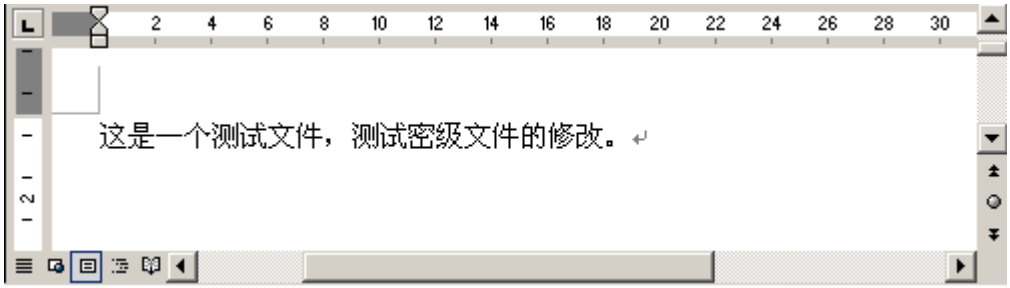


图 12-49　查看待审批文件内容

8. 审批员审核具体内容以后，如果允许修改，就再次返回“密级文件审批管理”界面，如图 12-50 所示。选择同意修改的文件（例如：test1.doc），单击“同意”按钮，系统会弹出提示框，确定后，将审批结果信息发送到服务器，如图 12-51 所示。

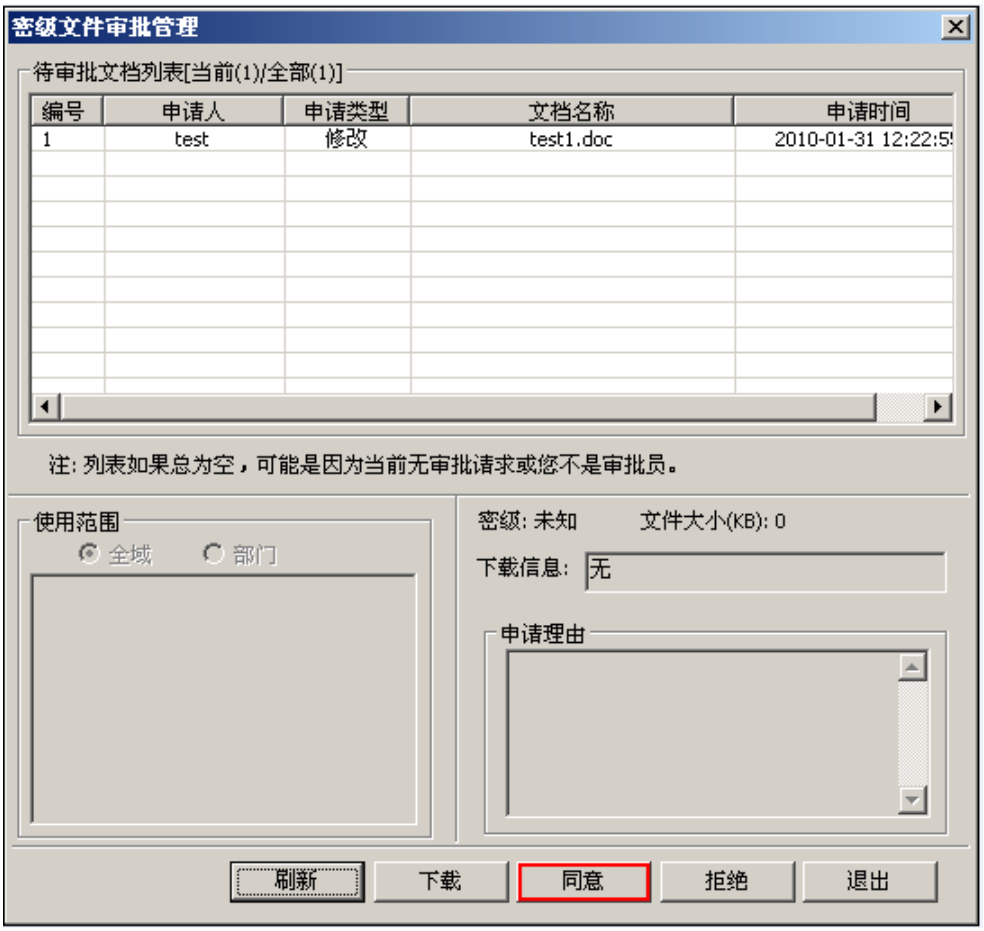


图 12-50　选择同意修改的文件

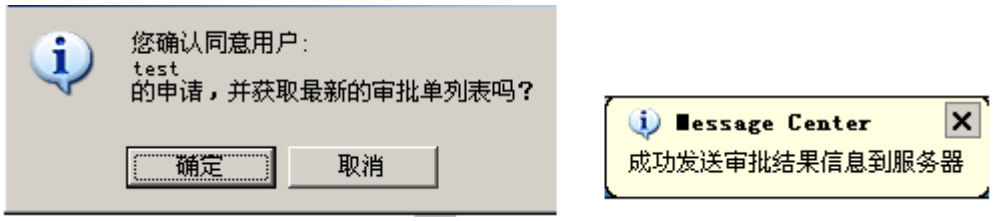


图 12-51　审批成功提示信息

9. 审批通过后，申请人所在的客户端就会弹出消息框，如图 12-52 所示。同时，通过审批修改的密级文件，文件密级和使用范围都会做相应的更改。

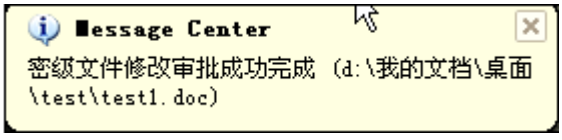


图 12-52　审批通过提示框

10. 选择已修改的密级文件，单击右键菜单“审批文件管理”→“属性查看”，可以看到密级文件的属性，如图 12-53 所示。

图 12-53　查看密级文件属性

12.7.3　销毁密级文件

Windows 操作系统所带的删除功能，只能对文件做删除标志，不能彻底删除文件。对于密级文件来说，如果不彻底删除的话，可能被恶意恢复，造成泄密事件的发生。一般情况下，我们采用“安全删除文件”功能，将本机上的普通文件和普通加密文件做彻底删除。但是，对于密级文件而言，不仅删除密级文件本身，还要删除它在各个机器、路径下流转的副本，这样才能更安全。所以，用户一定要利用密级文件的“销毁”功能，将不需要的密级文件执行销毁操作，流转的各个副本文件一并被自动删除，不留安全隐患。

1. 选择欲销毁的密级文件 test1.doc，单击右键菜单“密级文件管理”→“销毁”，弹出申请销毁密级文件界面，如图 12-54 和 12-55 所示。输入销毁密级文件的理由，最后单击“提交”按钮。

注意：在审批过程中，请不要移动文件，否则，会导致审批失败。

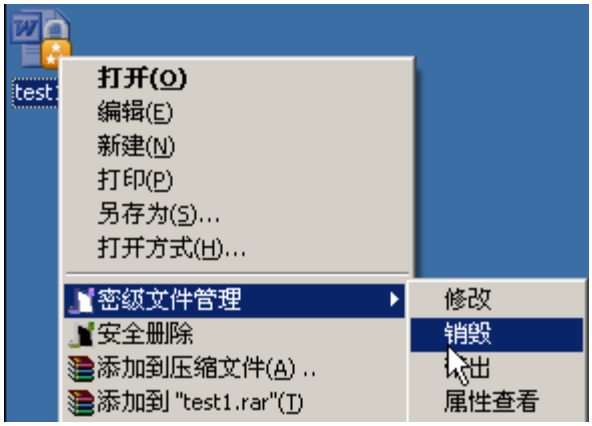


图 12-54　选择创建密级文件菜单

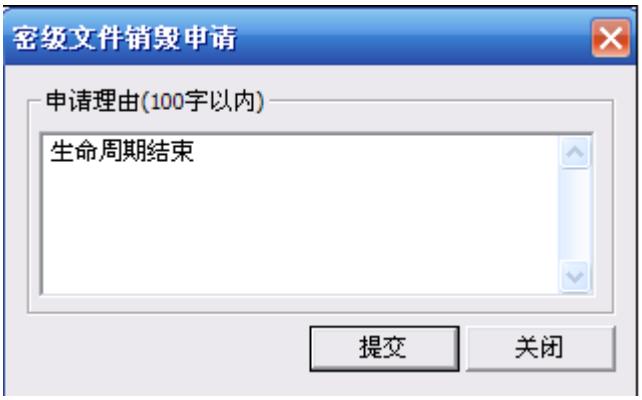


图 12-55　申请销毁理由

2. 待修改的审批文件上传服务器后，客户端会弹出消息框，如图 12-56 所示。

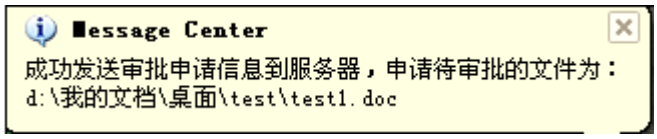


图 12-56　上传审批单成功提示

3. 审批员接到服务器派发的审批请求单，会在任务栏弹出消息框，如图 12-57 所示。

提示：审批员是由审批管理中审批规则确定的。

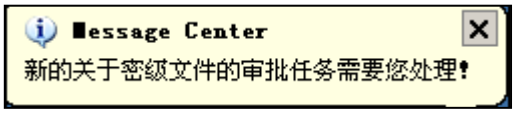


图 12-57　提示审批员有审批任务

4. 审批员单击客户端右键菜单“审批管理”→“密级文件审批管理”，进入“密级文件审批管理”界面，如图 12-58、12-59 所示。单击“刷新”按钮，显示待审批的文件。

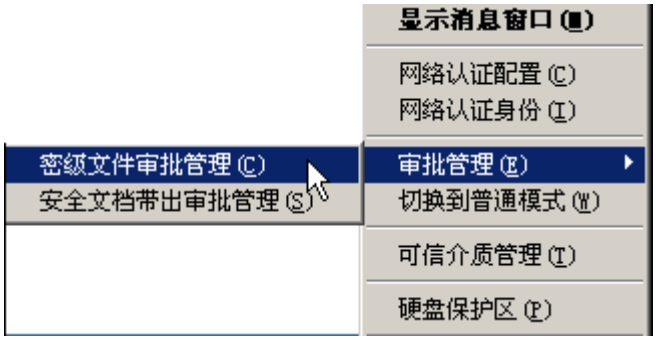


图 12-58　密级文件审批管理菜单

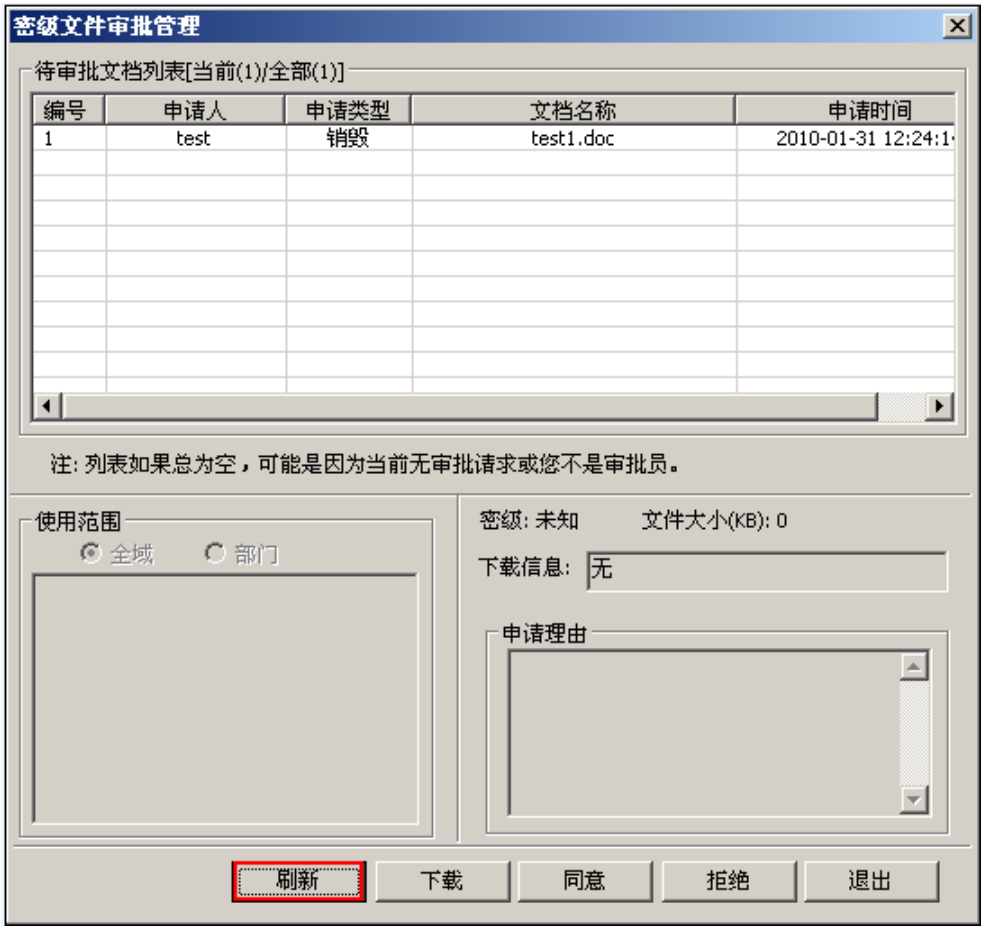


图 12-59　密级文件审批管理

5. 单击“下载”按钮，将待审批的文件下载到审批员指定的路径下，如图 12-60 所示。

图 12-60　选择下载路径

6. 如果文件比较大，下载过程可能比较缓慢，请耐心等待，不要关机或重启。下载完成后，弹出消息框，如图 12-61 所示。

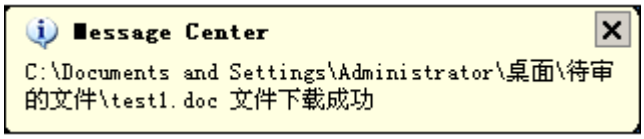


图 12-61　下载成功提示框

7. 审批员单击下载的文件，查看具体内容，如图 12-62 所示。

提示：这时的审批员可以打开任何密级的下载文件，不受密级文件策略限制。

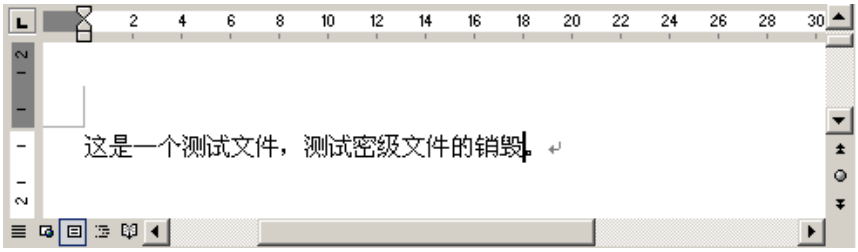


图 12-62　查看待审批文件内容

8. 审批员审核具体内容以后，如果允许销毁，就再次返回“审批文档列表”界面，如图 12-63 所示。选择同意销毁的文件（例如：test1.doc），单击“同意”按钮，系统会弹出提示框，确定后，将审批结果信息发送到服务器，如图 12-64 所示。

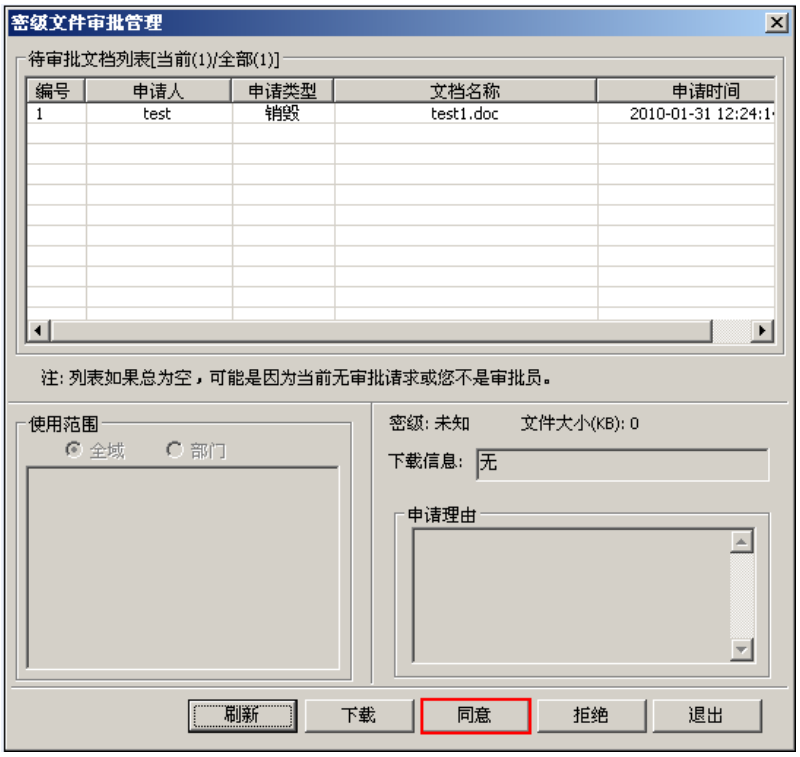


图 12-63　选择同意销毁的文件

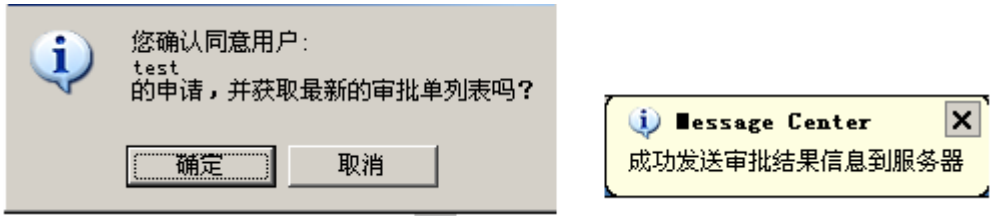


图 12-64　审批成功提示信息

9. 审批通过后，申请人所在的客户端就会弹出消息框，如图 12-65 所示。

被审批销毁的密级文件，如果在创建时启用了轨迹追踪，那么在销毁自身的同时，也一并销毁在各个机器和各个路径流转留下的副本。但对于不在线机器和 U 盘上的副本，不能一同销毁。当被销毁的副本再次被使用时，会提示用户“非法使用已销毁的文件副本”，并产生一条报警信息。

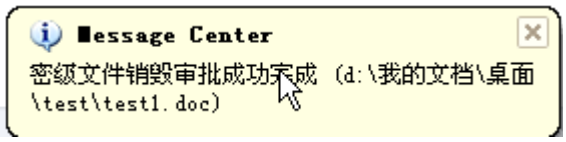


图 12-65　审批通过提示框

12.7.4　带出密级文件

当密级文件带出使用时，需要经过审批员审批。如果审批通过，生成自解密包，用户输入自解密口令即可解密使用。如果审批未通过，告诉申请人拒绝理由。

1. 选择欲带出的密级文件 test1.doc，单击右键菜单“密级文件管理”→“带出”，弹出申请带出密级文件界面，如图 12-66 和 12-67 所示。输入申请理由，最后，单击“提交”按钮。

注意：在文件被审批过程中，请不要移动和修改文件。否则，会导致审批失败。

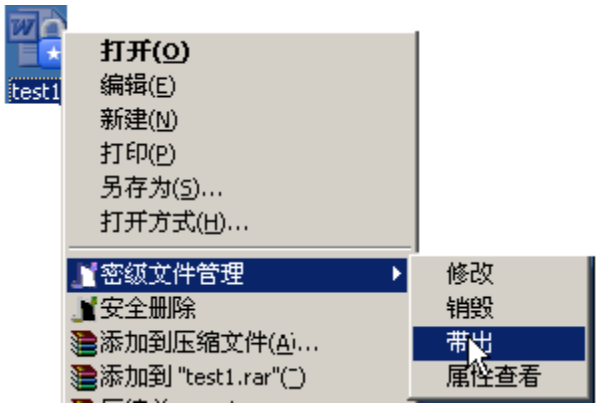


图 12-66　选择带出密级文件菜单

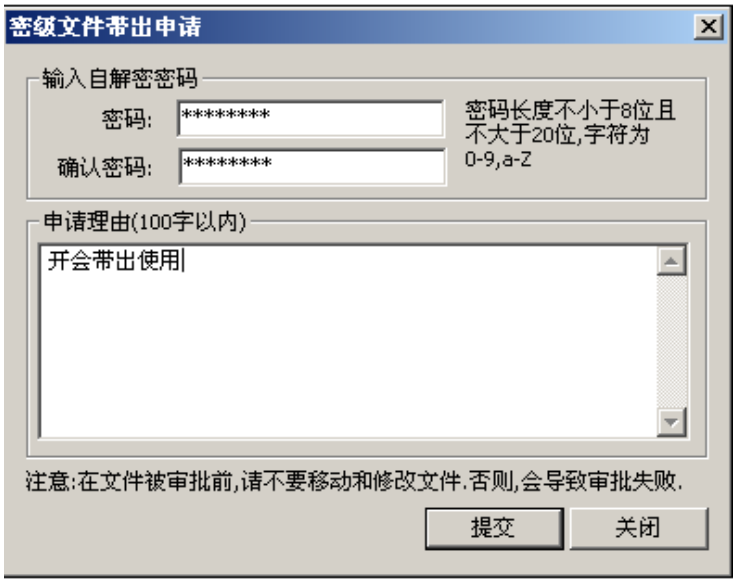


图 12-67　申请创建密级文件

2. 待审批的文件上传服务器后，客户端会弹出消息框，如图 12-68 所示。

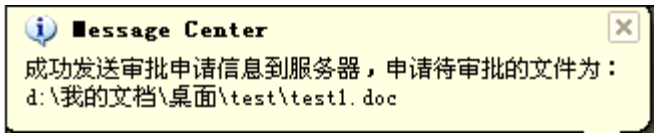


图 12-68　上传审批单成功提示

3. 审批员接到服务器派发的审批请求单，会在任务栏弹出消息框，如图 12-69 所示。

提示：审批员是由审批管理中审批规则确定的。

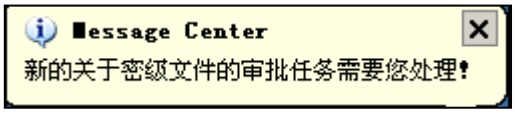


图 12-69　提示审批员有审批任务

4. 审批员单击客户端右键菜单“审批管理”→“密级文件审批管理”，进入“密级文件审批管理”界面，如图 12-70、12-71 所示。单击“刷新”按钮，显示待审批的文件。

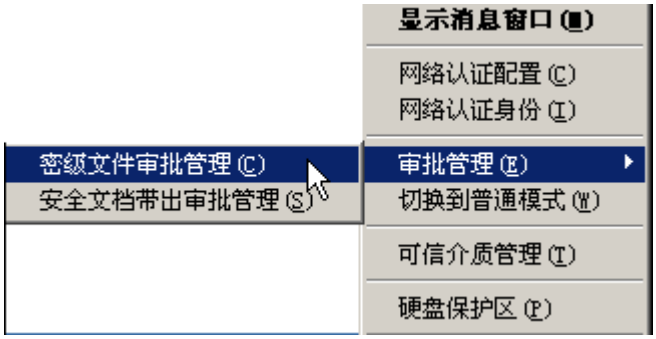


图 12-70　密级文件审批管理菜单

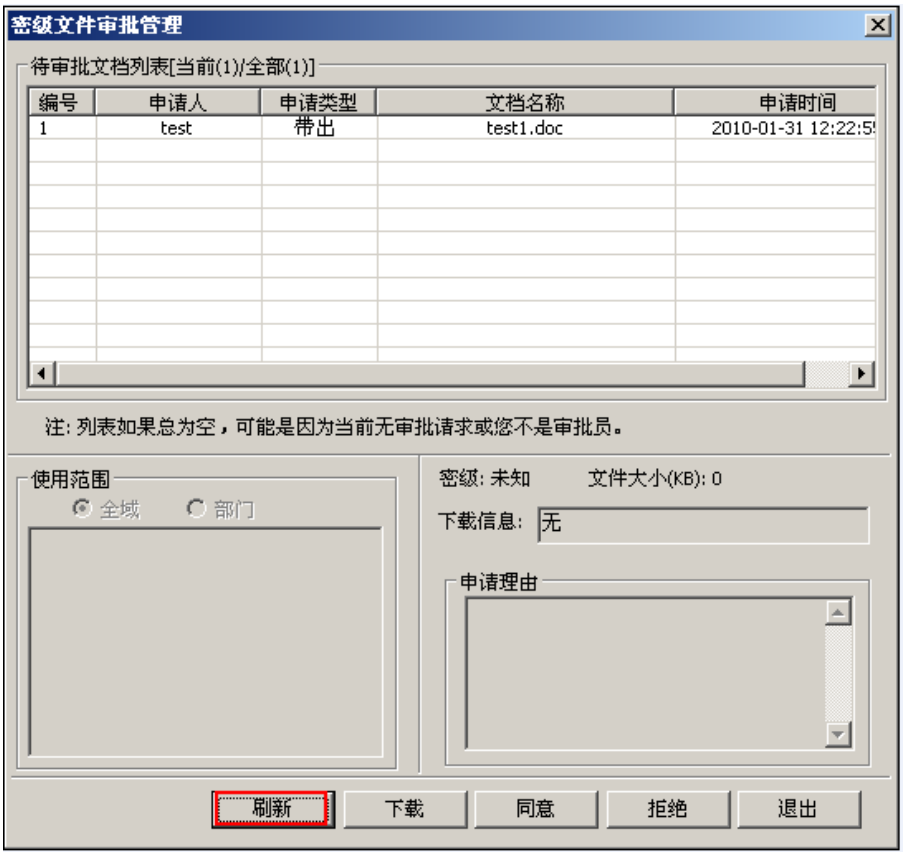


图 12-71　密级文件审批管理界面

5. 单击“下载”按钮，将待审批的文件下载到审批员指定的路径下，如图 12-72 所示。

图 12-72　选择下载路径

6. 如果文件比较大，下载过程可能比较缓慢，请耐心等待，不要关机或重启。下载完成后，弹出消息框，如图 12-73 所示。

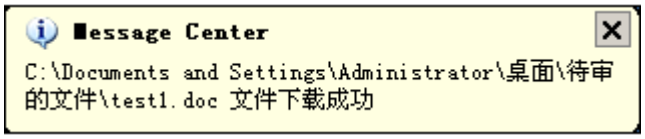


图 12-73　下载成功提示框

7. 审批员单击下载的文件，查看具体内容，如图 12-74 所示。

提示：这时的审批员可以打开任何密级的下载文件，不受密级文件策略限制。

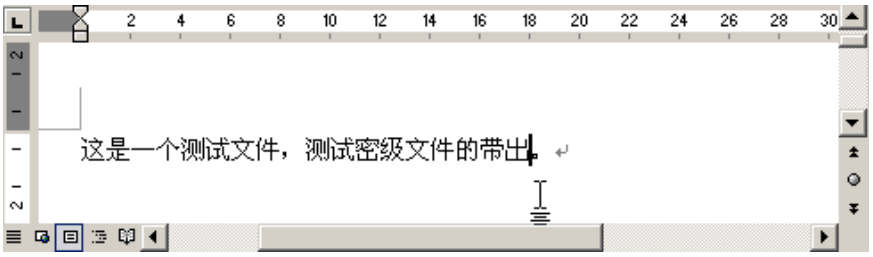


图 12-74　查看待审批文件内容

8. 审批员审核具体内容以后，如果允许带出，就再次返回“密级文件审批管理”界面，如图 12-75 所示。选择同意带出的文件（例如：test1.doc），单击“同意”按钮，系统会弹出提示框，确定后，将审批结果信息发送到服务器，如图 12-76 所示。

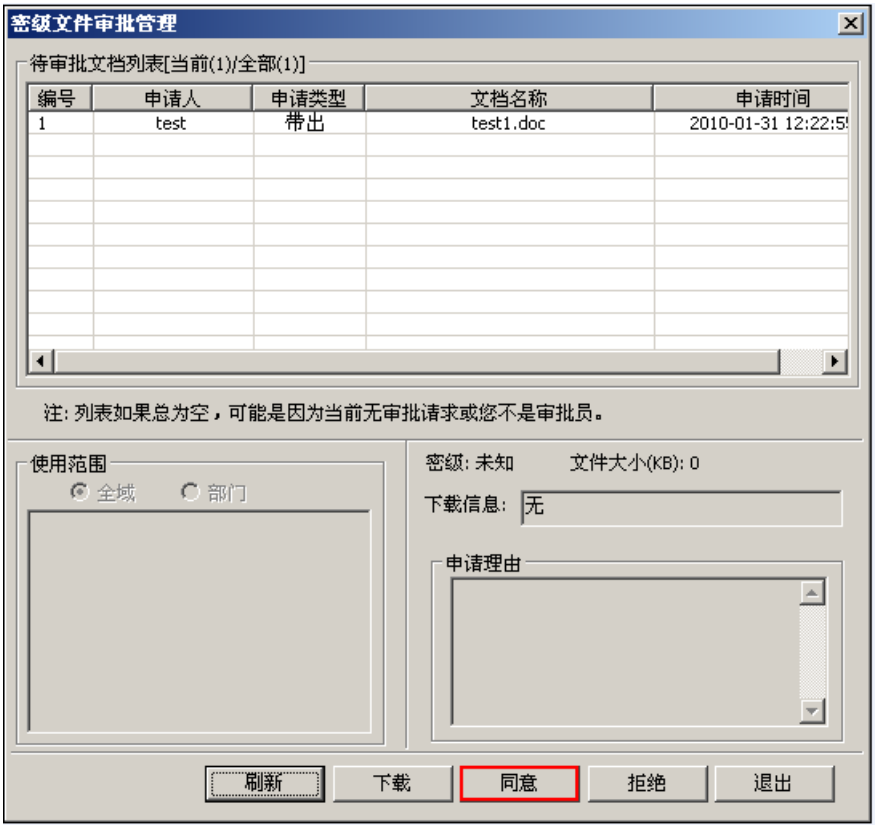


图 12-75　选择同意创建的文件

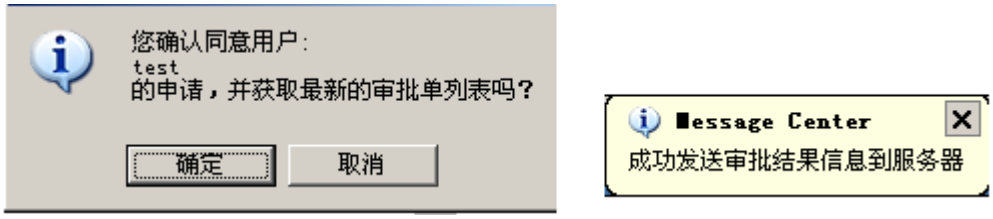


图 12-76　审批成功提示信息

9. 审批通过后，申请人所在的客户端就会弹出消息框，如图 12-77 所示。审批通过的文件变成自解密包，默认存放在带出文件所在的路径下，如图 12-78 所示。单击“是（Y）”按钮，自动跳转到自解密所在路径。

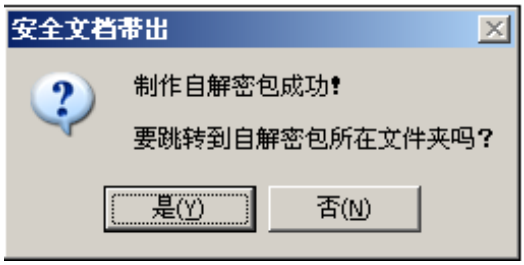


图 12-77　制作自解密包成功

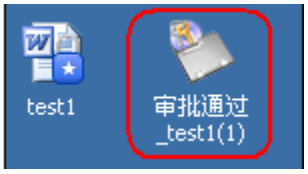


图 12-78　审批自解密包

10. 双击自解密包，弹出“文件浏览”界面，如图 12-79 所示。单击“Extract to”按钮，输入文件路径和自解密口令，将审批通过包解压到指定路径下。

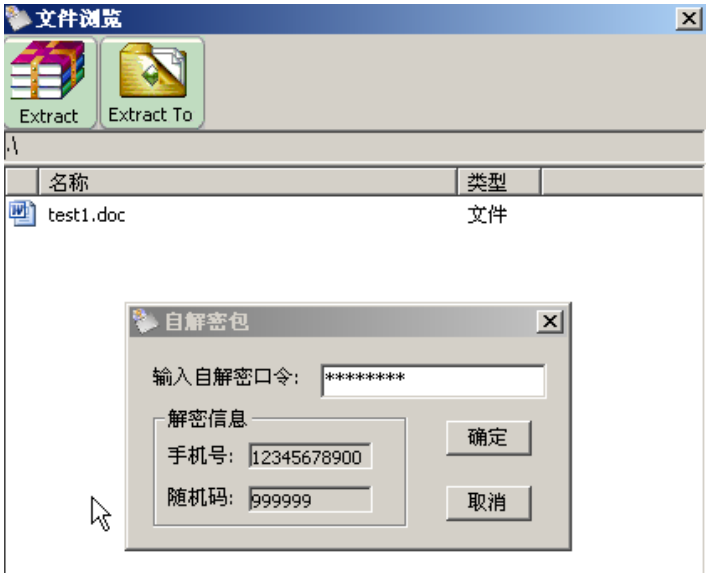


图 12-79　文件游览界面

11. 在指定路径下，可以看到解压后的审批通过包，如图 12-80 所示。

图 12-80　解压后的审批通过包

12. 双击解压后的审批通过包，可以看到里面的文件，如图 12-81 所示。这时，文件都已被解密，可以任意带出使用。

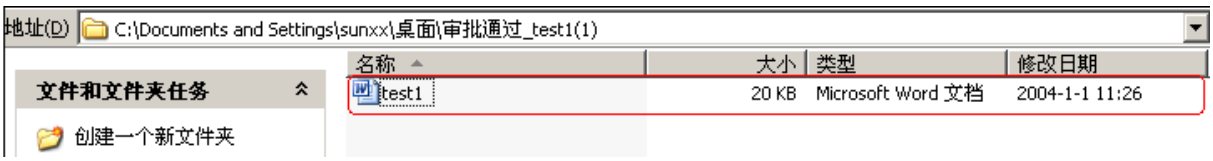


图 12-81　审批通过文件列表

13. 还有一种情况，这里也说明一下。如果审批员查看具体内容后，不同意申请人的申请。那么，他就要回到“密级文件审批管理”界面，如图 12-82 所示。选择拒绝申请的文件（例如：test1.doc），单击“拒绝”按钮，系统会弹出提示框，要求填写拒绝理由，如图 12-83 所示。

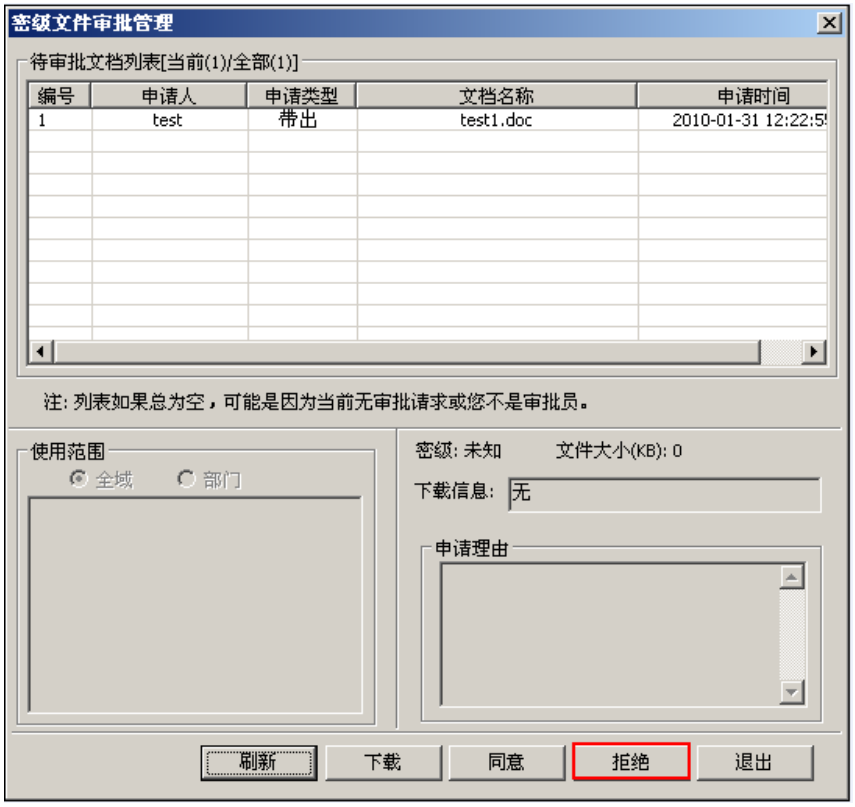


图 12-82　选择拒绝带出的文件

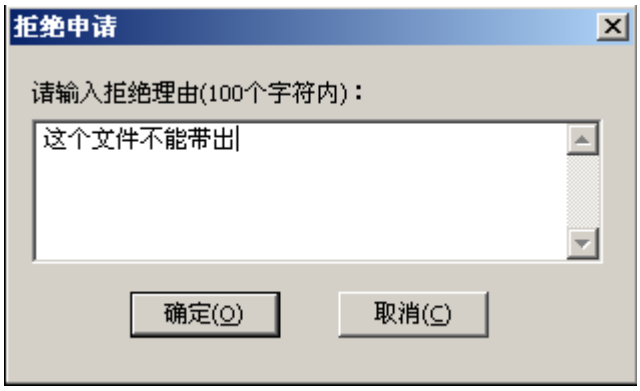


图 12-83　填写拒绝理由

14. 审批员拒绝申请文件后，系统弹出提示框，单击“确定”后，系统将审批结果信息发送到服务器，如图 12-84 所示。

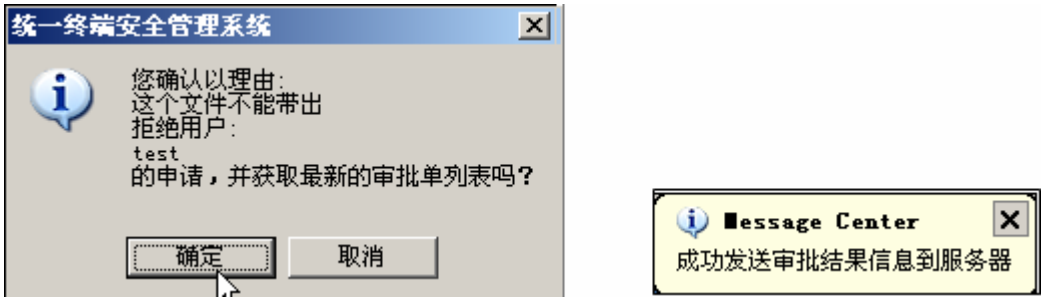


图 12-84　审批拒绝申请人的申请

15. 审批拒绝后，申请人所在的客户端也会弹出消息框，给出拒绝理由，如图 12-85 所示。审批没有通过时，申请的密级文件保持不变，不会被解密。

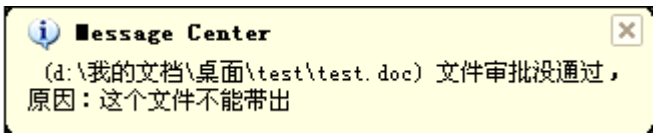


图 12-85　申请拒绝提示框

12.7.5　查看密级文件属性

选择密级文件 test1.doc，单击右键菜单“密级文件管理”→“属性查看”，可以查看密级文件的属性，如图 12-86 和 12-87 所示。

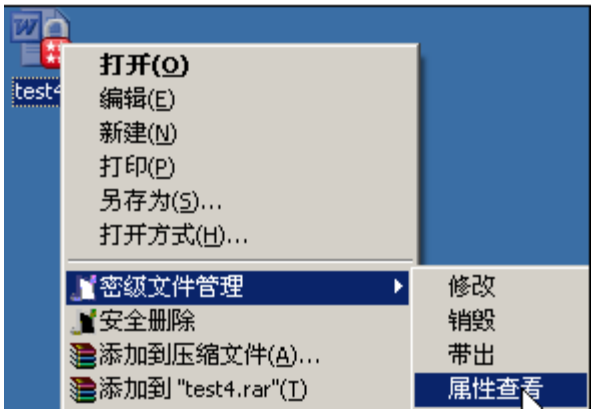


图 12-86　选择属性查看菜单

图 12-87　查看密级文件属性

12.8 接收、发送消息

1．客户端安装成功后，在桌面任务栏出现客户端图标，如图 12-88 所示。客户端的在线/离线状态发送信息给消息中心，消息中心接收到该消息后，动态变换本地的图标状态，在线显示，离线显示。

图 12-88　客户端图标

2．双击客户端图标或者单击右键菜单“显示消息窗口”，进入消息框，如图 12-89 所示。在下面的发送消息框书写内容，单击“发送消息”按钮，即可将消息发送到控制台。

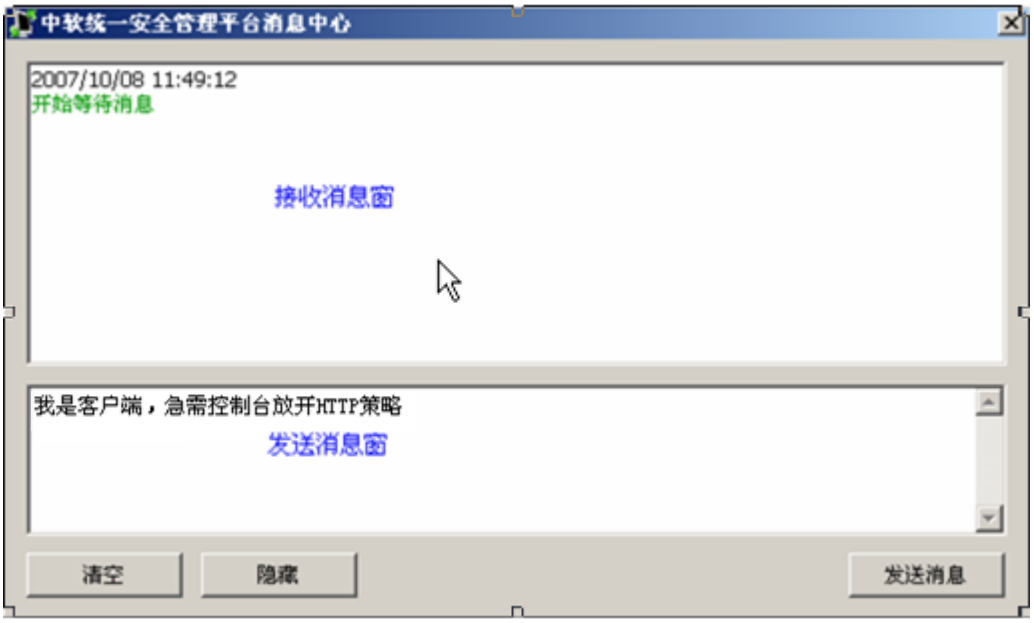


图 12-89　客户端发送消息

3. 控制台收到未阅读的消息，管理员可以双击打开查看，并做处理，如图 12-90 所示。然后单击“发送消息”窗口，回复客户端消息。

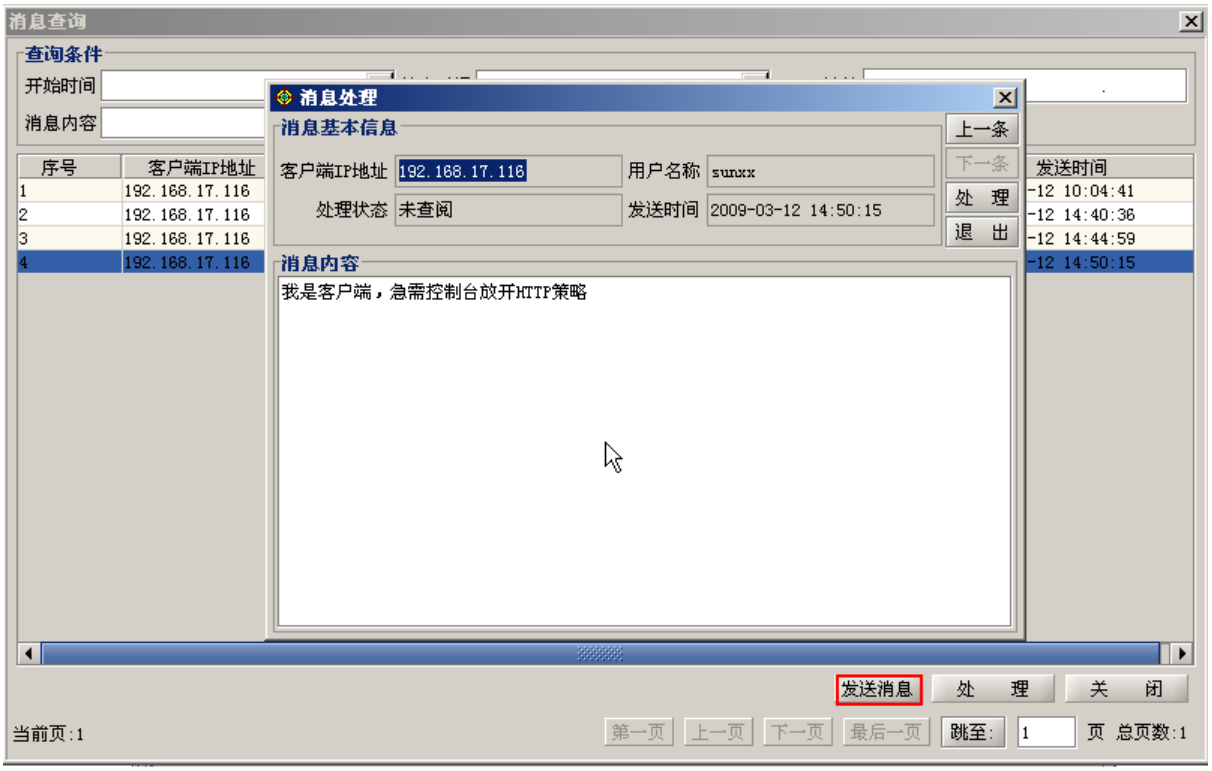


图 12-90　控制台查看消息

4. 客户端收到控制台发送来的消息时，会在任务栏弹出提示框，如图 12-91 所示。这样，客户端和控制台就可以互发消息，相互交流。

图 12-91　客户端收到消息

另外，控制台也可以在安全管理中心中，单击组织结构的右键菜单“远程消息”，向选定的用户或主机发送远程消息，如图 12-92 所示。

图 12-92　控制台右键菜单远程消息

12.9 配置网络认证

如果该系统启用了网络认证功能，当更换了不同品牌的交换机时，需要在客户端重新配置网络认证功能。正常情况下，客户端不需要配置网络认证功能，只需在安装客户端时，选择“启用网络认证”即可。

提示：在 Windows XP 及 Windows 2003 中，客户端启用网络接入认证时，需要把本机的“IEEE 802.1x”禁用。具体操作为：打开“本地连接”属性，在“常规”页中，点击“属性”，在弹出对话框的“验证”页中将“启用本网络的 IEEE 802.1x 验证”前面的对勾去掉，然后点击“确定”即可。

1．右键单击任务栏中客户端图标，选择“网络认证配置”，如图 12-93 所示。

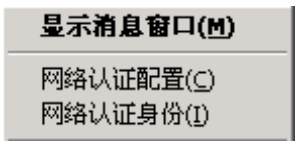


图 12-93　客户端右键菜单

2．在认证属性设置中，根据具体的交换机来设置，如图 12-94 所示。若使用华为设备，将“设备选项”选择为“华为交换设备”；若使用 CISCO 设备，选择“CISCO,3COM 交换设备”。

图 12-94　认证属性设置

12.10　网络身份认证

如果在控制台上更改了用户的密码，该用户启用了网络认证功能，必须在客户端重新输入新的密码。否则，该用户上不了网。

右键单击客户端图标，选择网络认证身份，重新输入新密码，如图 12-95 所示。单击“确定”按钮，即可恢复该用户上网功能。

图 12-95　网络身份认证

12.11　安全文档带出审批管理

12.11.1　安全文档在线审批过程

客户端用户带出使用加密文件时，因自身没有自解密功能，需经审批员审批，才能带出明文。单次审批带出时，最多可选择 10 个文件。当带出的文件数量大于 10 个时，需分多次申请，或者选择离线审批方式。

12.11.1.1　在线申请带出

1. 客户端用户选择欲带出的加密文件，单击右键菜单“在线申请带出”，弹出申请带出的文件信息，如图 12-96 和 12-97 所示。输入申请理由，单击“确定”按钮。

注意：在文档被审批前，请不要移动和修改文件。否则，会导致审批失败。

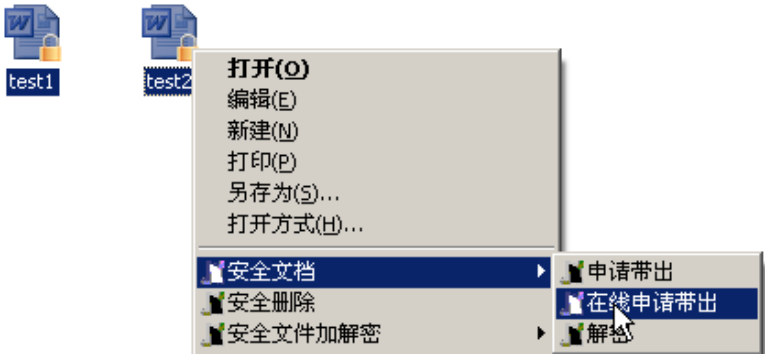


图 12-96　选择在线申请带出

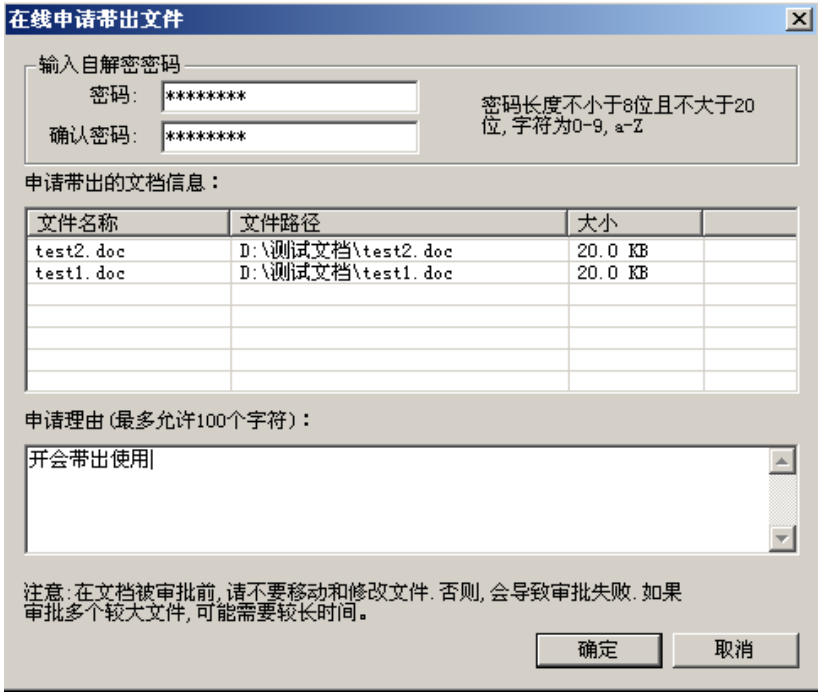


图 12-97　在线审批文档信息

2. 待审批的文件上传服务器后，客户端会弹出消息框，如图 12-98 所示。

图 12-98　上传审批单成功提示

12.11.1.2　在线审批带出

1. 审批员接到服务器派发的审批请求单，会在任务栏弹出消息框，如图 12-99 所示。

提示：审批员是由审批管理中审批规则确定的。

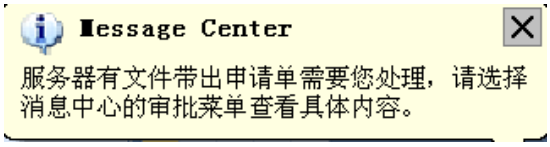


图 12-99　提示审批员有审批任务

2. 审批员单击客户端右键菜单“审批管理”→“安全文档带出审批管理”，进入“待审批带出文档列表”界面，如图 12-100 所示。该列表最多只能显示 10 个待审批的任务，当待审批的任务数多于 10 个时，需要把前面的任务审批了，才能刷新看到新的任务。

图 12-100　待审批带出文档列表

3. 单击“下载”按钮，将待审批的文件下载审批员指定的路径下，如图 12-101 所示。

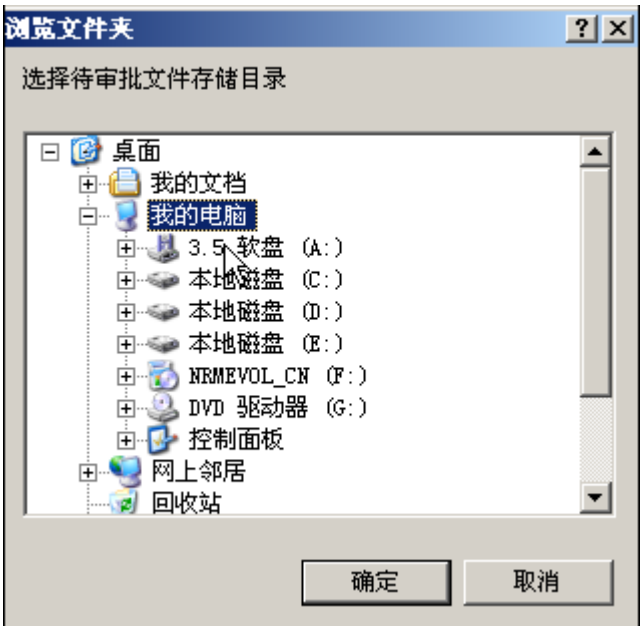


图 12-101　选择下载路径

4. 如果文件比较大，下载过程可以比较缓慢，请耐心等待，不要关机或重启。下载完成后，弹出消息框，如图 12-102 所示。

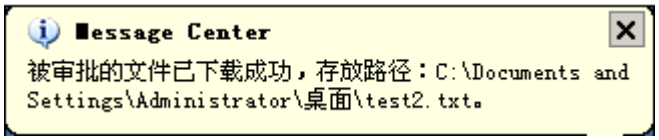


图 12-102　下载成功提示框

5. 审批员单击下载的文件，查看具体内容，如图 12-103 所示。

这里需要审批员具有打开加密文件的策略，否则，打开的是乱码，看不到具体内容。例如：待审批的文件是*.txt 加密文件，那么审批员就应用*.txt 文件的加密策略。

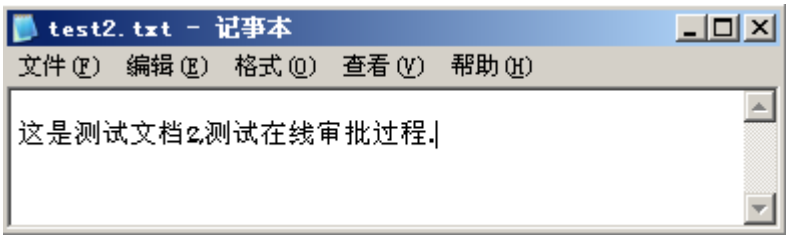


图 12-103　查看待审批文件内容

6. 审批员审核具体内容以后，如果允许带出，就再次单击客户端右键菜单“审批管理”→“安全文档带出审批管理”，进入“待审批带出文档列表”界面，如图 12-104 所示。选择同意带出的文件（例如：test2.txt），单击“同意”按钮，系统会弹出消息框，如图 12-105 所示。

图 12-104　选择同意带出的文件

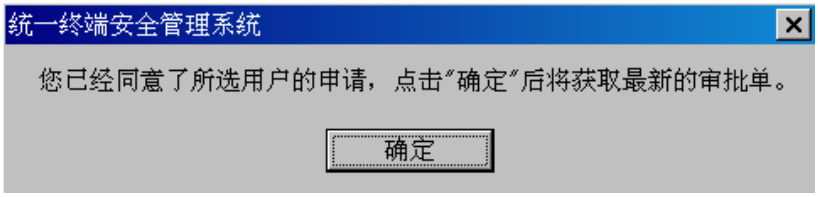


图 12-105　同意带出提示框

7. 审批通过后，申请人所在的客户端就会弹出消息框，如图 12-106 所示。审批通过的文件变成自解密包，默认存放在带出文件所在的路径下，如图 12-107 所示。单击“是（Y）”按钮，自动跳转到自解密所在路径。

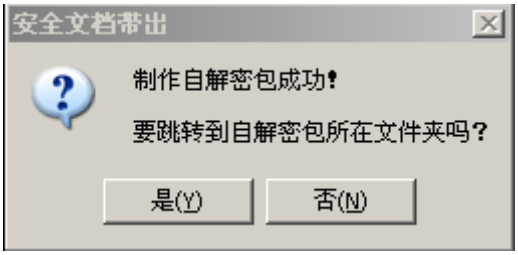


图 12-106　制作自解密包成功

图 12-107　审批自解密包

8. 双击自解密包，弹出“文件浏览”界面，如图 12-108 所示。单击“Extract to”按钮，输入文件路径和自解密口令，将审批通过包解压到指定路径下。

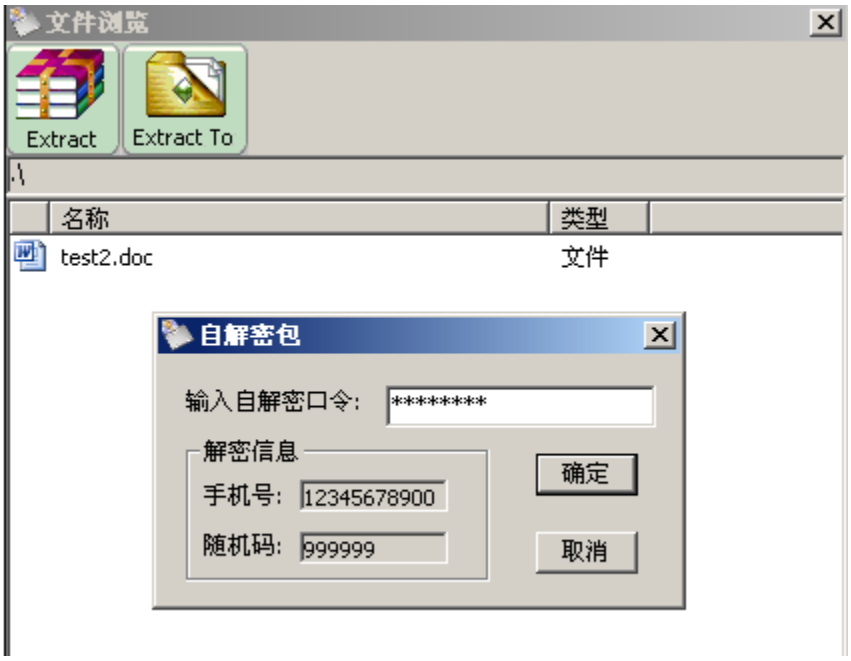


图 12-108　文件游览界面

9. 在指定路径下，可以看到解压后的审批通过包，如图 12-109 所示。

图 12-109　解压后的审批通过包

10. 双击解压后的审批通过包，可以看到里面的文件，如图 12-110 所示。这时，文件都已被解密，可以任意带出使用。

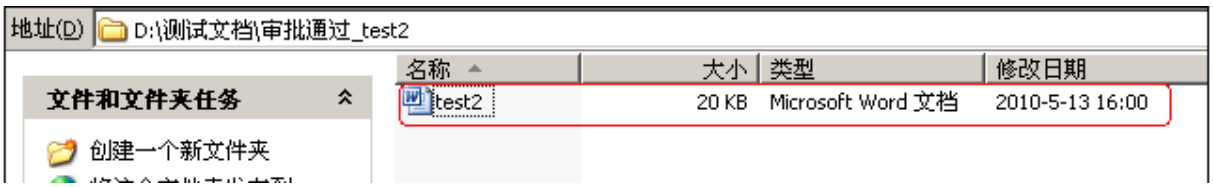


图 12-110　审批通过文件列表

11. 如果审批员查看具体内容后，不允许申请人带出。那么，他就要回到“待审批带出文档列表”界面，如图 12-111 所示。选择拒绝带出的文件（例如：test1.txt），单击“拒绝”按钮，系统会弹出提示框，要求填写拒绝理由，如图 12-112 所示。

图 12-111　选择拒绝带出的文件

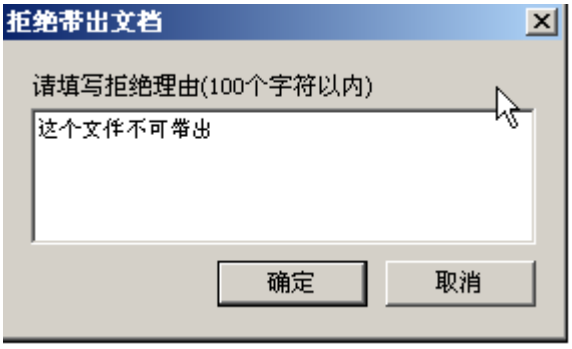


图 12-112　填写拒绝理由

12. 审批员拒绝带出文件后，系统后弹出提示框，如图 12-113 所示。

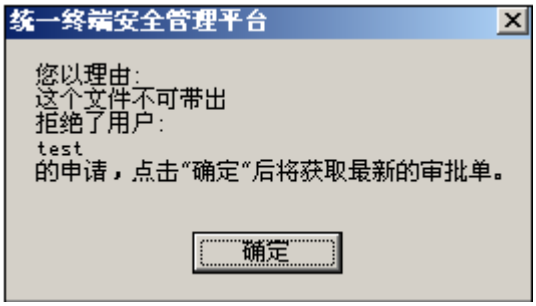


图 12-113　审批拒绝提示框（审批员）

13. 审批拒绝后，申请人所在的客户端也会弹出消息框，如图 12-114 所示。审批没有通过，申请文件还是加密文件，不解密。

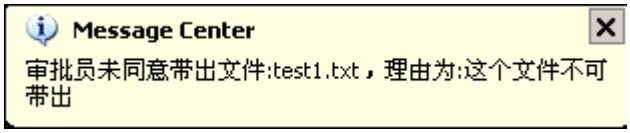


图 12-114　审批拒绝提示框（申请人）

12.11.2　安全文档离线审批过程

经过透明加密后的文件可以安全的存储在本地，如需要带出正常查看，须将密文转换成明文，这就要进行安全文档的审批操作。审批后的文档自动由密文转成明文，可以任意打开；否则带出的是密文，无法查看。

审批操作只能由指定的审批员进行，审批员是在审批管理中进行设定的。审批过程有在线审批和离线审批两种方式，这里我们讲离线审批过程。

12.11.2.1　离线申请带出

（1）在客户端，用户选择将要带出的密文，可以是单个文件，也可以是多个文件。单击右键菜单，选择“申请带出”，如图 12-115 所示。如果带出文件比较多，建议将文件放入一个文件夹中，统一带出。

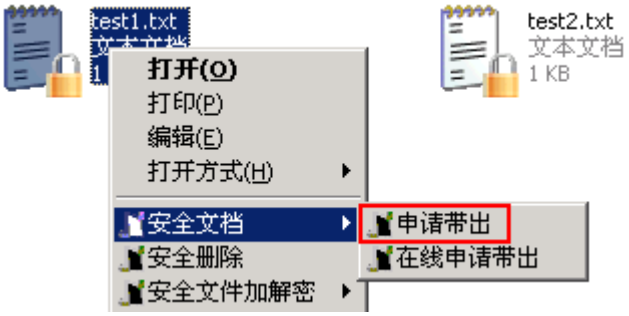


图 12-115　选择申请带出菜单

（2）在“制作审批包”界面中，输入加密密码，密码一般在 8～20 位之间，一定要记住密码。然后点击浏览按钮“ ··· ”，选择解密包存放路径，如图 12-116 所示。

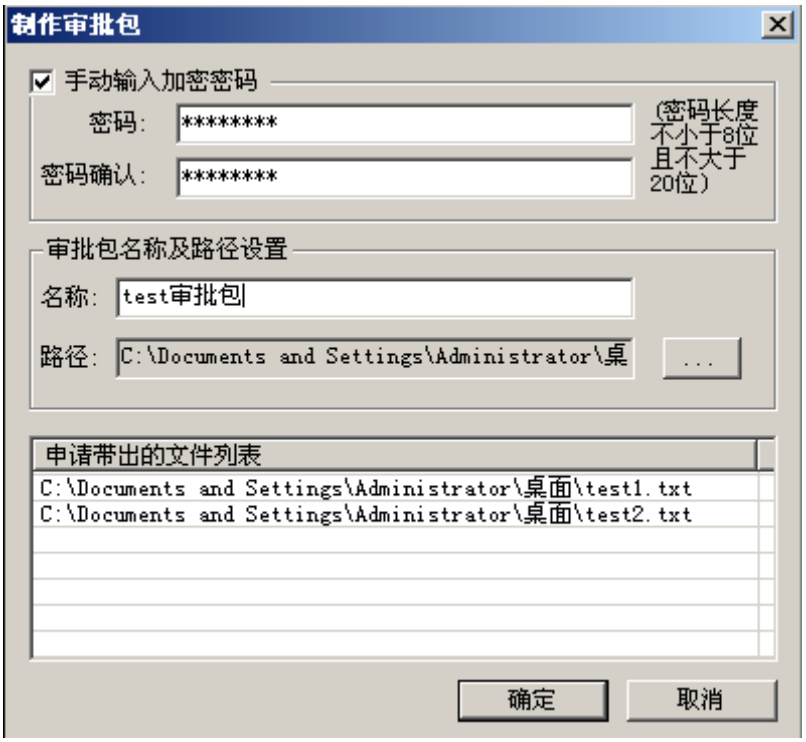


图 12-116　审批包目的路径选择

（3）在上面的“制作审批包”界面，输入选项结束后，单击“确定”按钮，弹出制作成功提示框，如图 12-117 所示。单击“是（Y）”按钮，跳转到自解密包所在文件夹，可以看到制作的审批请求包，如图 12-118 所示。

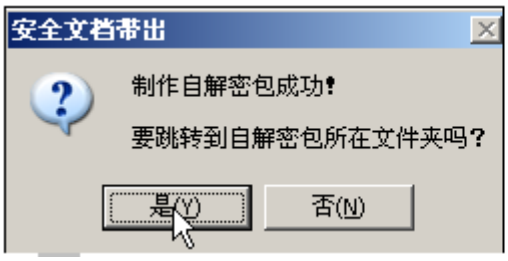


图 12-117　制作审批请求包成功提示框

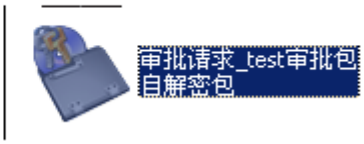


图 12-118　制作的审批请求包

12.11.2.2　离线审批带出

（1）用户可以将生成的审批请求包，以任意方式传输给审批员。审批员双击请求包，弹出“文件浏览”界面，如图 12-119 所示。

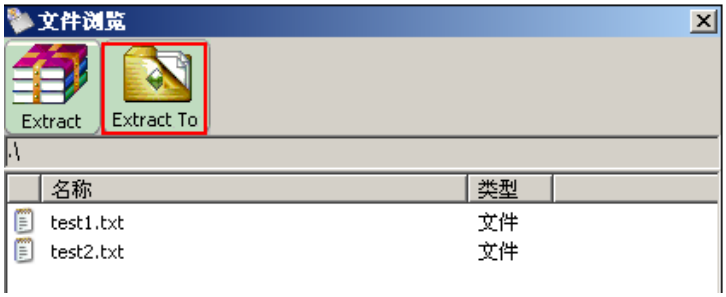


图 12-119　文件浏览界面

（2）单击“Extract to”按钮，输入文件路径和自解密口令，将审批请求包解压到指定路径下，如图 12-120 和 12-121 所示。

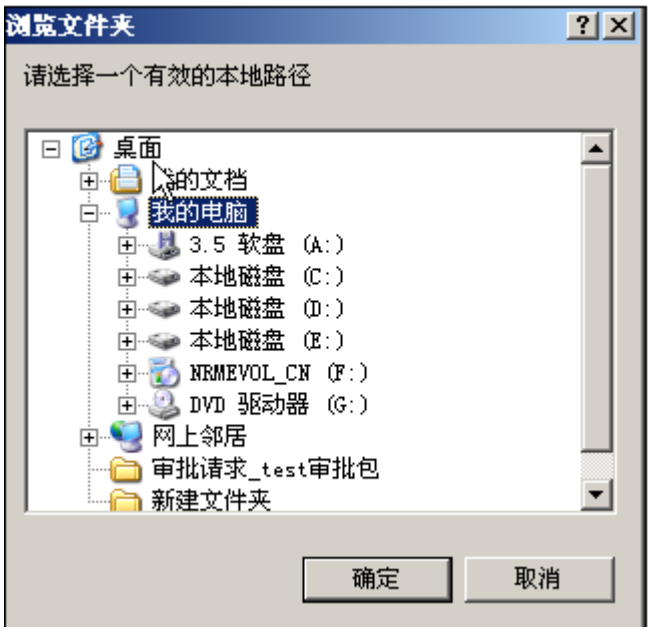


图 12-120　选择浏览文件夹路径

图 12-121　输入自解密口令

（3）在指定路径下，可以看到解压后的审批请求包，如图 12-122 所示。

图 12-122　解压后的审批请求包

（4）双击解压后的审批请求包，可以看到里面的文件，如图 12-123 所示。选择任一文件双击查看文件内容。

提示：这里需要审批员具有打开加密文件的策略，否则，打开的是乱码，看不到具体内容。

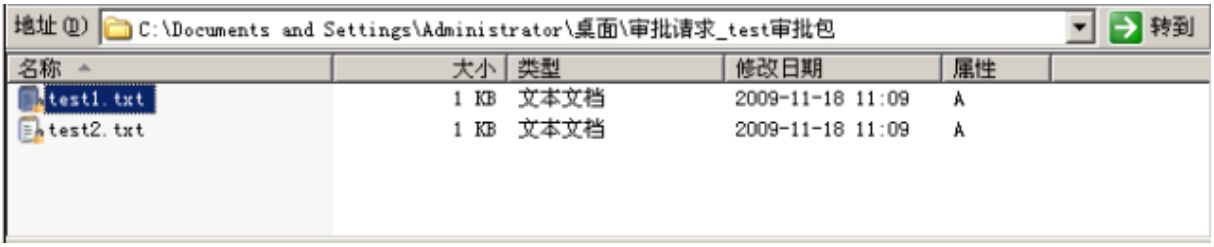


图 12-123　查看审批包文件内容

（5）如果审批员查看文件内容没问题，允许带出使用。那么，审批员就要选定审批请求包，单击右键菜单“审批”，如图 12-124 所示。这时“审批请求包”就变成了“审批通过包”，如图 12-125 所示。

图 12-124　选择审批菜单项

图 12-125　审批通过包

12.11.2.3　带出使用

（1）申请人得到审批通过包后，双击弹出“文件浏览”界面，如图 12-126 所示。单击“Extract to”按钮，输入文件路径和自解密口令，将审批通过包解压到指定路径下。

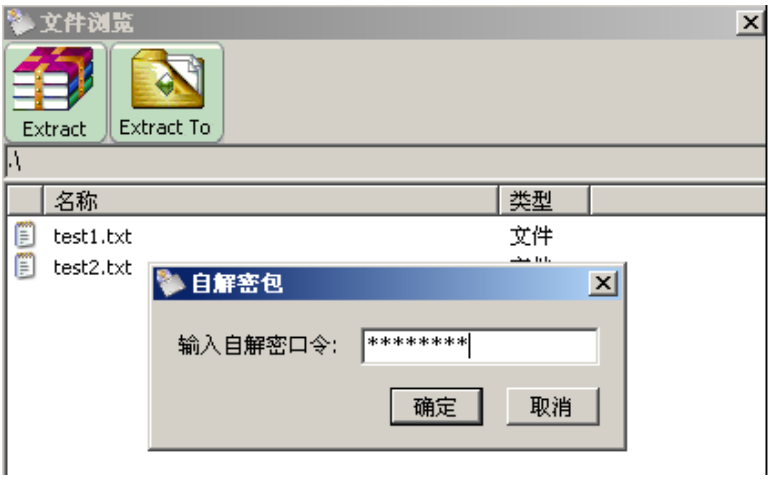


图 12-126　文件游览界面

（2）在指定路径下，可以看到解压后的审批通过包，如图 12-127 所示。

图 12-127　解压后的审批通过包

（3）双击解压后的审批通过包，可以看到里面的文件，如图 12-128 所示。这时，文件都已被解密，可以任意带出使用。

图 12-128　审批通过文件列表

提示:

（1）审批员只能审批管理范围内的其它用户的审批请求。

（2）审批通过后，可以将“审批通过包”拷在任何一台机器上使用。使用时，双击“审批通过包”，输入正确密码，单击“确定”按钮，将文件解密在同一路径下。

12.12 电子文档权限管理

客户端有主动授权管理策略的用户，可以通过右键菜单“在线授权”和“离线授权”方式制作出主动授权文件。这些文件带有特殊权限控制，用户只能在权限范围内打开使用。主动授权管理策略参见控制台的 电子文档权限管理部分。

12.12.1 离线授权

（1）客户端用户选择隔离文件或非隔离文件，可以一次选择多个文件，如图 12-129 所示。单击右键菜单“权限管理”→“离线授权”，弹出离线授权界面。非隔离文件包括普通文件和普通安全文档，不包括密级文件、主动授权文件和用“我的加密文件夹”加密的文件。

图 12-129　选择隔离文件或非隔离文件

（2）在授权界面中选择操作设置、权限信息和使用范围，如图 12-130 所示。在权限信息中选择是否允许使用范围内的用户修改、拷贝拖拽、打印、截屏以及重新授权该文件等等。

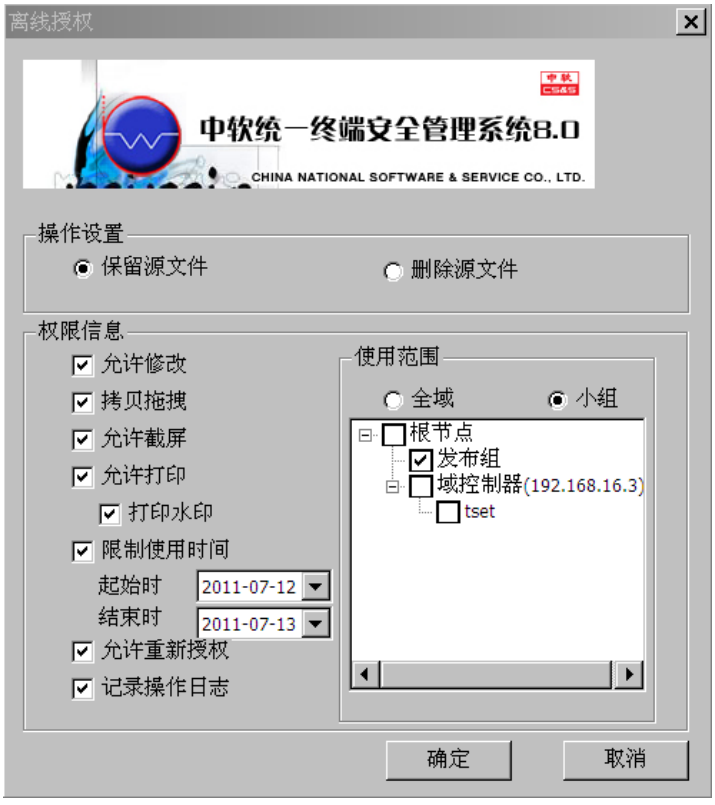


图 12-130　离线授权界面

提示：

不允许修改，是指使用人修改后无法保存；

允许拷贝拖拽，是指只允许将拷贝内容复制到加密进程控制的文件中；

允许截屏，是指允许使用截屏键，且只允许将截屏后的内容拷贝到加密进程控制的文件中，但

不能将截屏内容拷贝到非加密进程控制的文件中。

打印水印，是指打印控制台“主动授权控制”中设置的水印内容;

使用时间，“起始时间”和“结束时间”一样时，有效时间是指该天的 00：00—23：59;

允许重新授权，是指制作人和使用范围内的用户有对该主动授权文件进行重新授权的权利;

记录操作日志，是指记录客户端用户使用该授权文件的日志，并将日志信息上传到控制台统计审计分析的“安全文档”→“主动授权文件使用日志”中。

（3）单击“确定”按钮，弹出提示框，如图 12-131 所示。再次确定后，弹出气泡信息“离线制作自主授权文件成功”，如图 12-132 所示。

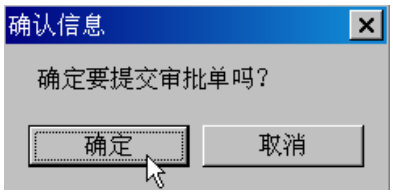


图 12-131　确认信息

图 12-132　提示主动授权文件成功

（4）制作成功的主动授权文件，分别显示在原文件所在路径下，文件图标有所不同，如图 12-133 所示。这些主动授权文件，只有使用范围内的用户可以打开，使用时受赋予的权限限制。

图 12-133　主动授权成功的文件

12.12.2 在线授权

客户端通过右键菜单的“在线授权”制作主动授权文件，详见附件三《安全文档审批系统使用手册》。

12.13　模式切换

在安全文档策略中，为客户端设置两个模式：工作模式和普通模式。如果下发“允许模式切换”策略，在客户端右键菜单中才会出现模式切换菜单项。

若当前客户端为工作模式，右键菜单显示为“切换为普通模式”；若当前客户端为普通模式，右键菜单则显示为“切换为工作模式”。

提示：安全文档策略的模式切换控制中有详述，请参阅。

12.14　本地备份策略设置

在安全文档策略中，如果允许客户端自定义备份策略，那么在客户端右键菜单中，才会出现“本地备份策略设置”项，如图 12-134 所示

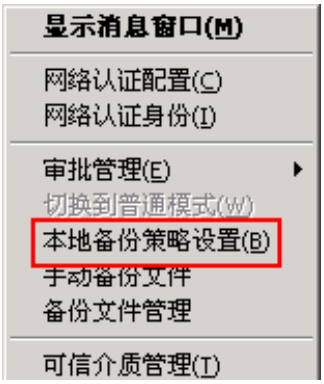


图 12-134　本地备份策略设置

单击“本地备份策略设置”菜单项，进入备份策略设置界面，如图 12-135 所示。在这里客户端可以设置自己的备份策略。如果控制台事先给他下发过备份策略，将做为缺省备份策略，客户端以自己制定的备份策略为准。

选项说明：

（1）勾选“启用自定义备份策略”，该页面中其他输入项、选择项可用，客户端将采用自定义的备份策略；不勾选“启用自定义备份功能”时，客户端执行控制台给他下发的缺省备份策略。

（2）设置备份频率时，最好在客户端参数设置中，将客户端和服务器时间同步。然后，从下拉框中选择定时备份的周期和时间点。

（3）选择“备份文件到原文件所在的分区（推荐）”，同时勾选“仅备份本地硬盘的加密文件，（推荐）”，那么仅备份本地硬盘的加密文件到原分区，不备份移动硬盘等设备上的文件。

（4）选择“备份所有文件到指定分区”，分区不能指定 U 盘和移动硬盘等设备。

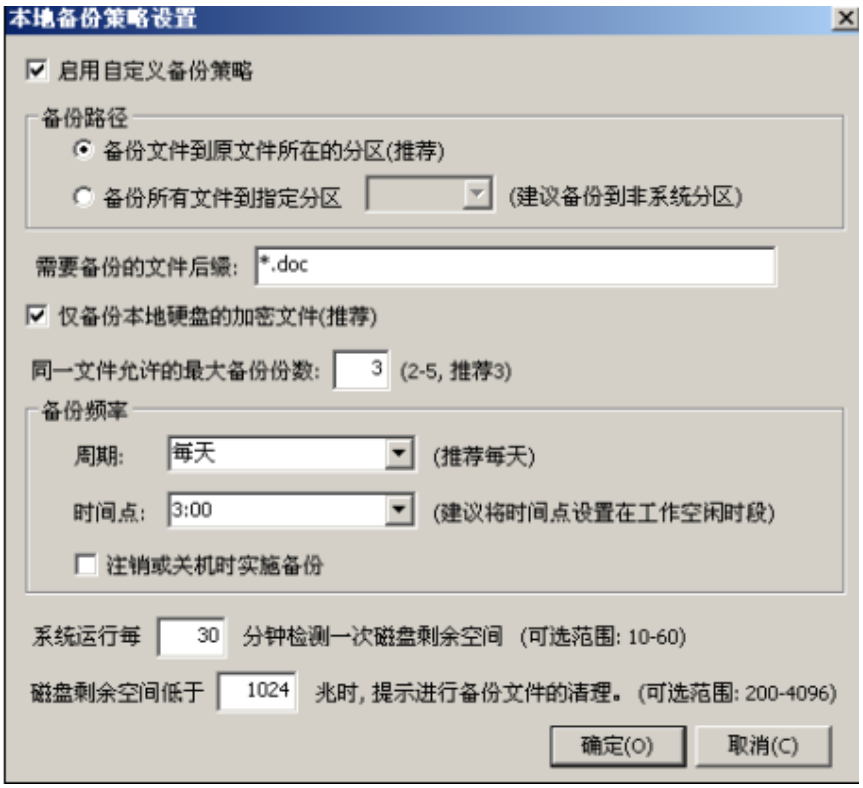


图 12-135　本地备份策略设置

提示:

1. 备份路径选择“备份文件到原文件所在的分区（推荐）”时，服务器会检测客户端上所有有盘符的磁盘。这时硬盘保护区、可信磁盘、移动硬盘都会被检测。如果这些磁盘的磁盘空间小于控制台设置的阈值都会在客户端报警提示。

2. 备份路径选择“备份文件到原文件所在的分区（推荐）”时，并且不勾选“仅备份本地硬盘的加密文件（推荐）”，这时会对本地硬盘、移动硬盘、可信磁盘或硬盘保护区上的加密文件执行备份，不会对网络硬盘上的加密文件执行备份。服务器除了检测本地磁盘的磁盘空间外，还会检测移动硬盘、可信磁盘和硬盘保护区的磁盘空间。如果不对移动硬盘、可信磁盘和硬盘保护区进行加密文件操作，就不检测这些磁盘的存储空间。

3. 备份的加密文件名长度限制最长为 180 个字符（包括后缀），超过 180 个字符可能会备份不成功。

4. 如果没有给客户端下发加密进程策略，那么它设置的备份策略也无效。

12.15　手动备份文件

如果客户端应用了备份策略，设置了备份文件的类型，那么，客户端对需要备份的文件做任何改动，系统都会将这些已改动的文件做标记，按照设置的周期定时备份。用户也可以按照自己需要，手动备份待备份的文件。

（1）点击客户端右键菜单“手动备份文件”，可以看到待备份文件列表，如图 12-136 所示。

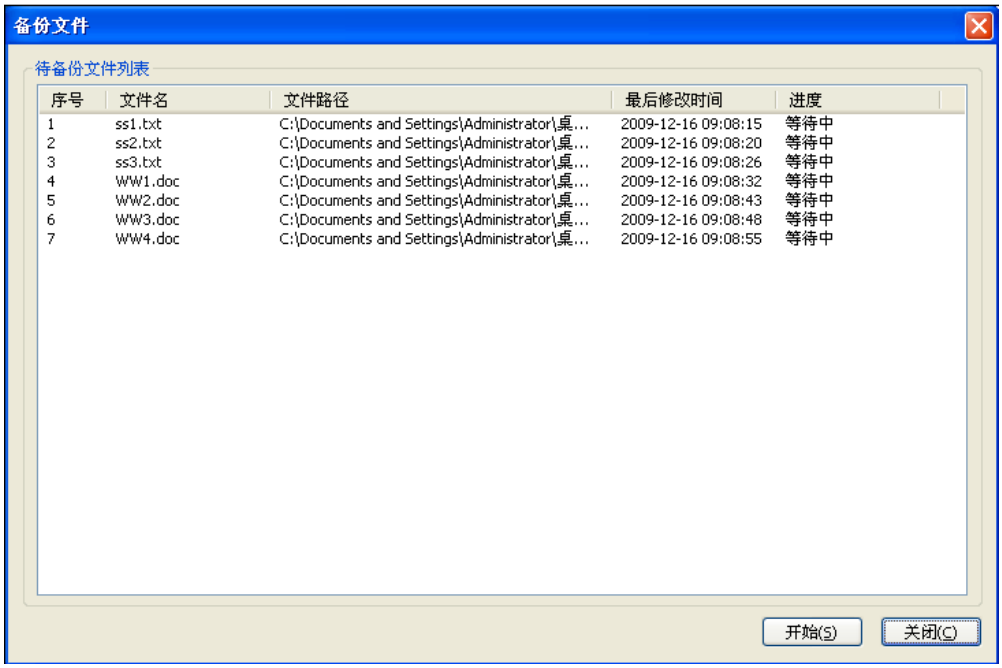


图 12-136　待备份的文件列表

（2）单击“开始”进行手动备份。备份时有进度条显示，备份完成后有提示框，如图 12-137 所示。

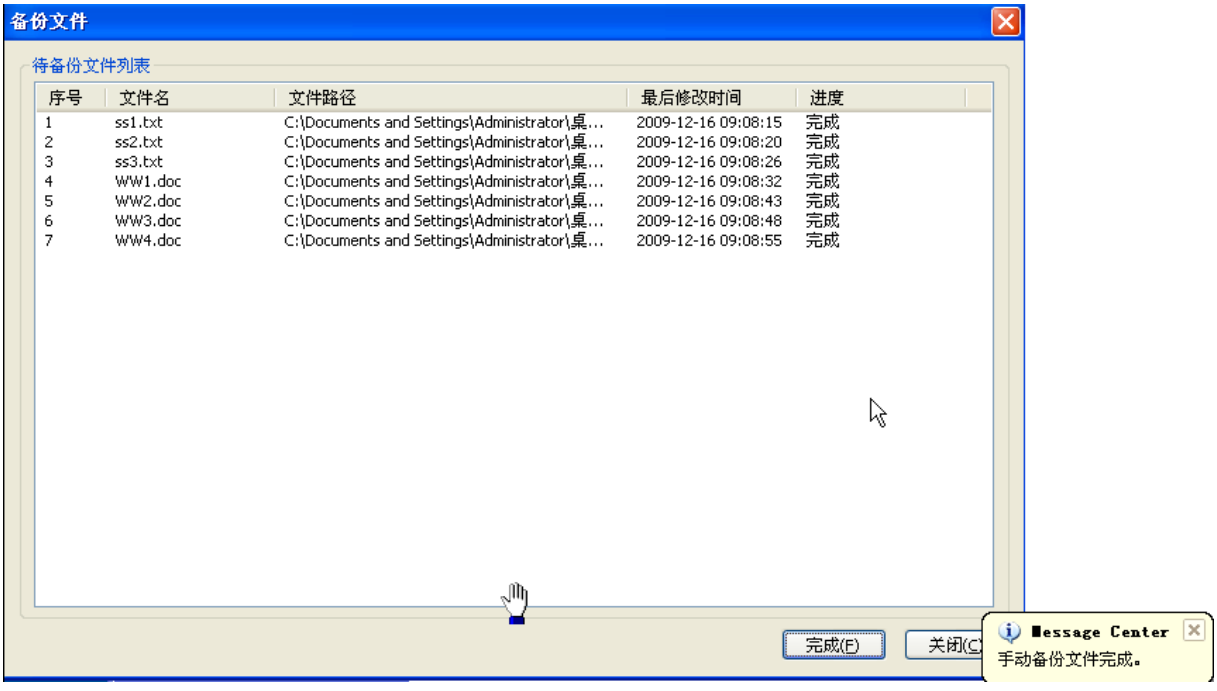


图 12-137　手动备份文件完成

提示：

（1）不管是手动备份，或是自动备份，都是备份“待备份文件列表”中的文件。如果将某文件进行了手动备份，就会在“待备份文件列表”中消失，定了定时备份时不再备份。

（2）如果将待备份文件移动了位置或者更改了文件名，备份时会出错。

（3）单击客户端消息框，能看到备份记录，如图 12-138 所示。如果待备份文件移动了位置或者更改了文件名，备份时会出错。备份出错的文件也将在这里显示。

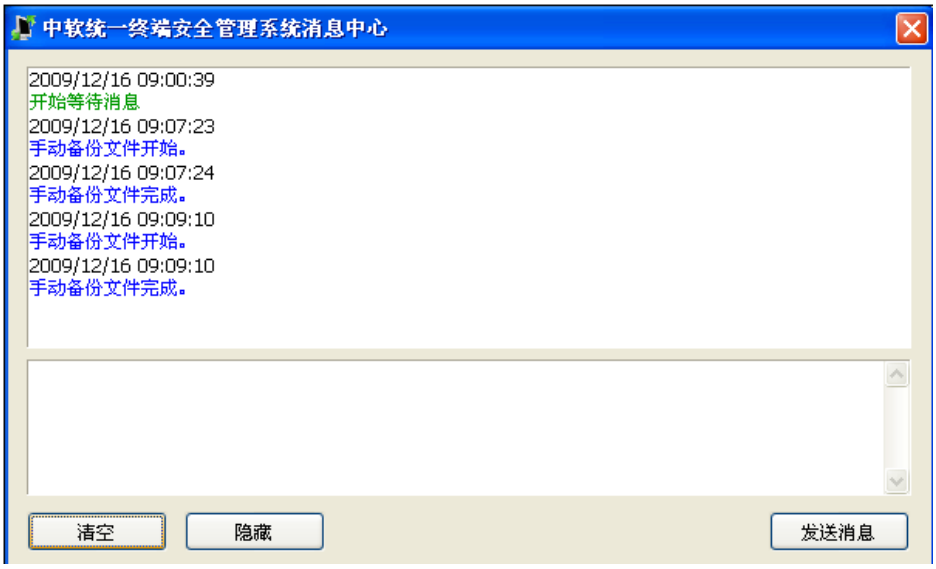


图 12-138　手动备份文件消息框

12.16　备份文件管理

通过备份文件管理，可以查看、还原、删除、查询已备份的文件。

（1）点击客户端右键菜单“备份文件管理”，可以看到已备份的文件列表，如图 12-139 所示。

这里的备份，包括手动备份和自动备份。备份几次，文件份数显示几，最多显示备份策略中设置的备份份数。也就是说，备份 2 次，显示份数为 2。如果备份策略设置备份份数为 3，那么备份 5 次，显示的份数也为 3，而且是最新的 3 份。

备份文件的有效性是指原文件是否还存在。“有效”表示备份文件的原文件还存在，“无效”表示备份文件的原文件不存在了。将备份文件的原文件删除后，在有效性一览都会显示“无效”。单击“清理”按钮，可以将所有无效备份记录快速清除。

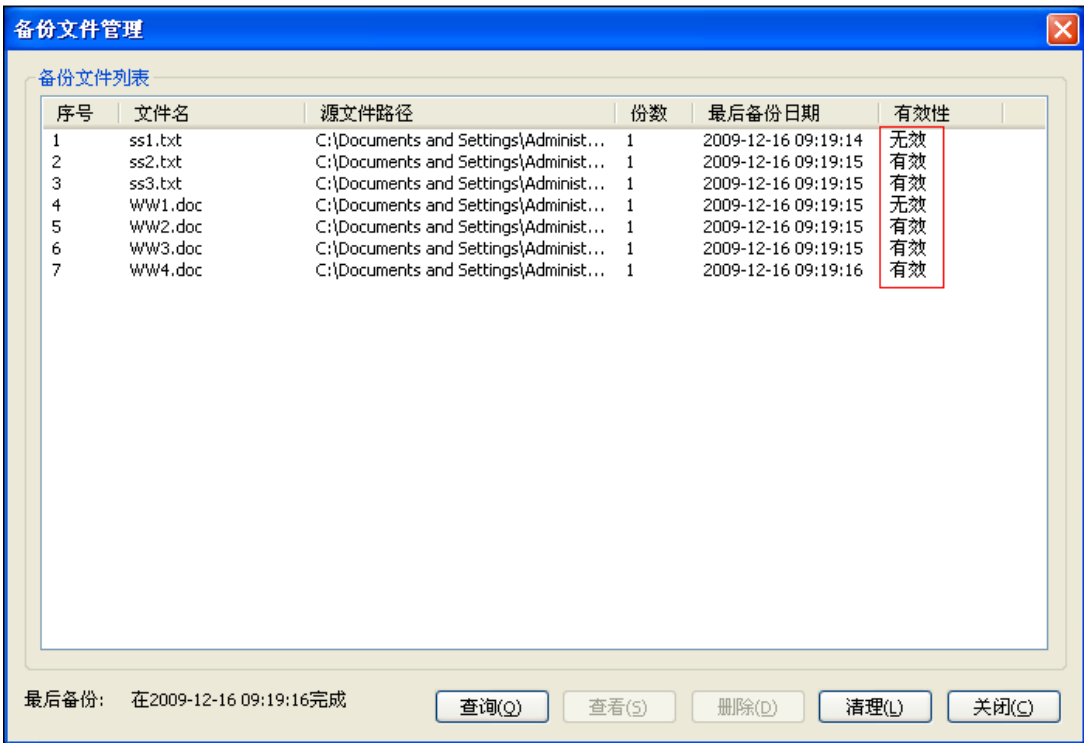


图 12-139　已备份的文件列表

（2）在备份列表中任选一备份文件，有效或无效都可，单击“查看”按钮，查看详细信息，如图 12-140 所示。备份份数是几，在备份文件详细信息中显示几个记录。这里的备份份数是 1，所以在备份文件详细信息中显示 1 个记录。

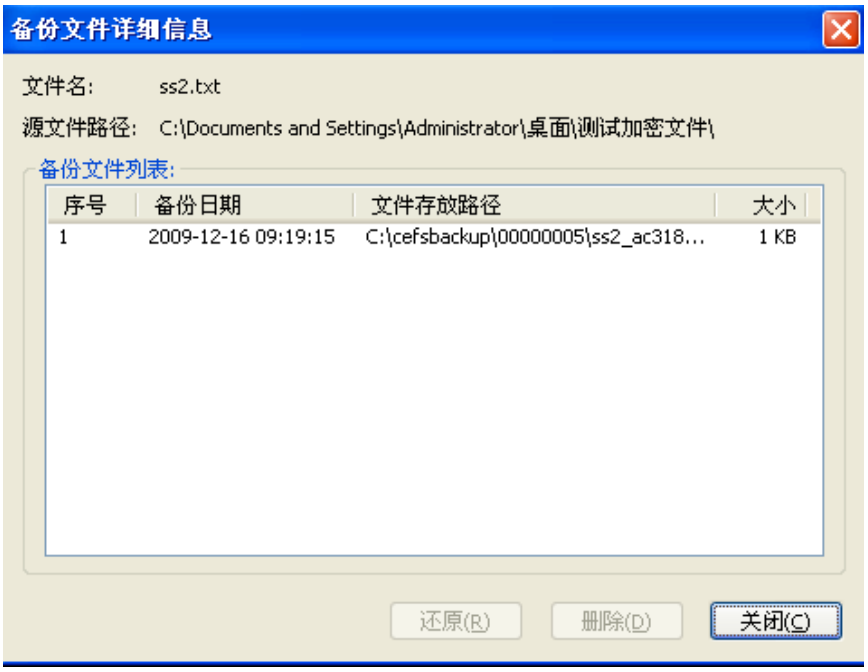


图 12-140　备份文件详细信息

（3）如果原文件已损坏，在详细信息列表中，选择一条备份记录，单击“还原”按钮，如图 12-141。选择还原文件存储路径，输入还原文件名称，将备份文件还原，如图 12-142 所示。还原文件成功后，有成功提示框。

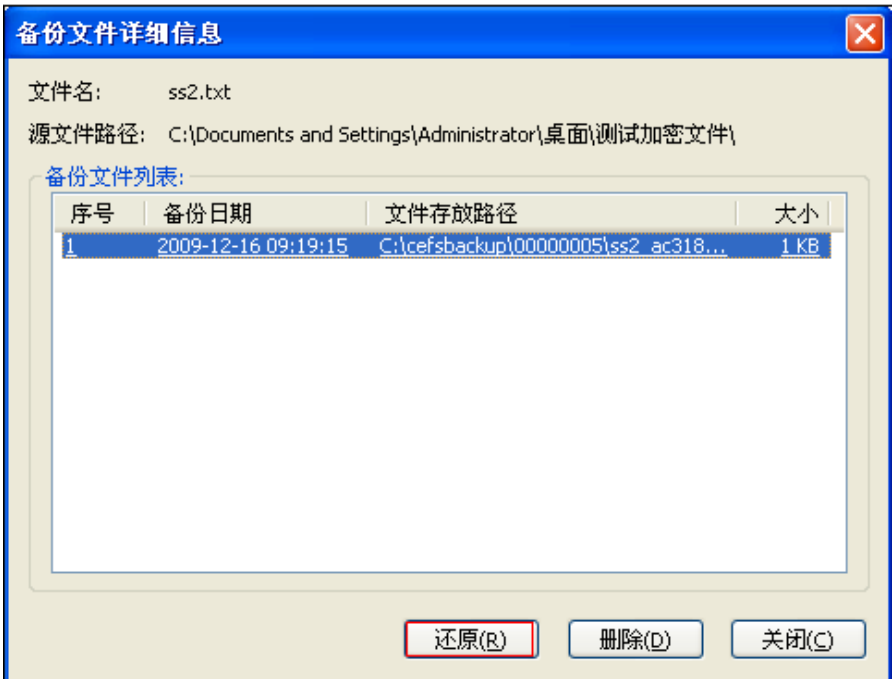


图 12-141　选择要还原的备份文件

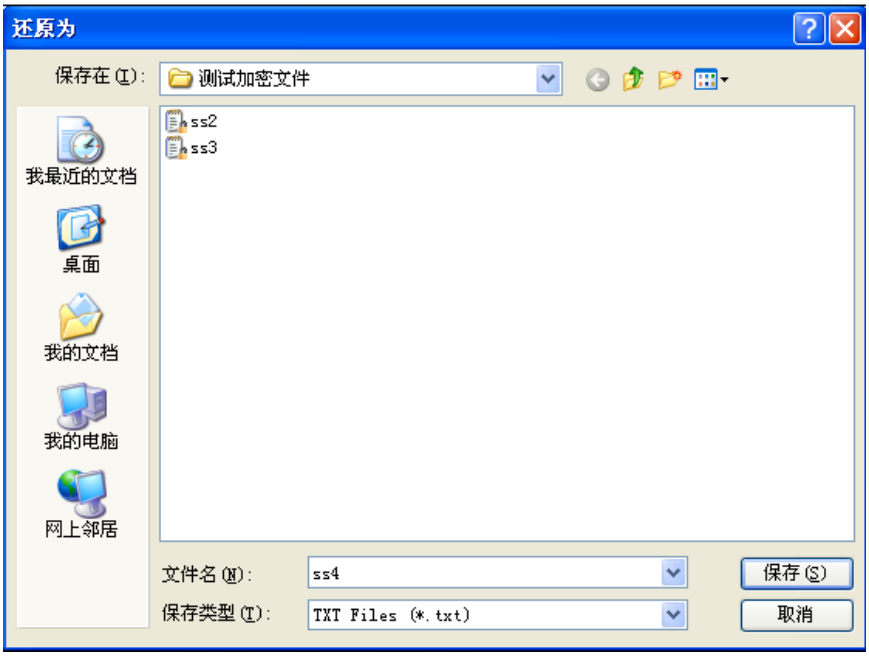


图 12-142　输入还原文件名称

（4）返回备份文件详细列表框，如果将最后一个备份文件记录删除，那么返回到备份文件管理中，就不再显示该备份文件了。例如：我们将 ss2.txt 的最后一个备份文件记录删除后，那么返回到备份文件管理中，就不再显示 ss2.txt 备份文件了，如图 12-143、如图 12-144 所示。

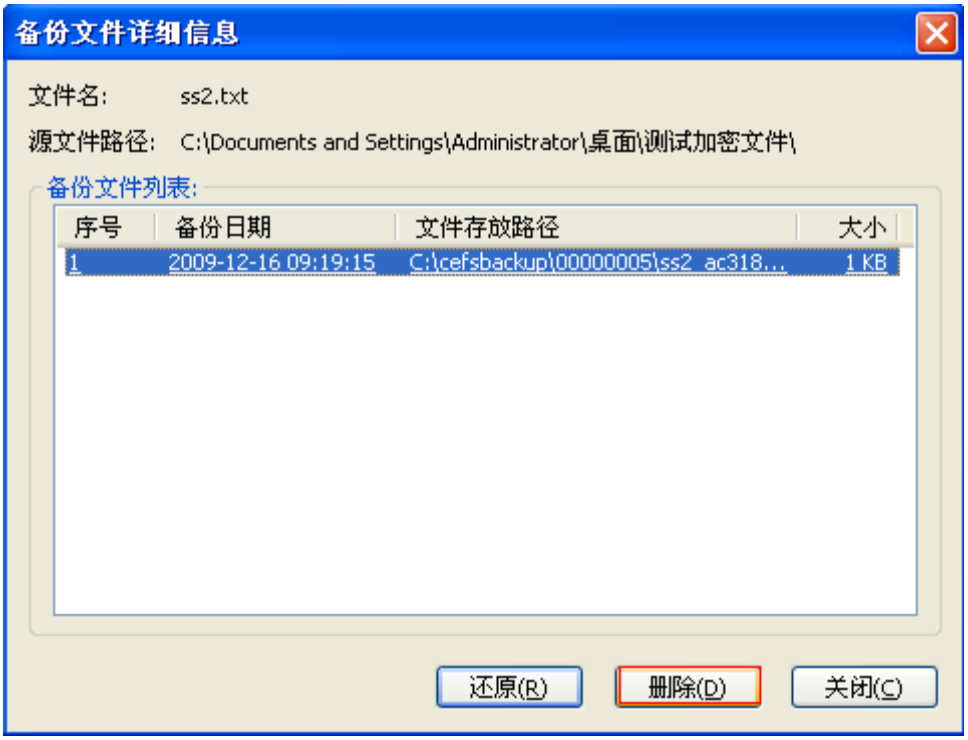


图 12-143　删除最后一个备份文件记录

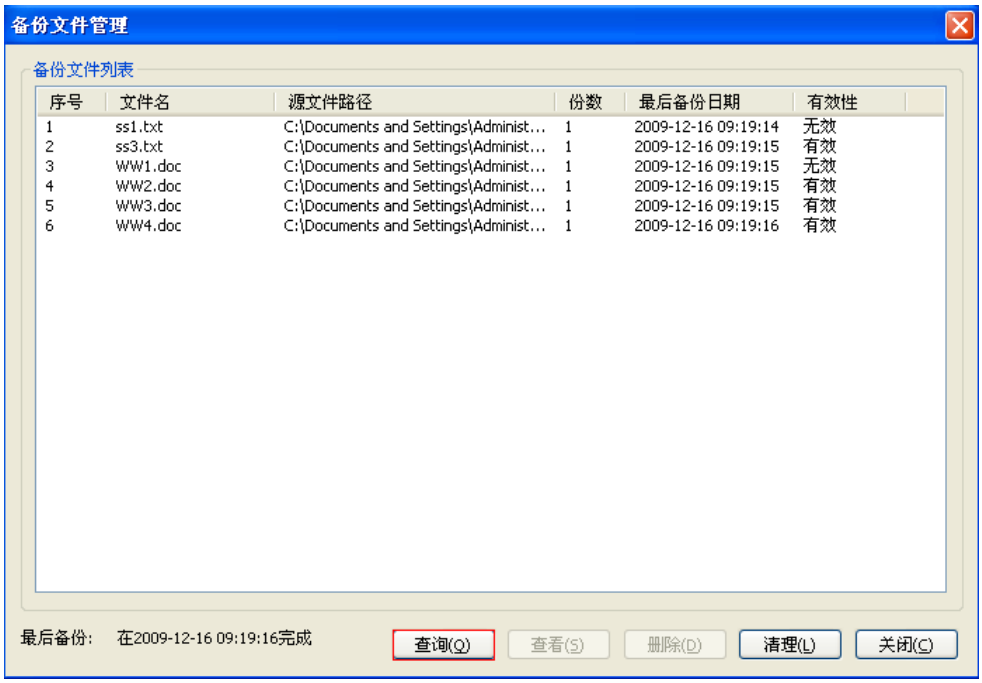


图 12-144　不再显示删除最后一个备份记录的备份文件

（5）在备份文件管理中，我们利用“查询”功能验证一下，上面删除最后一个备份记录的备份文件 ss2.txt 是否还存在。

单击“查询”按钮，在备份文件查询框中，输入查询文件名“ss2.txt”，如图 12-145 所示。单击“确定”按钮，将看不到要查询的文件。

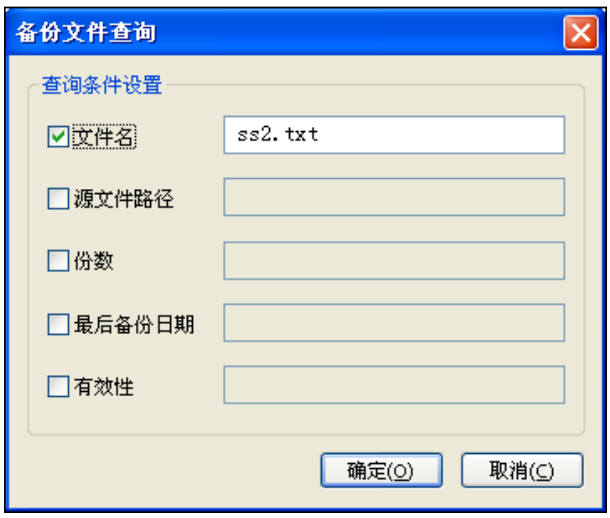


图 12-145　备份文件查询

（6）对于某些不需要的备份文件，用户可以单选或多选，单击“删除”按钮，直接从备份库中清除，如图 12-146 所示。

提示：对于有效或无效的备份文件，都可用“删除”按钮删除。

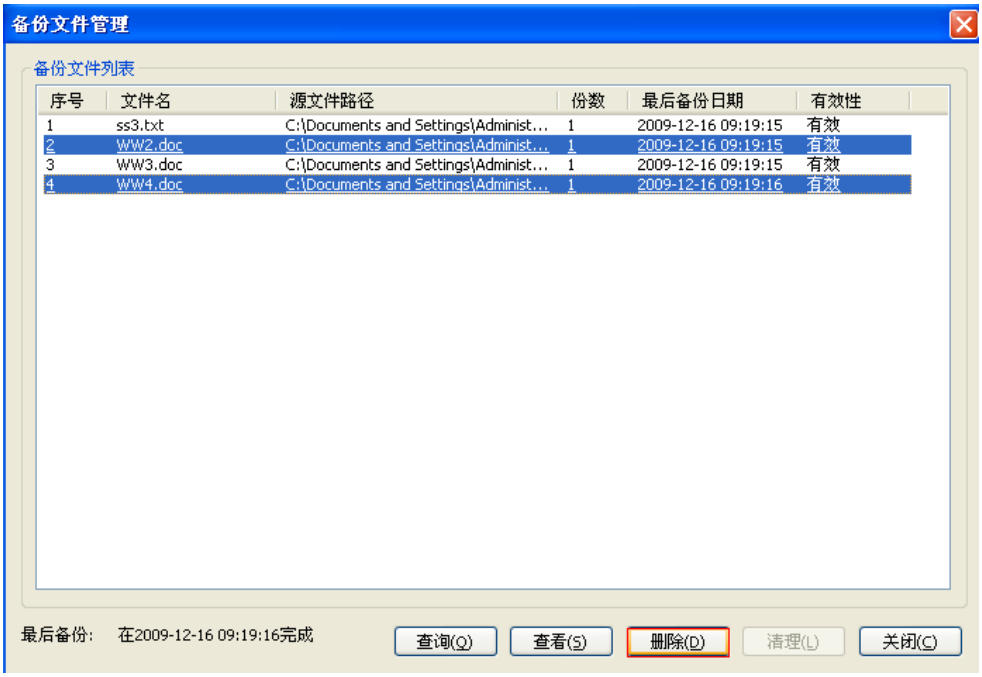


图 12-146　删除备件文件

12.17 文件打印审批

如果客户端被禁止使用打印机，当用户必须打印文件时，就需要按照审批规则向审批员提交自己的打印申请，待审批员批准后才可以打印。审批员可以查看打印文件，决定是否批准打印。客户端用户无法自行打印文件。

文件打印审批需要控制台操作员登录控制台，在审批管理中设置审批规则，指定待审批的组织、审批员、审批内容和优先顺序，详见审批管理章节。

（1）客户端打开要打印的文件，单击“打印”功能项，在弹出的打印选择框中，选择“审批打印机”及页面范围（页数选择决定审批后的打印内容，份数选择不起作用，可不选），然后，单击“确定”按钮，如图 12-147 所示。在这里我们推荐先将“审批打印机”设为默认打印机，选择某个要打印的文件，单击右键菜单“打印”，跳过该打印机选择界面。

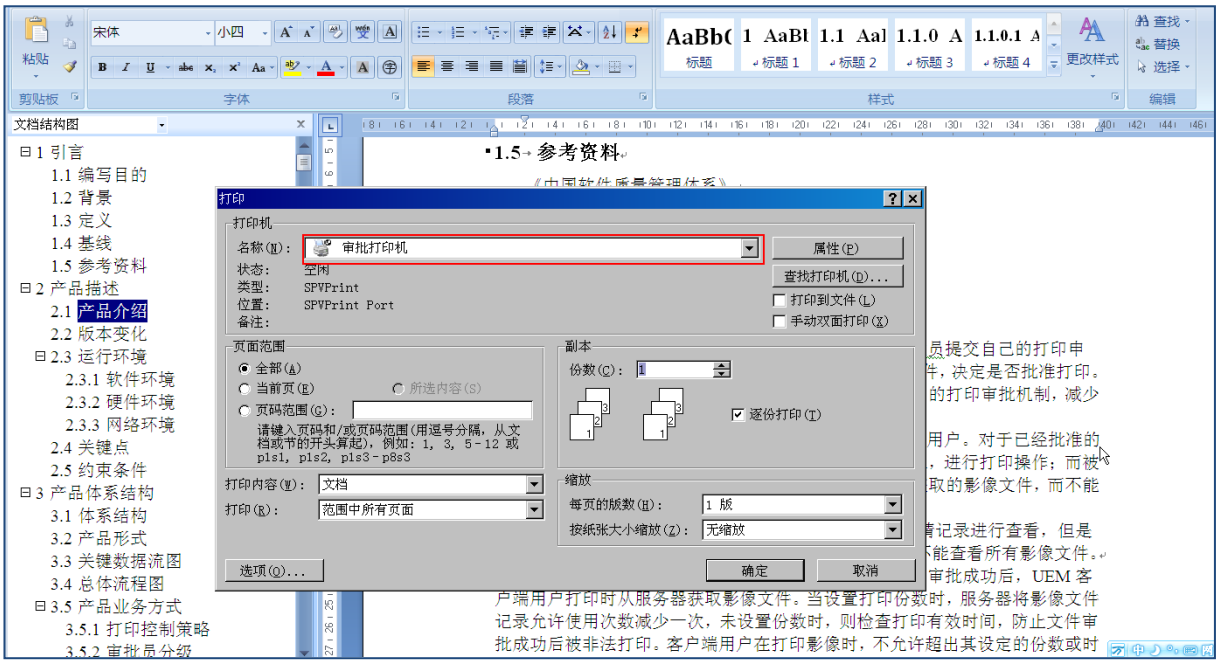


图 12-147　选择“审批打印机”打印文件

（2）稍等，出现打印申请界面，如图 12-148 所示。打印页数越多，等待时间越长，请用户耐心等待。

在“打印申请”界面中，我们可以自定义一个假文件名替换真实文件名，隐藏掉敏感信息，之后的审批过程中出现的均为该设定文件名。选择申请截止日期，默认为申请日往后顺延一周，请用户根据实际情况选择截止日期。申请单必须有使用份数或有效期控制，两者必居其一，也可同时选择。若勾选使用份数控制，请输入申请打印份数（1-65535）；若勾选使用有效期控制，请选择起止时间，默认打印有效期为一周。审批通过后，每打印一次，剩余份数自动减一，超过打印有效期或剩余份数为 0，都不能再次打印。

另外，如果申请人允许审批员查阅待审批文件，点选“允许查阅”；如果不想让审批员查阅待审批文件，点选“禁止查阅”。最后，填写申请打印的理由，单击“提交”按钮，上传给服务器。

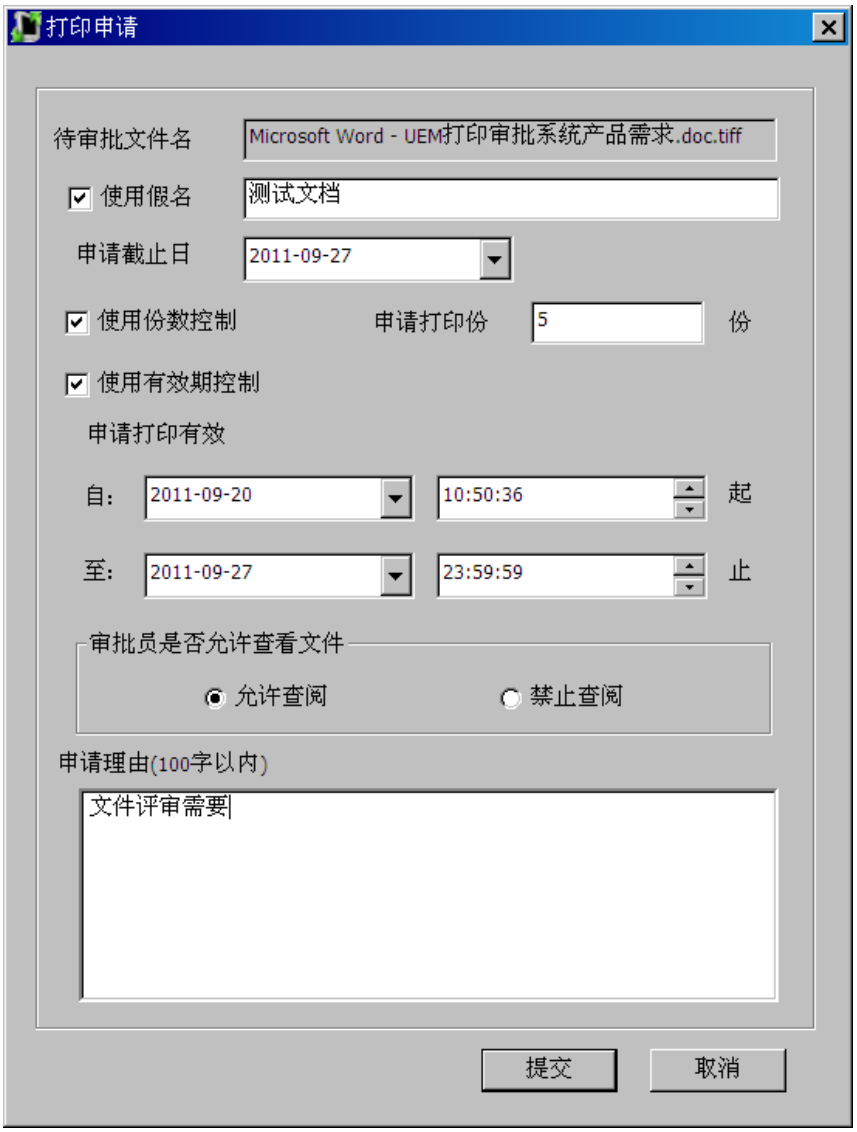


图 12-148　打印申请界面

（3）申请单成功提交后，申请人单击客户端右键菜单“审批管理”→“文件打印申请查看”，进入申请查看界面，可看到该申请处于“待审批”状态，等待审批，如图 12-149 所示。在打印申请列表中，如果到了申请截止日期，审批员还没有审批，该次申请自动作废。当然，申请人也可选择“待审批”的申请单，单击“撤消申请”按钮，将其撤消。

图 12-149　查看待审批的申请单

（4）在审批员一方，如果有新的审批任务，服务器将及时通知它，在屏幕右下方弹出汽泡式提示信息，如图 12-150 所示。

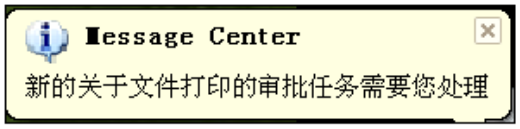


图 12-150　审批任务提示信息

（5）审批员单击客户端右键菜单“审批管理”→“文件打印审批管理”，进入审批管理界面，可看到当前的审批任务列表，如图 12-151 所示。选择某审批任务，如果申请人允许审批员查阅时，单击“查阅”按钮，可以看到该文件的打印影像

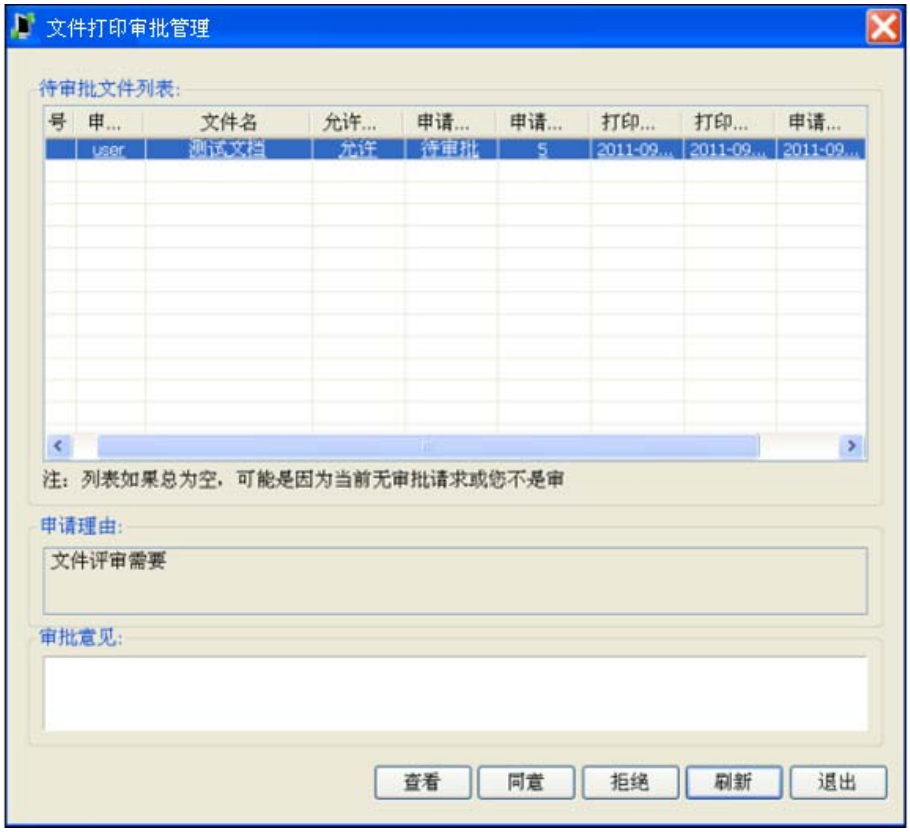


图 12-151　审批管理界面

（6）如果审批员对申请打印的文件内容没有什么异议，允许申请人在有效时间内打印申请的份数，则单击“同意”按钮，系统将弹出提示信息，确定后即可批准该申请单，如图 12-152 所示。

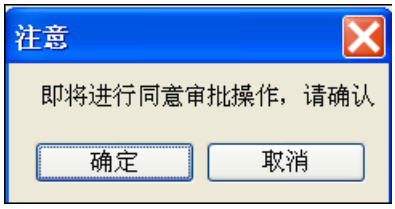


图 12-152　同意申请提示信息

（7）审批通过后，申请人客户端右下方将弹出汽泡式提示信息，如图 12-153 所示。

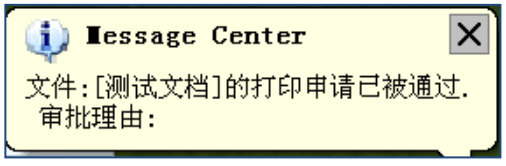


图 12-153　审批通过提示信息

（8）这时申请人单击客户端右键菜单“审批管理”→“文件打印申请查看”，进入申请查看界面，可看到刚刚审批通过的申请单，单击表头可以排序，如图 12-154 所示。在申请文件列表中，能看到审批通过和等待审批的打印申请，也能看到自申请之日起两周内，已经不能打印的打印申请。

不能打印的打印申请包括：审批拒绝、申请撤销、剩余打印份数为 0 或者超过打印有效期的打印申请。

图 12-154　申请文件列表

（9）申请人选择“已批准”的申请单，单击下方的“打印”按钮，选择打印份数，单击“打印”按钮，如图 12-155 所示。

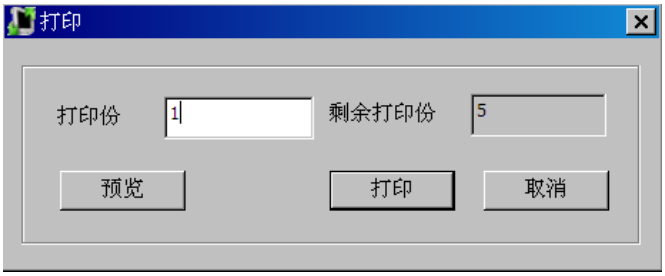


图 12-155　选择打印份数界面

提示：如果打印申请审批通过后，用户所在的客户端没有打印机，可以以同样的帐户登录到连打印机的计算机，进行异地打印操作。

（10）在打印机选择界面，一定要从下拉框中选择真实的打印机，如图 12-156 所示。选择打印份数，不能超过上个界面的打印份数，实际打印以这个界面的打印份数为准。如果选择页面范围，则打印出指定范围内的文件内容。

注意：打印页数与打印份数无关，就是只打印一页，也算打印一份，剩余次数会自动减一。

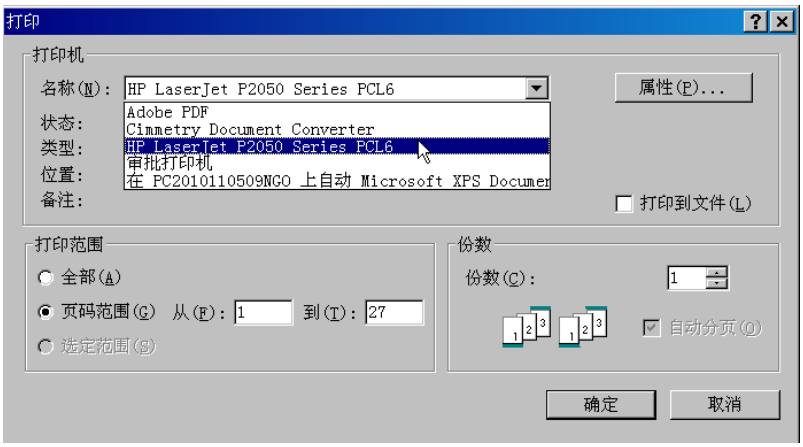


图 12-156　真实打印机选项

（11）还有一种情况需要说明。如果审批员不同意申请人打印待审批的文件，或者感到申请的打印有效期过长，打印份数过多等，则可单击“拒绝”按钮，拒绝其申请，如图 12-157 所示。审批员拒绝申请时，一定要写明拒绝理由，以便申请人修改后，再次提出申请。

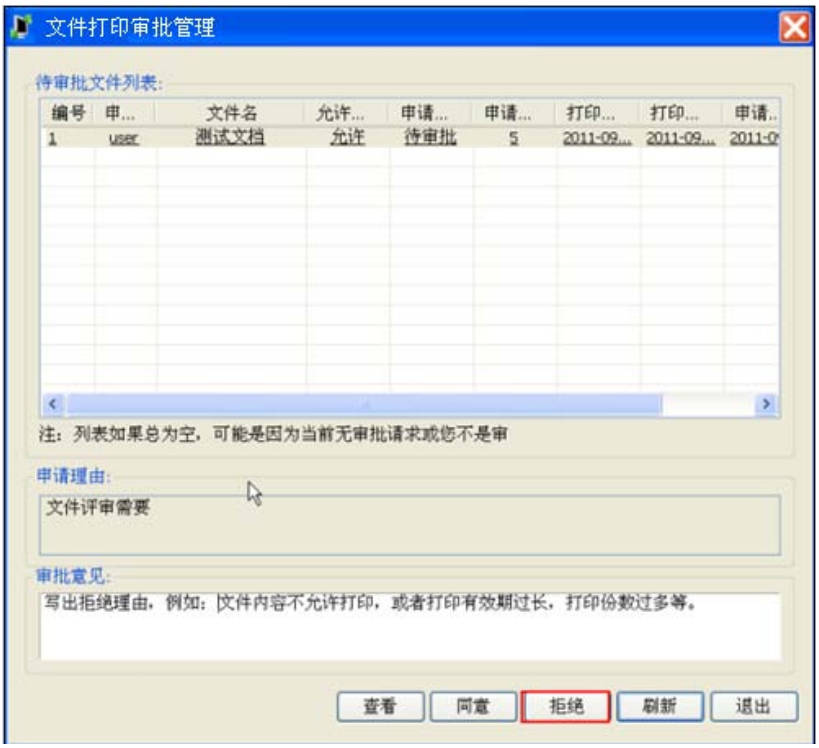


图 12-157　拒绝申请单

（12）审批被拒绝后，申请人客户端右下方将弹出汽泡式提示信息。申请人单击客户端右键菜单“审批管理”→“文件打印申请查看”，进入申请查看界面，可看到刚刚被审批拒绝的申请单，如图 12-158 所示。用户查看拒绝理由，修改后可再次提出申请。

图 12-158　查看被拒绝的申请单

12.18 电子文件复制审批

如果客户端被禁止使用移动存储设备或光驱设备，当用户必须通过移动存储设备或光驱带入带出文件时，就需要按照审批规则向审批员提交自己的复制申请，待审批员批准后才可以进行复制操作。复制操作包括带入和带出，带入是指将移动存储设备或 CDROM 中文件拷贝到客户端的过程，带出是指将客户端中文件拷贝到移动存储设备或刻录机的过程。

电子文件复制审批需要控制台操作员登录控制台，在审批管理中设置审批规则，指定待审批的组织、审批员、审批内容和优先顺序，详见审批管理章节。

12.18.1 带入操作

（1）申请人单击客户端右键菜单“审批管理”→“电子文件复制申请”，进入复制申请界面，如图 12-159 所示。首先选择操作类型“带入”，根据介质类型选择光盘、U 盘或移动硬盘。本例选择 U 盘或移动硬盘，也就是将 U 盘上文件通过审批后拷贝到客户端。

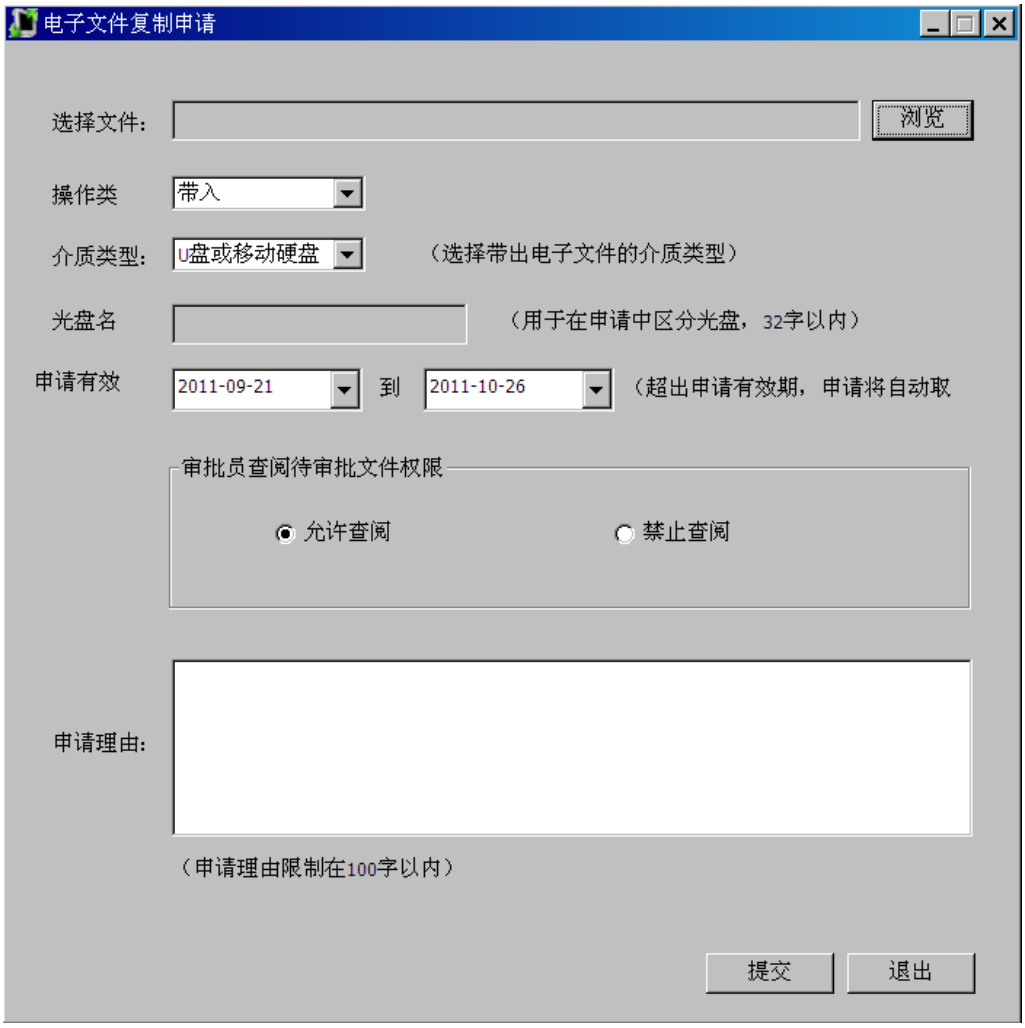


图 12-159　电子文件复制申请界面

单击“浏览”按钮，选择 U 盘或移动硬盘所在的磁盘分区，确定后进入文件列表界面，如图 12-160 所示。选择某个要带入的文件（不支持多选），确定后加载入选择文件框。

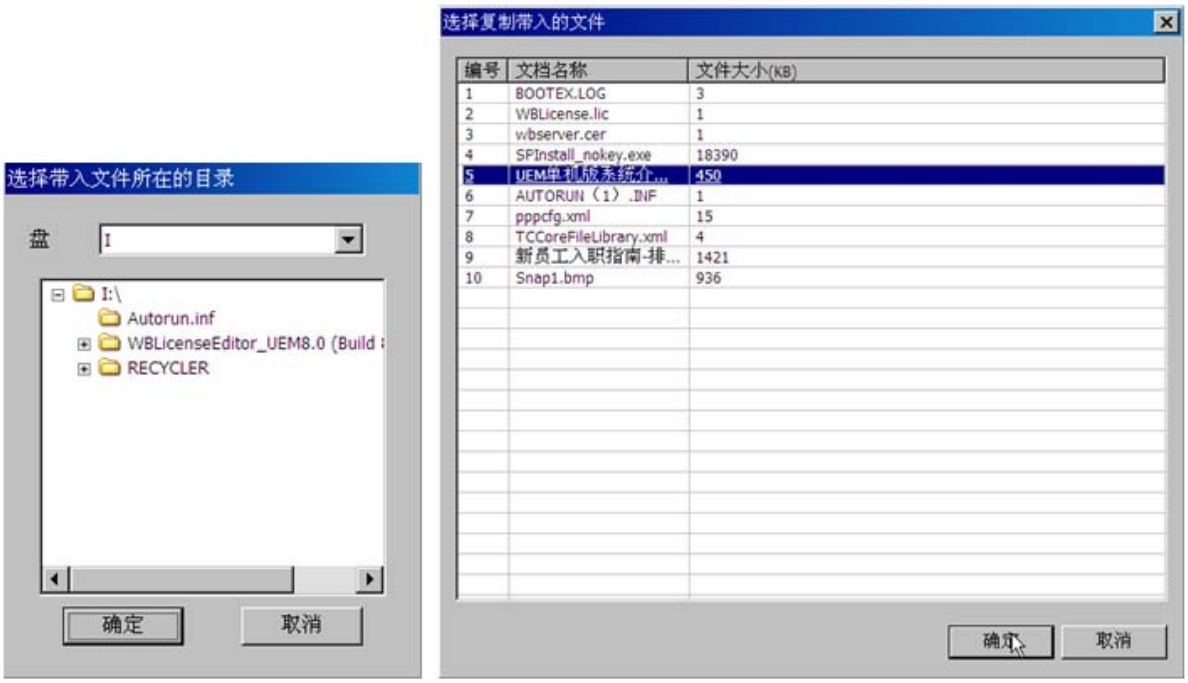


图 12-160　选择带入文件

申请有效期默认为一周七天，如果过了有效期，审批员还没有审批，该次申请自动取消，请用户根据实际情况选择有效期。

如果申请人允许审批员查阅待审批文件，点选“允许查阅”；如果申请人不想让审批员查阅待审批文件，点选“禁止查阅”。最后，填写申请带入的理由，不超过 100 个字符。最后，单击“提交”按钮，上传给服务器。

（2）申请单成功提交后，申请人单击客户端右键菜单“审批管理”→“电子文件复制申请管理”，进入申请查看界面，可看到该申请处于“待审批”状态，等待审批，如图 12-161 所示。如果过了申请有效期，审批员还没有审批，该次申请自动作废。当然，申请人也可选择“待审批”的申请单，单击“撤消审批单”按钮，将其撤消。

图 12-161　申请待审核的申请单

（3）在审批员一方，如果有新的审批任务，服务器将及时通知它，在屏幕右下方弹出汽泡式提示信息，如图 12-162 所示。

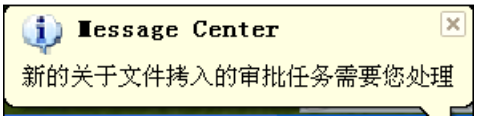


图 12-162　审批任务提示信息

（4）审批员单击客户端右键菜单“审批管理”→“电子文件复制审批管理”，进入审批管理界面，可看到当前的审批任务列表，如图 12-163 所示。选择某审批任务，如果申请人允许审批员查阅时，单击“下载”按钮，可以将待审批文件下载到本地查看内容。

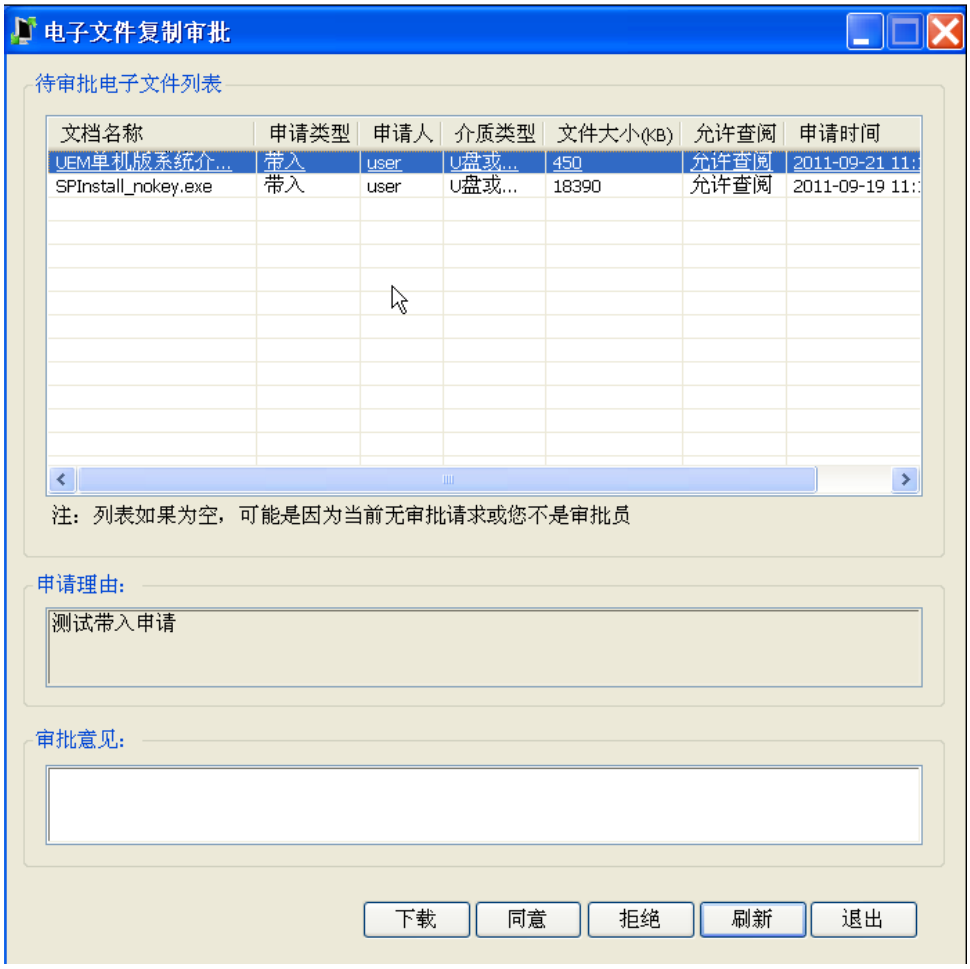


图 12-163　电子文件复制审批界面

（5）如果审批员对申请带入的文件没有什么异议，允许申请人拷贝至本机，则单击“同意”按钮，系统将弹出提示信息，确定后即可批准该申请单，如图 12-164 所示。

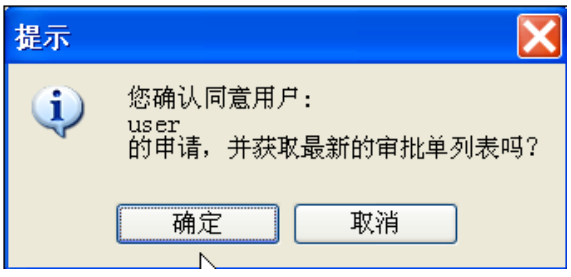


图 12-164　同意申请提示信息

（6）审批通过后，申请人客户端右下方将弹出汽泡式提示信息，如图 12-165 所示。

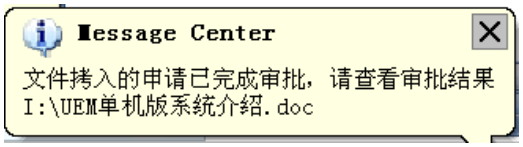


图 12-165　审批通过提示信息

（7）这时申请人单击客户端右键菜单“审批管理”→“电子文件复制申请管理”，进入申请查看界面，可看到刚刚审批通过的申请单，如图 12-166 所示。在申请文件列表中，能看到已批准和等待审批的复制申请，也能看到自申请之日起两周内，已经完成的复制申请。

图 12-166　电子文件复制申请列表

（8）选择“已批准”的申请单，单击“浏览”按钮，选择要带入到的文件路径，如图 12-167 所示。然后，单击“带入”按钮，将已批准的申请文件复制到用户指定的路径下。

图 12-167　将已批准文件带入

（9）还有一种情况需要说明。如果审批员不同意申请人带入待审批文件，则单击“拒绝”按钮，将其拒绝，如图 12-168 所示。审批员拒绝申请时，一定要写明拒绝理由，以便申请人明白为什么不能带入操作。

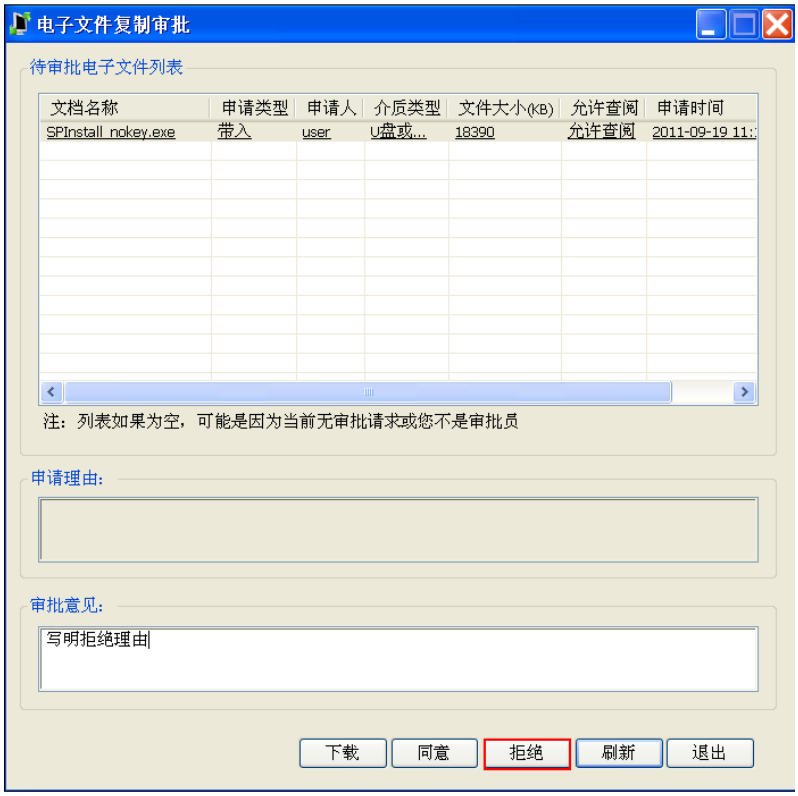


图 12-168　拒绝复制申请

（10）审批被拒绝后，申请人客户端右下方将弹出汽泡式提示信息，如图 12-169 所示。

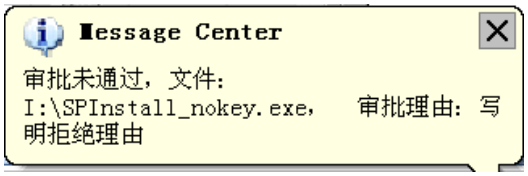


图 12-169　申请被拒绝提示信息

（11）申请人单击客户端右键菜单“审批管理”→“电子文件复制申请管理”，进入申请查看界面，可看到刚刚被审批拒绝的申请单，如图 12-170 所示。用户可查看拒绝理由，修改后再次提出申请。

图 12-170　查看被拒绝的申请单

12.18.2 带出操作

（1）申请人单击客户端右键菜单“审批管理”→“电子文件复制申请”，进入复制申请界面，如图 12-171 所示。首先选择操作类型“带出”，根据介质类型选择光盘、U 盘或移动硬盘。本例选择光盘，也就是将客户端本地文件经过审批后，刻录到光盘带出。

单击“浏览”按钮，选择客户端本地要审批带出的文件（光盘带出支持多选），确定后加载入选择文件框。

提示: 带出文件不能是打开状态，大小不能超过 100M。

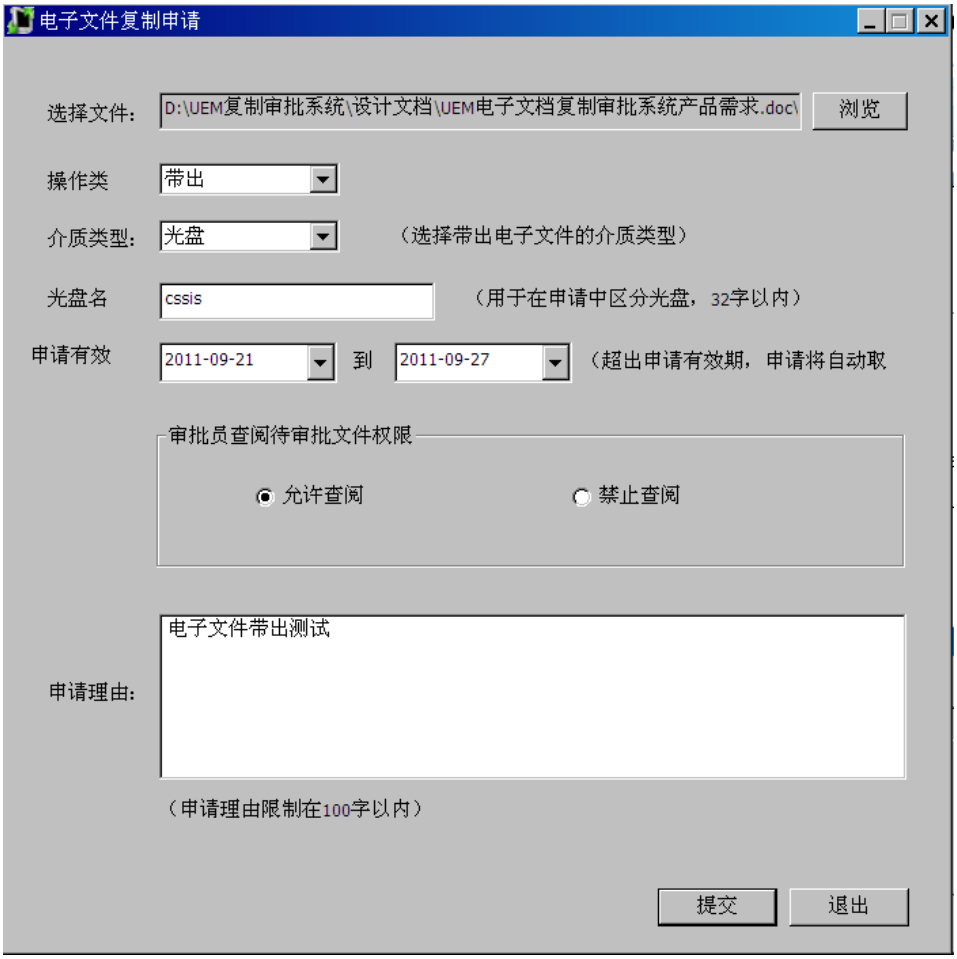


图 12-171　电子文件复制申请界面

申请有效期默认为一周七天，如果过了有效期，审批员还没有审批，该次申请自动取消，请用户根据实际情况选择有效期。

如果申请人允许审批员查阅待审批文件，点选“允许查阅”；如果申请人不想让审批员查阅待审批文件，点选“禁止查阅”。最后，填写申请带出的理由，不超过 100 个字符。最后，单击“提交”按钮，上传给服务器。

（2）申请单成功提交后，申请人单击客户端右键菜单“审批管理”→“电子文件复制申请管理”，进入申请查看界面，可看到该申请处于“待审批”状态，等待审批，如图 12-172 所示。如果过了申请有效期，审批员还没有审批，该次申请自动作废。当然，申请人也可选择“待审批”的申请单，单击“撤消审批单”按钮，将其撤消。

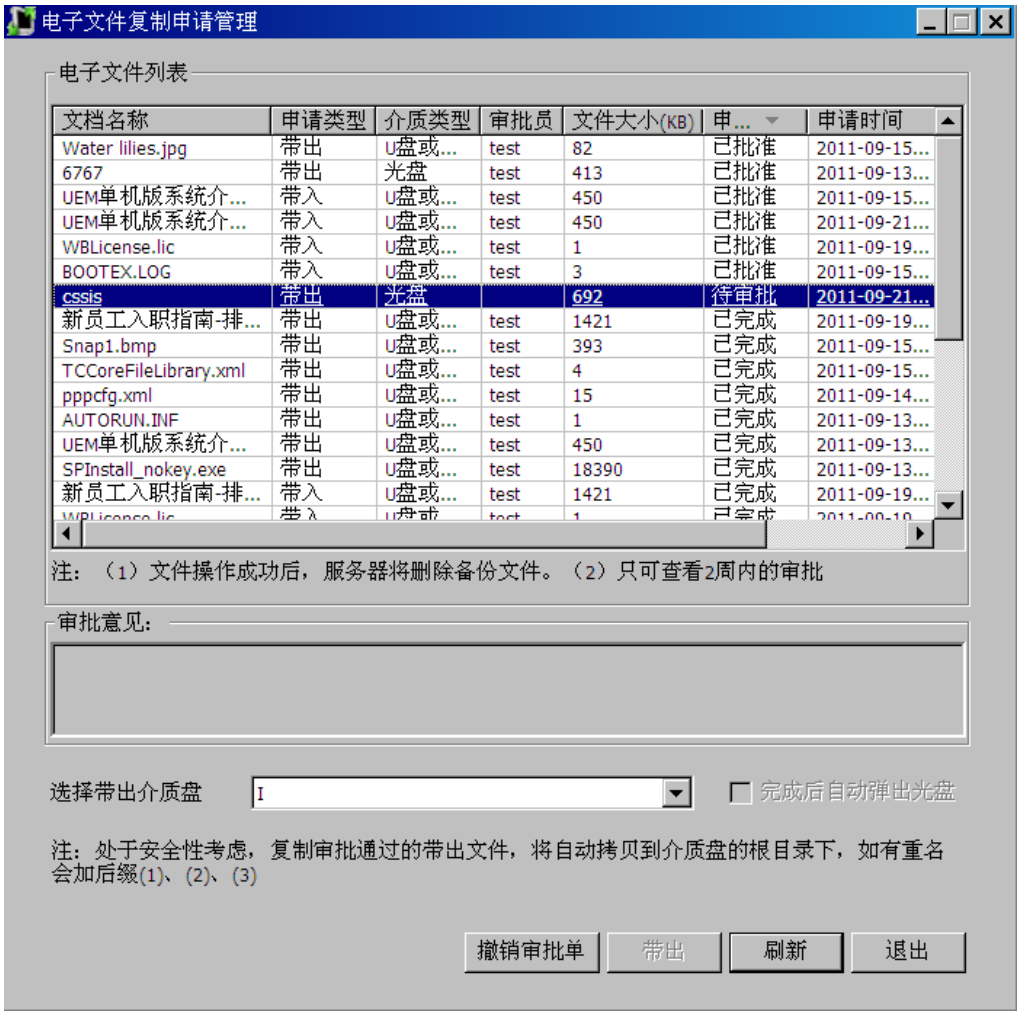


图 12-172　申请待审核的申请单

（3）在审批员一方，如果有新的审批任务，服务器将及时通知它，在屏幕右下方弹出汽泡式提示信息，如图 12-173 所示。

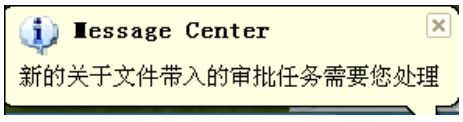


图 12-173　审批任务提示信息

（4）审批员单击客户端右键菜单“审批管理”→“电子文件复制审批管理”，进入审批管理界面，可看到当前的审批任务列表，如图 12-174 所示。选择某审批任务，如果申请人允许审批员查阅时，单击“下载”按钮，可以将待审批文件下载到本地查看内容。

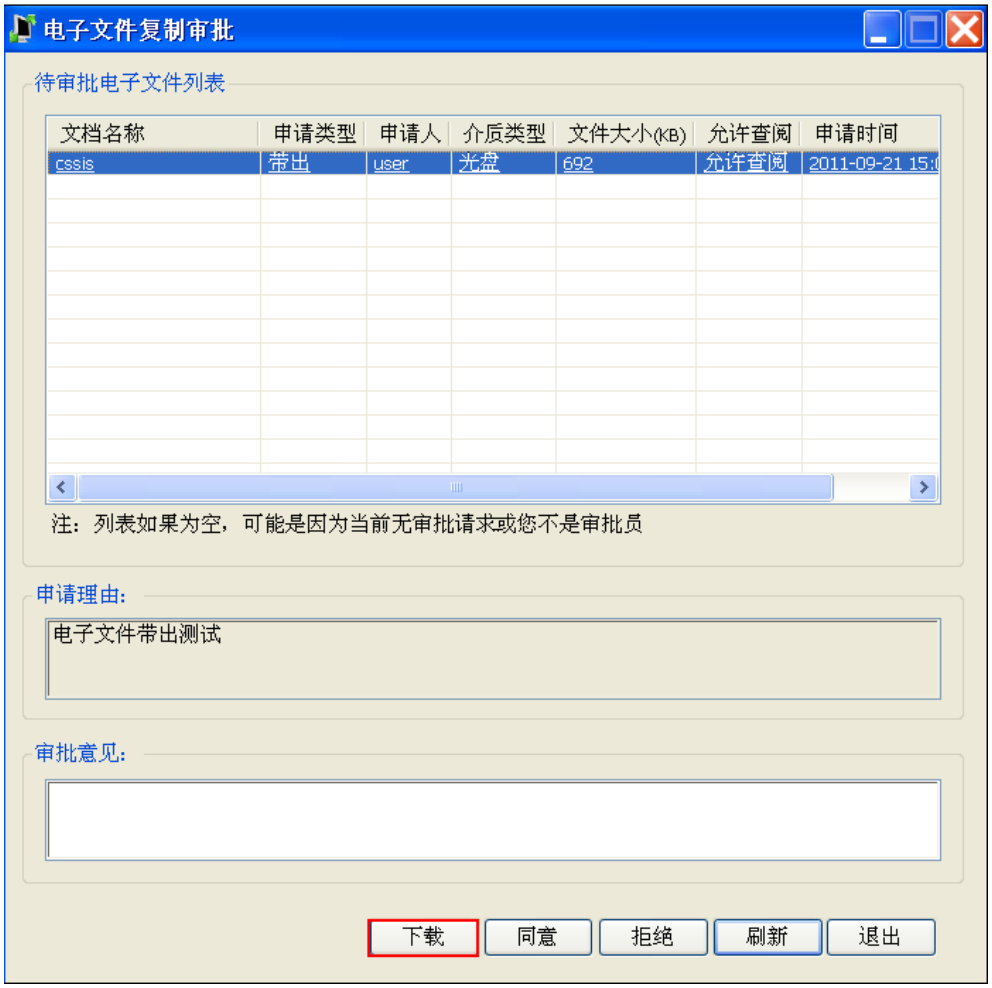


图 12-174　电子文件复制审批界面

（5）如果审批员对申请带出的文件没有什么异议，允许申请人拷贝至光盘带出，则单击“同意”按钮，系统将弹出提示信息，确定后即可批准该申请单，如图 12-175 所示。

图 12-175　同意申请提示信息

（6）审批通过后，申请人客户端右下方将弹出汽泡式提示信息，如图 12-176 所示。

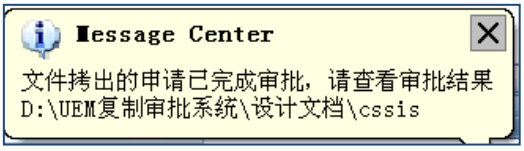


图 12-176　审批通过提示信息

（7）这时申请人单击客户端右键菜单“审批管理”→“电子文件复制申请管理”，进入申请查看界面，可看到刚刚审批通过的申请单，如图 12-177 所示。在文件列表中，能看到已批准和等待审批的复制申请，也能看到自申请之日起两周内，已经完成的复制申请。单击表头上下小箭头，可以按升序或降序排列。

图 12-177　电子文件复制申请列表

（8）选择“已批准”的申请单，以及带出介质（刻录机），如图 12-178 所示。单击“带出”按钮，那么“已批准”的申请文件将复制到光盘根目录下，如有重命名文件，自动加后缀（1）、（2）、（3）。

提示：（1）光盘带出不需要装 Nero 等刻录软件，UEM 系统提供的文件带出通道，由系统后台自动完成复制操作。**（2）**如果带出申请审批通过后，用户所在的客户端没有刻录机，可以以同样的帐户登录到带刻录机的客户端，进行异地光盘带出操作。**（3）**一些老系统尚不支持 DVD+-RW、DVD-RAM 及蓝光 RW 的多区段刻录操作（不可追加，可单次刻录），对 CD-R、CD-RW 及 DVD+-R 可以完全支持。

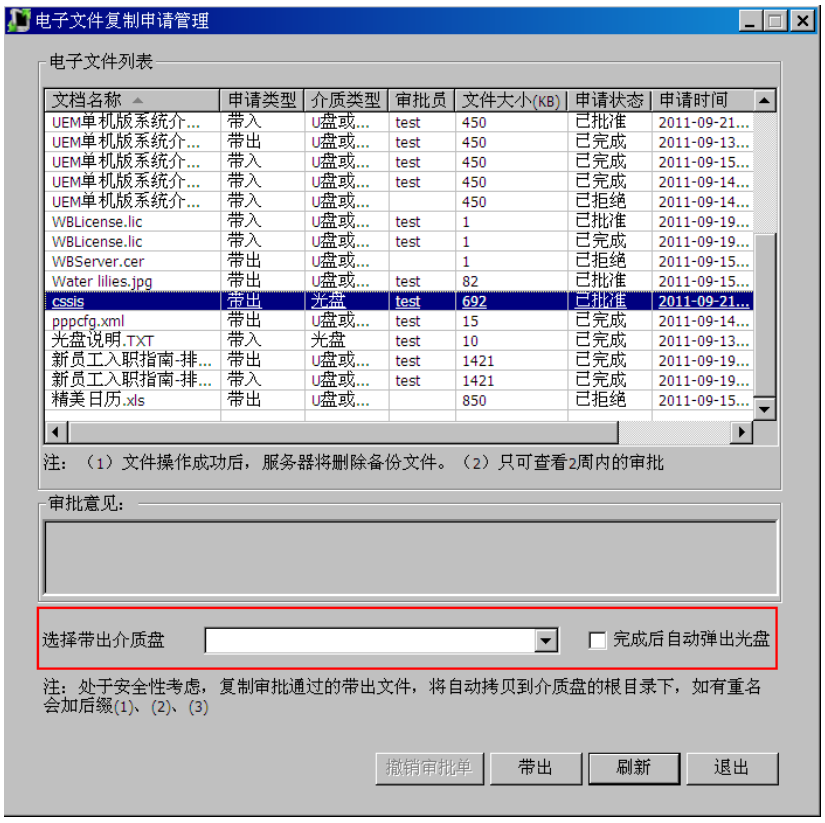


图 12-178　将已批准文件带入

（9）还有一种情况需要说明。如果审批员不同意申请人带出待审批文件，则单击“拒绝”按钮，将其拒绝，如图 12-179 所示。审批员拒绝申请时，一定要写明拒绝理由，以便申请人明白为什么不能带出操作。

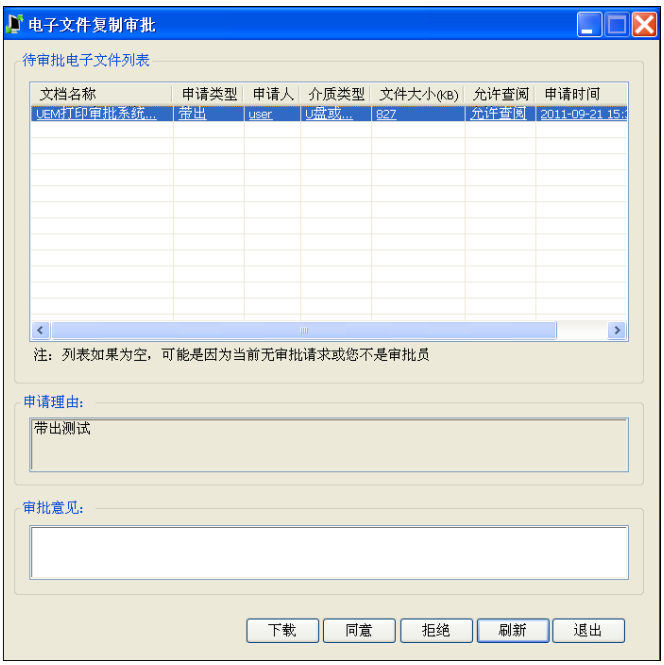


图 12-179　拒绝复制申请

（10）审批被拒绝后，申请人客户端右下方将弹出汽泡式提示信息，如图 12-180 所示。

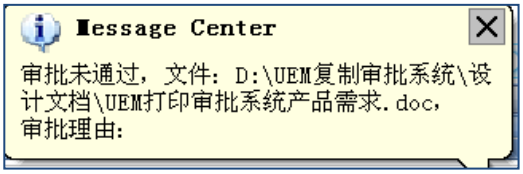


图 12-180　申请被拒绝提示信息

（11）申请人单击客户端右键菜单“审批管理”→“电子文件复制申请管理”，进入申请查看界面，可看到刚刚被审批拒绝的申请单，如图 12-181 所示。用户可查看拒绝理由，修改后再次提出申请。

图 12-181　查看被拒绝的申请单

12.19 可信介质管理

12.19.1 可信磁盘操作

在控制台制作的可信盘，在客户端正常加载后才能使用。如果可信盘在客户端不能自动加载，需要单击客户端图标的右键菜单，选择“可信介质管理→刷新”，在这里进行可信盘的加载、卸载和口令更改，如图 12-182 所示。

图 12-182　可信介质管理

■ **加载可信磁盘**

单击“加载可信磁盘”，如果授权为有口令加载，出现口令输入框，如图 12-183 所示。

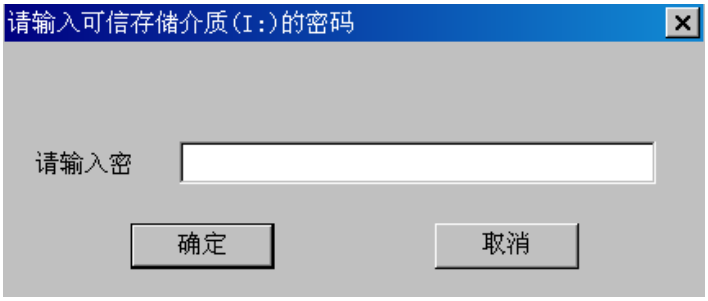


图 12-183　输入可信介质密码

输入密码后，单击“确定”按钮，即将该可信盘加载，如图 12-184 所示。系统也会弹出“成功加载”消息框。

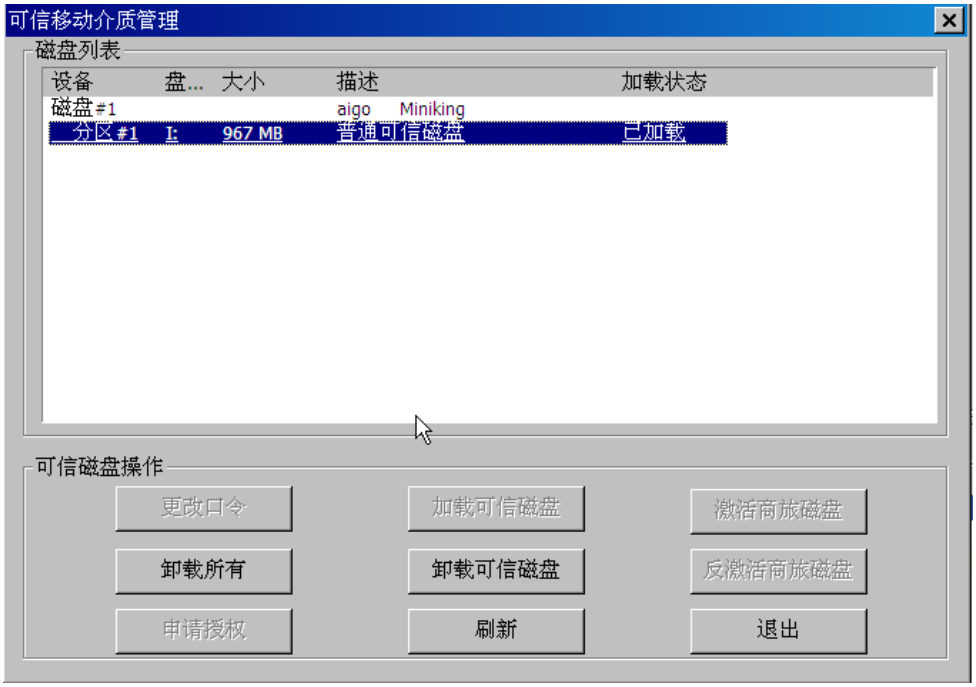


图 12-184　成功加载可信盘

■ **卸载可信磁盘**

可信磁盘在写入数据文件过程中拔出磁盘，可能会导致数据的丢失，所以一定要将可信磁盘正常卸载。

选择要卸载的可信盘，单击“卸载可信磁盘”，出现提示信息后，再单击“是（Y）”，即将该可信磁盘卸载，如图 12-185 所示。

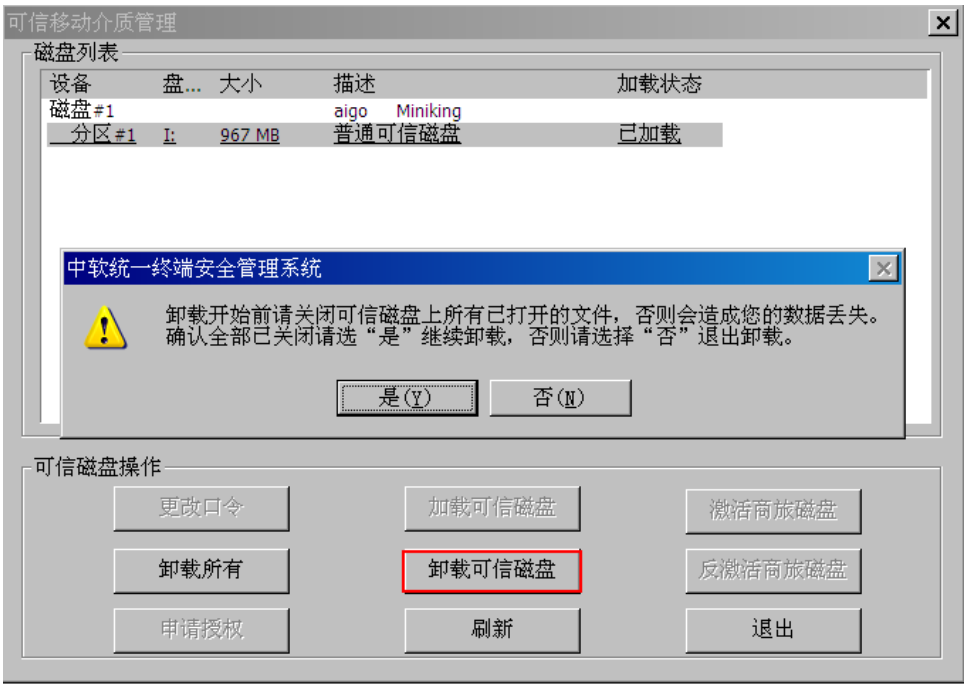


图 12-185　选择要卸载的可信盘

可信盘卸载后，磁盘列表中重新显示该磁盘为未加载，，如图 12-186 所示。同时系统弹出“卸载成功”消息框。

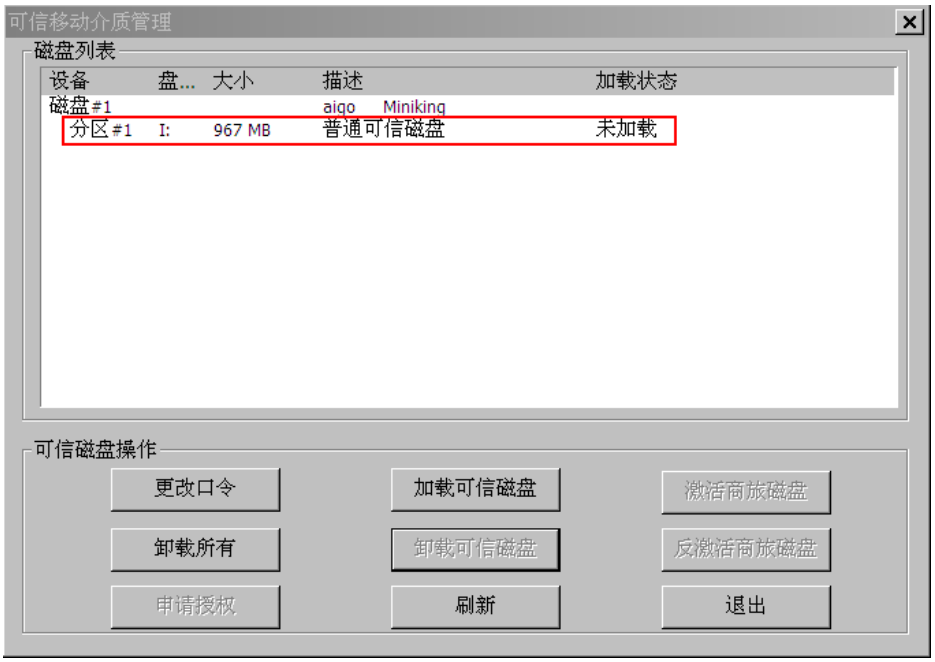


图 12-186　成功卸载可信盘

如果在卸载可信盘时，选择的是基本磁盘，如图 12-187 所示。

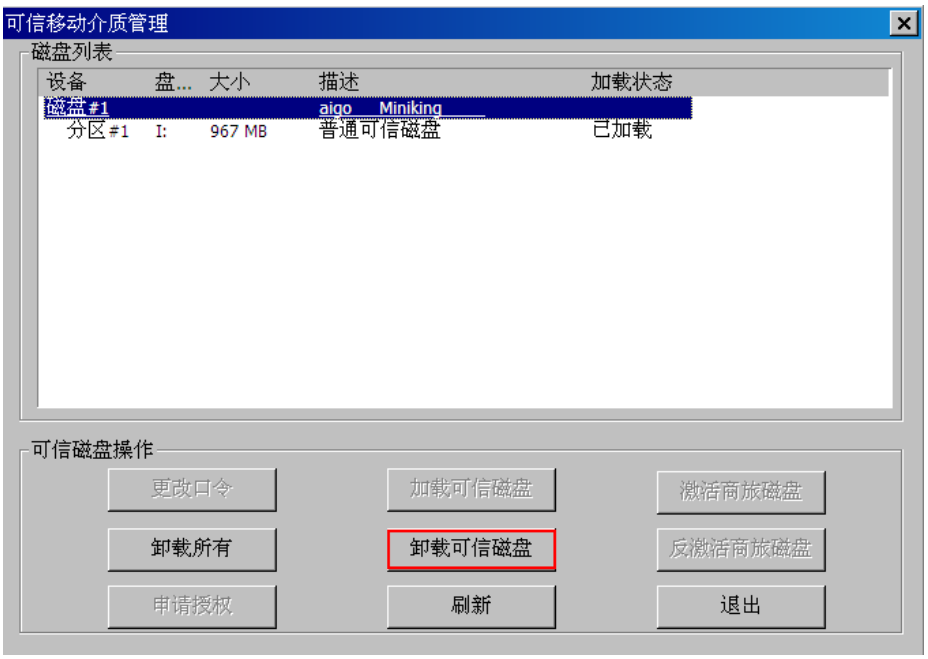


图 12-187　选择基本磁盘卸载

那么执行“卸载可信磁盘”操作后，对于已加载的可信磁盘，执行卸载操作。同时磁盘列表中不再显示该盘信息，相当于拔出移动介质，如图 12-188 所示。

图 12-188　成功卸载基本磁盘

■ **卸载所有**

如果用户同时插入多个可信盘，执行“卸载所有”操作后，会卸载所有盘，并安全地移除硬件，相当于拔出所有移动存储介质。

■ **更改口令**

在可信盘处于未加载状态时，能执行更改口令操作。如图 12-189 所示，选择要更改口令的可信盘，单击“更改口令”按钮。

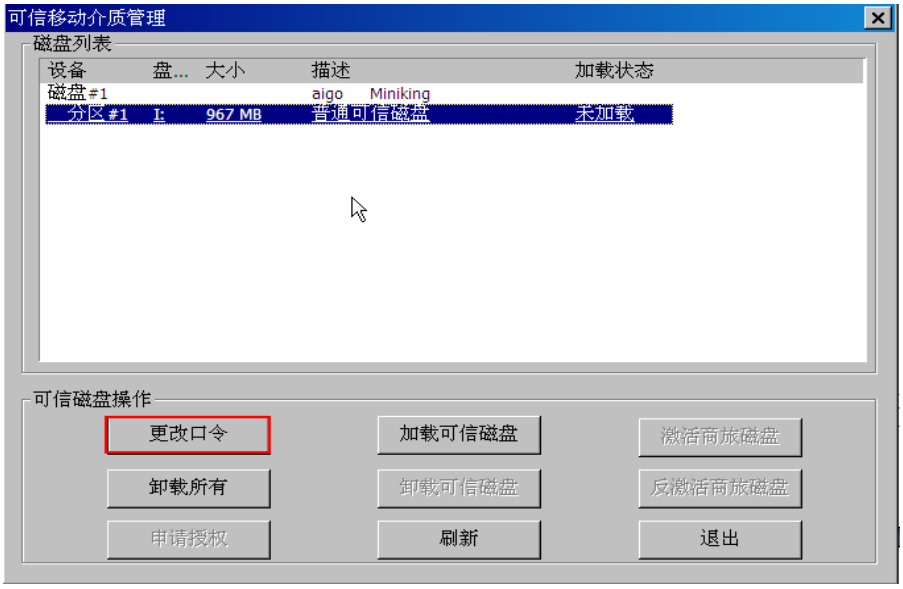


图 12-189　选择要更改口令的可信盘

当系统弹出“更改可信存储介质密码”界面时，输入新、旧密码，单击“确定”按钮。如图 12-190 所示。

图 12-190　更改可信存储介质密码

更改可信盘密码成功后，弹出消息框，如图 12-191 所示。

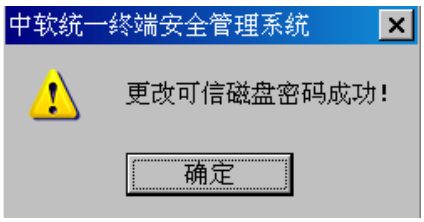


图 12-191　更改密码成功消息框

如果对客户端下发了“允许在本客户端激活/反激活商旅磁盘”策略，那么商旅磁盘插入该客户端，就会出现激活和反激活菜单，在客户端本地就能进行商旅磁盘的激活/反激活操作，不必再拿到控制台进行此操作了。

- **商旅磁盘的激活**

在可信介质管理中，商旅磁盘在未加载状态下能够执行磁盘激活操作，如图 12-192 所示。

图 12-192　可信介质管理—商旅磁盘激活

单击“激活商旅磁盘”按钮，弹出密码输入框，如图 12-193 所示。输入密码后，单击“确定”按钮。激活成功后，会弹出提示框，如图 12-194 所示。

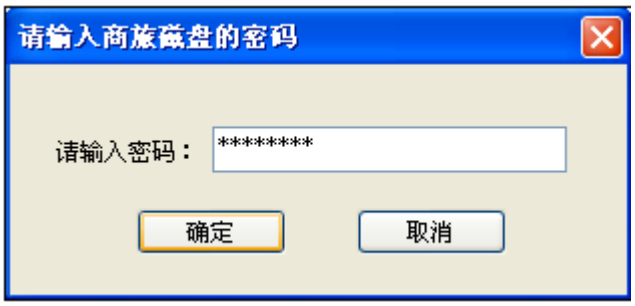


图 12-193　输入商旅磁盘密码

图 12-194　激活成功

注意：激活后的商旅磁盘在安全工作域内将变成只读模式，请确定所需数据已拷贝完全后再执行激活操作。激活后的商旅磁盘在普通终端上加载成功后，可以进行正常的读、写操作。

■ 商旅磁盘的反激活

激活后的商旅磁盘还可以在客户端进行反激活操作。

在可信介质管理中，激活后的商旅磁盘能够执行磁盘反激活操作，如图 12-195 所示。

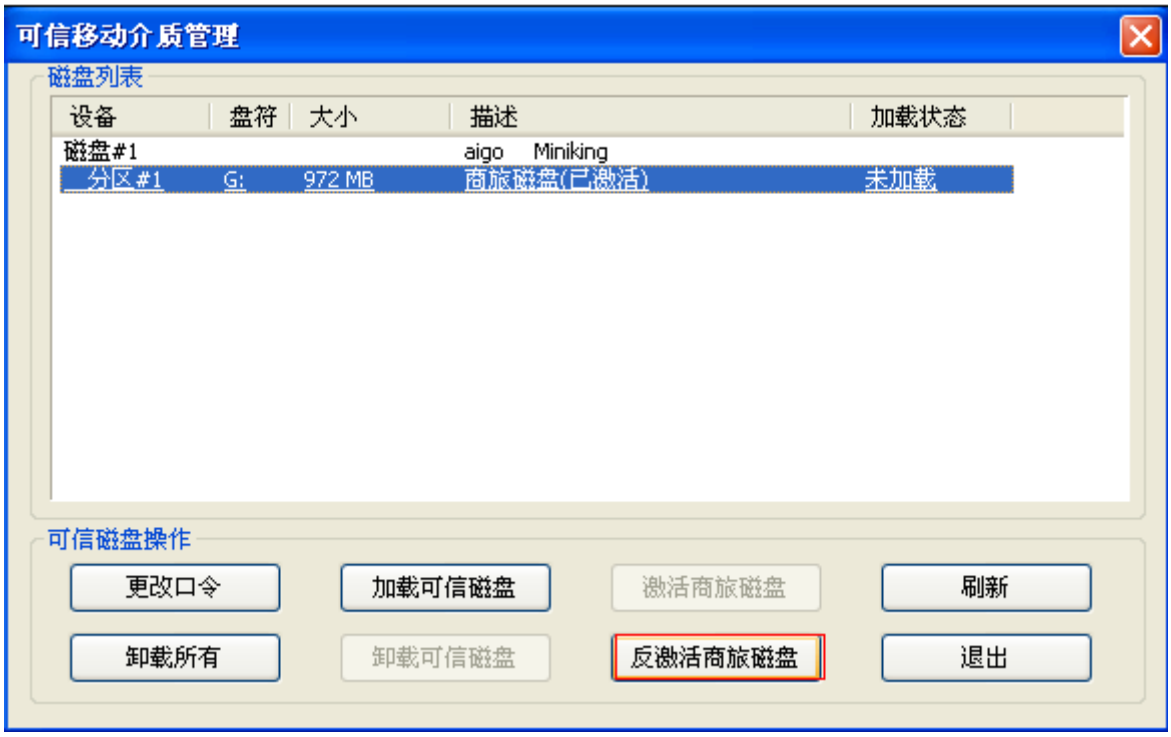


图 12-195　可信介质管理—商旅磁盘反激活

单击“反激活商旅磁盘”按钮，弹出密码输入框，如图 12-196 所示。输入密码后，单击“确定”按钮。反激活成功后，会弹出提示框，如图 12-197 所示。

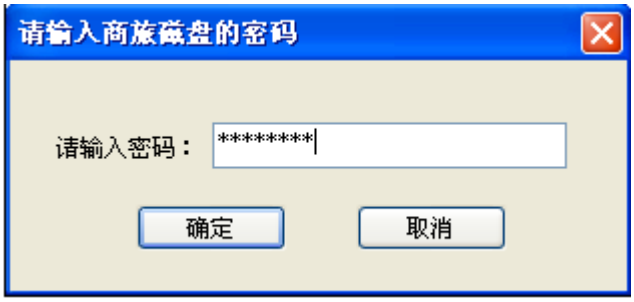


图 12-196　输入商旅磁盘密码

图 12-197　反激活成功

提示：反激活操作是将商旅磁盘恢复到未激活状态。反激活成功后，只能在可信终端上使用，在普通终端上不能使用。

12.19.2 在线审批可信授权

可信授权的在线审批过程需要有一定的审批规则，我们在审批管理中设置规则，指定待审批的组织、审批员、审批内容和优先顺序。参见审批管理章节内容。

（1）申请人将普通移动磁盘插入本机，在可信移动介质管理中，选择磁盘（不是分区），单击“申请授权”，如图 12-198 所示。

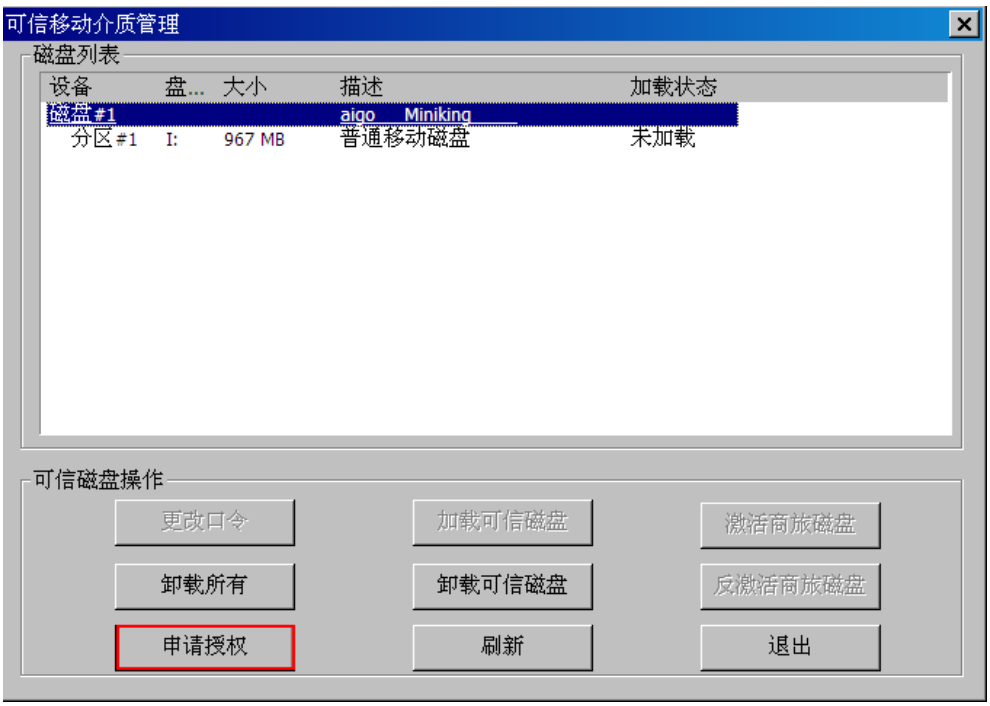
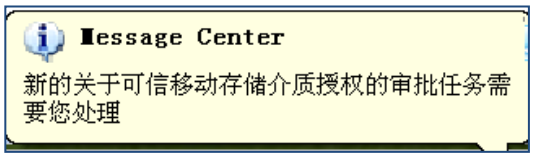


图 12-198　申请授权

（2）输入申请理由，如图 12-199 所示。单击“提交”按钮，确定后，向服务器提交申请单。

12-199　输入申请理由

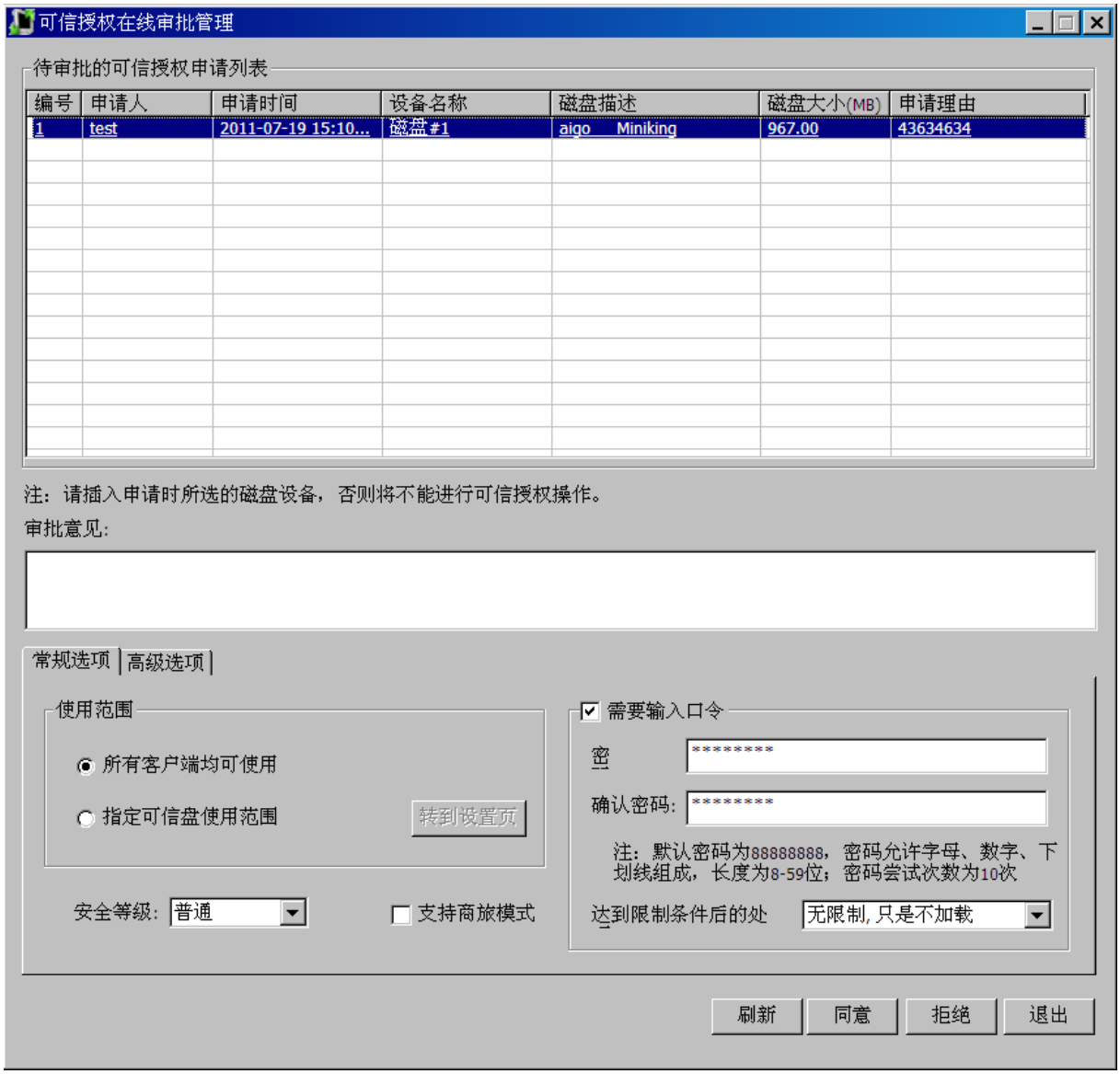
（3）根据审批规则设置，服务器会将申请单派发给指定的审批员，审批员所在的机器上会出现提示信息，如图 12-200 所示。



12-200　提示有审批任务

（4）审批员单击客户端右键菜单“可信介质管理”→“可信介质授权在线审批”，进入审批管理界面，在申请列表中将看到审批任务，如图 12-201 所示。

如果审批员允许申请人制作可信磁盘，会认真选择“常规选项”和“高级选项”，输写审批意见，最后，单击“同意”按钮，确定后，将审批结果上传。



12-201　在线审批管理界面

选项说明：

使用范围：系统默认可信磁盘的使用范围是所有客户端均可使用。如果用户需要指定使用范围，那么就要转到设置页，在高级选项的使用范围中选择组织。组织范围内的人员或计算机都可使用可信磁盘。

安全等级：安全密级提供了四个安全级别，按级别由低到高依次为普通、秘密、机密和绝密。用户可以根据自己需要选择，系统默认为普通级别。

是否商旅模式：可信磁盘分为普通模式和商旅模式。商旅模式可信磁盘用于和外界进行数据交互。未激活时，在可信环境下能读也能写，在普通环境下不能访问，启用跨服务器后才可以跨服务器访问；激活后，在可信环境下只读不能写，在普通环境下能读也能写，启用跨服务器后可以在跨服务器可信环境下只读。

口令设置：系统默认口令为 88888888，用户可以任意更改。如果不选择口令，系统将采用一随机数作为口令，进行数据加密，当磁盘接入可信终端上时，系统会自动加载，方便用户使用。但是，对于支持商旅模式的可信磁盘，必须设定认证口令。没有口令，也不支持跨服务器操作。

达到口令限制的处理方式：默认口令尝试次数为 10 次，当超出口令尝试次数时，系统提供三种处理方式：

无限制，只是不加载：允许用户重新尝试加载该磁盘，不需要拔除设备。

锁定，禁止使用：锁定可信移动存储设备，该设备必须到授权中心解锁后方可再使用。

自动破坏数据，不可恢复：销毁该可信移动存储设备中的数据，用户将无法恢复存储在其中的数据。为安全起见，建议在高密级的设备中使用。

使用条件限制：可信移动存储管理系统提供了两种磁盘使用限制条件：使用次数和使用日期。授权后的可信磁盘每正常加载一次，使用次数将自动减 1。当其变为 0 次后，磁盘的使用将会被控制。

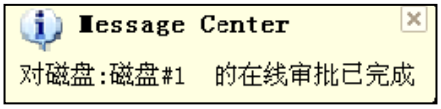
如果系统没有设定时间同步的话，因用户可以自行更改系统的日期，在一定程度上可以绕开使用日期的限制，所以，推荐采用使用次数作为限制条件。

达到使用条件限制的处理方式：以只读方式加载、锁定和自动破坏数据。当以只读方式加载时，用户可以查看磁盘中的内容，但不能再往磁盘中写入任何数据；选择“锁定”，则该磁盘将被禁止使用，必须到授权中心解锁后才能再使用；选择“自动破坏数据”，存储在磁盘中的数据将被破坏，不可恢复。

提示：

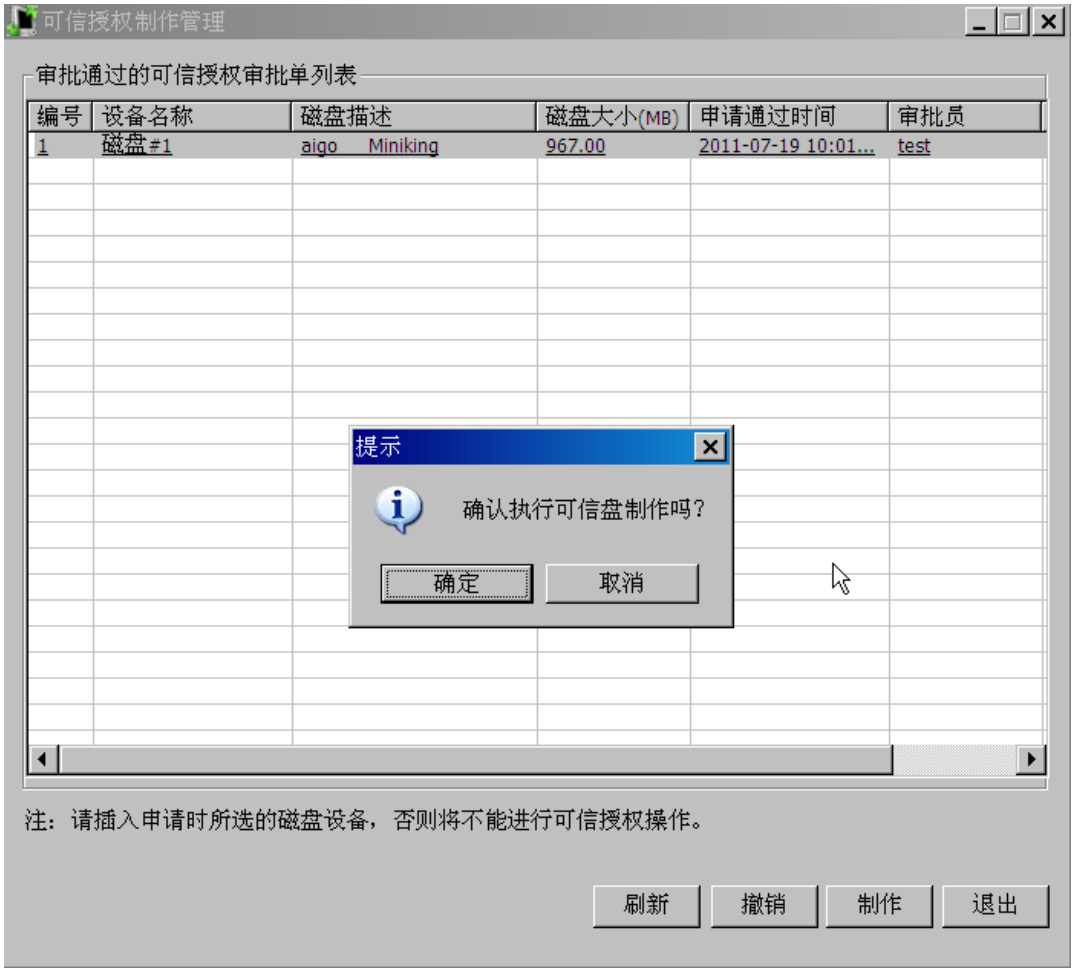
常规选项和高级选项都具有记忆功能，能记录上次用户选择项，做为用户下次使用时的默认值。例如：高级选项中口令的默认值是 88888888，审批员改为 1234567a，如果不退出审批界面，连续做审批，那么口令的默认值是 1234567a。当然，如果审批员退出了审批界面，再次进入做审批时，常规选项和高级选项都会初始化为默认值，口令也变做系统默认口令 88888888，而不是上次设置的 1234567a。

（5）申批通过后，申请人所在的客户端将看到提示信息，如图 12-202 所示。



12-202　在线审批完成

（6）申请人单击客户端右键菜单“可信介质管理”→“可信介质授权制作管理”，进入制作管理界面，如图 12-203 所示。单击“制作”按钮，确定后就执行可信盘制作。

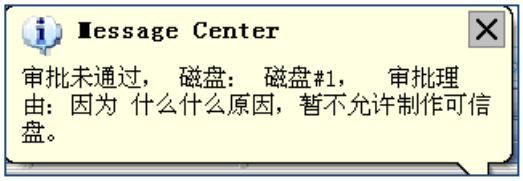


12-203　可信盘的制作

（7）还有一种情况，说明一下。如果审批员不允许申请人制作可信盘，会在审批意见中输写拒绝理由，单击“拒绝”按钮，将审批结果上传，如图 12-204 所示。

12-204　输写拒绝理由

（8）申请人所在的客户端同样能看到提示信息，知道没有审批通过的理由，如图 12-205 所示。



12-205　审批没有通过

12.20　硬盘保护区

硬盘保护区的管理功能主要包括创建、删除、加载、卸载、卸载所有、导入和更改密码，右键单击客户端图标，选择“硬盘保护区”菜单项，将弹出硬盘保护区的管理窗口，如图 12-206、12-207 所示。默认情况下是没有硬盘保护区的，需要用户创建。

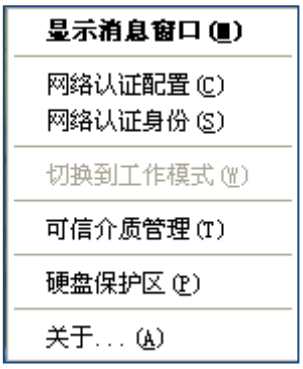


图 12-206　右键菜单硬盘保护区

图 12-207　硬盘保护区管理界面

■ **创建**

单击“创建”按钮，弹出“创建硬盘保护区”对话框，如图 12-208 所示。

图 12-208　创建硬盘保护区

硬盘保护区路径：硬盘保护区文件的完整路径，如：E:\test.wpa。注意：文件后缀必须是“wpa”，否则创建会失败。

保护区名称：名称需要用户输入，当输入的名称已经存在时会有重名提示，原则是同一个手机号下的硬盘保护区不能重名。

保护区大小：硬盘保护区所占磁盘空间的大小，不能大于当前逻辑磁盘的剩余空间。

保护区口令：为硬盘保护区设置的密码，此项比较重要，请用户牢记，长度介于 8～59 位。

保护区密级：当前客户端的机器密级。

责任人：当前登录到客户端的用户。

用户手机号：登录到客户端的用户的手机号码。手机号与当前主机绑定。

正确设置好以上各项后，点击确定开始创建硬盘保护区，创建所需时间根据输入的硬盘保护区的大小不同而不同。成功创建后，在硬盘保护区的管理界面会列出刚刚创建的硬盘保护区，如图 12-209 所示。

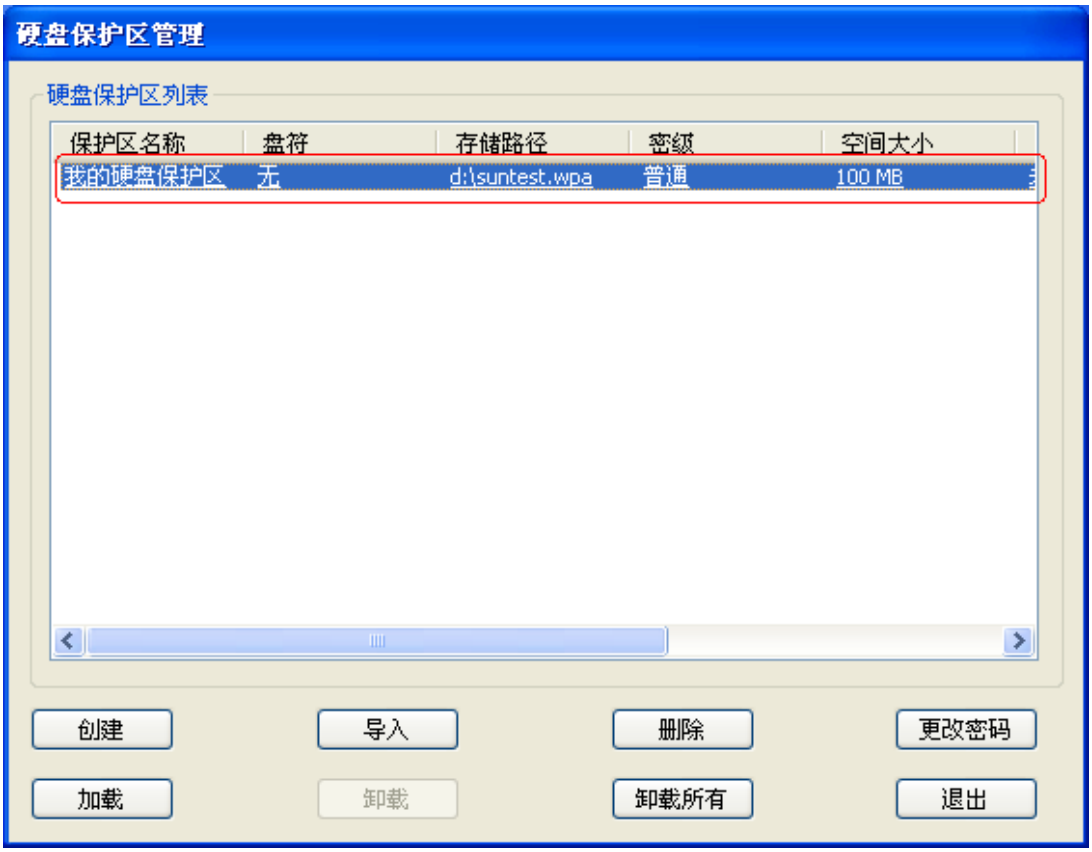


图 12-209　成功创建硬盘保护区

■ **加载**

在“硬盘保护区管理”对话框中，选择需要加载的硬盘保护区，比如上节创建的“我的硬盘保护区”，点击“加载”按钮，弹出密码输入对话框，正确输入创建硬盘保护区时的口令，如图 12-210 所示。

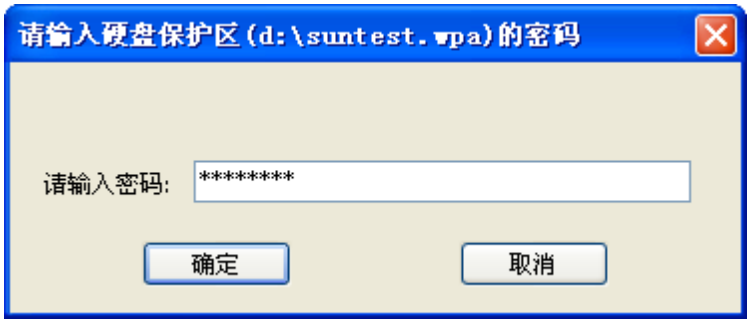


图 12-210　输入硬盘保护区的密码

硬盘保护区加载成功后，出现提示框，单击“确定”后，在“硬盘保护区管理”界面中，“我的硬盘保护区”的“加载状态”由“未加载”变为“加载”，如图 12-211 所示。

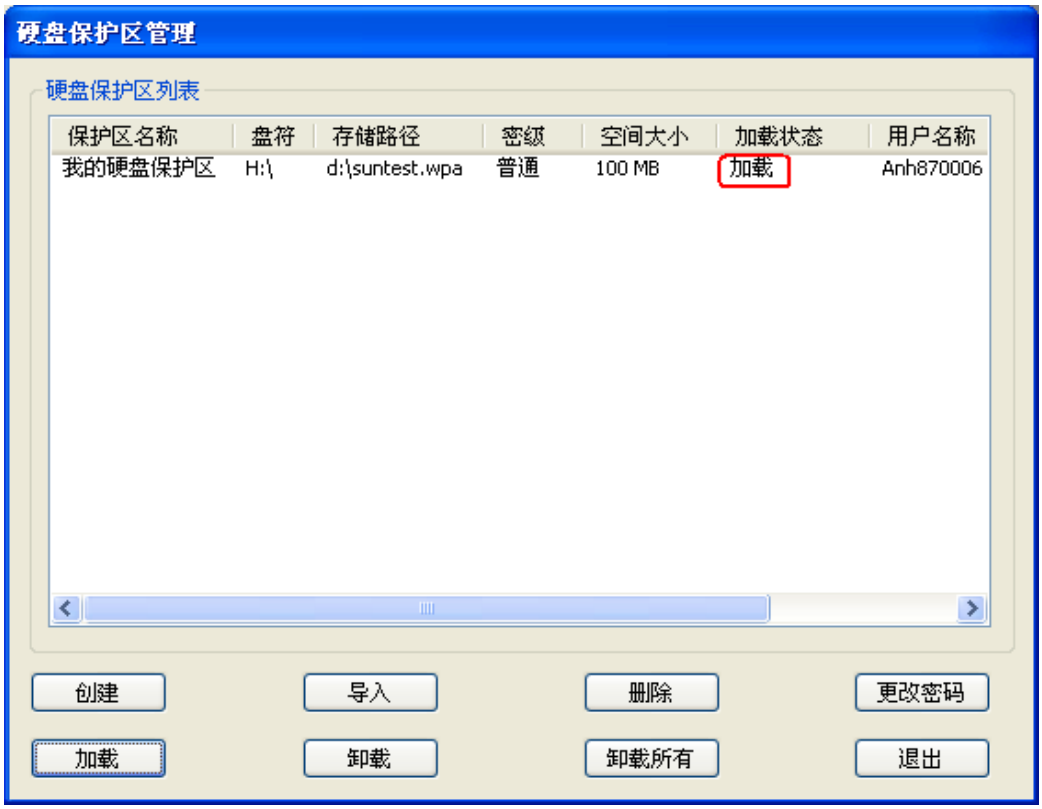


图 12-211　加载成功后的硬盘保护区

打开“资源管理器”或者“我的电脑”，如图 12-212 所示。这时会有个卷标为“可信存储区”的新逻辑分区，这就是加载后的虚拟磁盘，用户对此逻辑磁盘的所有操作都会自动加密。

创建保护区的用户输入口令正常加载该保护区后，看到存贮在本保护区对应的虚拟磁盘上的文件都是明文，拷贝带出也是明文，这种情况下，用户可以像用普通磁盘分区一样在“可信存储区”内正常读写文件；如果没有正常加载，看不到该保护区内的任何内容。对别的用户来说，因为不能加载该保护区，所以也看不到该保护区内的文件。所以，硬盘保护区对创建者来说是开放，可以任意读写，但对别的用户来说是保密，根本看不到，即使看到也是密文。

图 12-212　我的电脑中的硬盘保护区

■ **卸载**

在“硬盘保护区管理”的对话框中，成功加载后的硬盘保护区不再使用，可以手动将其卸载。

单击“卸载”命令，执行卸载操作。当卸载硬盘保护区成功后，出现提示框，单击“确定”后，在“硬盘保护区管理”界面中的“加载状态”由“加载”变为“未加载”。

■ **卸载所有**

当客户端同时有多个硬盘保护区加载时，可以点击“卸载所有”按钮，一次性卸载所有已经成功加载的硬盘保护区，使所有的硬盘保护区恢复到未加载状态。

■ **更改密码**

硬盘保护区未加载时，“更改密码”按钮是激活的，用户可以点击此按钮更改选定的硬盘保护区的密码。

■ **删除**

未加载的硬盘保护区不再使用时，可以点击“删除”按钮将其从磁盘中清除，从而释放占用的磁盘空间，但注意删除后的硬盘保护区不可再恢复。

■ **导入**

如果客户端卸载后，它创建的保护区内的文件将无法使用。这种情况下，我们可以在原来的服务器上，注册一个同名客户端，通过“导入”功能将原来的保护区重新导入进来，然后输入正确口令加载后，就可恢复原来保护区内的文件。具体步骤如下：

（1）在硬盘保护区管理界面中，单击“导入”按钮，弹出添加硬盘保护区界面，如图 12-213 所示。输入硬盘保护区名称，也可以和原来的不一样。单击“浏览”按钮，选择硬盘保护区文件，也可以直接输入保护区文件路径和名称。然后，单击“确认”按钮。

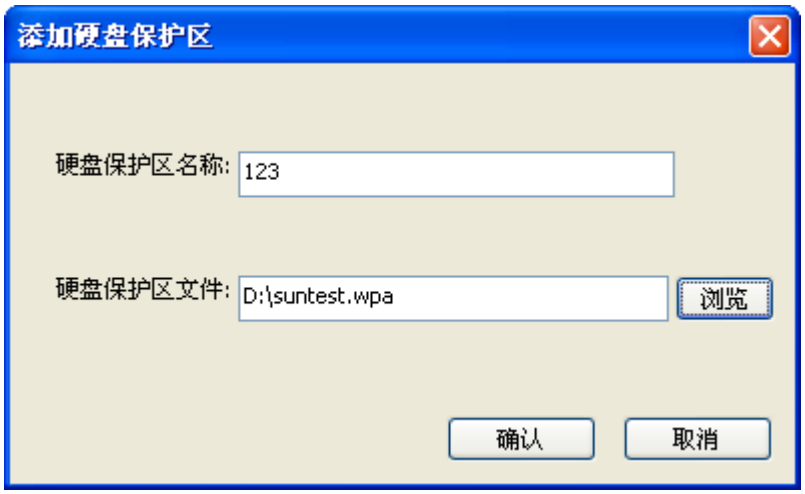


图 12-213　添加硬盘保护区

（2）在保护区密码验证界面中，输入正确密码，单击“确认”后，提示导入成功，如图 12-214 所示。

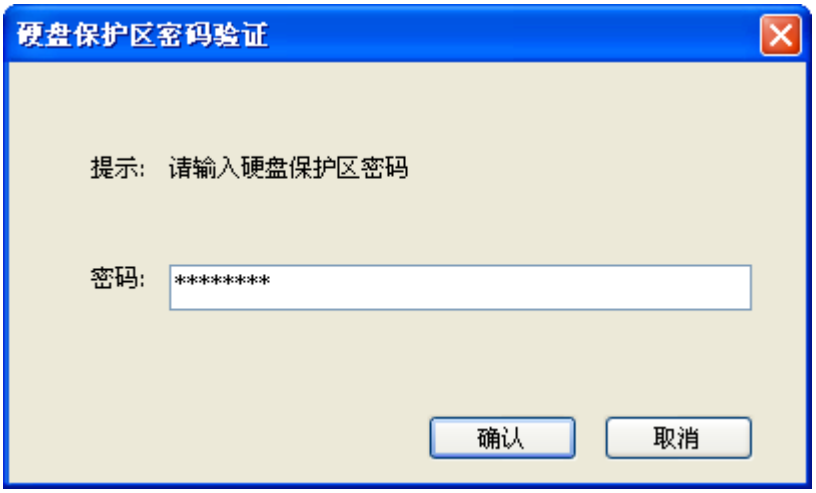


图 12-214　硬盘保护区密码验证

（3）用户可以在硬盘保护区列表中看到新导入的保护区，此时为未加载状态，需要用户正常加载后，才能读取里面存贮的数据，如图 12-215 所示

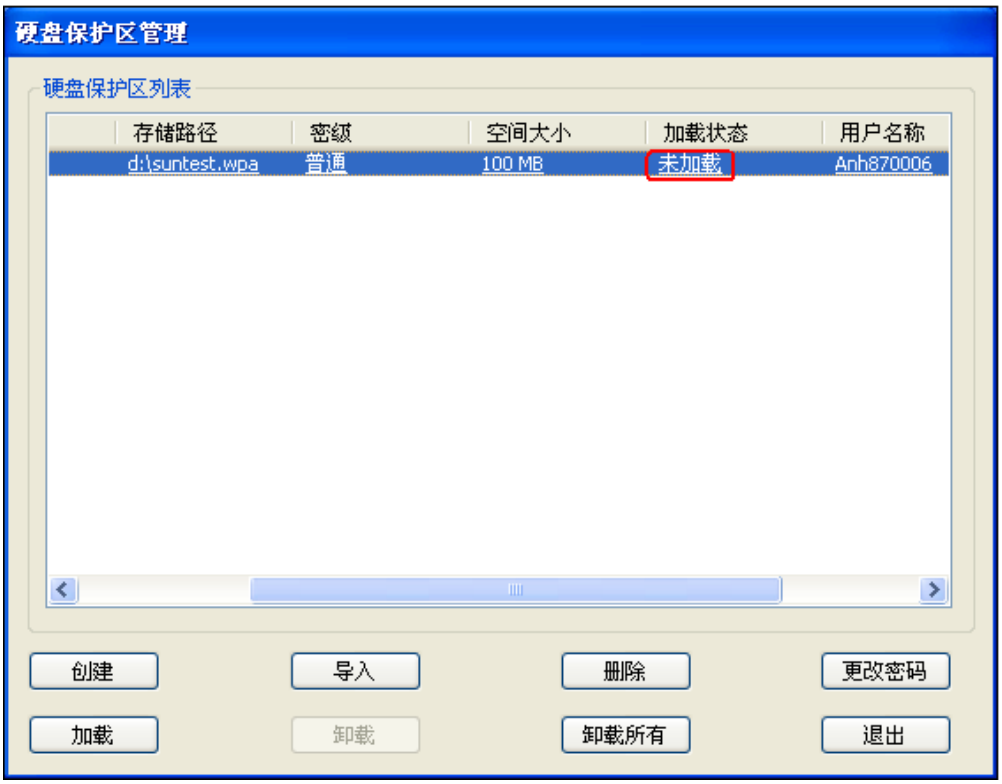


图 12-215　新导入的保护区未加载

注意：导入过程中，如果客户端的用户名和原来不一样，或者用户名一样，注册的服务器不一样，系统都会认为你不是保护区的创建者，禁止导入。因此导入原来的硬盘保护区时，必需是现在客户端用户的注册信息和创建该保护区时的注册信息一样，才能保证导入成功。

12.21　用户注册

如果客户端已经注册，菜单项中没有“用户注册”这一项。如果客户端改为其它 Windows 用户身份登录，菜单项中会出现“用户注册”这一项，需要客户端使用不同的用户重新注册。如图 12-216 所示。

图 12-216　用户注册

注册成功后，即看到同一台机器可以有不同的用户，如图 12-217 所示。正常情况下，每台机器可以带多个客户端。

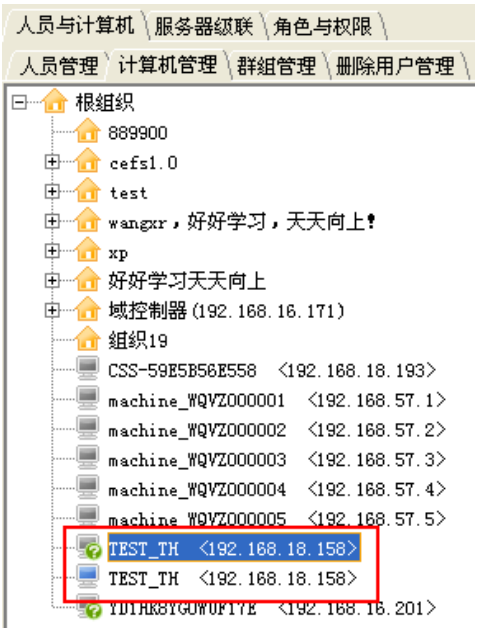


图 12-217　多用户管理

12.22　修改账户密码

12.22.1 UEM 普通用户（非 KEY）

UEM 客户端能在本地修改账户的密码。单击客户端右键菜单“修改账户密码”，进入修改 UEM 账户密码界面，如图 12-218 所示。输入新、旧密码，单击“确定”按钮，客户端将新密码发送至服务器保存。

注意：修改帐户密码功能，只针对于非 KEY 用户。

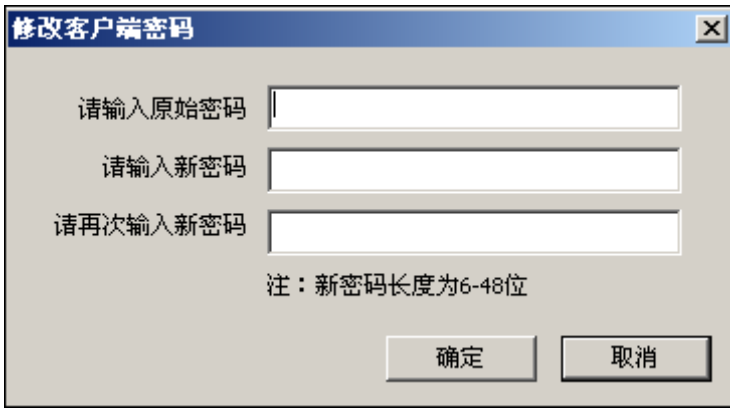


图 12-218　修改账户密码

12.22.2 UEM 客户端（KEY 用户）

如果客户端是 KEY 用户，右键菜单中会有“修改 KEY 设备密码”菜单项。

单击“修改 KEY 设备密码”菜单项，弹出修改 KEY 用户密码界面，如图 12-219 所示。输入新、旧密码，单击“确定”按钮，即可更改 KEY 用户密码。

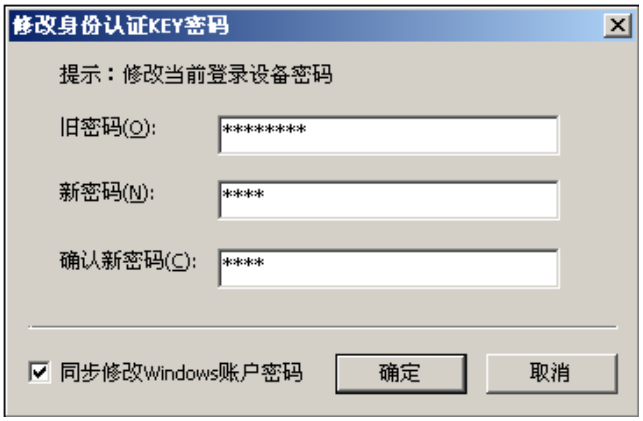


图 12-219　修改 KEY 用户密码

若选择“同步修改 Windows 账户密码”，将使用输入的 KEY 的密码作为 Windows 用户密码。在修改 Windows 用户密码时，系统首先采用与 KEY 口令相同的原密码和新密码。当原密码不正确时，自动获取 KEY 绑定信息的用户密码（有绑定的情况下）；如果绑定信息密码也不正确，弹出对话框供用户输入原始密码，如图 12-220 所示。完成密码修改后，更新 KEY 的绑定信息。

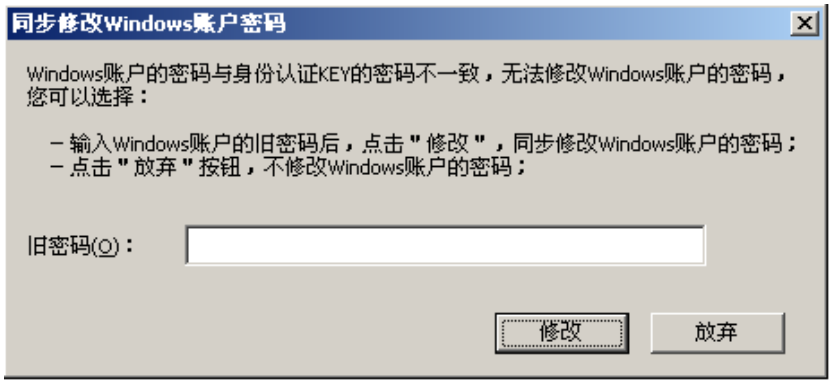


图 12-220　同步修改 Windows 账户密码

12.23　检查更新

单击客户端右键菜单“检查更新”，如图 12-221 所示。客户端会自动从服务器获取升级包版本号信息，并与自己当前的版本号做比较，以确定是否需要升级。

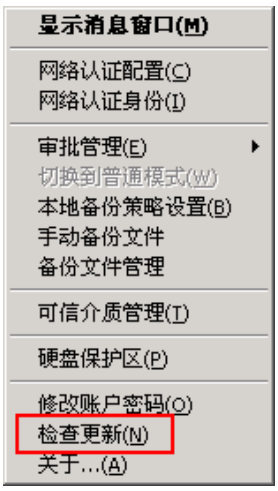


图 12-221　检查更新菜单项

如果服务器上没有比客户端当前版本高的升级包，弹出信息如图 12-222 所示。

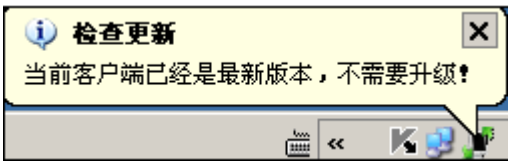


图 12-222　客户端不需要升级提示

如果服务器有高版本的升级包，则会询问用户是否升级客户端，如图 12-223 所示。用户点击“是”按钮，开始下载升级包，并更新客户端。否则，不对客户端进行升级。

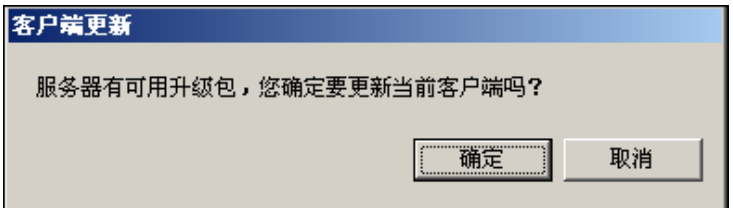


图 12-223　客户端是否更新提示

12.24　关于

该系统客户端支持服务器 IP 地址更改和服务器迁移。如果服务器 IP 地址更改了，客户端不需重新安装，通过“关于”菜单项的“修改 IP”功能，实现客户端和服务器的正常通讯；如果同一个单位有多个服务器，客户端需要从一台的服务器转移到另外一台服务器，可通过“关于”菜单项的“迁移服务器”实现，也不需要重新安装。

1．右键单击客户端图标，选择“关于”菜单项，弹出关于界面，可以看到内部版本号、登陆用户、用户密级、当前状态、系统用户、服务器 IP、安全级别、公司主页、版权所有等信息，如图 12-224 所示。在使用过程中遇到什么问题，请向厂家说明内部版本号，以便问题的快速解决。

图 12-224　客户端关于界面

2．单击“配置”按钮，进入“服务器配置管理”界面，如图 12-225 所示。

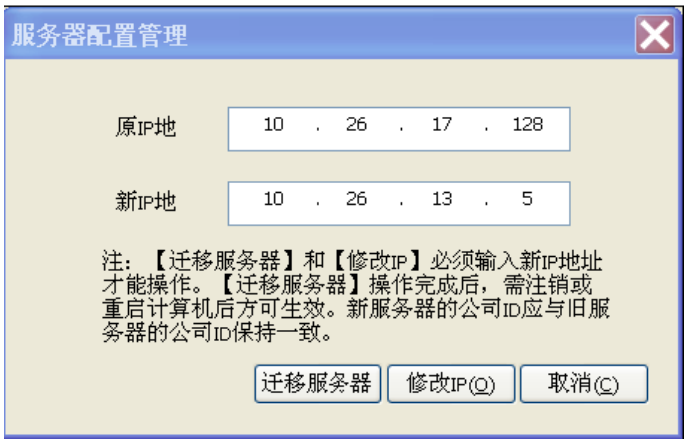


图 12-225　修改服务器 IP 地址

3．输入服务器新的 IP 地址，单击“修改 IP”按钮，可实现服务器 IP 地址更改后和客户端的正常通讯。

修改成功后，出现提示框，如图 12-226 所示。客户端需重新启动（有的不需要重启），在控制台原来的组织结构中可以看到它在线，这样服务器和客户端就能够正常通信了。

图 12-226　修改 IP 地址成功

注意：服务器端修改IP地址后，请重启UEM服务，或重启计算机，这样才能保证服务器正常运行。否则，控制台登录不上，客户端重启后也不能与服务器正常通信。

4．如果在服务器配置管理界面，输入新服务器的IP地址，单击“迁移服务器”按钮，可将客户端迁移到新的服务器。

迁移成功后，出现提示框，如图 12-227 所示。客户端注销或重启后，在新服务器的控制台组织结构中可以看到它在线，这样表示客户端迁移成功。

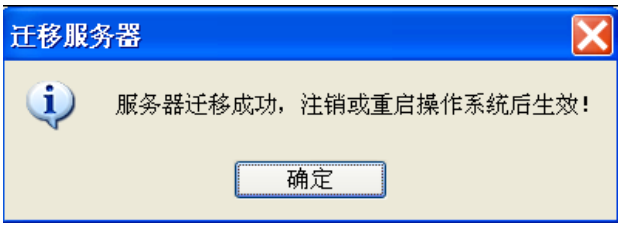


图12-227　客户端迁移到新服务器

注意：

1．迁移服务器时，要保证客户端和新服务器能够正常通讯，新服务器的公司ID和原来服务器的公司ID应一致。否则，迁移失败。（服务器的公司ID可通过控制台的“帮助”菜单，查看服务器授权信息的“用户编号”是否一致。）

2．如果新服务器的注册模式是验证模式，需要在控制台添加要迁移的客户端用户，用户名、密码必须和客户端原来的用户名、密码一致，否则，迁移失败，弹出错误信息。

如果新服务器的注册模式是自由注册，迁移服务器时，会自动按原客户端用户名和密码进行注册；如果新服务器上已有此客户端用户名，请保证密码和原客户端用户一致，否则，注销或重启客户端计算机后，需输入用户名和密码进行注册。

第十三章　审计系统操作指南

中软统一终端安全管理系统运行过程中，客户端大量的日志或文件监控记录上传到服务器，服务器数据库中的记录越来越多，我们利用“备份与恢复”工具将数据备份起来,然后根据备份的数据库和相关的文件搭建审计系统，实现“数据库内容审计”和“文件内容审计”相关联的审计功能，从而极大地提高了系统的审计能力。

审计系统是系统的一个组件，相对独立于现运行的中软统一终端安全管理系统，可以进行事后离线审计，对系统所产生的信息进行事后审计。

注意：审计系统不能和服务器同装在一台机器上，并且不能共用一个 SQLServer 数据库。

步骤 1　双击桌面上“离线审计”图标，如图 13-1 所示。或依次单击“开始→程序→CSS→审计系统”，启动审计系统。

图 13-1　离线审计图标

步骤 2　使用审计系统前，首先要从服务器端导出数据，然后，在这里单击“导入数据”按钮，将备份的数据导入进来，如图 13-2 所示。

图 13-2　单击“导入数据”按钮

步骤 3　选择要导入的备份文件（*.idx），输入文件密码，单击“确定”按钮，如图 13-3 所示。

提示：　导入数据时，也要按照压缩文件大小与实际的文件大小的大致比例，估算一下导入文件时数据库与日志文件所需要的空间，以免导入失败。如果数据库文件大小为 30M，导入后为 1G。如果压缩日志文件大小为 1G，导入后为 1G～2G。

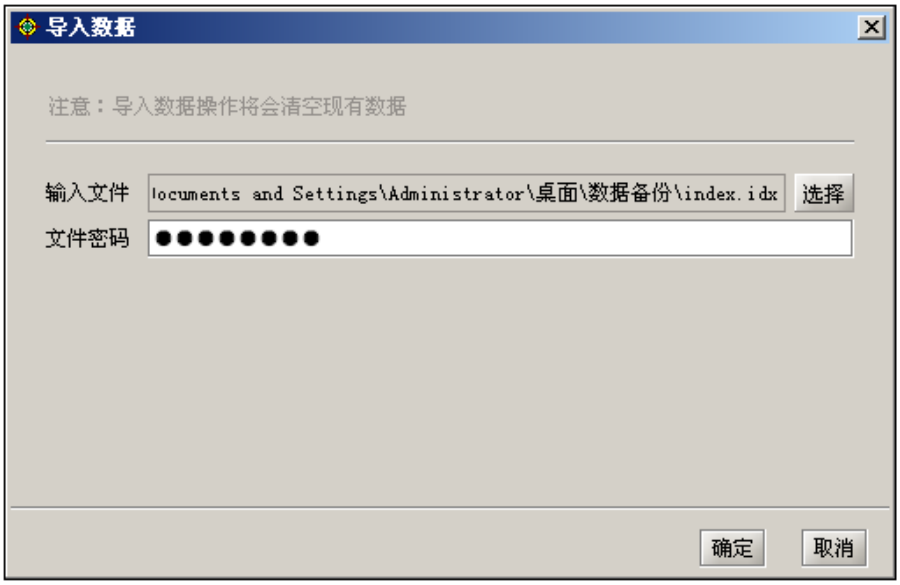


图 13-3　导入文件和密码

步骤 4　当弹出如图 13-4 所示的确认框时，单击“确定”按钮，开始导入过程。如果文件很大，导入时间可能会比较慢长，请耐心等待。

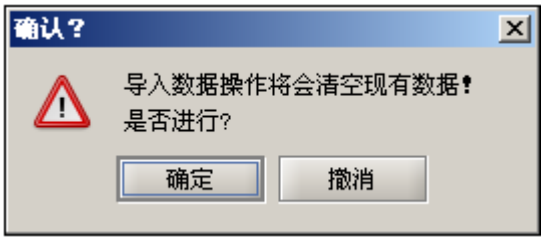


图 13-4　导入文件确认框

步骤 5　导入完成后，会有数据导入报告，请用户查看，如图 13-5 所示。单击“关闭”退出。

图 13-5　导入文件

步骤 6　导入数据完成后，返回审计系统登录界面。输入控制台有审计权限的用户名和密码，如图 13-6 所示。单击“确定”按钮，进入审计系统。

图 13-6　审计系统登录界面

步骤 7　进入审计系统后，就可以进行各项审计，如图 13-7 所示。使用方法详见第八章“统计审计分析”，这里不再赘述了。

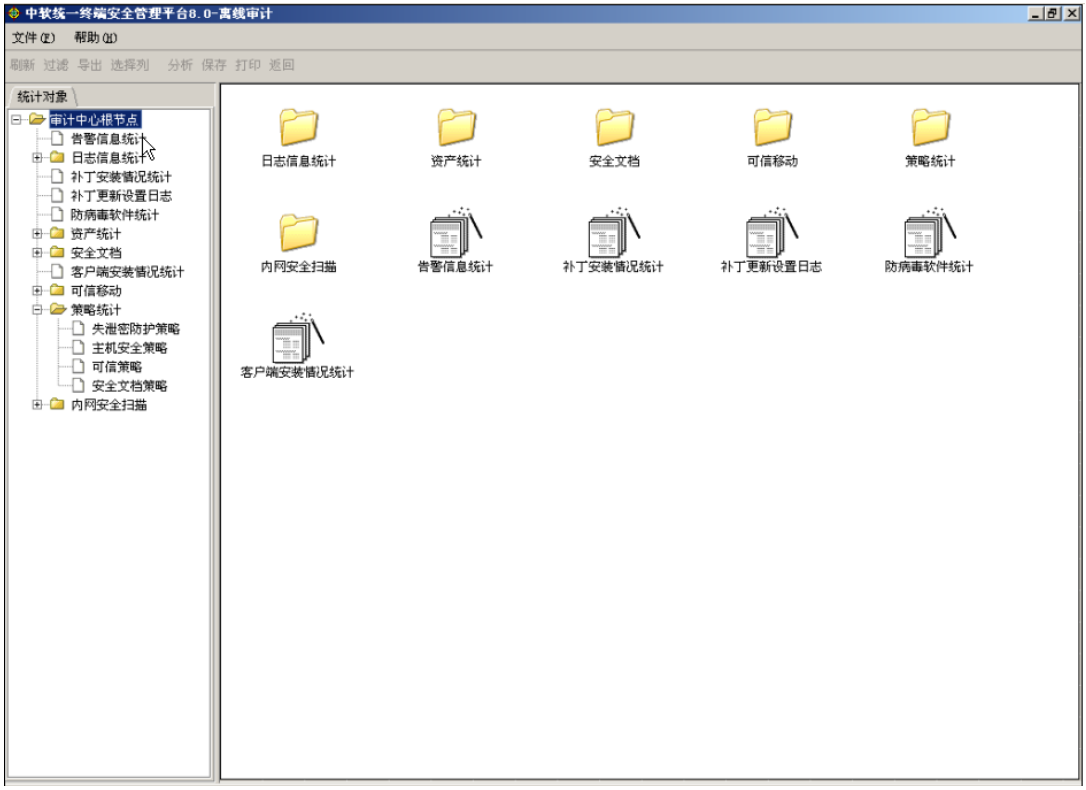


图 13-7　离线审计的操作

第十四章　技术支持

如果用户在安装和使用中软统一终端安全管理系统时，遇到了问题请及时告诉我们，我们将尽全力与您一起解决问题，最大限度地保护您的权益。

地址：北京市海淀区学院南路 55 号中软大厦 B 座一层
电话：010-51527766
Email: Waterbox@css.com.cn
World Wide Web: http://www.cssis.com.cn/list.asp?id=677

假如您利用网络和我们联系，请在问题报告中包含安全管理系统的版本信息、许可证信息、主机使用系统名称和尽可能详细的问题描述，以便于我们能尽快解决您的问题。

中国软件与技术服务股份有限公司为用户提供热情周到的服务，为您解决难题，提供技术支持。保护用户网络系统的安全是我们最大的心愿。

附件一：

UEM 系统双机热备份
操作手册

中国软件与技术服务股份有限公司

2008 年 11 月 16 日

目　　录

第一章　SQL Server 安装

SQL Server 2000 和 SQL2005 只需安装一个。

1.1 SQL Server 安装

一台服务器上，只能安装一个 SQL Server 默认实例，在群集中安装 SQL Server 也有此限制。本示例需要提供一个 SQL Server 默认实例，

1.2 安装 SQL Server2005 默认实例

SQL Server 安装可以在任何一个群集中的结点上进行安装。示例中选择“cluster01”来安装 SQL Server。

1.2.1 安装 SQL Server 之前的准备工作

在确保群集的工作正常的情况下，安装 SQL Server 2000 之前，我们需要先配置好 MSDTC（Microsoft 分布式事务处理协调器 ）群集资源。

注:如果只安装数据库引擎,则 MSDTC 群集资源不是必需的。如果安装数据库引擎、SSIS、Notification Services 或工作站组件，则必须安装 MSDTC。 此要求适用于 Windows 2000 和 Windows Server 2003 操作系统。

MSDTC 的安装只需要在群集中的任何一个联机的结点上进行。在任何一个联机的群集结点中打开添加/删除程序（开始—控制面板—添加或删除程序），在随后出现的“添加或删除程序”对话框中，单击左侧的“添加/删除 windows 组件”。在随后出现的“windows 组件向导”对话框中，找到并双击“应用程序服务器”项，如图 1 所示。在随后弹出的”应用程序服务器”对话框中，勾选“启用网路 DTC 访问”项，如图 2 所示。单击“确定”按钮回到“windows 组件向导”对话框，然后单击“下一步”进行 MSDTC 的安装。

图 1　应用程序服务器

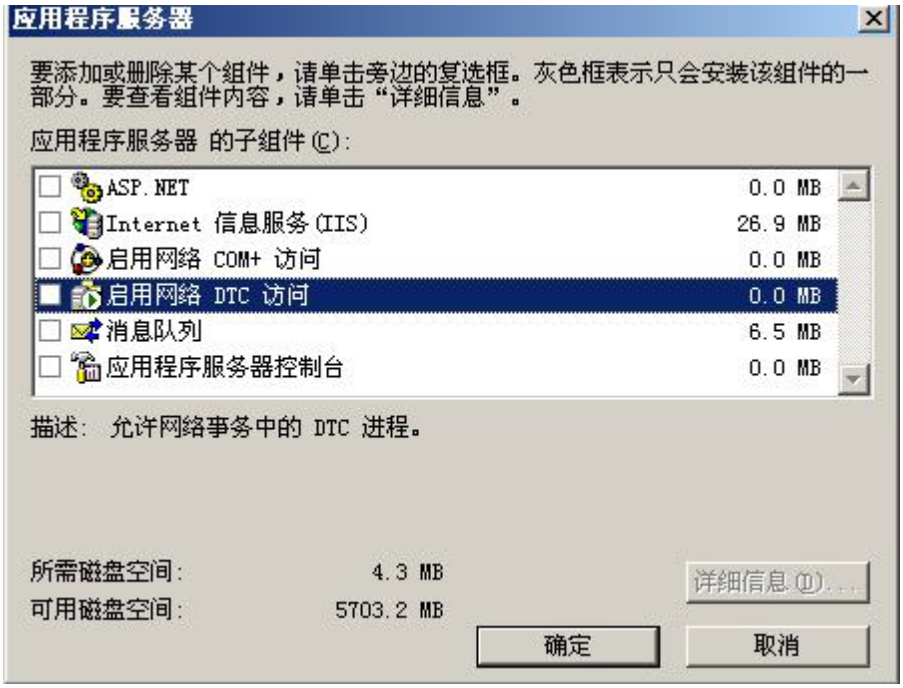


图 2　启用网络 DTC 访问

在群集中创建分布式事务协调器 DTC

1. 右键选择“资源”，选择“新建”“资源”，在名称中输入“uemdtc”，资源类型选择“分布式事务协调器（DTC）”，如图 3 所示。

图 3　新建资源

2. 在“可能的所有者”中确认“cluster01”和“cluster02”都在“可能的所有者”中，点击“下一步”，如图 4 所示。

图 4　可能的所有者

3. 在“依存”中“依存资源”选择“群集名”和“磁盘 S”，点击“完成”，如图 5 所示。

图 5　资源依存

4. 当“群集管理器”提示“成功建立了群集资源'uemdtc'”后，点击“确定”，如图 6 所示。

图 6　成功创建确认框

1.2.2 安装 SQL Server 2005

SQL Server 的安装只需要在群集中的任何一个联机的结点上进行。

1. 运行 SQL Server 安装程序，在“Start”页面中单击“Install”－“Server components, tools, Books Online, and samples”，如图 7 所示。

图 7　SQL Server 安装“Start”页面

2. 在随后出现的“Microsoft SQL Server 2005 Setup”对话框中，接受许可协议并单击“Next”按钮，如图 8 所示。接下来提示需要预先安装一些组件，单击“Install”按钮进行安装。

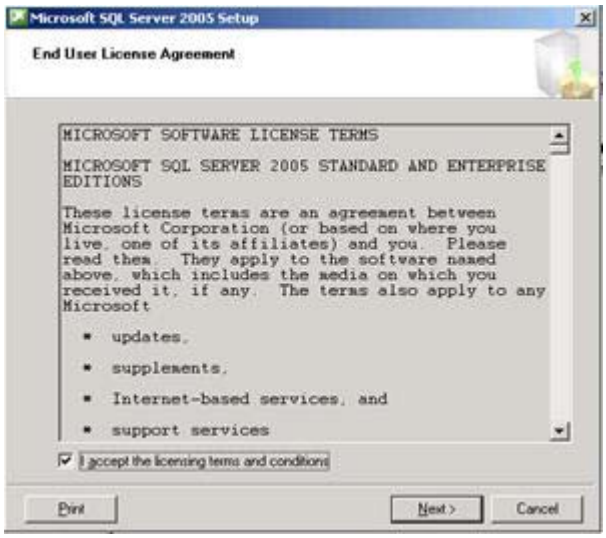


图 8　SQL Server 2005 Setup 对话框

3. 安装完成后，单击“Next”按钮，此时会初始化 SQL Server 的正式程序，如图 9 所示。待初始化完成后，会重新弹出“Microsoft SQL Server 2005 Setup”对话框，在该对话框中单击“Next”按钮。

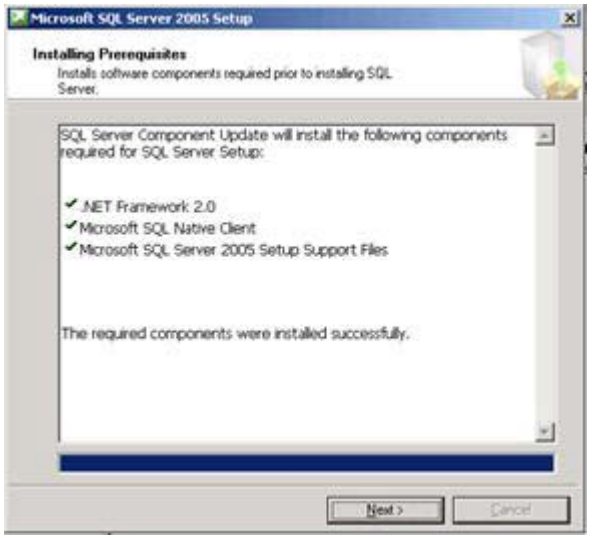


图 9　SQL Server 安装对话框

4．接下来安装程序会对群集中的每个结点做检查，确认检查结果没有问题后，单击“Next”按钮。在接下来的步骤中输入一些基本信息，然后单击“Next”按钮，如图 10 所示。

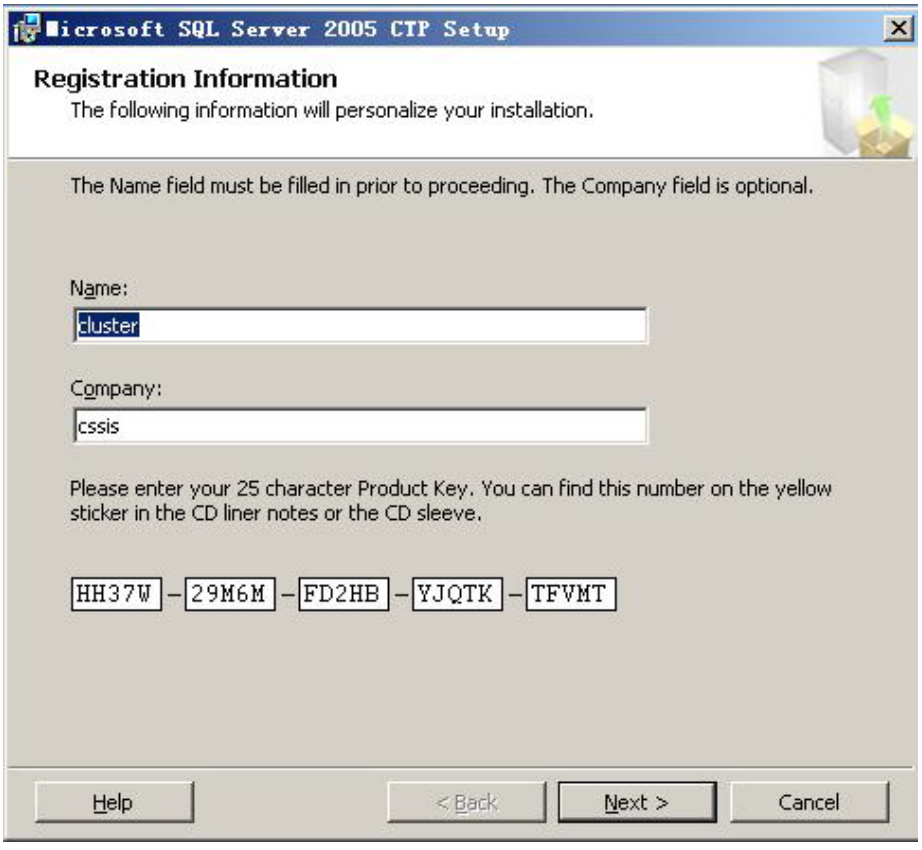


图 10　输入注册信息

5．接下来，选择要安装的 SQL Server 组件，在本示例中，选择“SQL Server Database Services”，由于是安装 SQL Server 群集，因此，勾选“Create a SQL Server failover cluster”，

选择“Analysis Service”同时勾选“Create an Analysis Server failover cluster”，勾选“Notification Service”“Integration Service”“workstation components， books online and development tools”然后单击“Next”按钮，如图 11 所示。在接下来的步骤中，选择“Default instance”， 然后单击“Next”按钮，如图 12 所示。

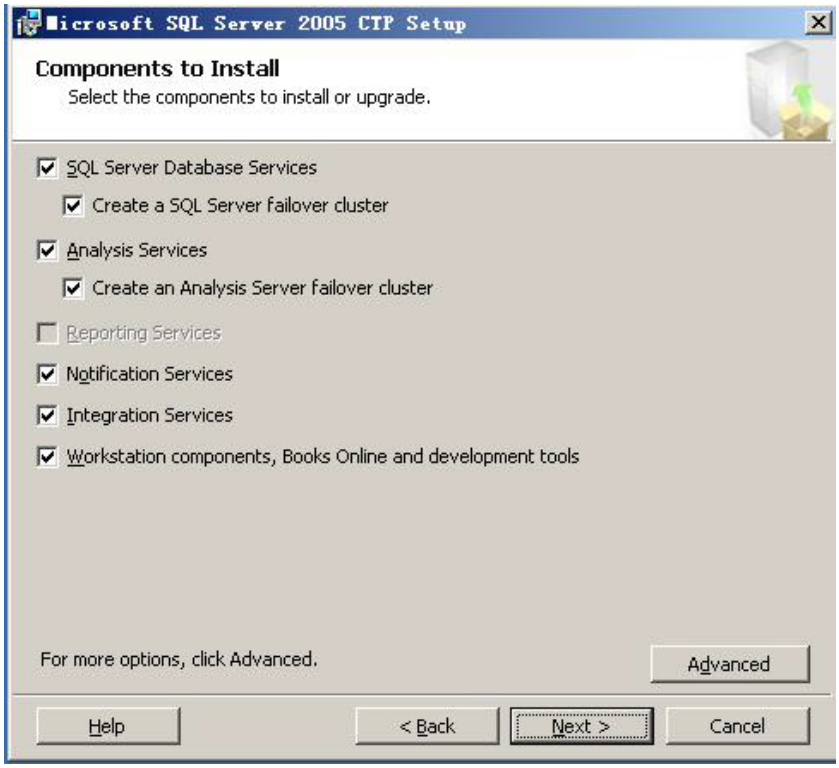


图 11　选择要安装的 SQL Server 组件

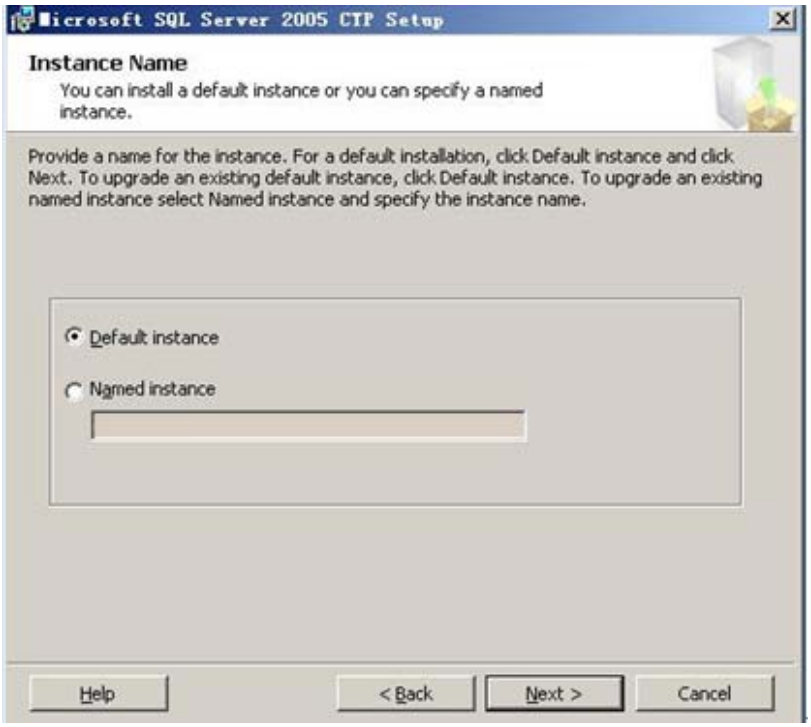


图 12　输入选项名称

6. 在接下来的步骤中，“Virtual server name”输入“uemsql”， 单击“Next”按钮。接下来的步骤设置“Virtual server”的 IP 地址，由于只提供对外服务，故“Network to user”选择“Public”，然后在“IP address”中输入“192.168.16.233”，然后单击“Add”按钮，完成后单击“Next”按钮，如图 13 所示。客户端访问 SQL Server 需要指定的服务器（名称和 IP）即这两个步骤中设置的“Virtual server name”和“Virtual server IP”。

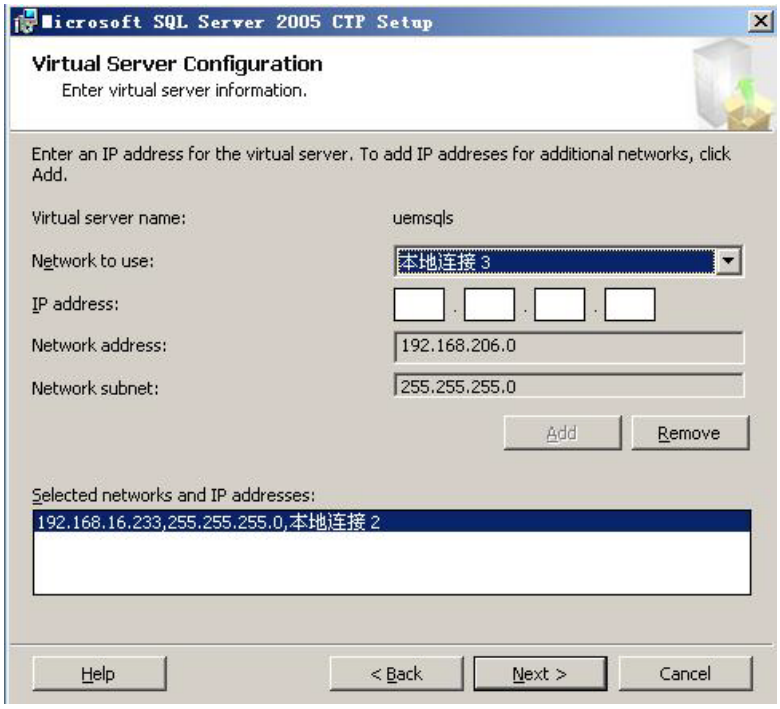


图 13　输入配置选项

7. 在接下来的步骤中，选择 SQL Server 要安装的群集 Group，选择“uemsql”，“Data file”会自动选择该组的共享数据盘，因为这个组只有一个共享数据盘，所以保持默认值，完成后单击“Next”按钮。接下来设置 SQL Server 群集涉及的节点，选择所有可用的结点（默认值），然后单击“Next”按钮，如图 14 所示。

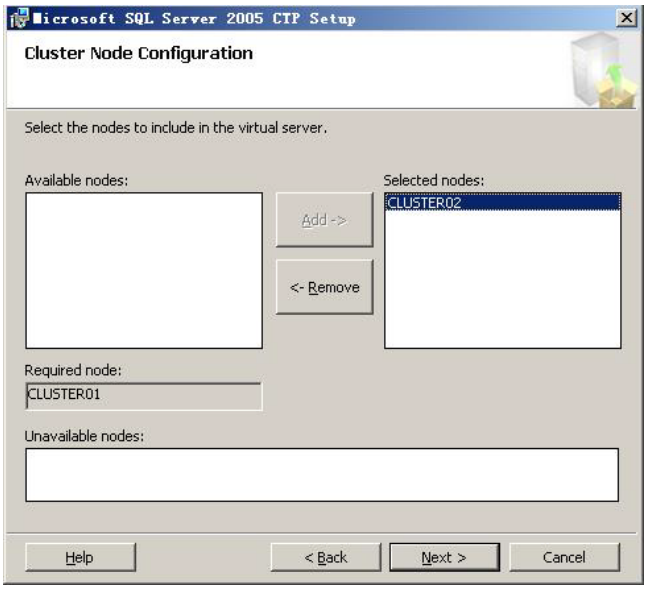


图 14　配置群集节点

8．接下来的步骤中，输入正确的群集服务用户密码，然后单击“Next”按钮，如图 15 所示。在接下来的步骤中，为要安装的 SQL Server 服务设置服务启动用户，这个要求是正确的域用户，设置为与群集服务相同的 ClusterService，完成后单击“Next”按钮，如图 16 所示。

图 15　群集服务用户密码

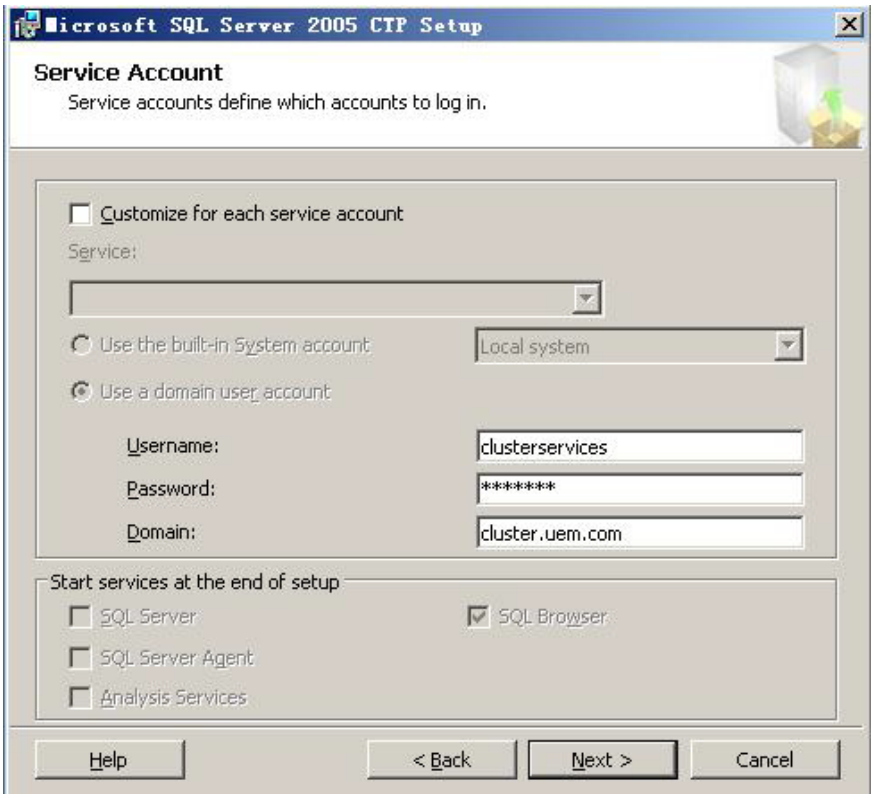


图 16　设置域用户

9．接下来的步骤设置群集服务的域组，将它设置为“CLUSTER\Domain Users”，然后单击“Next”按钮，如图 17 所示。接下来的步骤设置 SQL Server 的身份验证模式，选择混合验证方式，输入密码，然后单击“Next”按钮，如图 18 所示。

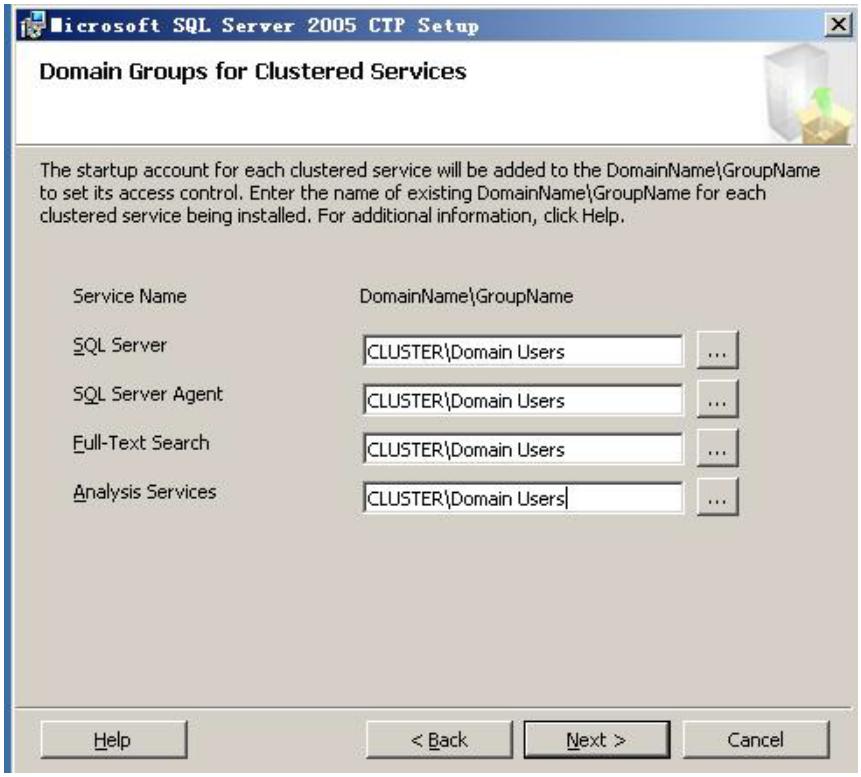


图 17　设置群集服务域组

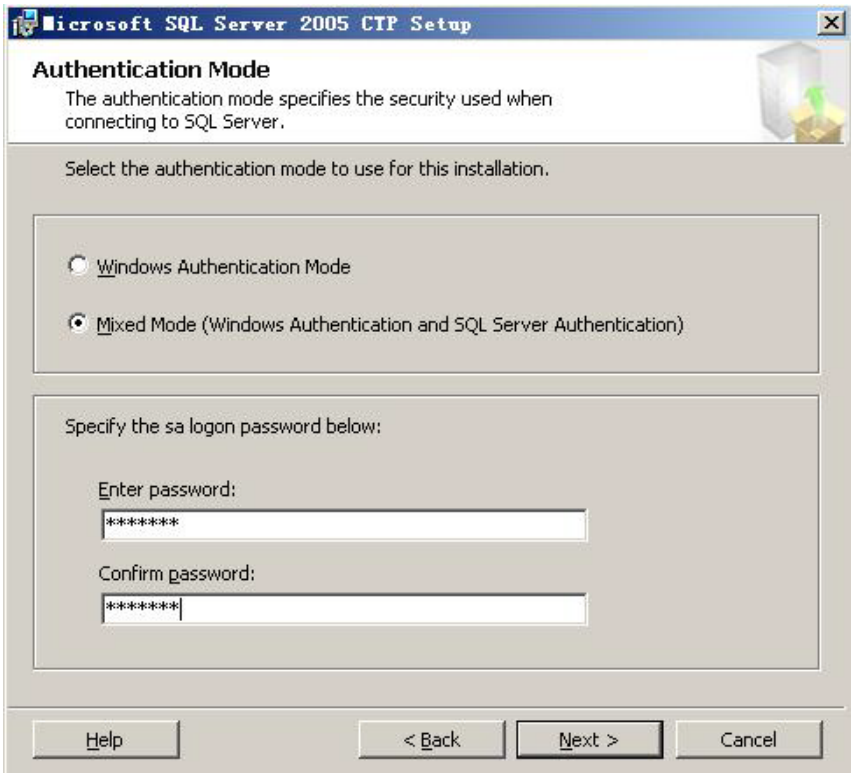


图 18　设置身份验证模式

10．接下来设置 SQL Server 的排序规则，完成后单击“Next”按钮，如图 19 所示。接下来设置错误报告，根据需要选择，然后单击“Next”按钮。

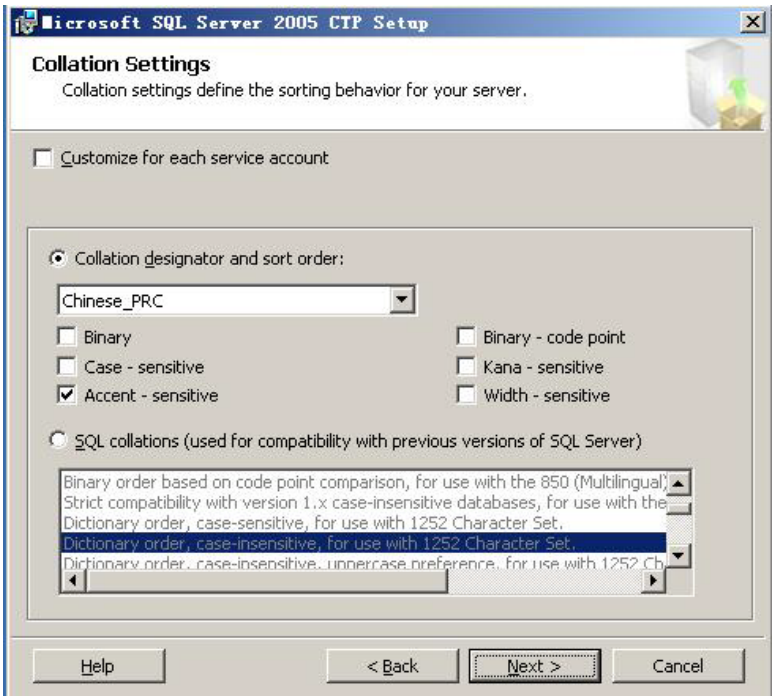


图 19　设置排序规则

11．接来的屏幕表示安装准备就绪，单击“Next”按钮。接下来的屏幕表示正在准备安装，这个需要一段时间，如图 20 所示。

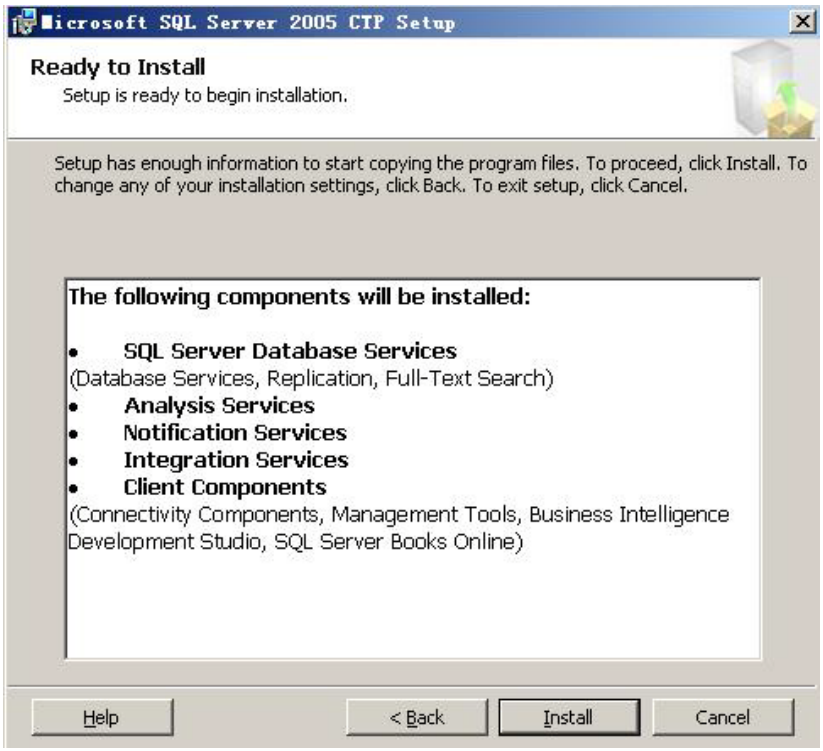


图 20　准备安装

12. 待安装准备完成后，会在各种群集结点上进行 SQL Server 的安装，可以单击“Node”下拉框选择不同的群集结点，查看在该结点上的安装进度。所有的安装完成后，单击“Next”钮，如图 21 所示。

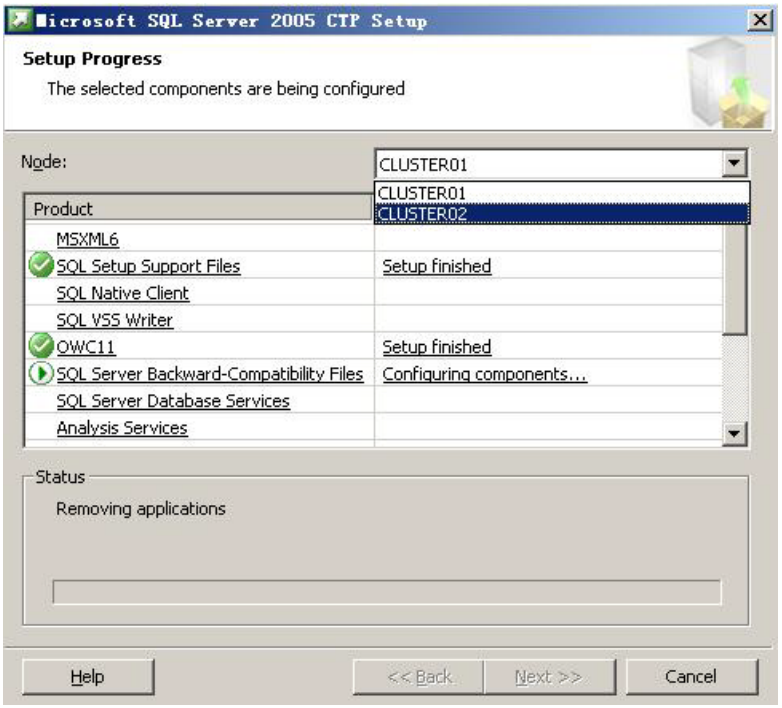


图 21　查看不同节点安装进度

13. 接下来的屏幕表示安装结束，单击“Finish”按钮。

SQL Server 正确安装完成后，在群集管理窗口中，单击安装 SQL Server 的组（本例中是 uemsql），可以看到 SQL Server 安装程序在里面自动创建了 SQL Server 群集相关的资源。可以测试一下，将“uemsql”移动到不同的群集结点，以此验证 SQL Server 安装的正确性，如图 22 所示。

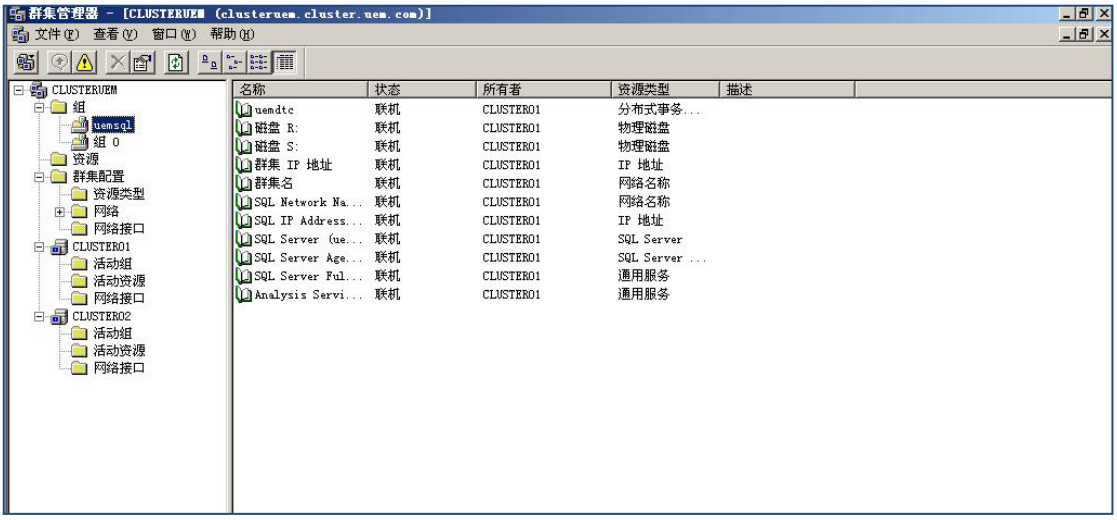


图 22　验证安装的正确性

1.2.3 安装 SQL Server 2000

SQL 的安装请参考 UEM 安装手册的 SQL2000 的安装部分，此处只说明需要更改的地方。

1. 在“服务帐户”中使用域帐户，由于是群集此处无法选择，如图 23 所示。

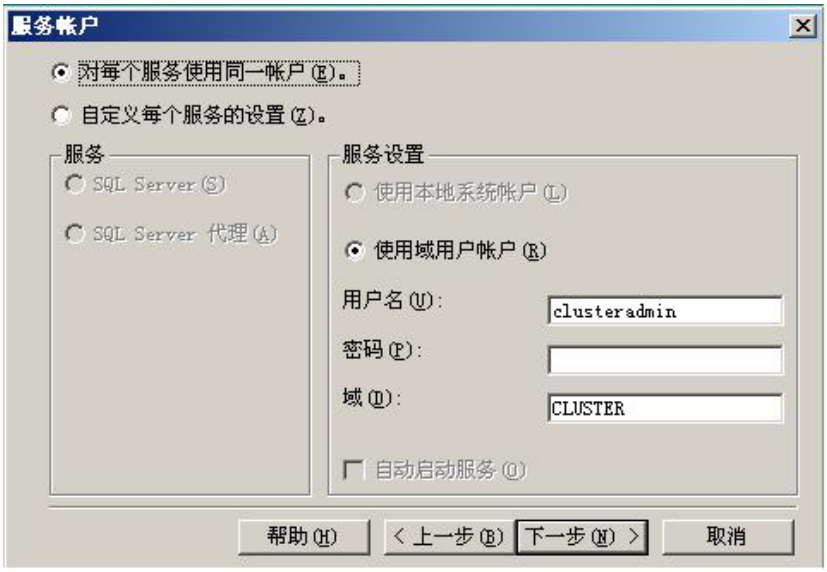


图 23　选择域帐户

2. 身份认证模式仍然采用混合认证模式。

3.“远程信息”中输入用户名“clusteradmin”和“clusteradmin”的密码，如图 24 所示。

图 24　输入用户名和密码

4．安装完成后，需要对 sql server 2000 升级到 sp4，升级时要在群集当前的活动节点中进行，这样所有的节点都升级完成。

第二章　安装 UEM 系统

2.1　在 cluster01 上安装 uem 服务器

1. 关闭 cluster02，在 cluster01 运行 uem 服务器的安装包 WBServerInstall.exe，安装完必要的组件后（请参考 uem 系统安装手册部分的服务器安装步骤），接受许可协议，选择定制安装，路径更改为 s:\css\waterbox，如图 25 所示。

图 25　选择安装路径

2．Sql server 中点击“浏览”选择 uemsql，如图 26 所示。

图 26　选择要连接的数据库

3．输入 sql 的密码，开始安装，如图 27 所示。

图 27　输入 SQL Server 密码

4．创建证书，配置 license，如图 28 所示。

图 28　创建证书

2.2 在 cluster02 上安装 uem 服务器

关闭 cluster01，开启 cluster02.，安装在 cluster01 上的安装步骤，在 cluster02 上安装 uem 服务器。

2.3 在群集中添加 uem 服务器所需的服务

2.3.1 添加通用服务 uemldap

1. 在群集管理器中选中“资源”，右键新建资源，新建资源名称为 uemladp，资源类型选择“通用服务”，勾选“在不同的资源监视器中运行该资源”，点击“下一步”，如图 29、30 所示。

图 29　新建资源名称

图 30　新建资源类型

2．在可能的所有者中，确认 cluster01 和 cluster02 都是可能的所有者，点击“下一步”，如图 31 所示。

图 31　可能的所有者

3．在“依存”中添加“资源依存”为“磁盘 S:”和“群集名”，点击“下一步”，如图 32 所示。

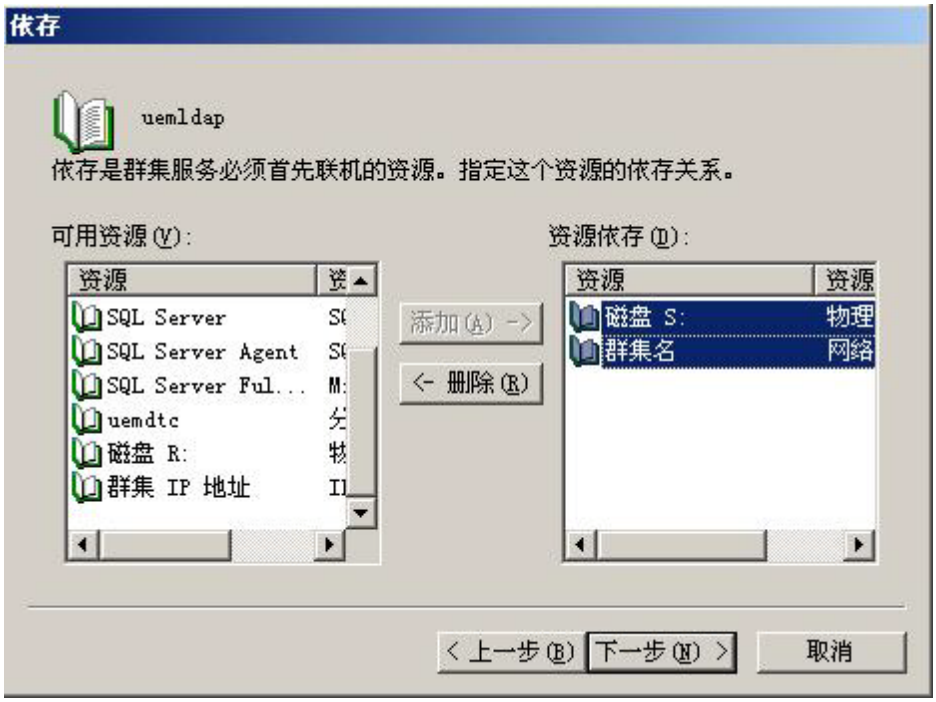


图 32　资源依存关系

4．在“一般服务参数”中，“服务名”填写“WBLdap”，“启动参数”填写“service”，点击“下一步”，如图 33 所示。添加完成后，将 uemldap 联机。

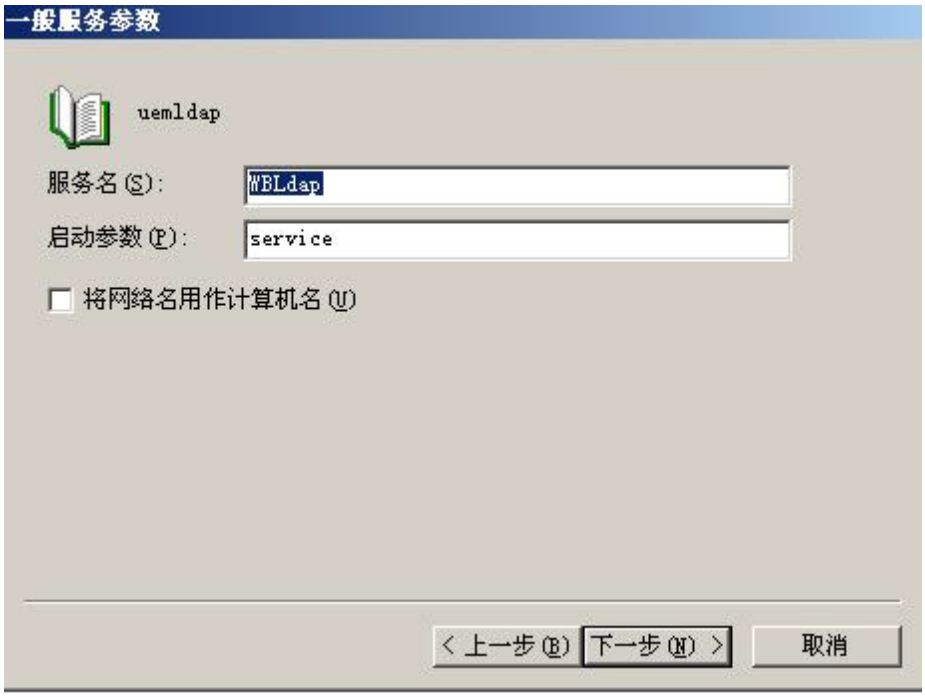


图 33　一般服务参数

2.3.2 添加通用服务 uemserver

1．添加过程同 ueml 的过程，在“一般服务参数”中“服务名”写“WBServer”，“启动参数”为空，如图 34 所示。

图 34　添加通用服务

2．添加完成后将 uemserver 联机

2.4 安装 uem 控制台

Uem 控制台的安装过程请参考 uem 系统安装手册的控制台安装部分

2.5 安装 uem 客户端

客户端的安装过程请参考 uem 系统安装手册的客户端安装部分，这里需要注意的是控制台登陆以及在客户端二次打包时使用最后一次服务器安装完成的 WBServer.cer，否则安装会失败。

附件二：

终端安全管理系统(web)使用方法

1. 启动

（1）终端安全管理系统(web)不需要单独安装，在任何一台机器上通过浏览器（IE6.0 以上）都可登录。在浏览器地址栏中输入 http://192.168.18.188:8080（其中 192.168.18.188 为服务器 IP 地址），即可转到登录界面，如图 1 所示。

图 1　终端安全管理系统（web）登录界面

（2）输入用户名和密码，点击“登录”按钮登录，如图 2 所示。

提示：

1. 用户名和密码是指任意控制台管理员的用户名和密码，系统默认的控制台管理员有两个：管理员 admin，密码 1234567a；安全官 security，密码 1234567a。

2. 如果不输入用户名和密码，以匿名方式登录，则只能看到安装升级包。

图 2　终端安全管理系统（web）界面

2. 用户管理

（1）在用户管理页面，在搜索框中输入任意字符，单击“搜索用户”按钮，可以搜出相关的用户，如图 3 所示。

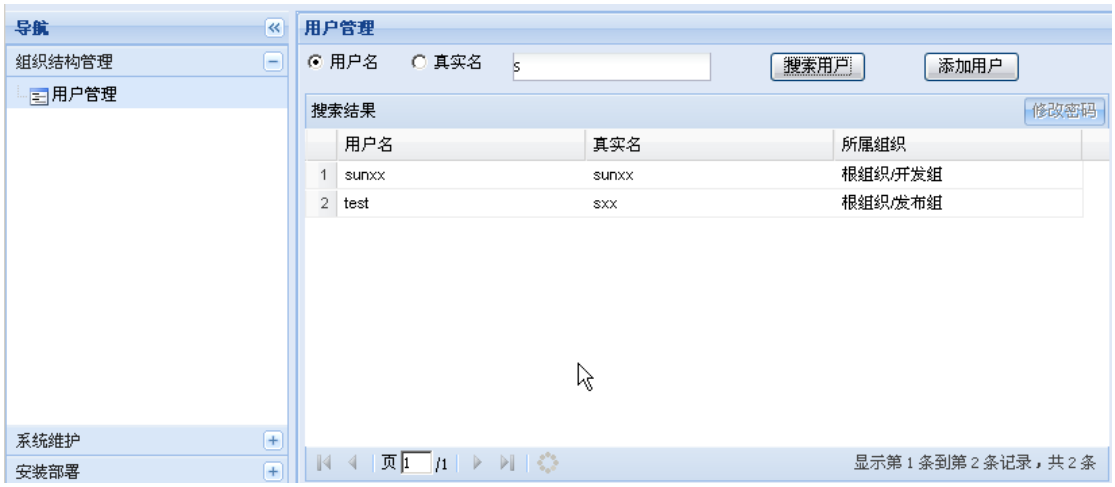


图 3　搜索用户

（2）单击“添加用户”按钮，弹出添加用户界面，如图 4 所示。输入用户名和密码，确定后即可添加用户。用户列表中显示新增用户，如图 5 所示。

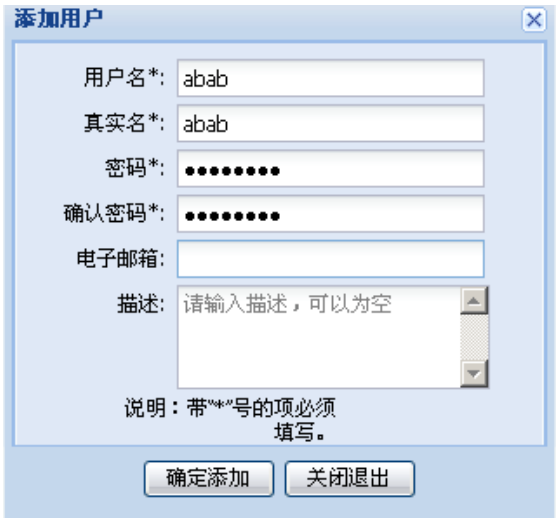


图 4　新增用户界面

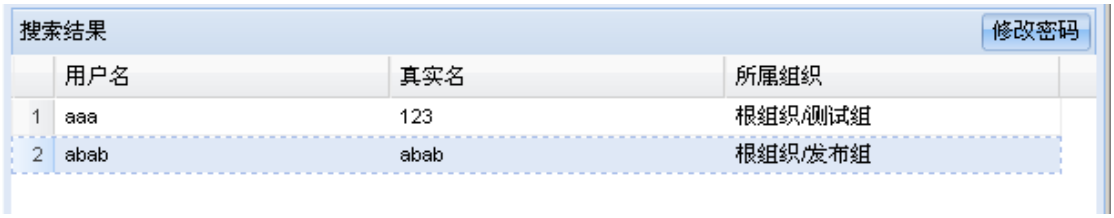


图 5　用户列表中显示新增用户

（3）在用户列表中选择某用户，单击“修改密码”按钮，可以重置用户的密码，如图 6 所示。

图 6　修改用户密码

3. 系统维护

在系统维护界面，可以看到服务器运行状况，显示服务器基本信息、CPU 使用状态、内存使用状态和磁盘使用状态等，如图 7 所示。

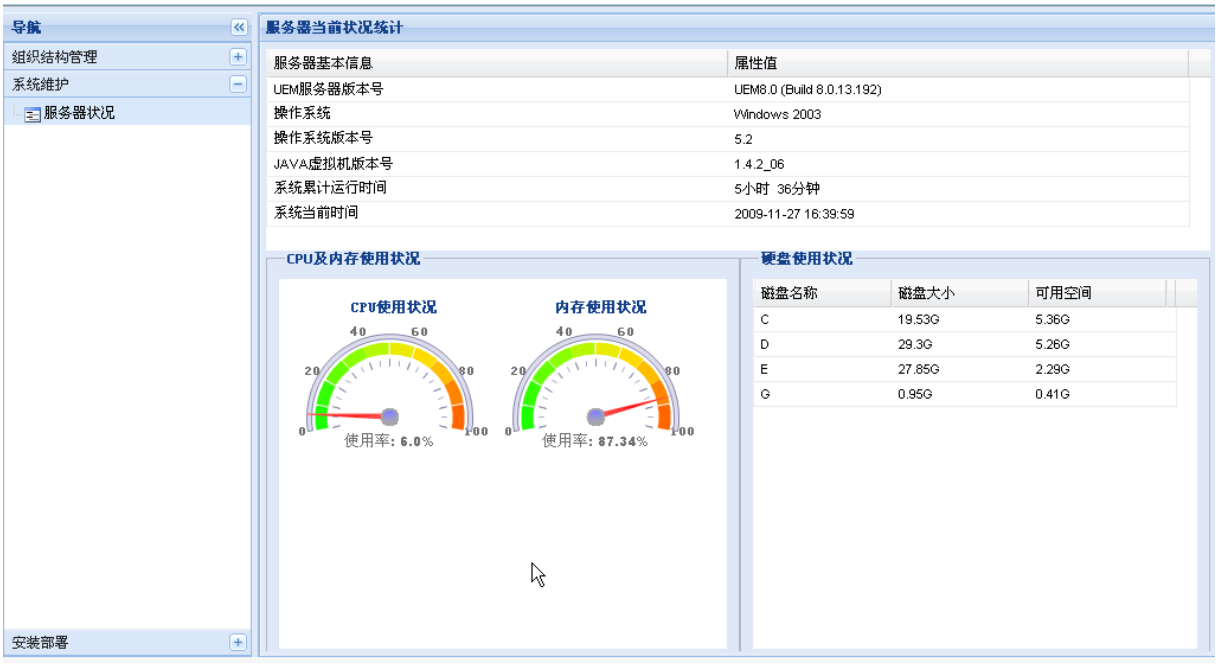


图 7　服务器运行状况

4. 安装部署

4.1 安装情况统计

在安装部署的安装情况统计页面，可以看到组织结构中人员和计算机的统计结果，多少在线、多少离线、多少未注册、多少被删除等，如图 8 所示。

图 8　安装情况统计

4.2　安装与升级包

（1）单击“安装部署”→“安装与升级包”，进入安装升级包界面，如图 9 所示。

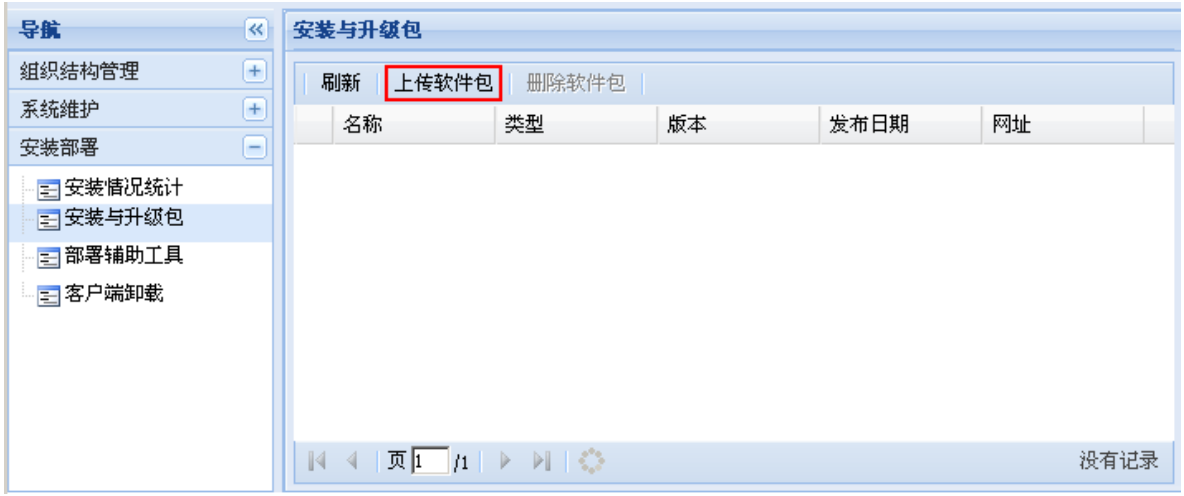


图 9　安装升级包界面

（2）单击“上传软件包”按钮，选择上传包类型，输入文件版本号（任意）、上传文件路径，确定后上传文件，如图 10 所示。

提示：上传文件目前支持的浏览器是 IE6 和 IE8，文件大小不要超过 200M。

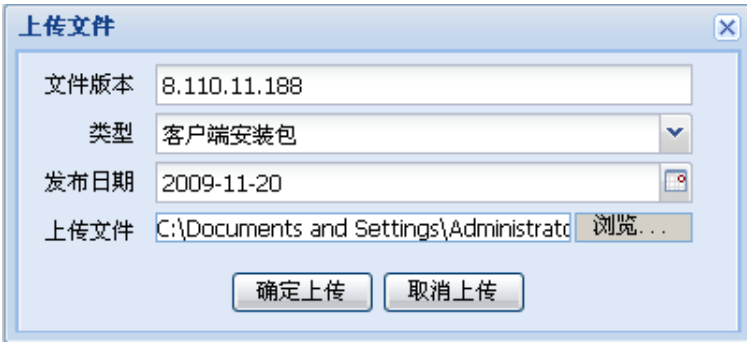


图 10　上传文件

（3）文件包上传成功后，在列表中显示，如图 11 所示。如果上传了错误文件包，可以单击“删除软件包”，将其删除。

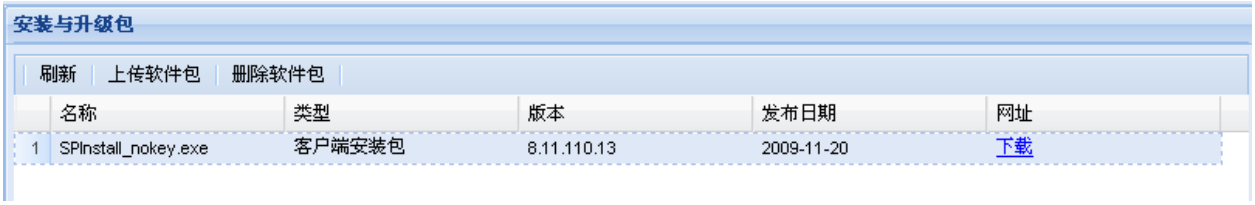


图 11　显示上传的文件包

（4）其它用户，可以在异地登录，下载需要文件包，如图 12 所示。

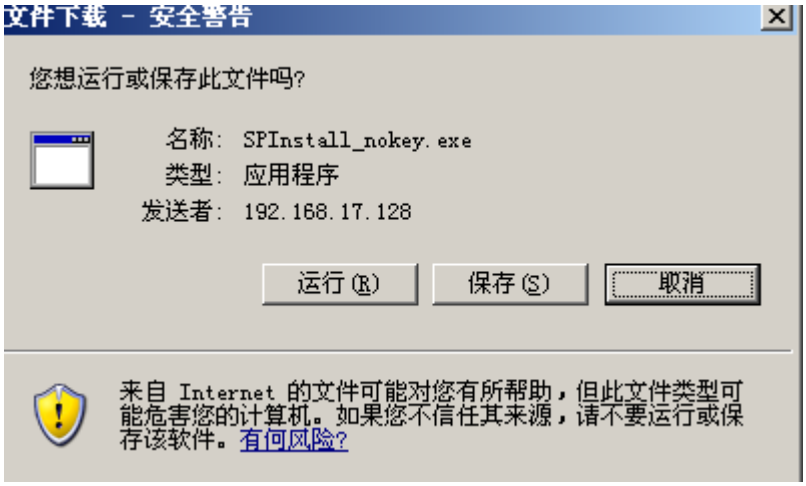


图 12　下载安装包

4.3　部署辅助工具

（1）单击“安装部署”→“部署辅助工具”，进入部署辅助工具界面，如图 13 所示。

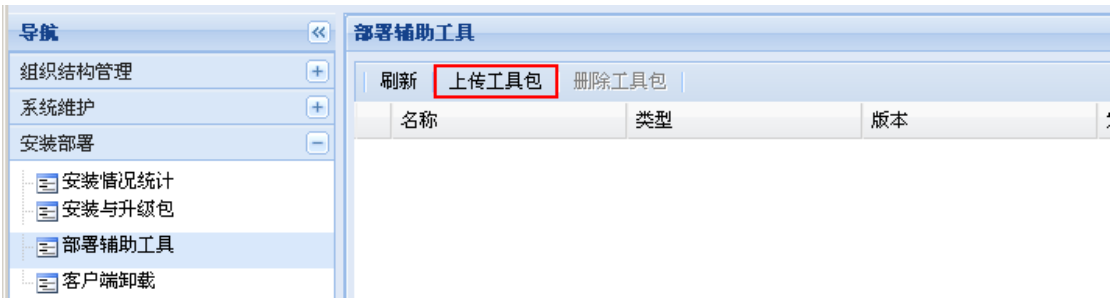


图 13　部署辅助工具界面

（2）单击“上传工具包”按钮，输入上传文件版本号（任意）、上传文件路径，确定后上传文件，如图 14 所示。

提示：上传文件目前支持的浏览器是 IE6 和 IE8，文件大小不要超过 200M。

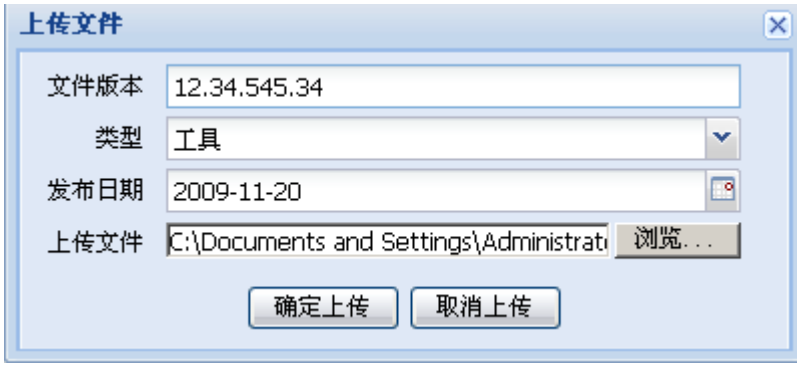


图 14　上传工具包文件

（3）文件包上传成功后，在列表中显示，如图 15 所示。如果上传了错误工具包，可以单击“删除工具包”，将其删除。

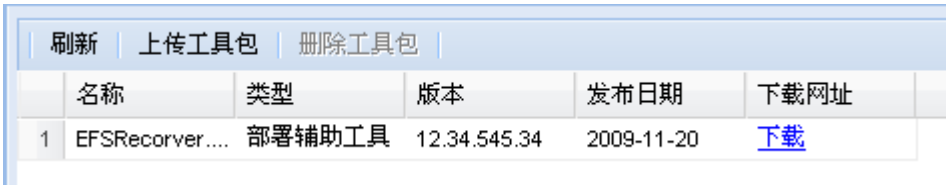


图 15　显示上传的工具包

（4）其它用户，可以在异地登录，下载需要文件包，如图 16 所示。

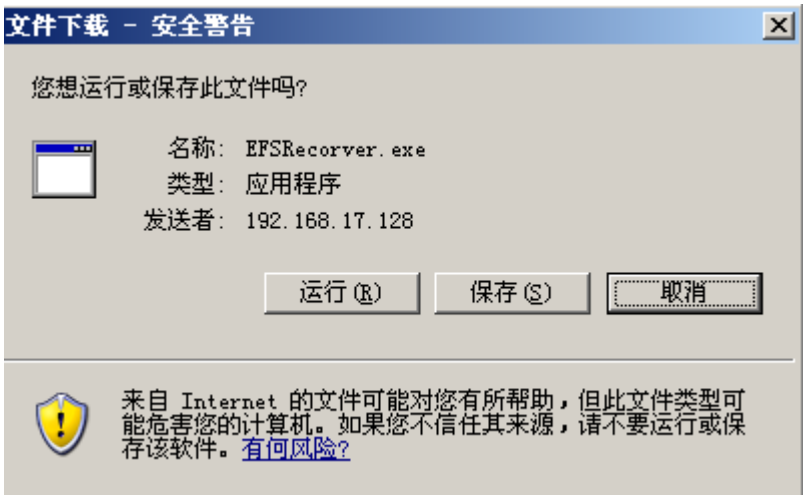


图 16　下载工具包

提示：

尽管在“部署辅助工具”下可以上传安装与升级包，在“安装与升级包”也可以上传部署辅助工具，但还是建议用户分类传输便于管理。另外，如果把安装升级包传输在“部署辅助工具”下，其它用户匿名登录的话，将看不到安装升级包。

4.4　客户端卸载

如果允许客户端本地卸载，将客户端本地卸载时生成的随机码，输入到这里，生成验证码，如图 17 所示。客户端获得验证码后，既可执行卸载。

图 17　客户端口令卸载

附件三：

中软安全文档审批管理系统使用手册

Version

第一章　系统的安装

中软安全文档审批管理系统（英文简称 SecDocAP），主要负责安全文档的在线审批，包括服务器和控制台两部分，服务器需要单独安装。

SecDocAP 服务器可以和 UEM 服务器装在一起，也可单独安装在外网上，便于每个能上网的客户都能访问到它。

1．将硬件加密锁插入服务器，在安装光盘中找到审批服务器的安装程序 SecDocAPInst.exe，双击开始安装，如图 1-1 所示。

图 1-1　SecDocAP 服务器安装程序

2. 启动安装画面后，稍等出现欢迎界面，如图 1-2 所示。单击“下一步”，继续运行。

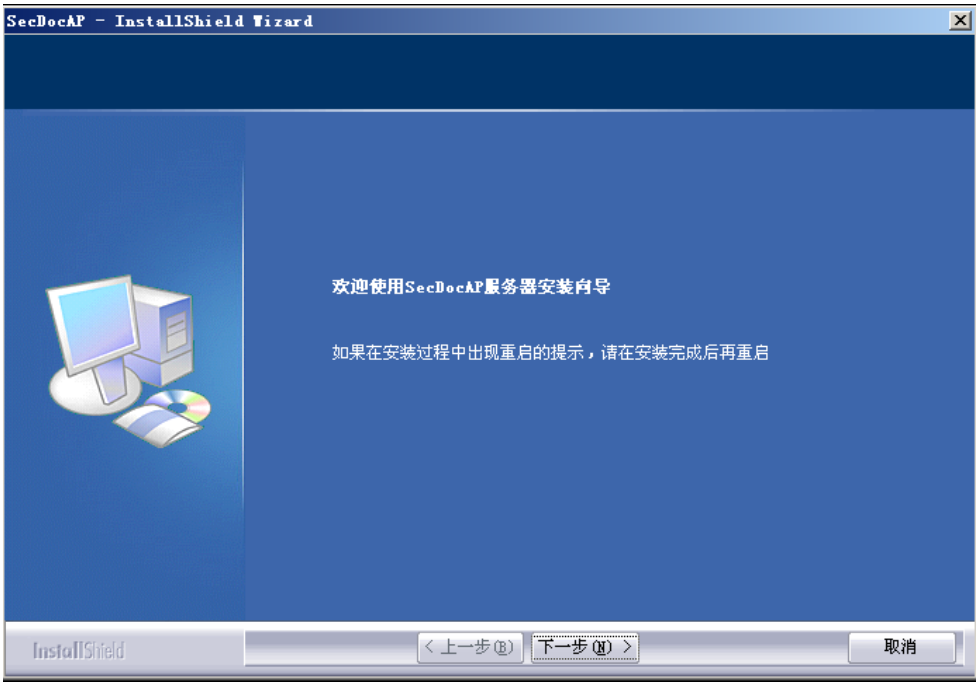


图 1-2　安装 SecDocAP 服务器欢迎界面

3. 输入用户名和公司名称后，单击“下一步”，如图 1-3 所示。

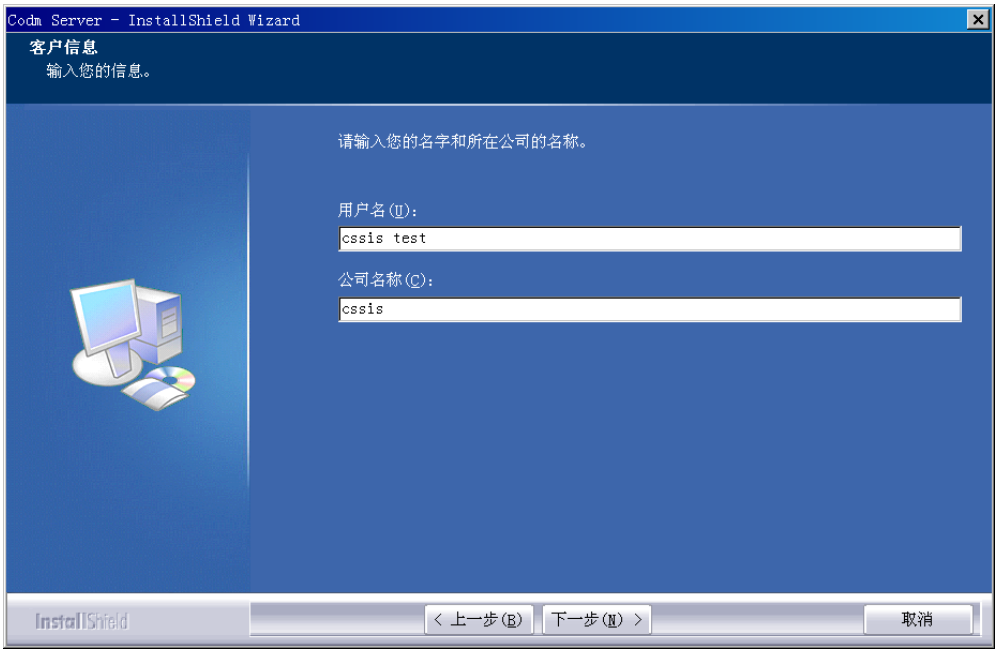


图 1-3　输入客户信息

4. 选择安装类型。默认采用“完全”方式，如图 1-4 所示。也可选用“定制”安装模式，更改安装路径，选择欲安装的功能组件。最后，单击“下一步”继续安装。

图 1-4　选择安装类型

5. SecDocAP 服务器默认安装在“C:\Program Files\CSS”，可以单击“更改”按钮，改变安装路径，如图 1-5 所示。

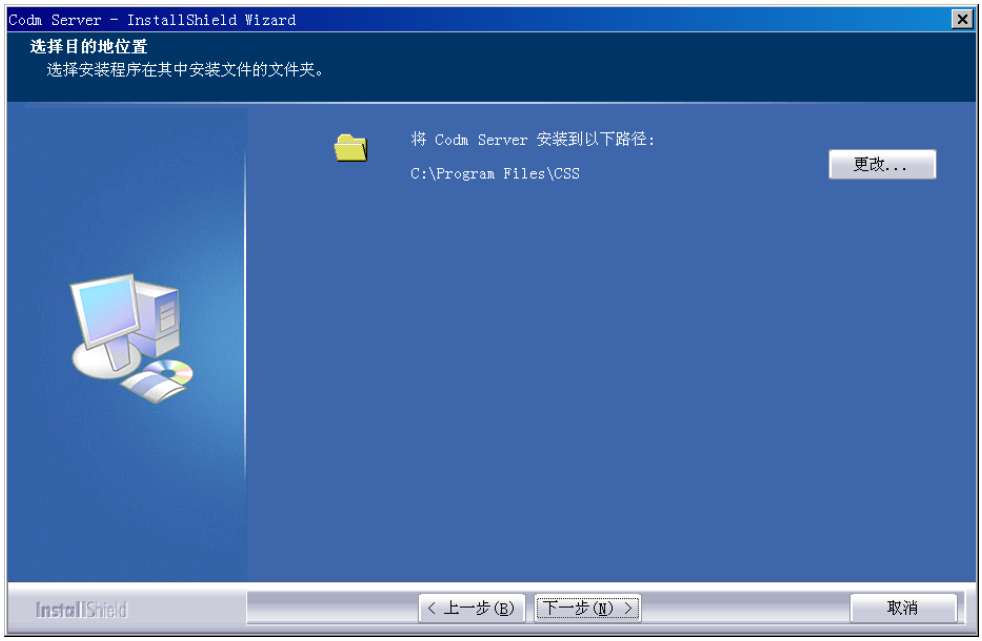


图 1-5　改变安装路径

6. 设置全部完成后，单击“安装”按钮，开始安装，如图 1-6 所示。如果要检查或更改任何安装设置，单击“上一步”。单击“安装”按钮，开始安装。

图 1-6　完成安装前设置

7. 单击“next”按钮，安装圣天诺加密锁驱动，如图 1-7 所示。

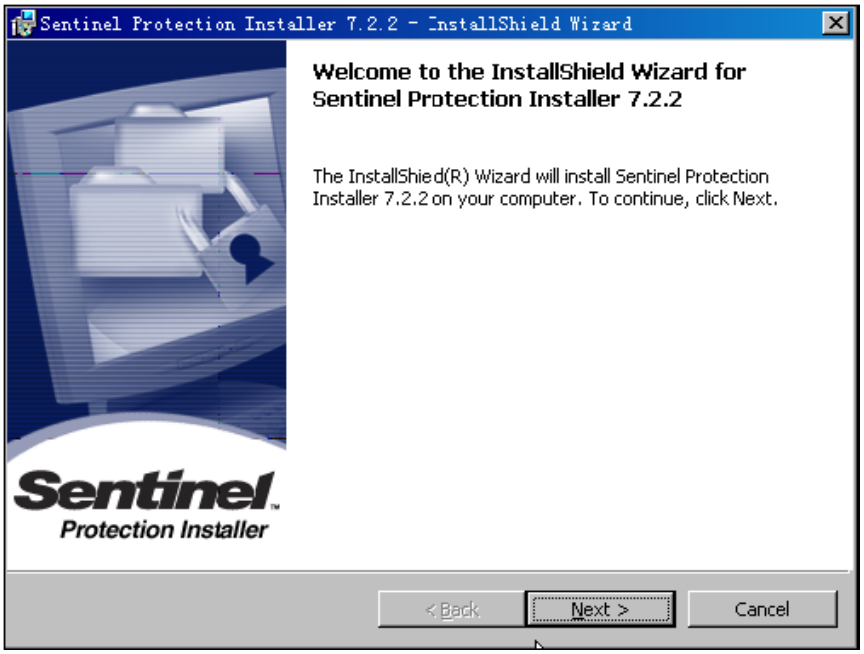


图 1-7　安装圣天诺加密锁驱动

8. 选择接受安装加密锁的许可协议，单击“next”按钮，如图 1-8 所示

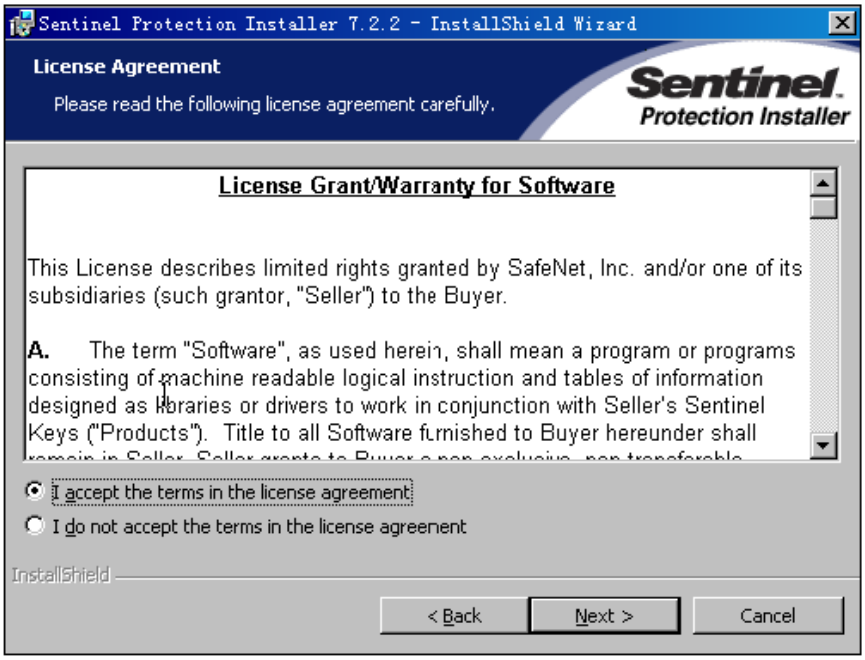


图 1-8　接受安装加密锁的许可协议

9. 选择完全安装模式，单击“next”按钮，如图 1-9 所示。

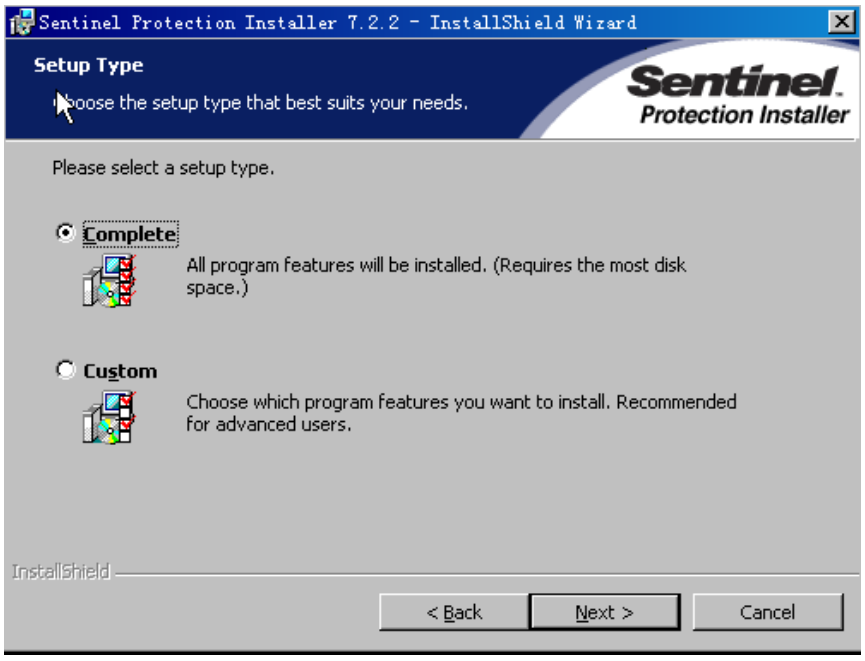


图 1-9　选择安装模式

10. 单击“Install”按钮，运行加密锁驱动程序，如图 1-10 所示。

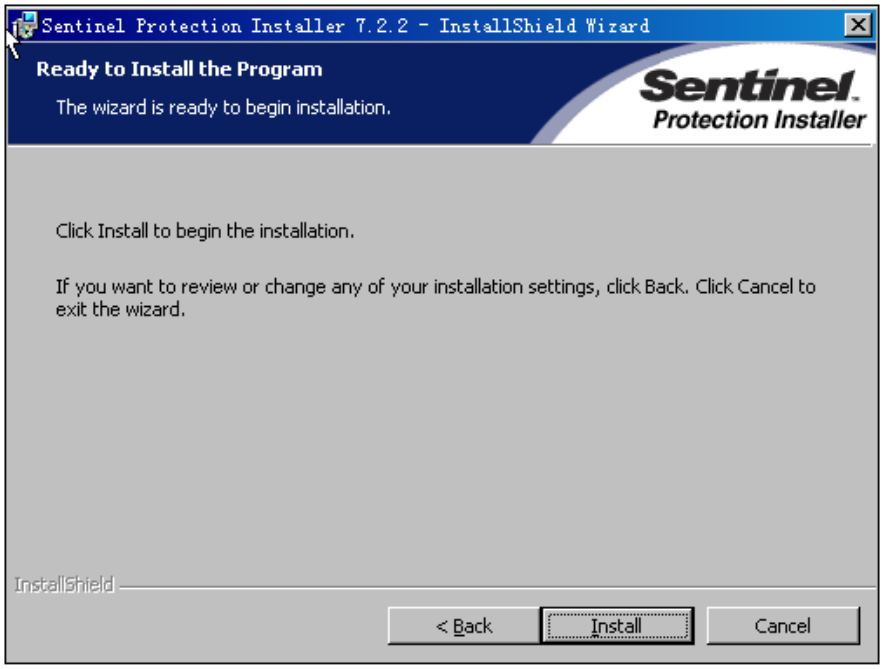


图 1-10　运行加密锁驱动程序

11. 加密锁驱动程序运行完成后，单击“Finish”结束，如图 1-11 所示。

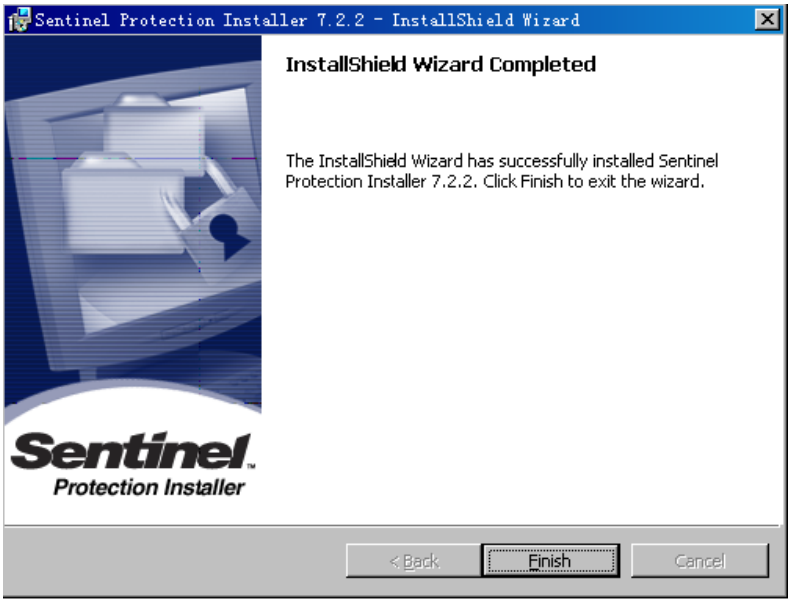


图 1-11　加密锁驱动程序运行完成

12. 接下来转入系统初始化界面。在数据库连接配置界面中，输入数据库所在计算机的 IP 地址、端口号，以及数据库类型、用户名和密码，如图 1-12 所示。输入完成后，单击“下一步”，提示连接数据库成功。

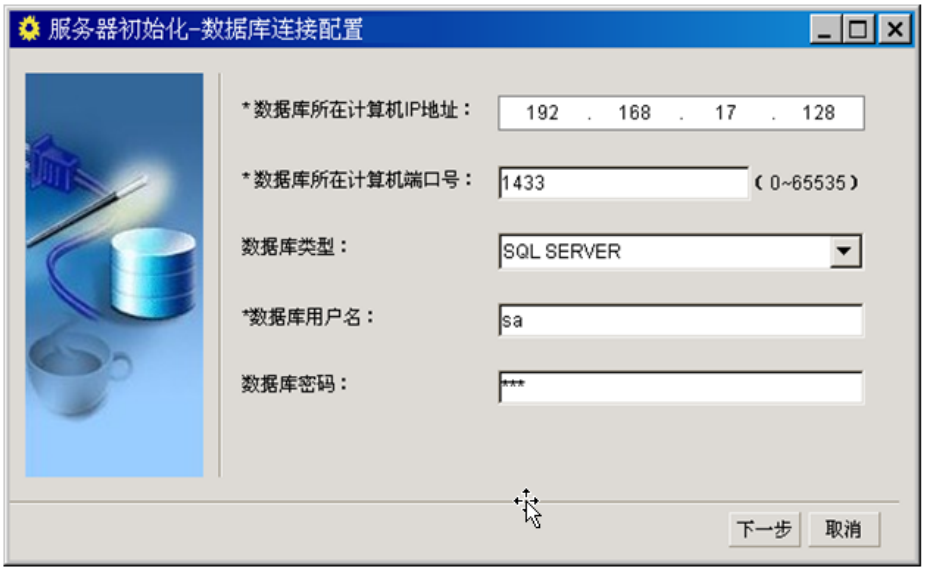


图 1-12　外发服务器数据库连接配置

13. 输入新建的数据库名，例如“CODM”， 如图 1-13 所示。单击“下一步”，提示创建数据库成功。

图 1-13　　新建数据库名

14. 输入初始用户密码，确认密码， 如图 1-14 所示。**请用户一定要记住该用户名和密码，首次登陆审批管理系统管理时，要用到此帐户。**参见系统管理章节。

图 1-14　设置初始用户密码

15. 配置服务器存储空间，如图 1-15 所示。服务器存储空间是制作外发包上传文件存储的地方，上传文件统一存储在指定盘符下的 FileStore 目录中，在这里可以配置多个存储空间。单击“完成”按钮，继续。

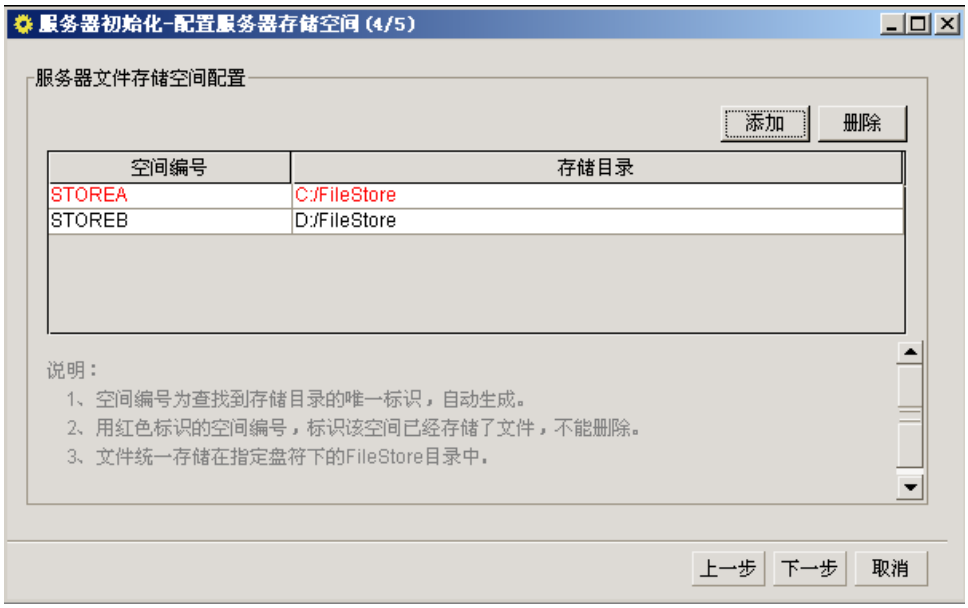


图 1-15　配置服务器存储空间

16. 输入服务器所在计算机 IP 地址、端口号，以及访问 web 地址的端口。然后，单击“完成”按钮，如图 1-16 所示。

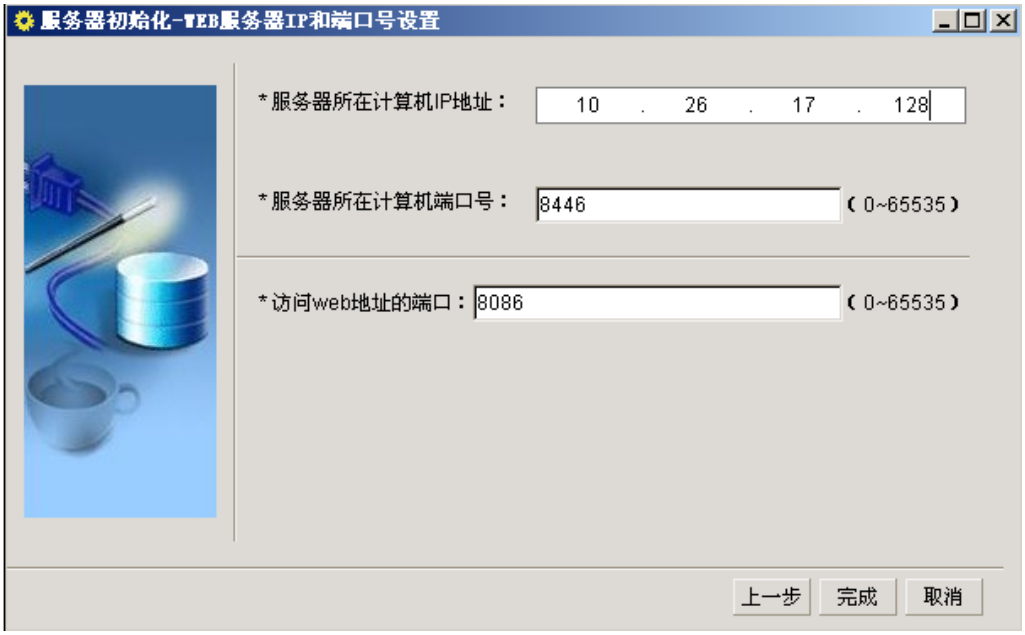


图 1-16　配置 web 服务器 IP 地址和端口号

17. SecDocAP 服务器全部安装完成以后，单击“完成”按钮退出，如图 1-17 所示。

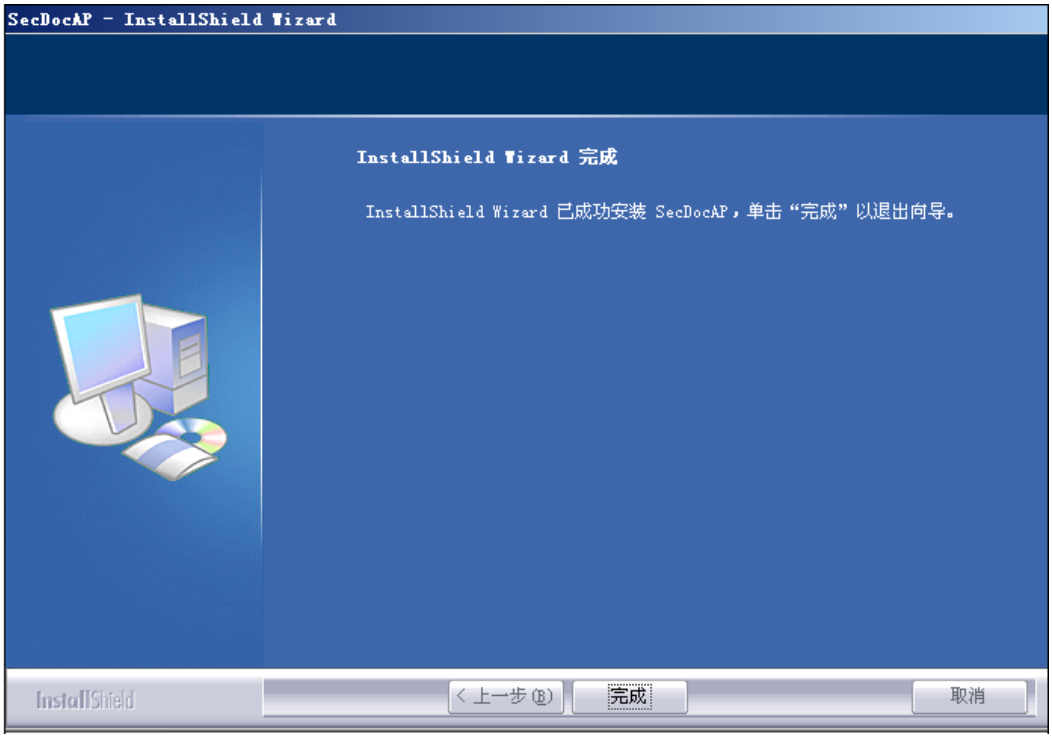


图 1-17　SecDocAP 服务器完成

完成了整个服务器的安装，在能够正常通讯的机器上，在 IE 浏览器地址栏中输入 http://192.168.17.128:8086/SecDoc（其中 192.168.17.128 为审批服务器 IP 地址），即可转到安全文档审批管理系统登录界面。

第二章　安全文档审批系统管理

安全文档审批系统管理包括：系统管理、审批管理和权限管理。系统管理主要添加、删除该系统的用户和角色权限，并记录控制台操作日志。审批管理和权限管理主要包含员工和分组管理、审批流程的制定和应用，以及在线审批日志的上传等。下面我们按菜单顺序一一介绍，有关联的章节按链接跳转。

2.1 系统管理

在浏览器地址栏中输入 http://192.168.17.128:8086/SecDoc（其中 192.168.17.128 为审批服务器 IP 地址），即可转到审批控制台登录界面。首先以默认帐户（用户名：admin　密码：1234567a，大小写要匹配）登录控制台，进入系统管理界面，如图 2-1 所示。上面是菜单栏，左侧是导航栏，右侧为信息展示区。

图 2-1　系统管理界面

2.1.1　用户与角色

SecDocAP 控制台不同的用户，有不同的角色和权限。初始化用户 admin，主要负责用户管理、角色管理和控制台操作日志管理。用户可以根据自己的需要，设置具有不同角色和权限的用户，来分管不同的业务，实现整个文件审批系统的分级分权管理。

2.1.1.1 角色管理

1. 在左侧导航栏中点击“用户与角色”→“角色管理”，进入“角色管理”界面。在角色列表中可以看到内置的管理员角色，选择该角色，在右侧可以看到它的权限信息，如图 2-2 所示。角色分两种：内置角色和非内置角色。内置角色是系统初始化时内置的基本角色，不能删除；非内置角色，是用户根据自己的需要自行添加的。已赋予用户的角色，也不能删除。

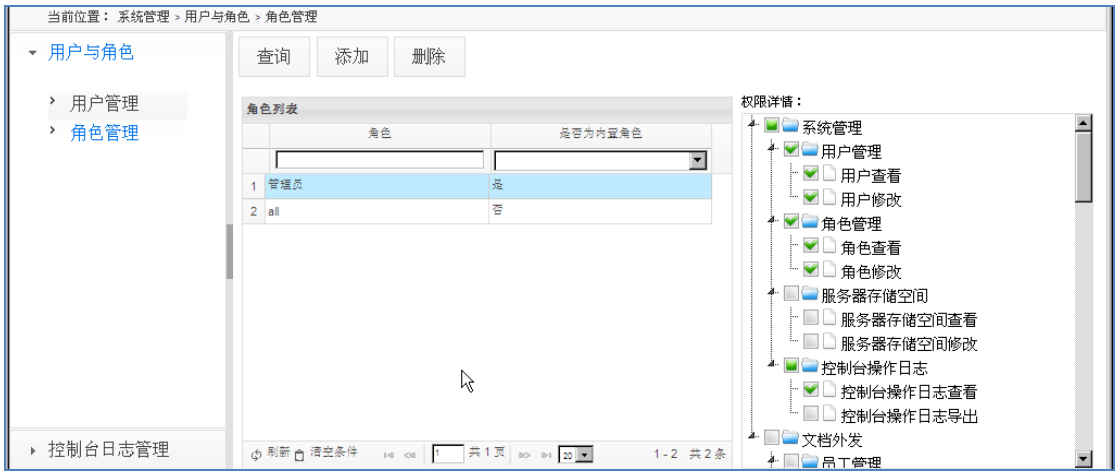


图 2-2　角色管理界面

2. 单击“添加”按扭，添加用户需要的角色，一定要包括审批管理和权限管理，如图 2-3 所示。角色名称：1-30 个字符，仅支持数字、字母、下划线和中文。

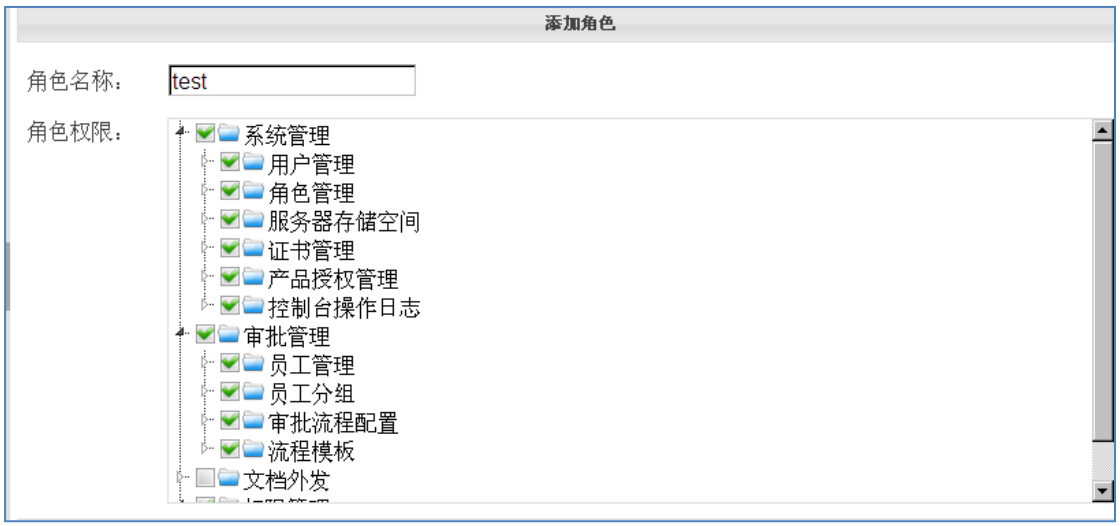


图 2-3　添加角色

3. 单击“确定”按钮，提示“添加角色”成功。在角色列表中，将看到新添加的角色，如图 2-4 所示。

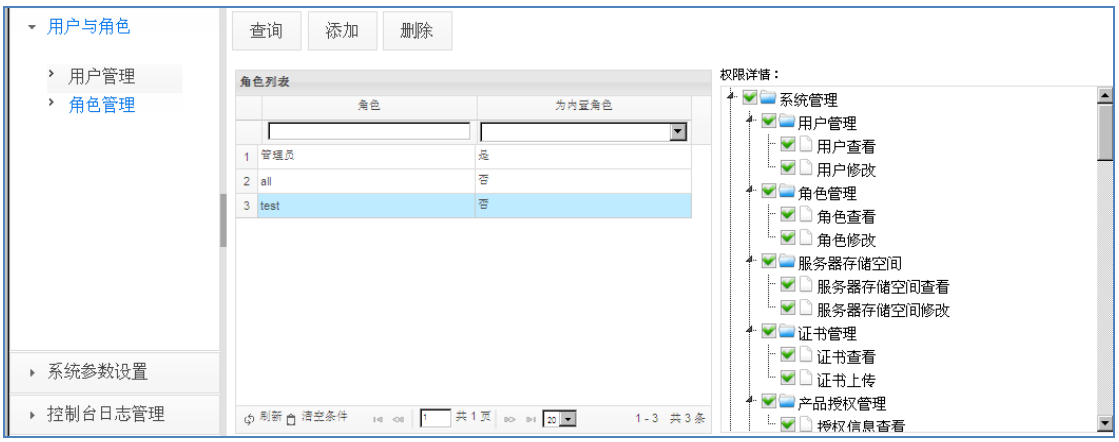


图 2-4　角色列表

4. 新增的角色不能修改，只能删除。选择要删除的新角色，单击“删除”按钮，确定后即可删除，如图 2-5 所示。

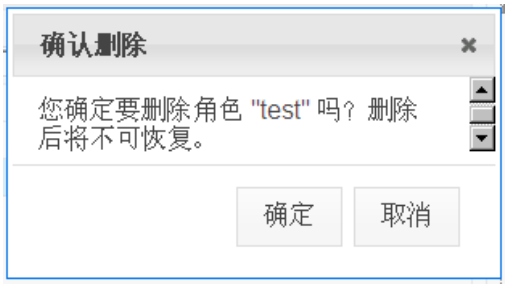


图 2-5　删除新增角色

5. 如果要删除角色是系统初始化内置的角色，提示不能删除，如图 2-6 所示。另外，删除的角色已经赋予了某用户，也不能删除，提示删除角色失败。

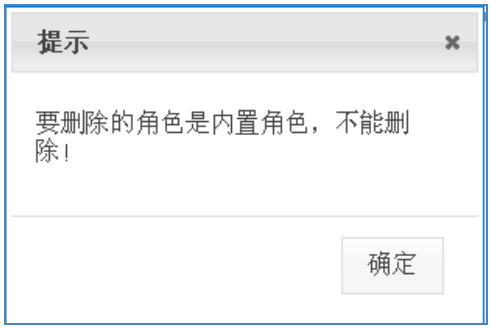


图 2-6　删除角色失败

6. 当角色列表中角色特别多时，单击列表项下面的空白框，输入查询条件，单击“查询”按钮或回车键，可以实现按条件查询，如图 2-7 所示。例如：在“是否为内置角色”下面的空白框中选择“否”，所有非内置角色都显示了出来。

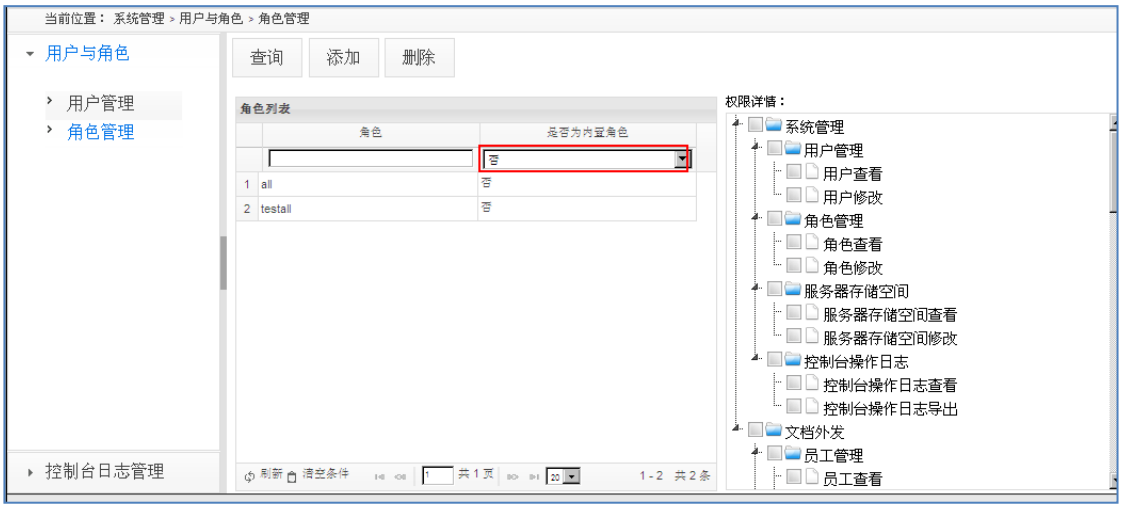


图 2-7　角色查询

2.1.1.2 用户管理

1. 在左侧导航栏中点击“用户与角色”→“用户管理”，进入“用户管理”界面。在用户列表中可以看到内置的用户 admin，以及它所属的角色名称，如图 2-8 所示。

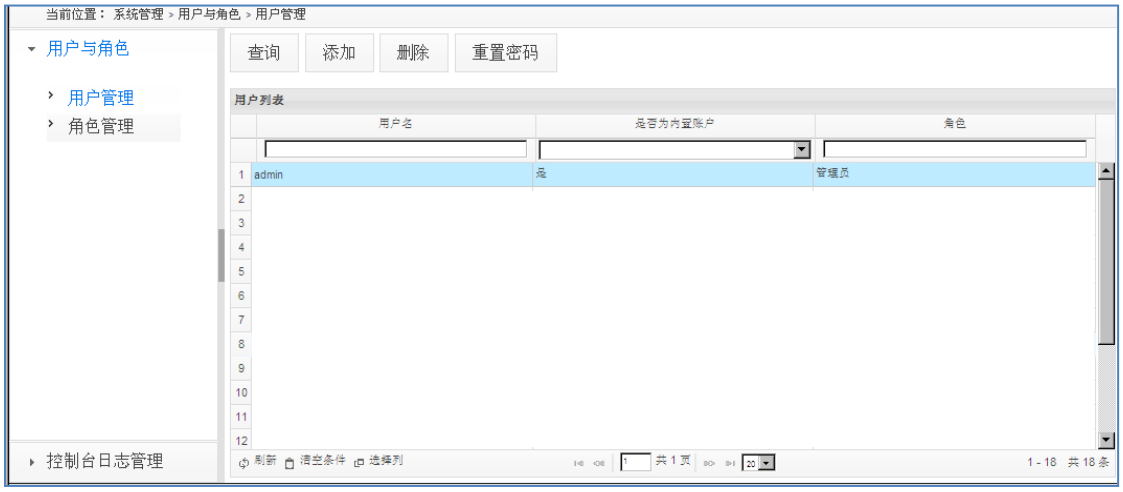


图 2-8　用户管理界面

2. 在“用户管理”界面中，单击“添加”按扭，添加需要的用户，如图 2-9 所示。登录管理员名称不支持中文，支持字母、数字、下划线，最长为 20 字符。角色名称从下拉框中选择，这里我们选择具有审批管理功能的角色 test。用户不需要设置口令，默认密码为 1234567a，登录后请及时修改。

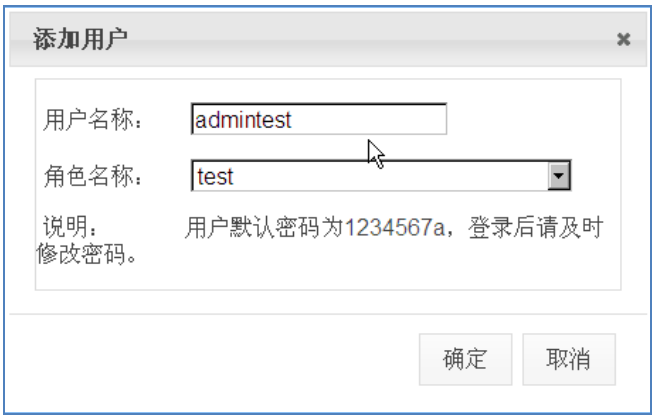


图 2-9　添加用户

2. 单击“确定”按钮，提示“添加用户”成功。在用户列表中，将看到新添加的用户，如图 2-10 所示。这是登录文档审批管理系统的用户，后面我们以此用户登录，介绍文档审批管理功能，详见文档审批章节。

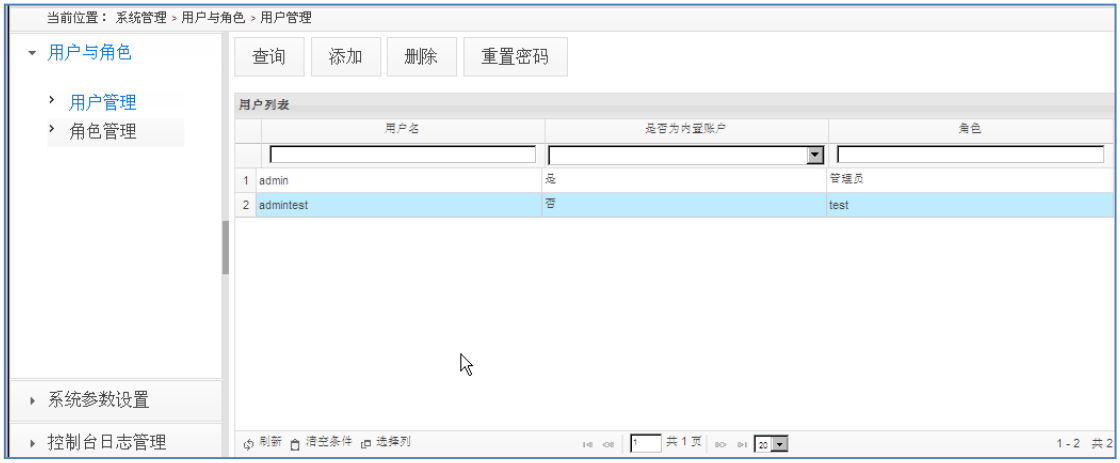


图 2-10　用户列表

3. 用户不能修改，只能删除。选择要删除的用户，单击“删除”按钮，确定后即可删除，并不可恢复，如图 2-11 所示。我们这里不删除，单击“取消”按钮，返回原来界面。

图 2-11　删除用户

4. 在用户列表中，选择初始化的内置用户，就不能被删除，提示删除用户失败，如图 2-12 所示。正在使用的用户可以直接删除，但是删除操作在下一次该用户尝试登录时生效。

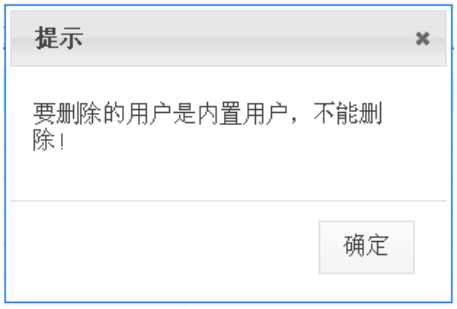


图 2-12　删除用户失败

5. 以新用户 admintest 登录，单击右上方的“修改密码”按钮，弹出修改密码框，如图 2-13 所示。输入新、旧密码，确定后，即可更改密码。单击右上方的“退出”按钮，admintest 用户将以新的密码登录。

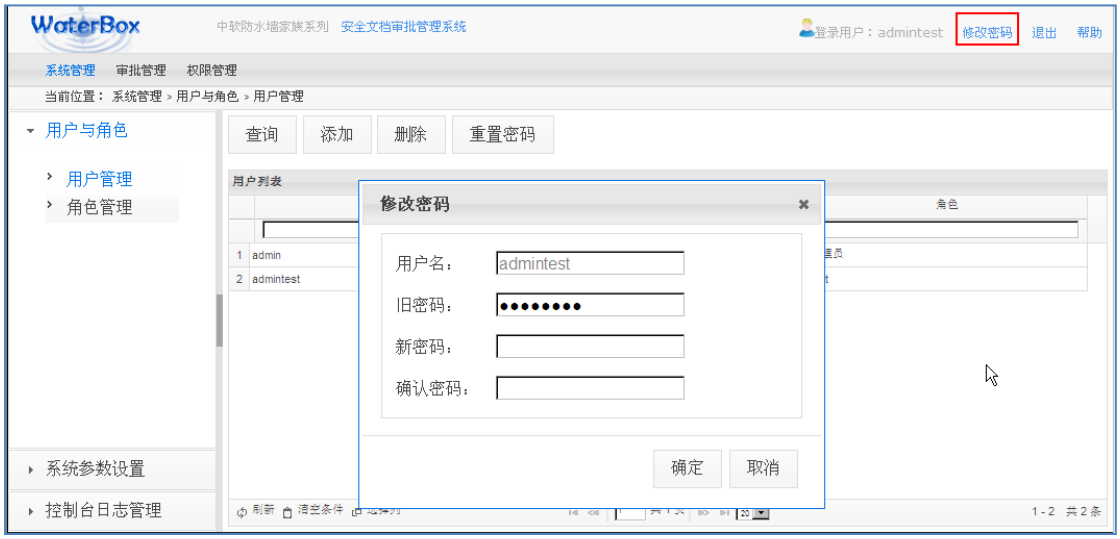


图 2-13　更改用户密码

6.在用户管理的用户列表中，选择某用户，单击“重置密码”按钮，出现提示信息，如图 2-14 所示。确定后，可以将某用户的密码重置为默认的 1234567a.

图 2-14　重置密码

7. 当用户列表中用户特别多时，单击列表项下面的空白框，输入查询条件，单击“查询”按钮或回车键，可以实现按条件查询，如图 2-15 所示。例如：在用户名下面空白框中输入字母 a，所有含 a 用户名都搜索了出来。

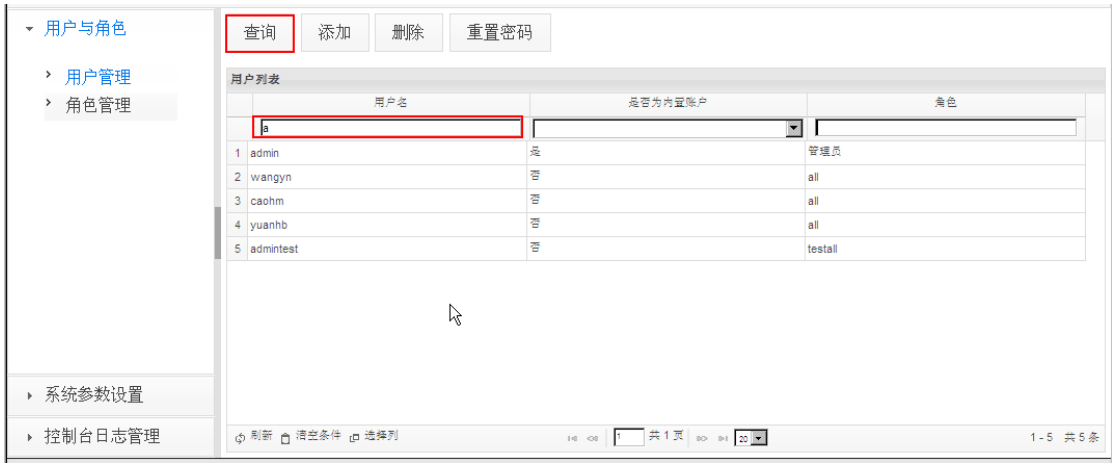


图 2-15　查询用户

8. 单击“用户列表”各列表项后面的上、下小箭头，可以实现该列信息按升序或降序排列，如图 2-16 所示。

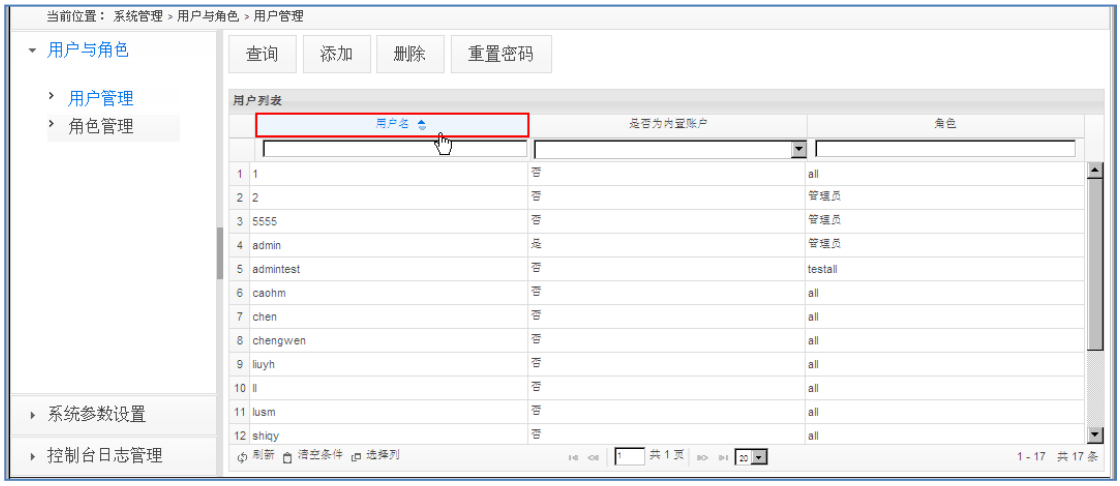


图 2-16　用户名有序排列

2.1.2 系统参数

2.1.2.1 服务器存储空间

在左侧导航栏中点击“系统参数”→“服务器存储空间”，进入服务器存储空间配置界面，如图 2-17 所示。

服务器存储空间是制作审批包上传存储文件的地方，上传文件统一存储在指定盘符的 FileStore 目录中。初始化时已经配置了默认的存储空间，用户在实际工作中，还可以在这里配置多个存储空间。当服务器的第一个文件存储空间存满时，会自动存入下一个存储空间中。

图 2-17　配置服务器存储空间

2.1.2.2 证书管理

UEM 系统是中软自主研发的统一终端安全管理系统，是内网安全的主流产品。当 UEM 系统的普通加密文件在线授权时，在制作主动授权文件的过程中，需要验证 UEM 证书。

1. UEM 证书默认位置在服务器 C:\Program Files\CSS\UEM\WBServer\server\default\conf\wbserver.cer，请用户将 wbserver.cer 文件备份。

2. 在左侧导航栏中点击“系统参数”→“证书管理”，进入 SecDocAP 系统证书管理界面，如图 2-18 所示。单击“浏览”按钮，找到 UEM 证书备份路径，单击“上传”按钮，将证书文件 wbserver.cer 上传至 SecDocAP 服务器。

图 2-18　导入 UEM 服务器证书

2.1.3 控制台操作日志

1. 以 admintest 登录，在左侧导航栏中点击“控制台日志管理”→“控制台操作日志”，进入控制台操作日志管理界面，如图 2-19 所示。在这里查看系统登录、用户管理、角色管理等操作日志。

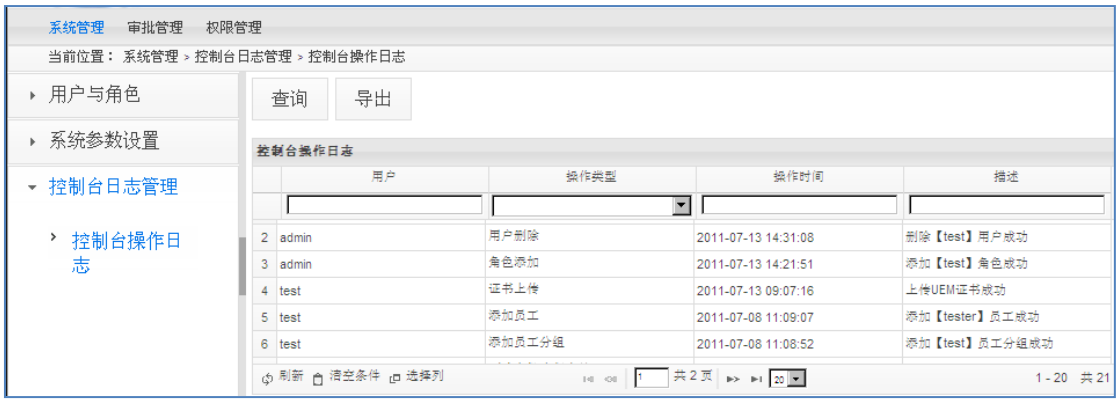


图 2-19　控制台操作日志界面

2. 单击列表项下面的空白框，输入查询条件，单击“查询”按钮或回车键，可以实现按条件查询，如图 2-20 所示。例如：在“操作类型”下面，选择“添加用户”，将看到控制台所有添加用户操作的日志记录。

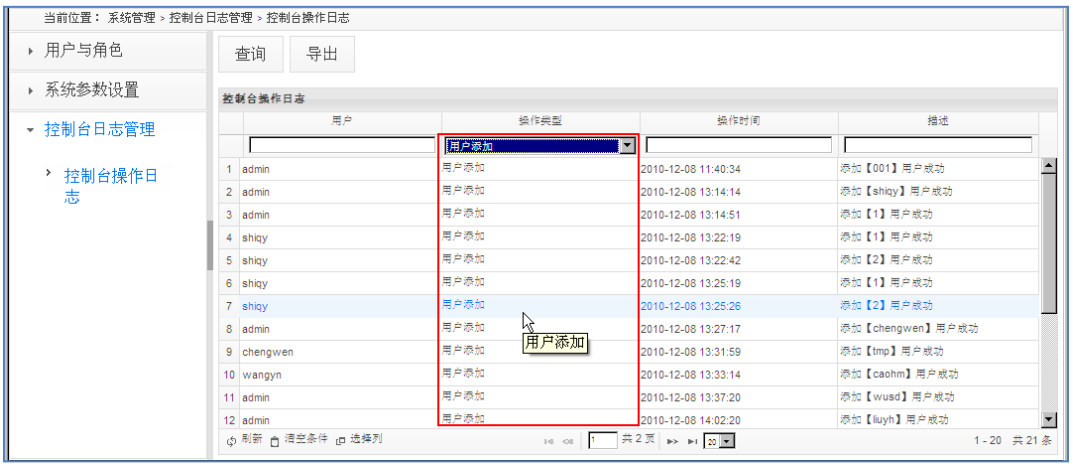


图 2-20　按条件查询操作日志

3. 单击各列表项后面的上、下小箭头或，可以将该列按升序或降序排列，如图 2-21 所示。

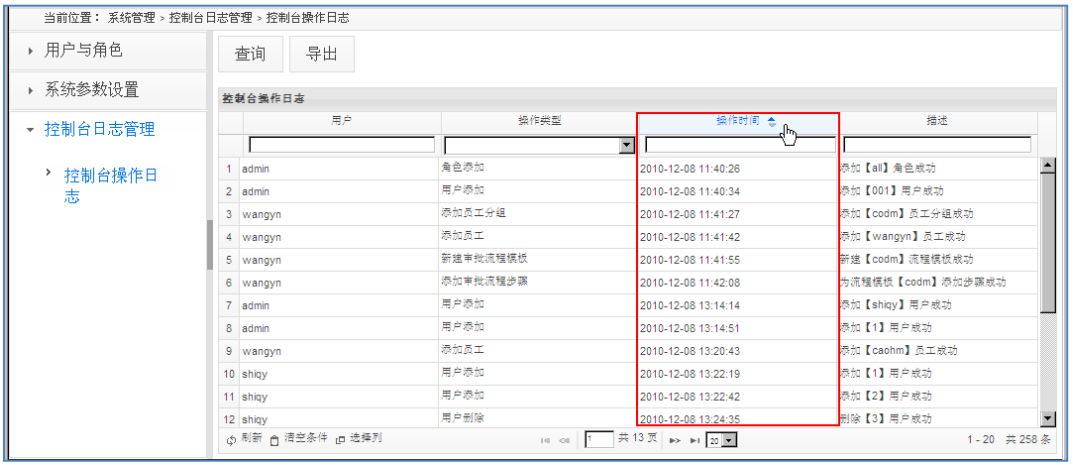


图 2-21　查询日志按升序或降序排列

4. 在操作日志列表中选择某一记录，双击弹出详细信息框，如图 2-22 所示。可以单击“上一条”、“下一条”逐条查看，这也是一种查看方式。

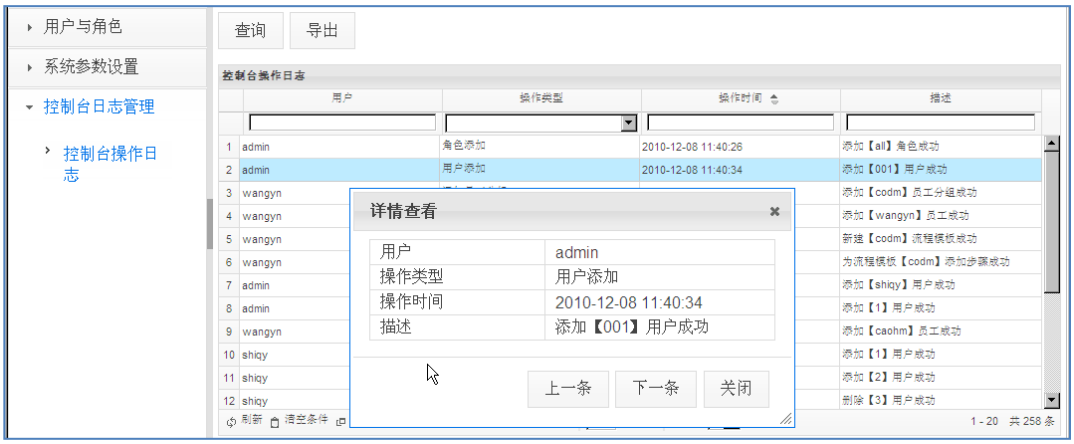


图 2-22　逐条查看操作日志详情

5. 单击“导出”按钮，可以将日志信息导出保存为*.zip 文件，如图 2-23 所示。

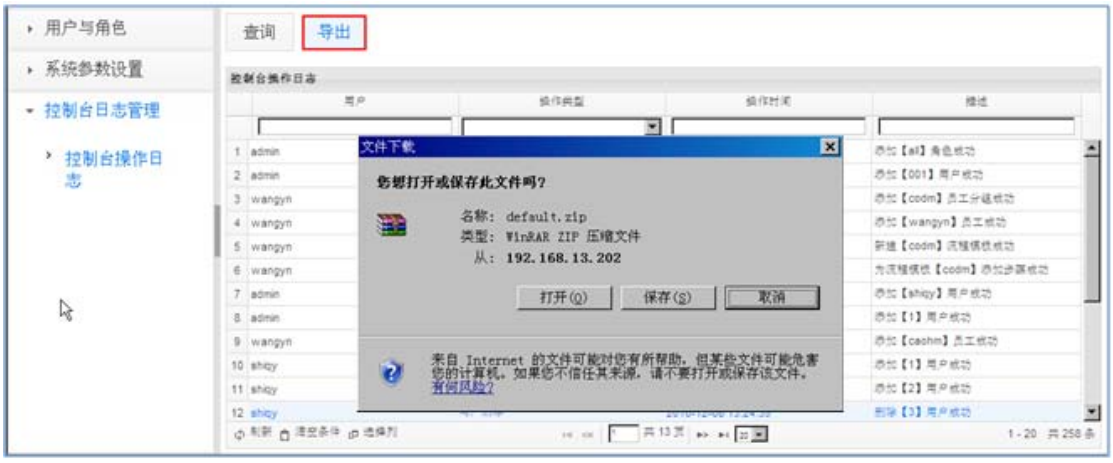


图 2-23　导出保存操作日志信息

6. 单击列表下方的“清空条件”，可以清除所有查询条件，列表中分页显示所有控制台操作日志记录，如图 2-24 所示。

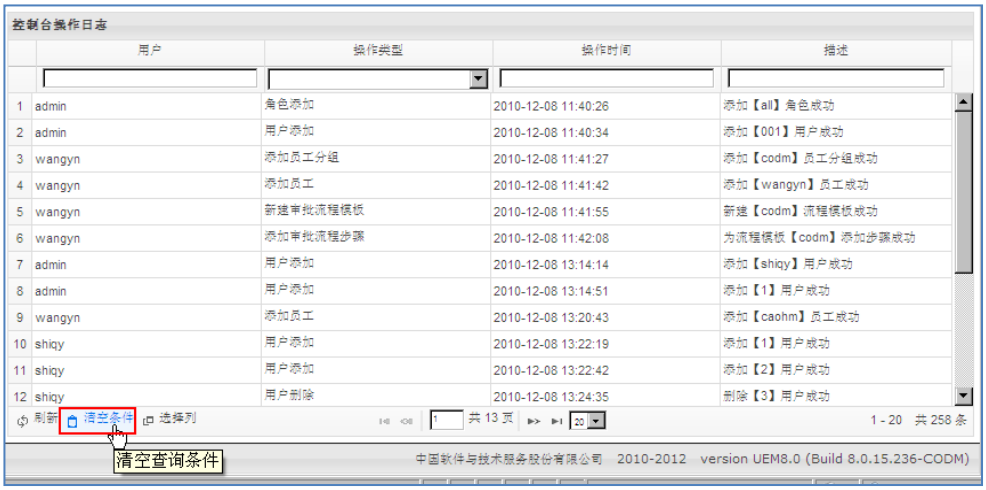


图 2-24　清空条件显示所有操作日志

7. 单击列表下方的“选择列”，弹出“选择列”界面，如图 2-25 所示。单击“+”号添加显示列，单击“一”号删除显示列。用户可以按个人喜好选择列表中显示的列，把不需要的列表项去掉不显示。

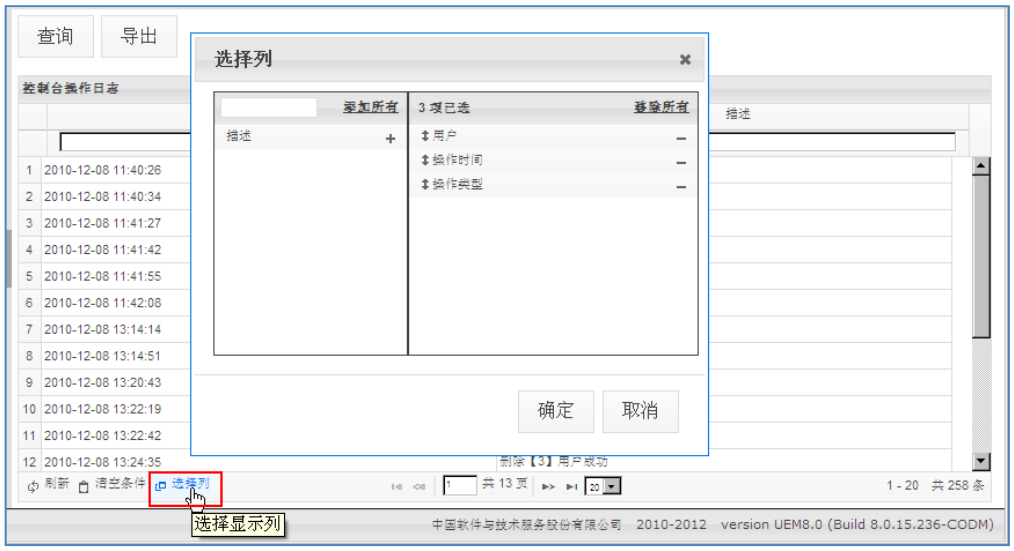


图 2-25　选择日志信息显示列

2.2 审批管理

2.2.1 员工管理

◆ 分组管理

审批系统的员工具有特殊的含义，它是登录审批系统工作台，申请、制作授权文件，或具有一定审批权限的特殊身份的用户。我们将员工分为不同的组，不同的组应用不同的审批流程，这样将员工进行群组化管理。新建的员工，如果属于某个员工分组，它就自动具有这个组的审批流程。

1. 在菜单栏单击“审批管理”，在左侧导航栏中单击“员工管理”，进入员工管理界面，如图 2-26 所示。系统没有内置的员工分组，用户需要自行添加。

图 2-26　员工管理界面

2. 单击上方的“添加”按钮，弹出“添加分组”界面，如图 2-27 所示。输入分组名称和备注信息。员工分组名称支持汉字、字母、数字、下划线，最长为 20 字符。如果该分组的员工需要有授权文件的审批任务，就要为该组员工应用一定的审批流程，参见审批流程管理章节。

图 2-27　添加员工分组

3. 单击“确定”按钮，提示“添加员工分组”成功。在员工分组列表中，将看到新添加的分组，如图 2-28 所示。根据实际需要，用户可添加多个分组。

图 2-28　显示添加的员工分组

4. 在员工分组列表中，选择某分组，单击上方的“修改”按钮，弹出“修改分组”界面，如图 2-29 所示。可以修改备注信息，不超过 50 个字符，但不能修改分组名称。

图 2-29　修改分组信息

5. 在员工分组列表中，选择某分组，单击上方的“删除”按钮，出现删除分组确认框，如图 2-30 所示。删除指定分组时，可以直接删除该分组下的所有员工，也可以将该分组下的员工迁移到新的分组，并自动应用新分组的审批流程。

直接删除该分组下的员工信息时，如果该分组下的员工有审批请求或者审批任务没有完成，则提示删除分组失败；将分组下的员工迁移到新分组时，如果该分组下的员工还有未完成的审批任务，则继续原来的审批任务，新建的申请单才执行新分组的审批流程。

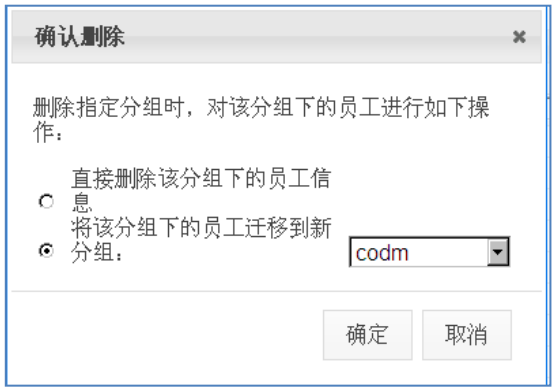


图 2-30　删除分组信息

◆ **员工信息**

1. 在组织结构树上选择某分组，单击上方的“添加员工”按钮，弹出“添加员工”界面，如图 2-31 所示。系统没有内置的员工帐号，管理员需要自行添加。这里添加的员工帐号，是登录安全文档外发工作台和审批工作台的帐号，请用户记好。参见安全文档审批工作台章节。

员工编号、员工帐号和真实名为必添项，支持字母、数字、下划线(真实名也可以是汉字)，最长为 20 字符，默认密码 1234567a。选择所属分组，将自动应用该分组的审批流程。参见审批流程管理章节。

图 2-31　添加员工界面

2. 单击“确定”按钮，提示“添加员工”成功。在员工列表中，将看到新添加的员工，如图 2-32 所示。根据实际需要，用户可添加多个员工。

图 2-32　显示添加的员工信息

3. 在员工列表中，选择某员工信息，单击上方的“修改”按钮，弹出“修改员工”界面，如图 2-33 所示。可以修改员工所属分组和真实名，员工帐号和员工编号是不能修改。如果用户修改了员工所属的分组，它将自动应用新分组的审批流程，执行新分组文档授权的审批规则。

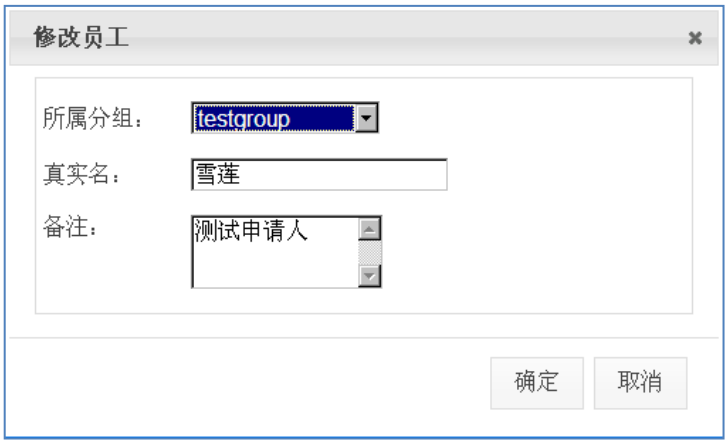


图 2-33　修改员工信息

4. 在员工列表中，选择某员工，单击上方的“删除”按钮，出现删除员工确认框，确定后即可删除，如图 2-34 所示。删除指定员工时，如果该员工有审批请求或者审批任务没有完成，则不能删除。

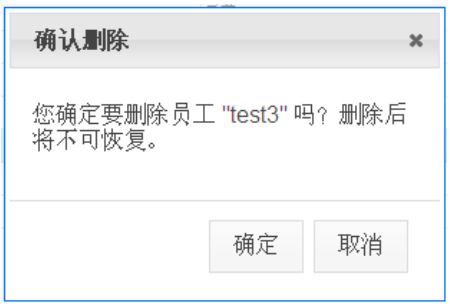


图 2-34　删除员工帐号

5. 新建的员工帐号可以登录安全文档外发工作台，初始密码为 1234567a，登录后可及时更改。如果用户遗忘了修改后的密码，可以申请系统管理员在这里重置密码。在员工列表中选择某员工，单击“重置密码”按钮，如图 2-35 所示。确定后，即可将该员工的密码重置为默认的 1234567a。

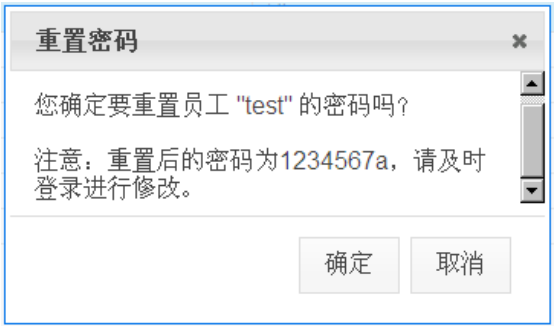


图 2-35　重置员工密码

6. 为了操作方便，我们可以将整个 UEM 数据库同步过来，省去一个个添加帐号的麻烦，如图 2-36 所示。如果 UEM 系统是多个服务器级联，同步多个数据 UEM 数据库时可能会出状况，建议只同步一个 UEM 数据库。

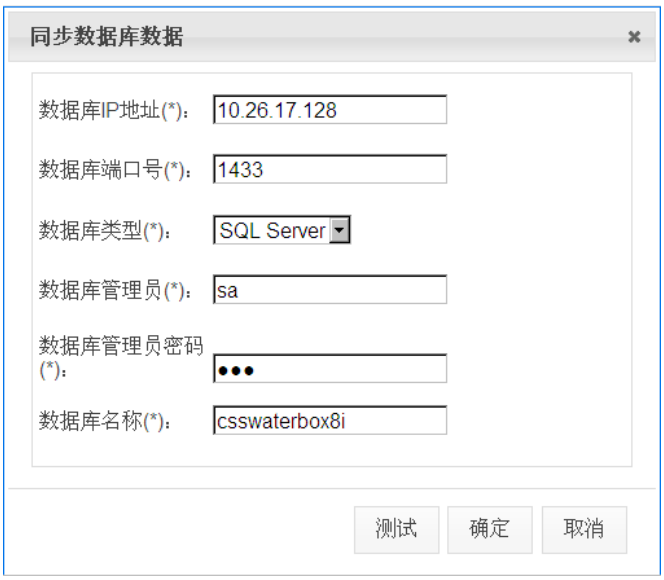


图 2-36　同步数据库

2.2.2 审批流程

SecDocAP 系统制作审批文件包时，需要有一定的审批程序。不同部门的带出文档都由谁来审批，中间有经过几个环节，这由审批规则确定。在实际使用过程中，我们首先建立审批流程模板，然后应用于不同的分组，使不同的分组都有自己的审批流程。

2.2.2.1 流程模板设置

1. 在菜单栏单击“文档审批”，在左侧导航栏中单击“审批流程管理”→“流程模板设置”，进入模板管理界面，如图 2-37 所示。系统没有内置的模板，需要由用户建立。

图 2-37　审批流程模板界面

2. 单击“新建模板”按钮，出现“新建流程模板”界面。输入模板名称，支持字母、数字和下划线，长度为 20 字符，如图 2-38 所示。确定后，将在右侧看到新添加的模板，系统提示“当前流程模板没有审批步骤！”

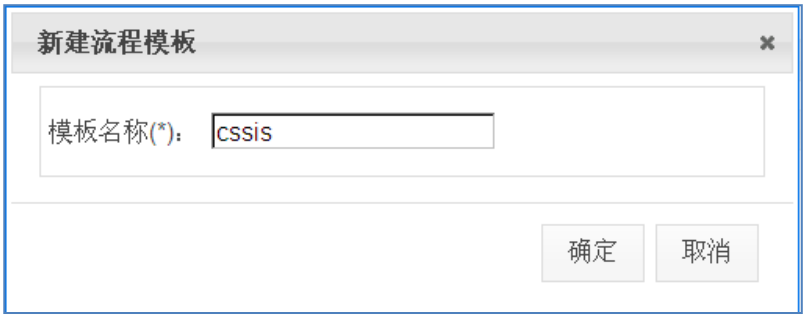


图 2-38　新建流程模板

3. 单击“添加步骤”按钮，输入步骤名称，选择审批方式。从组织结构树中选择员工，添加到右侧审批员列表中，同一步骤的多个审批员没有先后次序之分。然后，单击“确定”按钮，完成该步骤的添加。按照同样方法，可添加多个审批步骤，如图 2-39 所示。

审批方式有三种：全部审批通过才通过、多数人审批通过就通过、只要有一个审批通过就通过。

全部审批通过才通过：是指全部人员审批通过才通过，只要有一个拒绝就拒绝。
只要有一个审批通过就通过：是指只要有一个审批通过就算通过，全部拒绝才算拒绝。
多数人审批通过就通过：是指等于或大于过半人审批通过就通过，大于过半人拒绝就拒绝。

图 2-39　添加审批步骤

4. 返回流程模板界面，可以看到添加的审批流程，如图 2-40 所示。审批过程中任何一个步骤出现拒绝，就会将申请单打回到草稿状态。申请人可以查看拒绝理由，修改后再次提交。详见我的申请单章节。

图 2-40　新建的审批流程

5. 如果用户对某个审批步骤不满意，可以选择该步骤，单击“修改步骤”按钮，在修改界面中进行修改，如图 2-41 所示。修改完成后，单击“确定”按钮保存。

图 2-41　修改审批步骤

6. 如果用户感到某个审批步骤不需要，可以选择该步骤，单击“删除步骤”按钮，将其步骤删除，如图 2-42 所示。

图 2-42　删除审批步骤

7. 这样通过添加、修改、删除等操作建立一个完善的审批流程模板，用户可用之制作模板副本。在右侧选择已建立的审批模板，单击上方的“制作模板副本”按钮，输入副本名称，确定后保存，如图 2-43 所示。用户可将副本流程稍做修改，应用于相似的审批过程，加快模板的建立速度。

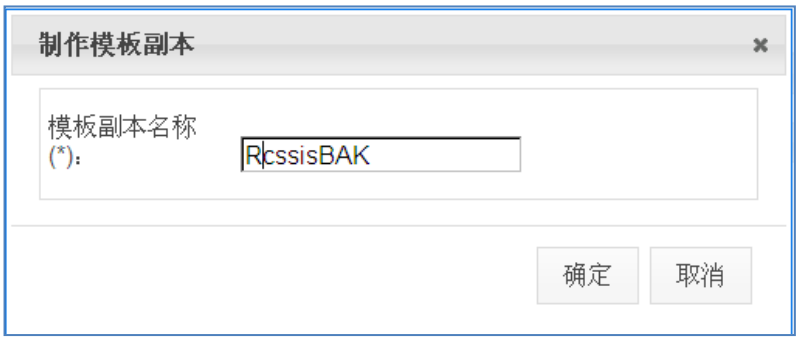


图 2-43　制作模板副本

2.2.2.2 审批流程配置

1. 在菜单栏单击“文档审批”，在左侧导航栏中单击“审批流程管理”→“审批流程配置”，进入员工分组流程界面，如图 2-44 所示。在右侧组织结构中选择员工分组，如果该分组还没有应用过审批流程模板，会提示“当前分组上没有审批流程!”

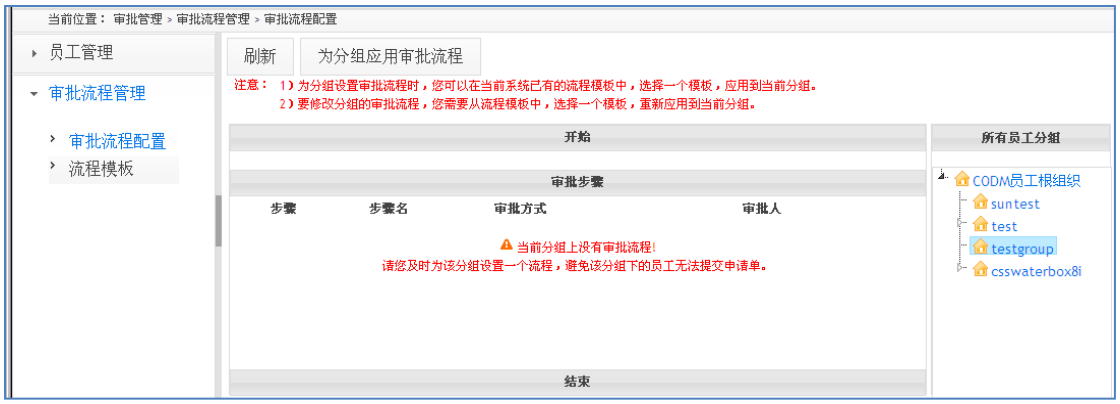


图 2-44　审批流程管理界面

2. 单击上方的“为分组应用审批流程”按钮，弹出为“员工分组应用审批流程”界面，如图 2-45 所示。从下拉框中选择待应用的审批流程模板，确定后，将之应用于所选的员工分组，该分组人员将自动执行模板所规定的审批流程。

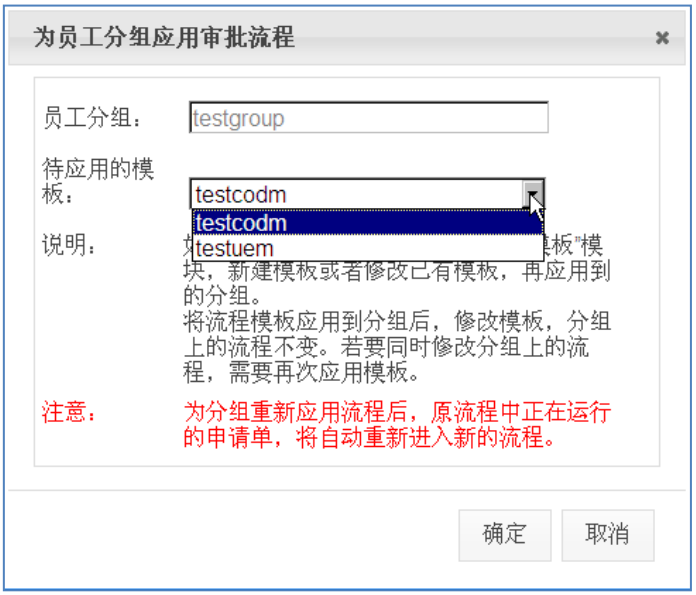


图 2-45　为员工分组应用审批流程

如果更换分组流程模板（或者修改模板后重新应用），该分组将执行新模板的审批流程。正在执行的审批任务将终止执行，打回到申请人的草稿状态，须申请人重新提交后，走新模板的审批流程。如果只在流程模板中更改模板，没有重新应用于使用该模板的分组，分组还是原来的审批流程不变。

流程模板的应用是以分组为单位的，同一分组的员工具有相同的审批流程，可能出现申请人也是审批员的现象。

3. 设置流程成功后，将看到所选员工分组的审批流程，如图 2-46 所示。

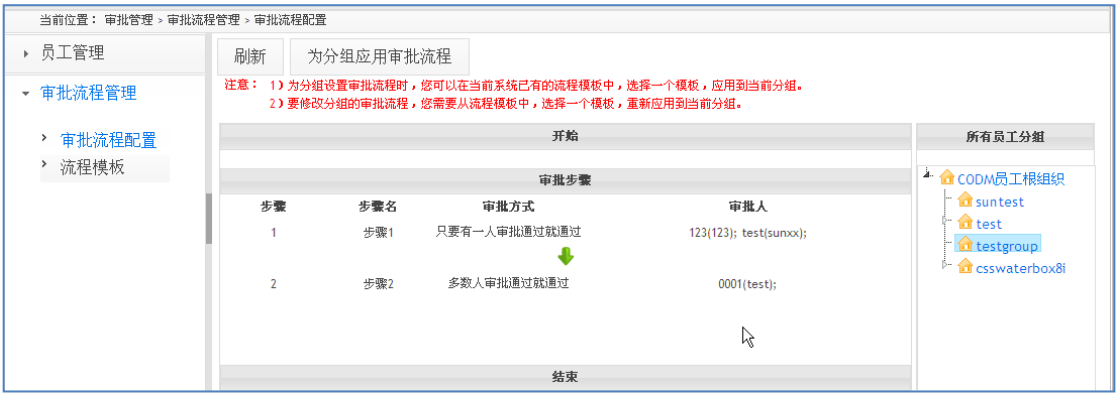


图 2-46　为员工分工设置的审批流程

2.3 权限管理

2.3.1 在线审批日志

1. 在菜单栏单击“权限管理”，在左侧导航栏中单击“日志管理”→“在线审批日志”，进入在线授权审批日志界面，如图 2-47 所示。在线授权审批日志列表中，显示授权文件的名称、标识、类型、申请人、申请时间、审批人、审批时间、审批结果等信息，请用户查看。

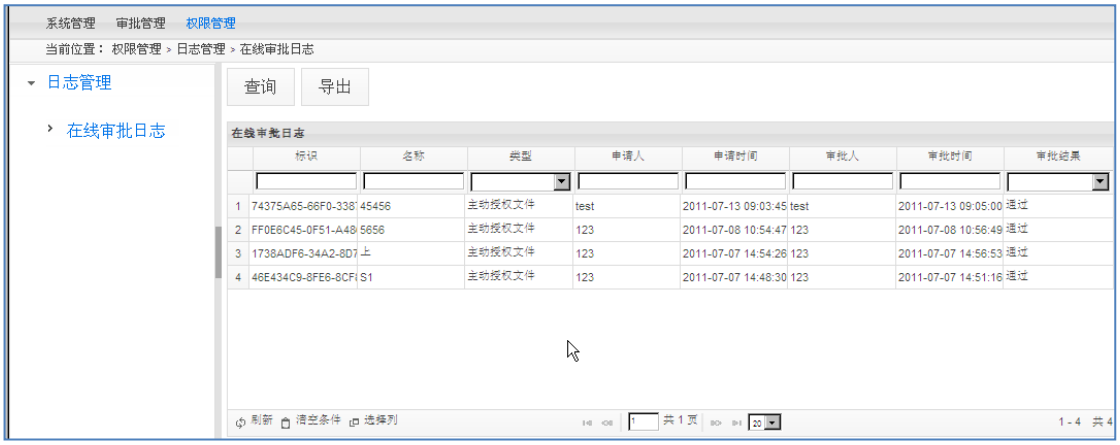


图 2-47　审批包在线审批日志

2. 单击列表项下面的空白框，输入查询条件，单击“查询”按钮或回车键，可以实现按条件查询，如图 2-48 所示。例如：在申请人下方输入“123”，可以看到该申请人所有在线审批日志。单击下方的“清空条件”，将重新显示所有在线授权审批日志。

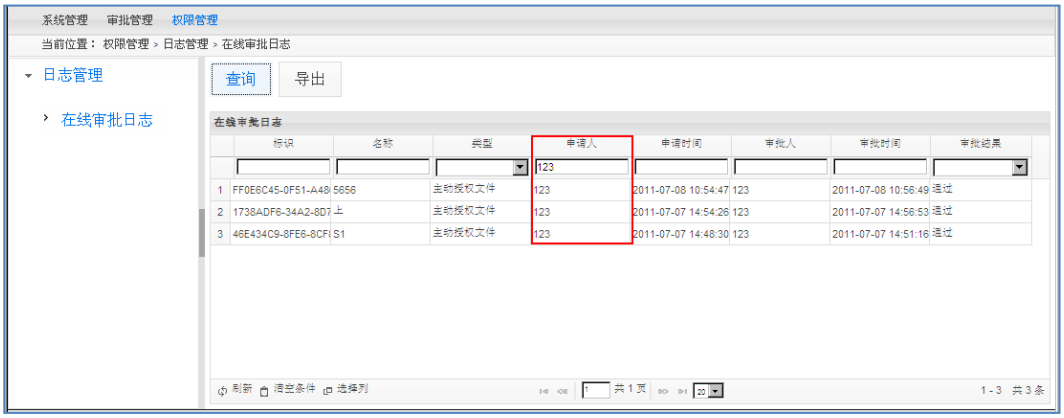


图 2-48　按条件查询在线授权审批日志

3. 单击列表下方的“选择列”，弹出“选择列”界面，如图 2-49 所示。单击“+”号添加显示列，单击“一”号 删除显示列。用户可以按个人喜好选择列表中显示的列，把不需要的列表项去掉不显示。

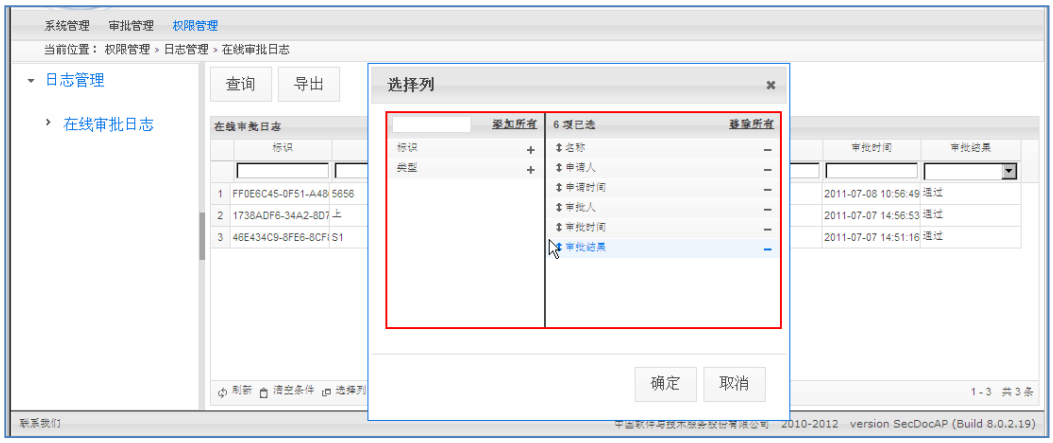


图 2-49　选择列表显示列

4. 单击“导出”按钮，可以将审批包使用日志信息导出保存为*.zip 文件(默认 default.zip),如图 2-50 所示。

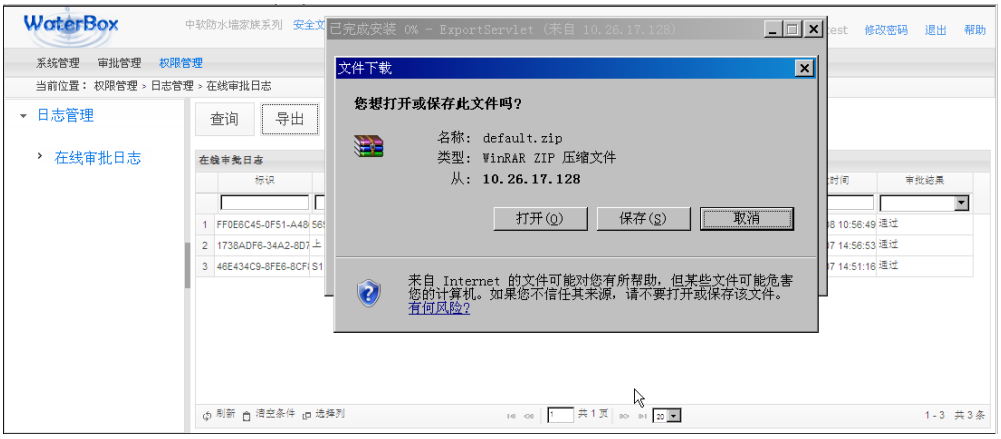


图 2-50　导出审批包在线审批日志

第三章　安全文档审批工作台

安全文档审批工作台是员工建立申请单、审批申请单、制作审批包和下载文件包的地方，是员工工作的中心。在使用过程中，员工首先要建立申请单，提交给服务器后，由员工组审批流程规定的人员来审批。审批全部通过后，才允许申请人制作授权文件包，最后由申请人下载，供使用范围的人打开使用。下面按使用顺序，介绍这部分功能。

3.1 登录工作台

在浏览器地址栏中输入 http://192.168.17.128:8086/SecDoc（其中 192.168.17.128 为审批服务器 IP 地址），即可转到审批控制台登录界面，如图 3-1 所示。以系统管理中建立的员工帐户（参见员工帐户管理）登录文档审批工作台。

提示：对于主动授权文件在线审批，可以直接通过右键菜单的“在线授权”自动登录工作台。

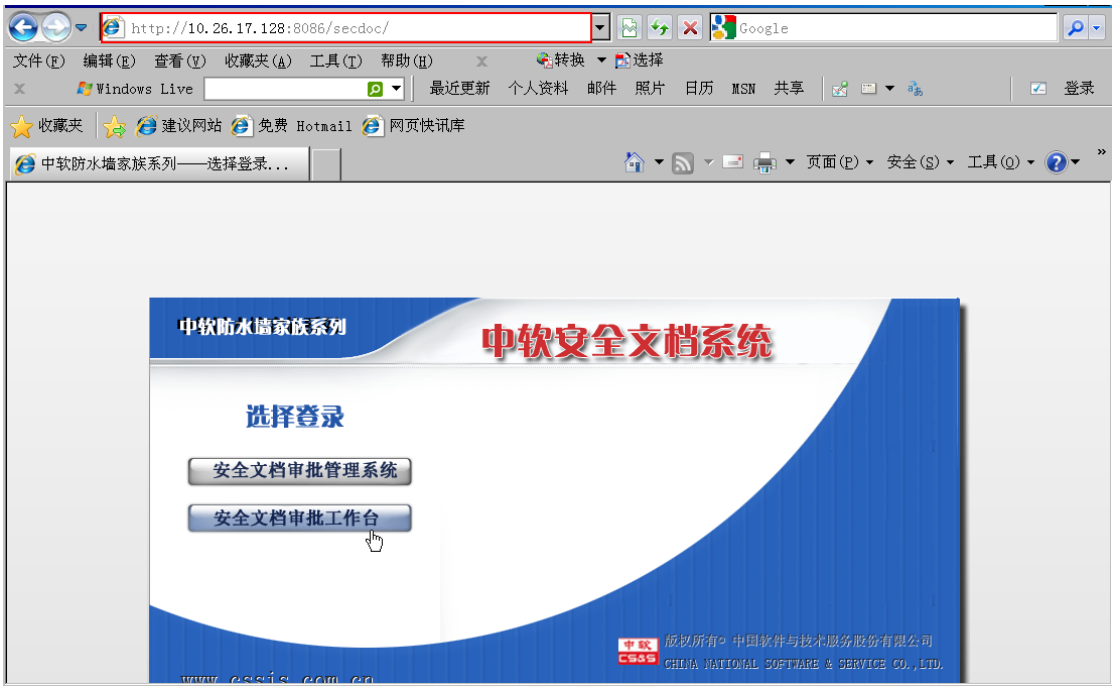


图 3-1　安全文档审批工作台登录界面

3.2 我的申请单

1. 员工登录工作台后，系统默认进入“我的申请单”界面，显示建立的申请单列表信息，如图 3-2 所示。

图 3-2　我的申请单界面

2. 单击上方“新建”按钮，弹出“新建申请单”界面，如图 3-3 所示。从下拉框中选择申请类型——主动授权文件，输入申请单名称。单击“确定”按钮，进入下面我的申请单设置界面。

图 3-3　新建申请单

3. 在我的申请单“基本信息”页面，输入申请原因和文件包描述，如图 3-4 所示。

图 3-4　基本信息

4. 在我的申请单“包内文件”页面，单击“浏览”按钮，上传.zip 包或单个文件。上传完成后，在下方列表框中展示已上传的文件，如图 3-5 所示。

图 3-5　上传包内文件

上传文件支持 zip 文件类型，我们需要事先把要上传的文件或目录压缩成 zip 包，文件最大不要超过 4G。也可选择单个文件，不需要压缩，逐个追加上传。但无论采用哪种方式上传文件，上传的文件类型必须是隔离文件或非隔离文件。非隔离文件包括普通文件和普通安全文档，不包括密级文件、授权文件和用“我的加密文件夹”加密的文件。

如果错传文件了，可以在下方文件列表框中单选或多选错文件，单击“删除文件”按钮，将其删除；也可重新上传一次 zip 包，覆盖上次上传的文件。

5. 在我的申请单“基础权限”页面，设置权限信息，如图 3-6 所示。设置完成后，注意单击“保存”按钮，保存当前权限信息。系统对权限信息具有记忆功能，下次新建申请单设置权限时，会自动调用上次保存的权限信息。

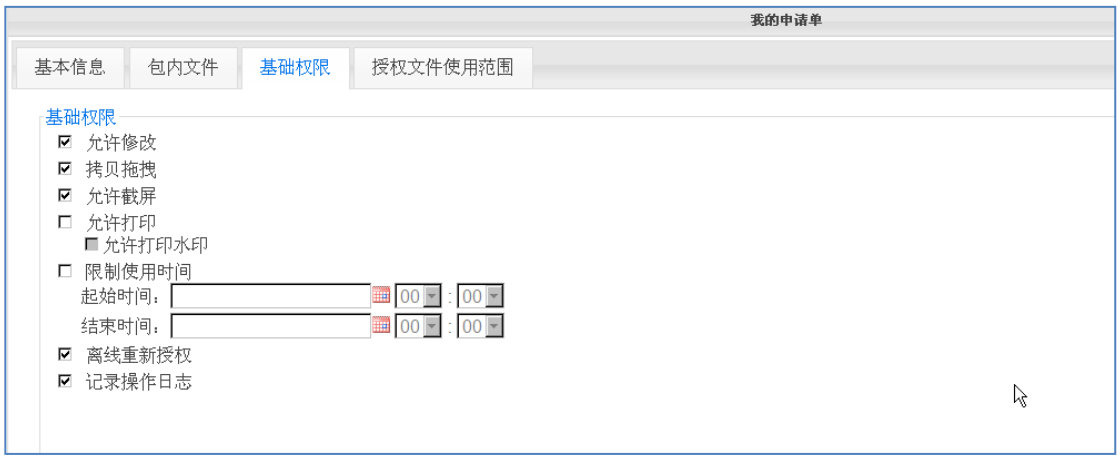


图 3-6　设置基础权限

权限设置说明：

不允许修改，是指使用人修改后无法保存。

允许拷贝拖拽，是指只允许将拷贝内容复制到加密进程控制的文件中。

允许截屏，是指允许使用截屏键，且只允许将截屏后的内容拷贝到加密进程控制的文件中，但不能将截屏内容拷贝到非加密进程控制的文件中。

打印水印，是指打印控制台“主动授权控制”中设置的水印内容。

使用时间，“起始时间”和“结束时间”一样时，有效时间是指该天的 00：00—23：59。

离线重新授权，是指制作人和使用范围内的用户有对该主动授权文件进行重新授权的权利。

记录操作日志，是指记录客户端用户使用该授权文件的日志，并将日志信息上传到控制台统计审计分析的“安全文档”→“主动授权文件使用日志”中。

6. 选择授权文件的使用范围，如图 3-7 所示。这样，只能使用范围内的用户才能打开使用授权文件，这些用户必须是 UEM 客户端。

图 3-7　授权文件的使用范围

7. 各页面设置完成后，没有提交前，都属于草稿状态，申请人可以检查修改各项设置。等确认无误后，再单击“提交”按钮提交申请单，如图 3-8 所示。申请单提交后，就不能再修改。

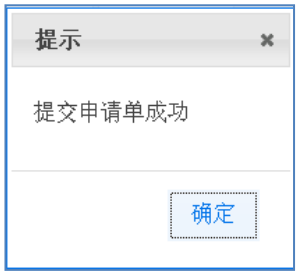


图 3-8　提交申请单

3.3 申请单的审批过程

申请单提交后就进入审批流程，具体有哪些人来审批，中间要经过几个步骤，这是有申请人所在的员工组决定的。不同的员工组，审批流程也可能不同，参见流程模板设置和审批流程配置章节。

例如：我们添加的员工帐号 sunxx 属于 suntest 组，就要遵从 suntest 组的审批规则。sunxx 提交的每个申请单，都需要两个步骤，两个人（123、test）来审批，如图 3-9 所示。

图 3-9　员工所在的审批流程

1. 以第一步骤的审批员帐户(123)登录文档审批工作台，在“待审批的申请单”中将看到待审批的单子，如图 3-10 所示。

图 3-10　待审批的申请单

2. 在“待审批的申请单列表”中选择某申请单，单击上方的“审批”按钮，查看申请单基本信息、权限信息、包内文件等详细信息，如图 3-11 所示。审批员可以在包内文件列表中选择某一文件，单击“查看文件”按钮，将文件打开或下载到本地查看详细内容。

图 3-11　查看申请单详细内容

3. 审批员查看申请单详细内容后，确定该申请单可以通过，就单击“审批通过”按钮，如图 3-12 所示。审批通过后，该申请单自动从“待审批的申请单”中消失，添加到“已审批的申请单”列表中，审批员可逐条查看详情。

图 3-12　第一个审批员审批通过申请单

4. 按照审批流程，第二内审批员（test）登录文档审批工作台，详细查看申请单内容后，点击“审批通过”，如图 3-13 所示。

两个审批员是同一步骤的两个审批人，他们的审批过程没有先后次序之分。如果多个审批员是不同步骤的审批人，必须在前面步骤的审批员审批完成后，申请单才能流转给后面的审批员。

图 3-13　第二个审批员审批通过申请单

5. 如果审批全部完成后，申请人将在“我的申请单”列表中，看到已审批通过的申请单后面出现“制作”按钮。单击“制作”按钮，完成审批包的制作，如图 3-14 所示。

提示：审批包制作完成后，转入“我的文件包”，申请人可自行下载使用。

图 3-14　制作审批包

6. 还有一种情况，介绍一下：如果在审批过程中，审批员查看申请单详细内容后不同意，可以上方单击“审批拒绝”按钮，填写拒绝理由，如图 3-15 所示。申请单在审批过程中，任何步骤遭到拒绝，都会打回到申请人的初始草稿状态。

图 3-15　审批员拒绝申请单

7. 申请人的登录工作台，在“我的申请单”中能够看到审批拒绝的申请单，如图 3-16 所示。单击查看拒绝理由，修改后可再次提交。

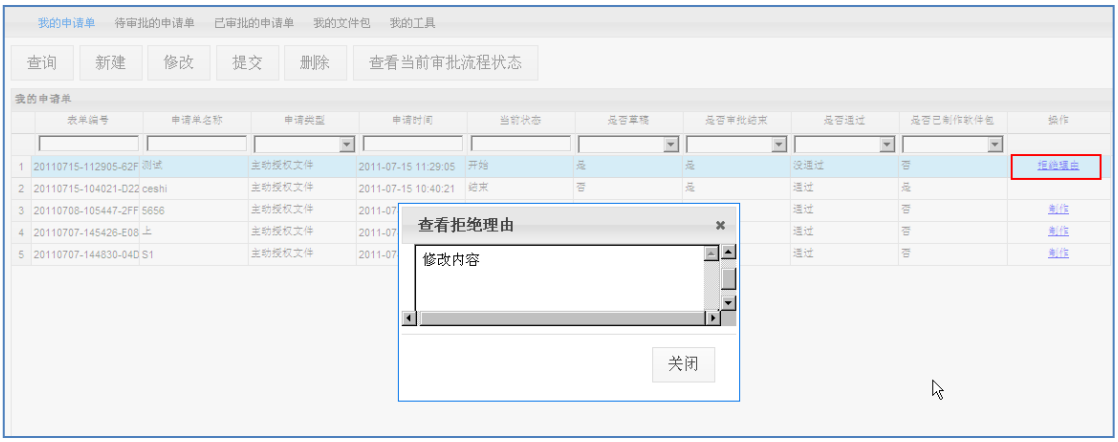


图 3-16　申请人查看拒绝的申请单

8.如果在审批过程中，系统管理员修改了申请人所在组的审批流程，那么该组所有人提交的申请单都无法继续原来的审批流程，将被打回到申请人原始的草稿状态，如图 3-17 所示。申请人需要再次提交申请单，才能按新的审批流程进行审批。

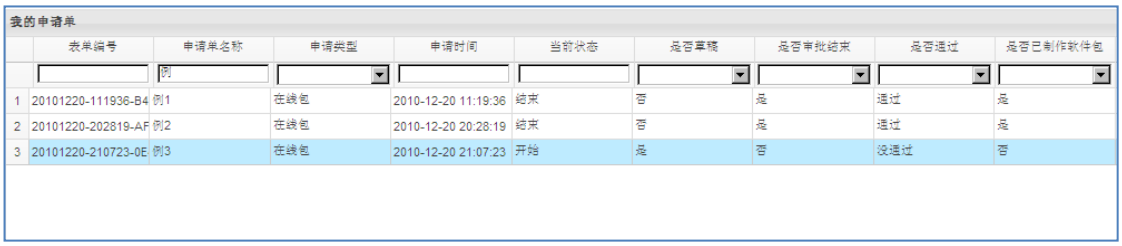


图 3-17　改变审批流程后需再次提交申请单

3.4 我的审批包

1. 审批包制作成功后，申请人在“我的文件包”列表中能够看到可下载使用的文件包，如图 3-18 所示。

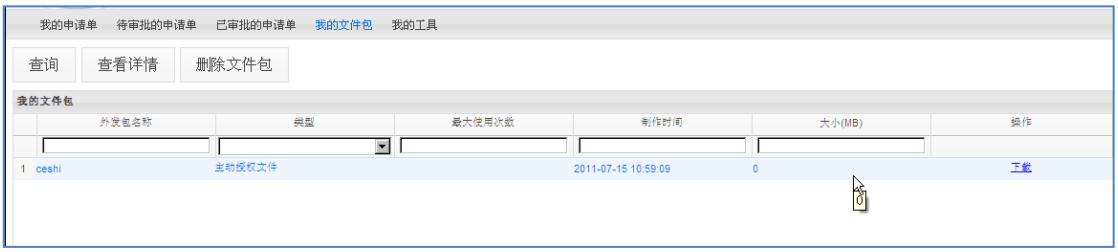


图 3-18　我的文件包列表

2. 选择某文件包，单击后面的“下载”链接，申请人可以将文件包下载，如图 3-19 所示。文件包内的授权文件由权限限制，可以由使用范围内的人打开使用。

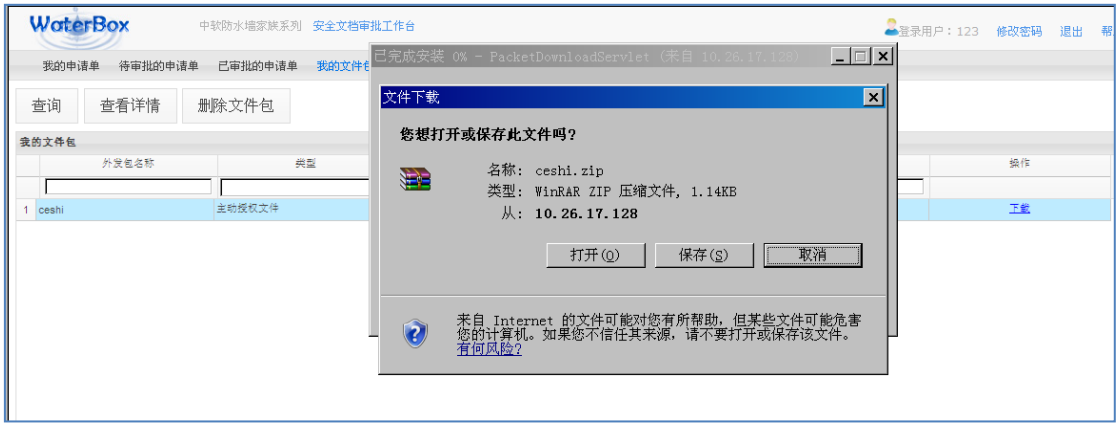


图 3-19　下载我的文件包

3. 申请人下载文件包不受时间和次数限制，如果某些文件包已经不再需要了，可以选择这些文件包，单击“删除文件包”按钮，将其删除，如图 3-20 所示。

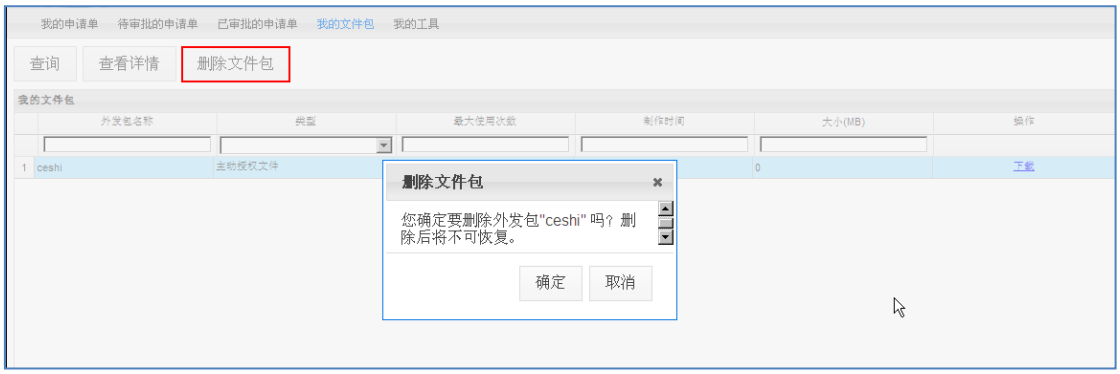


图 3-20　删除文件包

附件四：

基于 WEB 页面的客户端自动检测与安装

UEM 系统可以将检测脚本集成到企业的办公系统中，用户在访问 OA 主页的时自动检查是否安装了客户端，如果没有安装，自动从指定服务器下载安装包，并实施安装。客户端安装成功后才能访问 OA 主页，否则不能正常访问。

一．配置检测文件

将安装包中 UEM 系统文件：test.jsp 、checkuemclient.cab、SPInstall.exe（客户端安装文件）拷贝到 OA 网站的根目录下，对 test.jsp 文件进行配置，更名为网站主页文件。具体步骤如下：

假设网站的网址为 192.168.16.171，网站的首页源文件名称为 index.jsp，需要进行 UEM 客户端检测的网段为“192.168.*.*”，客户端安装包为 SPInstall.exe。安装包支持 exe 格式和 msi 格式，如果不是该名称的，请修改成对应的名称。

配置方法：

（1）打开 test.jsp 文件，修改第 6 行到第 8 行为：

String checkIPRange = "192.168";
String ipStart = "\""+"192.168.0.0"+"\"";
String ipEnd = "\""+"192.168.255.255"+"\"";

将红色部分的值改为网站监控网段的具体值

（2）修改 test.jsp 文件的第 9 行：

String UEMpackName = "SPInstall.exe";

将红色部分的值改为客户安装包真正的名称。

（3）将网站首页源文件 index.jsp 改名为其他名称，例如改为 homepage.jsp（新名称）

（4）修改 test.jsp 文件的第 10 行：

将 String homePage = "realmain.jsp";**改为** String homePage = "homepage.jsp";

引号中的名称改为网站首页新名称（homepage.jsp）

（5）修改 test.jsp 的名称为 index.jsp（网站的首页源文件名称），作为网站的新入口。

网站主页经过上面检测配置后，如果用户计算机处于 UEM 客户端检测的网段之外，访问监控网站时不做控制，直接转向网站主页；如果用户计算机处于 UEM 客户端检测的网段之内，那么用户访问监控网站时要提示安装 ActiveX 插件，进行 UEM 客户端的安装，否则不能访问网站主页的内容。

二．安装 ActiveX 插件

（1）访问网站，在地址中输入网址(http://192.168.16.171:8080)， 出现以下界面，如图 1 所示。点击出现的停止提示横条，选择安装 ActiveX。

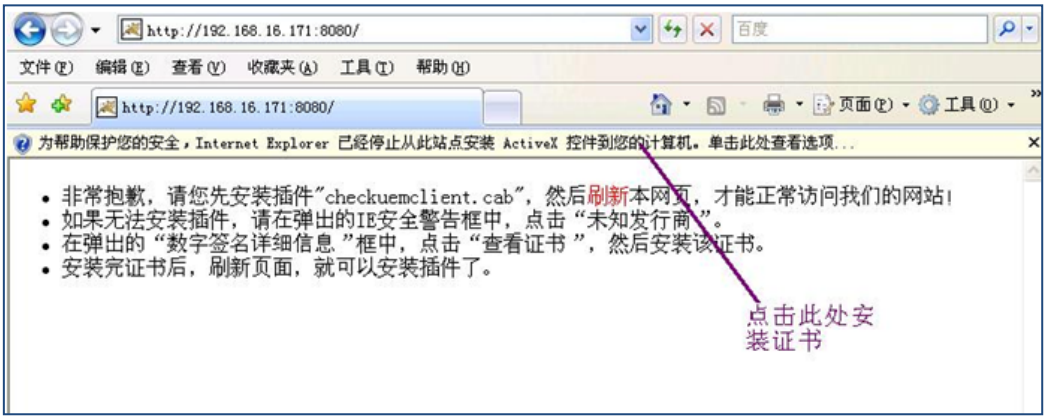


图 1　浏览网站出现停止条

（2）在如图 2 所示的界面中，点击“确定”是没有反应的，需要点击“未知发行商”。

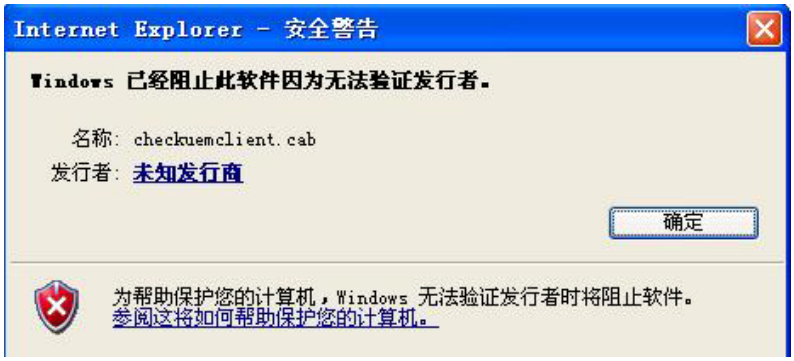


图 2　点击未知发行商

（3）然后，点击查看证书、安装证书，如图 3、4 所示。

图 3　查看证书

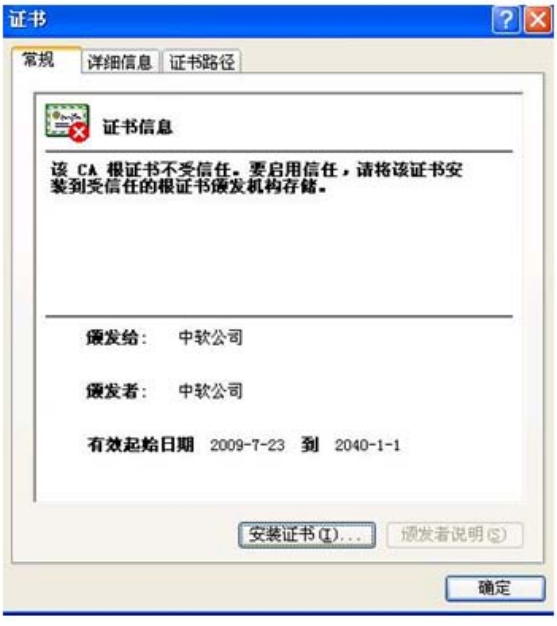


图 4　安装证书

（4）安装证书结束后，刷新页面，再次单击安装提示横条，如图 5 所示。

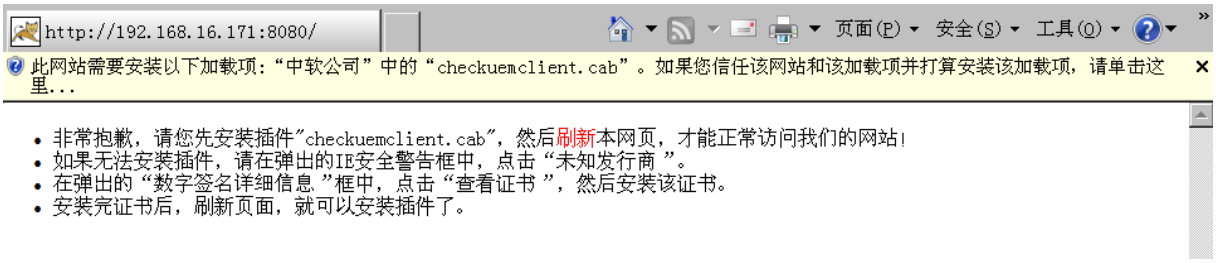


图 5　安装证书后刷新页面

（5） 选择“安装”，如图 6 所示。再次刷新后，点击“这里”下载客户端，如图 7 所示。

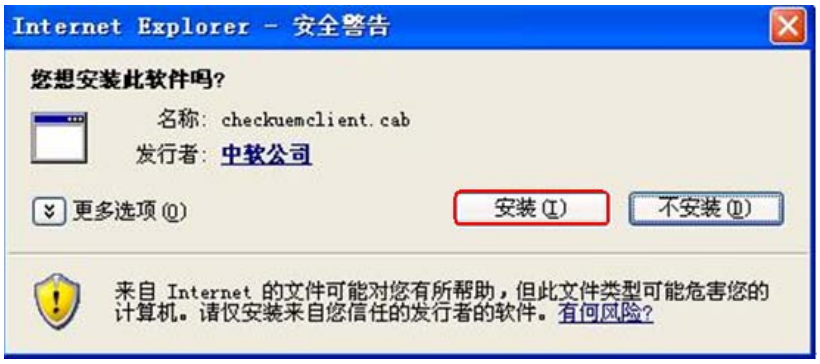


图 6　安装客户端

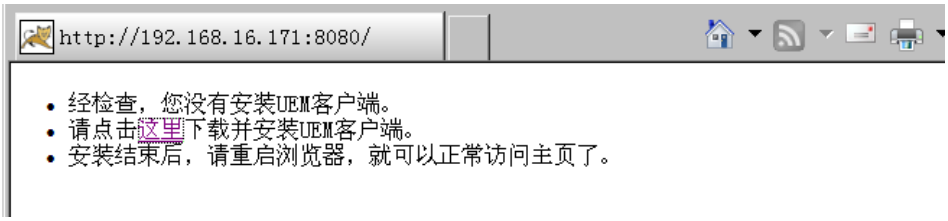


图 7　点击这里下载安装包

（6）客户端安装结束后，以后访问网站就可以不受控制，进入正常的主页啦！

附件五：

名 词 解 释

UEM8.0：中软统一终端安全管理系统 8.0 的英文简称，英文全称是：CSS United End-point System management 8.0，简称为 UEM8.0。

Windows 系统日志：是指 Windows 操作系统本身纪录的日志,主要有三类：应用程序、系统、安全；向系统所发送的日志的类型分为：信息、警告、错误、成功审计、审计失败。

第二块网卡：除去与服务器通信的网卡之外的所有其他网卡，我们都统称为第二块网卡。

软件黑名单：非法软件的关键字列表。给客户端应用软件开放策略时，可附加一份黑名单，黑名单中列出的软件将被禁止安装和使用。

软件白名单：合法软件的关键字列表，给客户端应用软件禁止策略时，可附加一份白名单，只有白名单中列出的软件才可安装和使用。

软件基线：是软件安装的一个标准，规定客户端只能安装基线列表中的列出的软件，多了或少了都将报警。

MAC 地址：MAC 地址也叫物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。IP 地址与 MAC 地址在计算机里都是以二进制表示的，IP 地址是 32 位的，而 MAC 地址则是 48 位的，如：08:00:20:0A:8C:6D 就是一个 MAC 地址。只要你不去更改自己的 MAC 地址，那么你的 MAC 地址在世界上是唯一。

日志上传：是指将客户端生成的操作日志上传到服务器，服务器把上传的日志信息分类保存到数据库中，用户可以在控制台的统计审计分析中查看。

时间同步：客户端本地时间与服务器本地时间保持一致。可以在系统参数中设置时间同步的最小误差和频率。

心跳信号：客户端向服务器定时发送的连接信号，如果服务器在规定的时间段内收不到客户端发来的连接信号，则判定客户端离线。

MSI 类型：软件分发包中的主执行文件，是 Microsoft Windows Installer 类型的文件。

静默安装：静默安装表示软件包在后台执行安装，不需与用户交互。

交互安装：软件分发安装类型是交互安装，表示分发软件包时安装程序会弹出安装界面，用户可根据交互安装界面提示进行安装。

最大连接数：指系统能建立的 TCP 连接的最大数目。

最大并发连接数：在单位时间内系统能创建 TCP 连接的最大数目。

默认策略是针对新注册的计算机或者用户，在管理员没有给其特别设置策略的情况下，由系

统默认执行的一套策略。该策略在计算机或用户第一次上线时，由客户端从服务器获取并执行。

在线策略是客户端主机和服务器通讯正常情况下运行的有效策略集，它通过控制台配置、修改下发。在线策略可分为两类：基本策略和时间段策略。主机在线的情况下，默认会执行基本策略；如果管理员设定了时间段策略，则在生效的时间段内优先执行时间段策略。基本策略是管理员必须配置的策略，时间段策略依据需求，可以配置也可以不配置。

离线策略是客户端的备用策略，由控制台配置并下发，正常情况下不会生效。当客户端一旦与服务器之间的网络通讯断开了，则立即启用离线策略。通常离线策略相当严格，以保护客户端主机的安全。

WSUS：Windows Server Update Service 即微软的补丁服务器。通过使用 Windows Server 更新服务 (WSUS)，管理员可以快速而可靠地将 Windows 操作系统和应用程序及时更新，修复系统漏洞，获取最新功能。

可信终端：安装了可信移动存储系统客户端的主机称为可信终端。没有安装可信移动存储系统客户端的主机称为普通终端。

普通移动存储介质：未经可信移动存储管理系统授权的移动存储介质，称为普通移动存储介质，简称普通磁盘。

可信移动存储介质：经过可信移动存储管理系统授权的移动存储介质，包括 USB 设备、软盘等移动存储设备，简称可信磁盘。依据授权类型的不同，可以将可信移动存储介质分为支持商旅模式和不支持商旅模式两类。支持商旅模式的可信移动存储介质有两种状态：可信状态和商旅状态；不支持商旅模式的可信移动存储器永远处于可信状态。处于商旅状态的可信磁盘允许在普通终端自由使用，用于在可信终端与普通终端之间进行数据的交换。

商旅移动存储介质：处于商旅状态的可信移动存储介质，称为商旅移动存储介质。该介质在可信终端上只能读取该介质上的内容，不可以往该介质中写入任何数据。在普通终端上正常加载后，可以进行读写操作。

激活：将移动存储介质由可信状态转换为商旅状态的过程，称为激活。反之，将商旅状态转换为可信状态的过程，称之为反激活。

计算机密级标识：为涉密计算机设定的安全级别，安全级别包括普通、秘密、机密和绝密。

移动存储介质密级标识：在对移动存储介质进行授权的过程中，会给其设定一定的安全级别，用以说明该介质的涉密安全程度。涉密介质的安全级别包括普通、秘密、机密和绝密。

锁定：可信移动存储介质在违反规定使用时的一种处理方式，被锁定的可信移动存储介质将被限制使用，需解锁后方可在安全工作域内使用。

自毁：可信移动存储介质在违反规定使用时的一种处理方式，被自毁的可信移动存储介质上的数据将被随机数所填充，存储在该介质上的文件数据将不可被恢复。

域帐户：域帐户是指域服务器中的帐户，使用域帐户可以登录到该帐户设定范围内的任意计算机。

同步域帐户：同步域帐户是指当 UEM 服务器设置为跟域服务器同步时，UEM 服务器首先获取域服务器“Active Directory”中的由用户建立的组织单位和用户帐号，并对其进行监控，即每当这些组织单位和用户帐号改变时，UEM 服务器中的组织结构也会发生相应的改变。

网络接入认证：UEM 的网络接入认证是指 802.1x 协议认证。其基于 Client/Server 的访问控制和认证协议。它可以限制未经授权的用户或设备通过接入端口访问网络。在认证通过之前，802.1x 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

策略集：策略集是指针对特定范围对象（比如某一小组的人员、具有某一身份的用户等），预先定义的一套安全策略（如失泄密控制策略、主机安全策略等）。该策略集作为一个对象，可供管理员随时查看、修改、添加和删除。

单项策略：一个大策略集中的某一项小策略，比如失泄密策略中的打印控制策略、HTTP 控制策略等。在 UEM 中，单项策略必须是能在一个具体策略设置界面编辑完成的。

群组：具有某一类相同属性的人员或者计算机的集合，用于对人员或计算机进行逻辑上的分组。

群组管理：对于群组进行增、删、改等操作，增减群组内的人员和计算机，为群组设置相应的安全策略，这些操作统称为群组管理。

群组策略：关联到群组的一组安全策略（如失泄密控制策略、主机安全策略等），当人员或者计算机添加到某个群组中时，将会自动应用该群组的安全策略。

安全文件加解密：一套非透明的、主动的文件加解密系统；在部署了 UEM 客户端的机器上，用户通过文件加密功能选项，主动进行文件的加解密操作（比如通过资源管理器中的右键菜单“安全文件加解密”或者拖拽文件到“我的加密文件夹”等）。该系统产生的加密文件以.wsd 后缀结尾，文件图标表现为左侧带一把小锁的形式，不同于加密前文件的图标。

安全文档管理系统：一套基于 Windows 文件系统内核的、透明的文件加解密系统（通常简称为安全文档）。当用户使用由管理员设定的某类进程（称之为加密进程）编辑文件的时候，会自动将文件数据加密存储到磁盘上；当用户使用加密进程打开该文件的时候，能够在后台自动解密文件数据；文件数据的加解密操作均在操作系统的内核完成，用户感觉不到加解密过程的存在。该系统所产生的加密文件保留了原有的文件后缀，文件的图标表现为在原有文件的图标基础上，在右下方附加了一把黄色的小锁。

加密进程：在安全文档管理系统中，由管理员设定的一类能够自动对文件数据进行加解密处理的进程；当用户使用这类进程编辑并保存文件时，能够自动将数据加密存储在磁盘上；同时，在用户使用这类进程打开被加密文件时，能够自动将数据解密。

写权限打开文件：为了保障文件的安全，Windows 操作系统对一个文件提供了多种访问控制

权限，如读权限（可以读取文件数据）、写权限（可以将新的数据添加到文件中）、删除权限（可以删除文件）、执行权限（如运行 EXE 程序）等。当用户使用一个应用程序打开一个文件的时候，操作系统会要求该应用程序申请访问该文件的权限；只有应用程序申请了某个权限，应用程序才有资格进行相应的操作（比如，只有申请了删除权限，应用程序才有资格删除该文件）。写权限打开文件就是说应用程序在打开文件的时候，会申请对该文件的写操作权限。一般情况下，应用程序在打开一个文件的时候，只会申请读的权限。当用户真正编辑并要求保存的时候，才会重新申请写权限。

预加密文件类型：加密进程在以写权限打开明文文件的时候，会在打开之前先对指定类型的文件进行加密处理，这种加密处理叫做预加密，指定的文件类型即为预加密文件类型。

无效备份文件：在安全文档管理系统中，某一个备份文件所对应的原始文档不存在（被删除或者移到其他路径下），称这样的备份文件为无效备份文件；

自动备份文件：在安全文档管理系统中，依据设定的时间点，系统自动对该时间点之前用户修改过的加密文件实施备份，这个过程称为自动备份文件。

手动备份文件：用户通过 UEM 系统客户端托盘区菜单主动发起的，对用户修改过的加密文件进行备份操作的过程，这个过程称为手动备份文件。

审批管理：在安全文档管理系统中，企业内的敏感文件会被强制加密。为了能将被加密的文件带出使用，需要向系统管理员提出申请，并经具有相应权限的审批员审核同意后，方可解密文件并带出。从提交申请，到审批员审核，再到加密文件的解密，这个过程称为审批管理。

在线审批：用户将审批请求和文件发送给服务器，由服务器完成审批逻辑的处理，自动交给具有审批权限的用户进行审批的方式；

离线审批：用户将要审批的文件制作成审批包，通过网络或 U 盘等移动介质拷贝到具有审批权限的用户机器上完成审批的过程；

UEM 的安全模式：当安装 UEM 客户端的机器不满足终端安全检查条件要求（如 Windows XP 系统未安装 SP3 补丁、未安装杀毒软件等）时，UEM 客户端会将该机器设置为安全模式；当计算机被设置为安全模式后，该计算机将只能访问 UEM 服务器和其它被指定的机器(安全服务器)，而不能与其他机器通讯。

安全服务器：一个单位内部，供终端计算机进行安全升级时访问的服务器，如防病毒软件服务器、补丁更新服务器等。部署了 UEM 客户端的计算机因安全检查被设置为安全模式后，该计算机将只能访问控制台指定的安全服务器列表中的计算机。

基于密级标识的文档安全系统：英文名称 Tag-based File Protection System，缩写为 TBFPS。

可信工作域：客户所在的组织机构内部署了 UEM 环境的计算机集合。

保密性级别：用于标记主体（用户）或客体（文件）的安全等级，在本文档中简称**密级**。

密级文件：已经由密级文件管理员设置了密级的电子文件。

密级文件管理员：具有密级文件管理权限的客户端用户。

密级文件附加属性：包括文件名、密级、产生时间、生命周期、文件来源、应用范围等。

密级文件带出：密级文件通过某种途径传播到可信工作域之外。

密级文件交流：密级文件所有者通过审批机制，将带有密级标识的文件发送给安全工作域内其他用户使用。

文件操作：包括创建、读取、写入、删除、重命名、拷贝、剪切、粘贴、销毁等操作。

文件分类：从文件是否加密角度，将文件分为非加密文件、普通加密文件（无密级标识的加密文件）、密级文件（带密级标识的加密文件）。

密级文件生命周期：密级文件的创建操作是密级文件生命周期的开始，密级文件被销毁后，密级文件的生命周期结束。在密级文件创建到销毁期间，可对此密级文件进行修改，带出等操作。

在线审批：用户通过 UEM 系统提供的电子审批管理机制，发出申请给密级文件管理员，管理员通过系统提供的界面对申请进行审批，并通过系统自动将审批结果反馈给用户，这个过程，我们称之为在线审批。

离线审批：UEM 系统中安全文档模块中提供的审批功能，此功能不依赖于用户的在线状态，用户将审批的文件制作成审批包，通过网络或移动存储介质途径将此审批包发给审批员，审批员执行审批后，再通过网络或移动存储介质途径将审批结果发回用户，此过程我们称之为离线审批。

可信计算：UEM 系统能够自动收集受控终端的运行进程信息，并对收集的进程信息实施分类管理。通过可信计算策略控制，防范关键进程的重命名行为；另外，UEM 系统对操作系统文件进行完整性校验，并实现强制访问控制，确保操作系统核心系统文件的安全，保证操作系统免被病毒或木马侵袭，实现操作系统的可信。

附件六：

UEM8.0 常见问题解答

（Version：8.0.12.161）

1. 产品概要

系统架构

1. UEM 系统由哪几个部分组成？

答：由 UEM 服务器，UEM 控制台和 UEM 客户端三部分组成。同时还提供的一些辅助工具，如：审计系统、备份与恢复工具、全盘扫描加密工具、安全文档灾难恢复工具等。

2. UEM 系统控制台和服务器之间支持 B/S 架构吗？

答：从 UEM R7 开始，将支持 B/S 架构，但只是部分功能，详见本文档“附件二”。

3. 在 UEM 系统中，将控制台和服务器分开，这样做的好处是什么？

答：控制台和服务器分开的好处有两点：(1) 是控制程序和数据接收服务分离开来有利于提高系统工作效率，减少出错几率；(2) 方便管理员远程通过服务器对客户端进行管理，不受地理位置的限制，可以在与服务器能建立 TCP 双向连接的任何机器上安装控制台，对客户端进行管理。

4. 什么是 UEM 客户端？它的作用是什么？

答：UEM 客户端是安装于受控主机上的软件系统。主要作用：接收服务器下发的策略，并按照该策略控制和记录本机所有可能造成敏感信息泄漏的信息传递过程，包括网络行为、移动存储、打印机和可能造成泄密的外设接口等。

5. UEM 系统支持多控制台吗？多控制台操作时需要注意什么？

答：支持。注意避免同时对同一个客户端进行策略下发操作，因为客户端最后收到的策略将覆盖以前收到的策略。也不能同时用同一个帐户登录控制台。

环境需求

6. UEM8.0 服务器端支持什么操作系统？

答：UEM8.0 服务器端支持 Windows 2003 Server、Windows 2003 Advanced Server 操作系统。对其他系列版本的 windows 系统不建议用作安装 UEM 服务器。

7. UEM8.0 服务器运行的最低硬件配置？

答：UEM8.0 服务器根据所注册的客户端个数不同所需要的硬件资源也不同，在挂接 500 个客户

端的情况下，建议使用如下硬件配置：CPU P4 3.0、 RAM 2G、Disk 120GB。

8. UEM8.0 补丁服务器和 UEM 服务器可以分开安装吗？

答：UEM8.0 补丁服务器可以和 UEM 其他服务器组件分开安装，且补丁服务器需要在 Windows 2003 Server 或 Windows 2003 Advanced Server 系统上安装，同时需要 IIS 支持。

9. UEM8.0 客户端支持什么操作系统？

答：UEM8.0 客户端支持 Windows 2000 Professional、Windows 2000 Server、Windows 2000 Advanced Server、Windows Xp、Windows 2003 操作系统。

10. UEM8.0 服务器使用了什么数据库？该数据库是由厂家免费提供的吗？

答：UEM 服务器支持 Microsoft SQLServer 2000 或者 SQLServer 2005，不是由厂家免费提供的。

11. UEM8.0 控制台支持什么操作系统？

答：UEM 控制台支持 Windows 2000 Professional、Windows 2000 Server、Windows 2000 Advanced Server、Windows Xp、Windows 2003 操作系统。

12. UEM8.0 审计系统需要哪些环境支持？

答：UEM 审计系统支持 Windows 2000 Professional、Windows 2000 Server、Windows 2000 Advanced Server、Windows Xp、Windows 2003 操作系统。同时需要 SQL SERVER 2000 或者 2005 的支持。

13. UEM 系统支持一台机器安装多个 Windows 操作系统的情况吗？

答：支持多操作系统，但是每个操作系统都必须安装了 UEM 客户端。

功能简介

14. 防水墙系统和 UEM 系统有什么区别。

答：防水墙系统主要关注内部信息失泄密防护，UEM 系统不仅关注信息泄露防护，还关注终端主机的集中、统一管理问题，从终端安全管理、终端运维管理、用户行为管理、数据安全管理、终端接入管理等多个方面实现了终端主机的集中管理。

15. UEM8.0 系统是从哪五个方面保障终端主机的安全？

答：UEM8.0 系统从用户行为管理，终端安全管理，终端运维管理，数据安全管理，终端接入管理五个方面实现终端主机的安全管理。

16. UEM8.0 终端安全管理功能包括哪些子功能？

答：终端安全管理包括：终端健康检查、终端安全策略管理、身份认证管理、网络进程管理、补丁管理、防病毒软件检测、文件安全删除管理等功能。

17. UEM8.0 终端运维管理功能包括哪些子功能？

答：终端运维管理包括：软件分发管理、资产查看、运行状况监控、以及远程帮助等几个方面。

18. UEM8.0 用户行为管理功能包括哪些子功能？

答：用户行为管理主要是包括网络失泄密防护、非法外联控制、媒体介质管理、打印机管理、键盘控制、以及外设接口管理几个方面对用户的各种操作行为进行控制，并记录用户的操作日志等。

19. UEM8.0 数据安全管理功能包括哪些子功能？

答：数据安全管理包括：桌面安全保险箱（我的加密文件夹）、可信移动存储介质管理、以及安全文档策略。这三大功能从不同层面不同深度实现了各种数据的保护。

20. UEM8.0 终端接入管理功能包括哪些子功能？

答：终端接入管理包括网络接入认证功能和非法主机扫描功能，其中非法主机扫描工具我们将在未来的版本中发布。

21. 什么叫桌面安全保险箱？

答：桌面安全保险箱就是我的加密文件夹，是安全保存终端用户自愿加密保存的重要文件，在该保险箱内的文件均以.wsd 后缀加密保存，解密成功后不再有.wsd 后缀。

系统特点

22. UEM 系统具有哪些特点？

答：UEM 系统具有以下特点：全面的终端防护能力、分权分级的管理模式、方便灵活的安全策略、周全详细的系统报表、丰富的应急响应知识库、完善的插件式系统架构、方便快捷的安装、卸载和升级。

安装与卸载

23. UEM 各组件按照什么样的先后顺序进行安装？

答：建议以先安装服务器、再安装控制台、最后安装客户端的顺序进行安装。

24. UEM 服务器、控制台、客户端可以安装在一台主机上吗？

答：服务器和控制台可以安装在一台主机上，控制台和客户端安装在一台主机上，也可能出现问题，建议服务器、控制台、客户端安装在独立机器上。

25. UEM 服务器可以和审计系统安装在一台主机上吗？

答：服务器不能和审计系统安装在一台主机上，服务器和审计系统都需要独立 SQL server 服务器作支持。

26. 安装服务器后，在哪里可以获得证书。

答：在服务器安装目录下 CSS\UEM\WBServer\server\default\conf\ wbserver.cer

27. 为什么在安装完服务器和控制台之后，控制台无法连接服务器？

答：在排除其他网络问题的情况下，请检查 SQL SERVER 2000 的 SP4 补丁是否已经安装。如果使用 SQL SERVER 2000 作为 UEM 服务器的数据库，必须安装 SQL SERVER 2000 的 SP4 补丁。

28. 客户端注册方式有几种？他们之间有什么区别？

答：客户端用户注册方式分：自由模式、认证模式和 KEY 模式三种，其中服务器可以在自由模式和认证模式间进行设置，KEY 模式为服务器内置模式，不需要进行单独配置，此 Key 是指格尔 Key。

认证模式：该模式下要求管理人员在服务器中添加注册用户名，供客户端用户注册时使用。客户端用户注册时需要手动输入用户名、密码，服务器会验证用户名和密码的有效性，如果验证成功，执行注册；如果验证不成功，提示错误信息。

KEY 模式：该模式为与 KEY 结合版本提供支持，属于服务器内置功能。KEY 模式注册时，客户端会验证 KEY 的 PIN 码的有效性，验证通过后，由客户端自动提取用户名进行注册，服务器自动添加 KEY 用户名到数据库。该模式支持网络身份认证功能。

自由模式：为方便大规模快速部署等简化管理而设，该模式不验证新用户的用户名及密码。如果客户端注册的用户名在服务器中不存在，服务器将该用户名及密码添加到数据库中；如果客户端注册的用户名在服务器中存在，服务器负责验证用户名及密码的有效性，若用户名及密码正确，注册成功，否则返回错误提示。在该模式下可以设置客户端为自动注册以便于进行大规模部署。具体设置为：使用客户端二次打包工具对客户端安装包进行自动注册配置，有四种选项，分别是用户名@域名、计算机名、计算机 IP 地址和计算机 MAC 地址。安装时，客户端会按设置好的规则自动提取用户名进行注册。

注意：UEM8.0 支持用户身份认证功能，在开启该功能时，服务器要求验证用户名和密码的有效性，由于自由模式时不要求用户名、密码在数据库中存在，无法验证用户身份的有效性，故非 KEY 版本客户端（KEY 版本除外）启用网络身份认证功能时，忽略服务器端设置，统一按照认证模式进行注册。

29. 为什么在注册客户端重新启动机器后出现了卸载现象？

答：客户端只有在收到卸载命令时才会进行卸载操作。

客户端注册成功后重新启动机器后立即卸载的原因：一般在计算机进行本地删除或重新安装操作系统后，将控制台上的无效用户删除后产生。原理为：在控制台上将用户删除后，服务器会下发卸载命令，在同一用户登录后，会将该命令传递给该客户端，并清除信号，而客户端未接收卸载命令即重装系统或本地卸载，服务器上的信号不会清除。客户端重新安装时，由于同一台计算机（物理机）的机器 ID 一致，再使用同一用户名进行注册，会产生相同的用户 ID，登录后，上一次无效用户的卸载信号会下发给该新安装客户端，出现卸载现象。

30. 在 XP 系统下重启客户端后,提示无法识别硬件 KEY 怎么办?

答：出现这种情况，重新插入一次 KEY 即可。

31. UEM8.0 客户端能否支持在普通用户权限安装？

答：UEM8.0 客户端不支持在普通用户权限安装。

32. 为什么我们建议 UEM8.0 客户端在 Administrator 用户环境下安装？

答：因为 UEM8.0 客户端的安装和运行时需要有对磁盘和操作系统注册表的写入等权限，User 用户环境下可能因没有上述必需的权限而造成安装失败，所以安装 UEM8.0 客户端必须在 Administrator 用户环境下进行。

33. 如何知道 UEM8.0 的当前安装版本？

答：用户可以点击系统状态栏 UEM8.0 客户端托盘图标，在“关于 UEM8.0”窗口中可以看到 UEM8.0 版本号和客户端的注册用户等信息。一般情况下，我们保持 UEM 的各组件以同一版本号发布。

34. 安装 UEM8.0 客户端时，针对不同的操作系统，需要注意的问题是什么？

答：Windows 2000 系统需要打SP4补丁，Windows XP 系统需要打SP2补丁，Windows 2003 系统需要打SP1补丁。

35. 跨网段经过防火墙时，防火墙要开放哪些端口？

答：1433、8443、1098、1099、4444、4445 等端口。

36. 在安装 UEM8.0 时突然断电会对系统产生什么影响？

答：对操作系统本身没有任何影响，但可能会造成 UEM8.0 系统无法注册、无法卸载等异常情况。

37. UEM 控制台出厂时内置的账户和口令是多少？

答：UEM 控制台出厂时提供了两个内置账户，分别是：

系统管理员账户：Admin 口令：1234567a

系统安全官账户：security 口令; 1234567a

38. UEM 审计系统出厂时内置的账户和口令是多少？

答：UEM 审计系统出厂时默认用户名：Admin 密码：12345678

39. 客户端安装时，为什么会出现“注册统一终端安全管理系统库文件失败!”？

答：原因是杀毒软件等注册表监控软件禁止安装程序写注册表。解决办法：当杀毒等监控软件提示安装程序修改某注册表项时，允许其修改；如果是瑞星等不提示的杀毒软件，建议关闭实时监控功能然后进行安装。

40. 安装统一终端安全管理系统控制台时被金山毒霸防御监控拦截，有时需要云鉴定，怎么办？

答：出现该故障是因为控制台安装程序 WBConsoleInstall.exe 无法签名，杀毒软件对屋签名的运行程序都会进行拦截，在安装有金山毒霸的主机上此故障无法避免，在金山毒霸出现拦截框时点击“允许本次操作"，控制台即可顺利安装，

如果控制台安装包是从局域网、U 盘、光盘复制到主机，此时金山会提示进行云鉴定，须进行云鉴定，鉴定完成后即可安装.

系统维护

41. 如何查看 UEM8.0 系统的版本号？

答：UEM 系统各组件都提供了版本号查看功能，控制台通过查看“帮助”-“关于”菜单可以看见类似 UEM8.0（Build 8.0.8.x）的字样，其中 8.0 是 UEM 系统的大版本号，8.0.8.x 为 UEM8.0 维护版本的小版本号。服务器通过 Windows 任务栏的 UEM 服务器备份工具查看版本号，客户端通过 Windows 任务栏的客户端托盘中“关于”菜单查看。

42. 如何升级 UEM8.0 服务器？

答：通过运行服务器安装包，并通过“修复”功能执行重新安装即可，升级前确保所要升级的服务器安装包的版本号比当前运行中的服务器版本号高。升级服务器不能删除以前的数据库。

43. 如果遇到新装服务器无法进行初始化的情况，怎么办？

答：因为 UEM8.0 卸载服务器后，不删除 SQLServer 数据库和 Ldap 数据库，所以重新安装服务器时无法进行初始化，这时可以执行如下步骤：

（1）停止服务器安装程序；

（2）使用 SQLServer 备份 CSSWaterbox8i 数据库；

（3）删除 CSSWaterbox8i 数据库；

（4）重新执行服务器安装程序；

（5）使用 SQLServer 还原原来备份的 CSSWaterbox8i 数据库；

（6）执行 wbserver\bin\sx_initial.bat；

（7）执行 wbserver\bin\updateldap.bat；

（8）重新启动服务器。

44. 如何升级 UEM8.0 控制台？

答：通过运行控制台安装包，并通过“修复”功能执行重新安装即可。UEMR7 以后增加控制台自动升级功能。在控制台的系统参数设置中，上传升级包和版本号，设置是否自动升级。在登陆控制台的时候，系统会检测新版本，并弹出提示框，询问用户是否要升级。

45. 如何升级 UEM8.0 客户端？

答：UEM8.0 客户端升级支持两种方式：（1）本地运行方式：用户自行将 UEM8.0 升级包下载至本地，运行进行升级。（2）在线自动升级方式：系统管理员配置升级参数，并将升级包放置升级目录中，客户端主机重启过程中自动检测并从服务器获取升级包进行升级，且前提是升级包

版本号比客户端程序版本号高。

46. UEM 客户端可以通过软件分发功能进行安装吗？

答：不能，软件分发功能需要依赖客户端程序来运行。

47. 能随意更改运行中 UEM 服务器 IP 地址吗？

答：19 版本以前的ＵＥＭ服务器，是可以修改 IP 地址的，只要修改完毕后重启服务即可。19 版本以后的ＵＥＭ服务器，在安装完 UEM 服务器以后，服务器所在的计算机不建议修改 IP 地址。如果必须修改 IP 地址，那么，需要修改注册表中如下参数：（以旧 IP 地址为 10.26.13.206 为例）

（1）KEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services/WBSever/Paramters

修改其中的“JVM Option Number 11”的值，将“-Djava.rmi.server.hostname=10.26.13.206”中的旧 IP 地址，更改为用户新的 IP 地址。

修改其中的“Start Param Number 4”的值，将“-Dhornetq.remoting.host=10.26.13.206 ”中的旧 IP 地址，更改为用户新的 IP 地址。

（2）KEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services/WBSever/WBBusiness01

修改其中的“JVM Option Number 11”的值，将“-Djava.rmi.server.hostname=10.26.13.206”中的旧 IP 地址，更改为用户新的ＩＰ地址。

系统兼容性

48. 个人防火墙和 UEM 客户端会发生冲突吗？

答：会，由于 UEM8.0 客户端和个人防火墙功能有所重叠，在对受控主机的软件和硬件环境的控制权上发生冲突，所以建议安装 UEM 之前卸载个人防火墙或者降低防火墙防护水平，否则 UEM8.0 客户端可能无法正常工作。

系统安全性

49. 用户可以终止 UEM 客户端的进程吗?

答：不能。UEM 客户端进程受保护的，用户通过正常方式无法终止。

50. 用户可以删除客户端安装目录中的文件吗?

答：不能。UEM 客户端程序文件受保护的，用户通过正常方式无法删除。

51. 用户可以删除服务器端的上传的客户端用户数据吗?

答：不能。UEM 服务器的日志文件受保护的，用户通过正常方式无法删除。

52. 数据库的数据是加密保存的吗?

答：不是。

53. 禁止所有 IP 或端口意味着什么？在这种情况下，我们的 UEM8.0 系统还能正常运行吗？

答：禁止所有 IP 或端口意味着客户端将不能与网络中除服务器以外的任何一台计算机建立 TCP 连接。因此 UEM8.0 可以正常运行。

54. 终端安全性检查切断网络之后，为什么还能与服务器进行通信?

答：对于 UEM 的服务器，系统是默认放开的。

系统性能

55. 为什么用户在登录 UEM8.0 客户端，CPU 占用率较高？

答：UEM8.0 客户端在登录时，需要获取一些初始化信息并运行相关的后台服务进程，故此阶段 CPU 占用率较高。

56. 客户端程序对客户机的影响是什么？内存占用率和 CPU 使用率是多少？

答：客户端对客户机的主要影响包括启动速度、运行速度、网络速度。经过严格测试表明系统正常情况下所受影响很小。客户端总的内存使用量在 18M 以下，CPU 使用率一般低于 5%，平均在 3%左右。

57. 控制台远程杀死客户端用户进程，是否会引起客户端操作系统崩溃或者客户端本身失效？

答：会，因为 UEM8.0 终止进程的权限比较高，一般进程都可以杀死，如果杀死的为系统进程操作系统就会重启。

2. 产品功能

失泄密防护

58. 在 HTTP 策略中我需要输入完整的 WEB 地址吗？

答：不需要，只需要输入WEB地址的一部分即可。例如：对于http://www.sohu.com可以输入www.sohu.com或sohu.com

59. 为什么禁止 NETBIOS 后，用户不能使用网络打印功能或者访问 VSS 服务器？

答：因为 NETBIOS 的禁止策略执行的是双向禁止，即别人不能访问本机的 NETBIOS 服务，本机也不能访问网络上的 NETBIOS 服务；所以，Windows 网络打印和 VSS 服务等使用 NETBIOS 协议的服务也将被禁止访问。

60. 对被禁止的设备，如果用户试图使用该设备，UEM8.0 系统记录日志吗？

答：系统提供违规日志记录功能，用户在设置并应用记录违规日志的策略后就可以在控制看到警报，并在告警信息中查询到该违规日志。

61. 对用户的哪些可能造成失泄密的行为作文件备份？

答：收发邮件、FTP、打印、以及移动介质带出文件等操作系统提供了记录文件内容的功能。

62. 如何查看备份的文件？

答：通过统计与审计分析视图，找到对应的日志，并通过鼠标右键点击“下载文件”后可以查看文件内容。

63. 失泄密策略一般分为哪几个层次？

答：全部禁止、全部开放、禁止只允许白名单，开放禁止黑名单。

64. 什么是黑名单、白名单？

答：黑名单即禁止名单，黑名单中的记录被禁止访问或使用；白名单即信任名单，白名单中的记录允许访问或使用，而且不记录日志。

65. 为什么安装了 UEM 客户端后，无法访问需要帐户登录的网站？

答：如果禁止 WEBMAIL 发送邮件，会将所有需要密码登录的访问都禁止（如：邮件、博客、网站等），因为这两种场景都使用了相同的通信协议。

媒体介质管理

66. 如果没有安全文档策略模块的强制加密，当用户拷贝带出文件时，如何设置策略对文件进行加密？

答：启动控制台，进入安全管理中心。从左侧的人员视图中选择一用户，单击“用户策略设置”→“用户策略”→“存储介质控制”→“可移动介质控制”，在基本策略编辑页面中选择“允许使用移动存储设备拷贝，但拷贝数据加密存储。”然后，将策略应用下发，客户端收到策略后，用移动存储设备拷贝带出的文件就是加密的。

67. 为什么在 2003 SERVER 下插入大容量的移动硬盘，在移动存储设置自由读写的策略下，硬盘变成了只读？

答：这是 2003 SERVER 的一个问题，2003 SERVER 系统不能自动识别大容量的移动硬盘并为之分配盘符。此时一般通过系统的设备管理器人工为之分配盘符。在这种情况下， UEM 客户端程序在无法识别到盘符，但为了系统的安全，即使移动存储设置策略为自由读写，也默认设置移动硬盘为只读形式。
此时用户可以拔出移动硬盘，再插入即可恢复自由读写。

68. 为什么会出现设备禁用失败的问题？

答：当插入机器的设备正在使用,或被一些系统进程打开进行操作的时候,所有对此设备进行禁用的操作都有可能失败,所以就会出现在"设备管理器"中看到已经禁用,但实际可用的情况.

打印机管理

69. 打印机控制具有哪些策略？

答：有四种策略：（1）自由使用；（2）禁止使用；（3）允许使用，记录打印文件名；（4）允许使用，记录打印文件名，并记录文件内容。

70. 为什么我不能打开并查看到打印文件的内容？

答：在打印截获时，打印控制模块会对源文件进行查找，并保存下来。对于 IE 等无原文（数据缓存在内存中）的打印操作，只能进行打印影像数据的截获，该影像文件的数据格式与打印机及打印驱动相关，无法进行有效解析，可以通过影像重新输出到打印机的形式进行内容的查看。

键盘管理

71. 禁止截屏键能禁止住一些截图软件的截图功能吗？

答：不能。可以通过控制进程来禁止一些截图软件。

外设接口管理

72. UEM 系统可以监控哪些外设接口？

答：UEM 系统可以监控下列外设接口： USB 接口、SCSI 总线、蓝牙接口、串行总线、并行接口、红外接口、PCMCIA、软盘控制器、DVD/CD-ROM 驱动器、无线网卡接口、1394 接口、第二块网卡可进行策略设置。

73. 先插入 USB 设备，再下发禁止 USB 策略，是否能禁止 USB 的使用？

答：可以。

74. 什么叫第二块网卡？

答：除去与服务器通信的网卡之外的所有其他网卡，我们都统称为第二块网卡。

75. 如果设置了某外设接口禁用策略，是否记录客户端尝试使用接口行为？

答：可以记录，UEM 系统提供了违规行为记录功能，只要在策略中启用了违规日志记录功能就可以。

安全策略管理

76. 为什么下发密码口令长度验证策略对已经建立的账户无效？

答：在 UEM 当前版本中，该策略只能对新建账户生效或者对下发策略后的修改密码的账户生效，对下发策略之前建立的账户不生效。

防病毒软件监控

77. 已经应用了病毒库未及时升级禁止连接网络的策略，为什么病毒库未及时升级仍可连接网络？

答：这是因为有些防病毒软件的更新时间 UEM8.0 当前版本还监测不到。现能获取到病毒库更新时间的杀毒软件有：KILL， 瑞星， 金山毒霸， 江民 2006，熊猫，VirusBlock，McAfee，PC-cillin，Kill6.0，东方卫士，BitDefender。对监测不到的软件，UEM 默认为合乎要求，允许连接网络。

78. 为什么客户端安装了某防病毒软件，但控制台仍然报警系统未安装防病毒软件？

答：UEM8.0 当前版本基本能识别绝大多数的防病毒软件，对有些不常见的防病毒软件可能不识别，此时系统会认为未安装防病毒软件，UEM8.0 当前版本能识别的防病毒软件有：KILL， 瑞星， 金山毒霸， 江民 2006，熊猫，VirusBlock，McAfee，PC-cillin，Kill6.0，东方卫士，BitDefender，卡巴斯基-个人版，诺顿，卡巴斯基 6，KV2007。

文件安全删除管理

79. 在安装安全管理系统客户端的机器上，右击文件时有一项菜单项叫“安全删除文件”，请问什么叫“安全删除文件”？

答：“安全删除文件”并不是简单的将文件直接删除掉，它在删除文件之前将存储该文件的磁盘区域覆盖 n 次数据，每次覆盖分三步：第一步用一个 8 位的字符（0）覆盖，第二步用该字符的补码（1）覆盖，最后用一个随机字符覆盖。其中 n 的值可以在“安全管理中心”→“主机策略”→“终端安全管理”→“安全操作配置”中，设置数据回添次数。文件被安全删除后，将不能用磁盘数据恢复工具恢复。

80. 为什么使用安全删除功能删除的文件没有日志记录？

答：因为采用安全删除删除文件时会产生大量的日志，因此将其屏蔽。

81. 为什么有时在 WIN7 下安全删除文件不成功？

答：win7 操作系统，对本地磁盘或移动硬盘上的主分区根目录下的文件，进行文件安全删除操作不成功。这是因为 win7 系统对上述路径进行了权限保护，只有操作系统管理员权限（Adminstrator）才能此进行操作。这时我们可以在在 win7 系统下避开对下列路径下的文件，进行文件安全删除操作。包括：win7 的安装分区根目录（例如 C 盘根目录）；win7 安装路径的 windows 文件夹下所有路径（例如 C:\windows\...）；移动磁盘的主分区（一般为加载的移动硬盘的第一个分区）。

补丁管理

82. 为什么补丁分发功能的立即下载并安装执行的很慢？

答：如果补丁服务器地址设置为通过默认的微软网站更新，补丁则通过 Internet 的微软补丁网站

下载，如果补丁很大，则下载时间会很慢。

83. 为什么补丁分发功能中客户端未安装补丁列表不一定是最新的？

答：当下发获取补丁列表命令时，管理界面显示的是上次查询的未安装补丁列表结果，同时下发命令通知客户端连接补丁服务器，通过补丁服务器查询未安装的补丁信息。

84. 补丁管理策略中，WSUS 地址的格式需要注意什么？

答：WSUS地址是 http://IP:PORT。如使用 80 端口，则端口号可以省略。

85. 安装补丁服务器时对磁盘有什么要求?

答：系统分区和安装 WSUS3.0 的分区都必须使用 NTFS 文件系统进行格式化。
建议：（1）系统分区至少留出 1GB 的可用空间；（2）WSUS 用于存储内容的卷至少留出 20GB 的可用空间，但最好留出 30GB 的可用空间；（3）WSUS 安装程序安装 Windows® Internal Database 的卷至少留出 2GB 的可用空间；（4）不能使用压缩的盘符(No Compressed)。

86. 安装补丁服务器时对权限有什么要求?

答：（1）内置组用户或 NT Authority\Network Service 帐户（在 Windows Server 2003 上）应具有 WSUS 内容目录所在驱动器上的根文件夹的读取权限。如果没有此权限，BITS 下载将会失败。（2）NT Authority\Network Service 帐户应具有 WSUS 内容目录（通常为 <SystemDrive>:WSUS\WsusContent）的“完全控制”权限。此权限是由 WSUS 服务器安装程序在创建该目录时设置的，但某些安全软件可能会重置此权限。如果没有此权限，BITS 下载将会失败。（3）NT Authority\Network Service 帐户应具有以下文件夹的“完全控制”权限以使“WSUS 管理”管理单元能够正确显示：

%windir%\Microsoft .NET\Framework\v2.0.50727\Temporary ASP.NET Files

%windir%\Temp

87. 如果 WSUS 和 Internet 之间设有企业防火墙，如何配置企业防火墙？

答：如果 WSUS 和 Internet 之间设有企业防火墙，则可能需要配置防火墙以确保 WSUS 能够获取更新。要从 Microsoft Update 获取更新，WSUS 服务器将端口 80 用于 HTTP 协议，而将端口 443 用于 HTTPS 协议。不能对该设置进行配置。

如果您的组织不允许对所有地址打开端口 80 或端口 443，则可以限制只访问以下域以使 WSUS 和自动更新能够与 Microsoft Update 进行通信：

http://windowsupdate.microsoft.com

http://*.windowsupdate.microsoft.com

https://*.windowsupdate.microsoft.com

http://*.update.microsoft.com

https://*.update.microsoft.com

http://*.windowsupdate.com

http://download.windowsupdate.com

http://download.microsoft.com

http://*.download.windowsupdate.com

http://wustat.windows.com

http://ntservicepack.microsoft.com

运行状况监控

88. 运行状况监控可以监控哪些对象？

答：运行状况监控可以监控计算机名的修改、系统 CPU、内存、网络流量的超量使用、监控共享文件夹的变化、文件操作监控、用户和组的变化、系统服务的变化、网络配置的修改、系统进程的监控、主机系统日志的上传管理等。

89. 运行状况监控设置的策略是用户策略还是主机策略？

答：运行状况监控设置的策略是主机策略，该主机的资源信息和文件的操作过程均受该策略监控。

90. 控制台可以实现对客户端用户和组的运行监测，请问这里的用户和组信息指的是操作系统的相关信息还是 UEM8.0 的相关信息？

答：是记录操作系统的相关信息的变化状况。

91. 能通过控制台禁止住正在运行的客户端主机进程吗？

答：不能，对已经启动的进程，下发禁止进程策略后，该进程不会被终止，禁止进程只对未启动的进程生效。

92. 如何能够查看 Windows 系统日志？

答：启动控制台，进入安全管理中心。从左侧的人员视图中选择一用户，单击“远程管理”→“系统日志”，稍等可以在浏览视图中，显示所要查看计算机的系统日志。

93. 如何能够下发 Windows 系统日志策略？

答：启动控制台，进入安全管理中心。从控制台中央的选项卡中单击“主机策略设置”，然后从左侧的计算机视图中选择一计算机，单击“主机策略”→“运行状况监控”→“系统日志”。最后，在控制台中央的策略设置面板中选择“上传系统日志”,设置“上传时间间隔”;如果想在上传后删除本地系统日志,请选中“上传后删除本地日志”，单击应用按钮向客户端下发策略。客户端在收到策略后就会执行该策略，进行系统日志的上传。

94. 为什么移动存储设备在本用户数据共享加解密时复制操作记录的类型为新建？

答：这个与 Windows 的实现机制有关。

95. 为什么用命令行 copy 命令复制文件到移动磁盘，记录提示为修改。而用界面操作复制文件到移

动磁盘，却提示为新建？

答：这个与 Windows 的实现机制有关。

96. 问：断网行为发生后会不会中断主机与服务器之间的通信，致使主机处于离线状态？

答：对网络进行断网使用的是一种安全断网行为，客户端与服务器之间的网络通信不会被中断。客户端与服务器之间依然保持在线状态。

97. 问：实时网络流量超过设定值被中断后，如果修改了原有策略，网络会怎样恢复连接状态？

答：当改变实时网络流量的某一项策略时，网络的恢复条件按新设定的策略执行。

98. 问：当网络总体流量超过阈值后，如果对网络进行了中断，将如何对网络进行恢复？

答：网络总体流量是从主机开机时开始计算的所有网络流量，如果超过阈值被中断，只能通过重新启动计算机的方式恢复网络连接。

资产查看

99. 为什么在资产查看界面中有些硬件的属性无法看到？

答：这是由于有些硬件厂商，并未把所有的硬件属性，都写入其相应的硬件设备中导致的。

100.为什么有些软件在安装时 UEM8.0 没有监测到呢？

答：对于一些绿色软件，安装和卸载时没有在控制面板的添加或删除程序里列出，UEM8.0 无法获知。

101. 资产查看实时监控的软件有哪些？

答：应用软件和操作系统补丁。

102.资产查看中硬件资源有哪些？

答：硬件信息有：监测的客户端硬件包括八项，均为容易被用户更换的计算机部件，分别包括：1、CPU　2、BIOS　3、硬盘　4、内存　5、网卡　6、显卡　7、光驱　8、声卡

103.使用状态监测阈值如何设定比较合理？

答：根据机器的软、硬件资产配置，需要合理设置各个阈值。设定的阈值不应太低，因为如果阈值比较低，则客户端报警信息则相对比较频繁，对服务器和客户端造成的压力都比较大。

软件分发

104.软件分发中分时间段下载，如果在时间段内下载没有完成怎么办？

答：将会在第二天的同一个时间段继续下载。

105.软件分发，如果下载（或安装）时间类型是时间点，但设置的时间点在客户端当前时间点之前时，客户端怎样执行？

答：客户端在此情况下，当接收到命令后会立即下载（或安装）对应软件包。

106.软件分发功能支持 UEM 客户端安装包的分发和安装吗？

答：不支持，软件分发功能使用的前提是客户端主机已经安装了 UEM 客户端，并授权了软件分发功能。

107.软件分发模块中什么样格式的安装包支持静默安装？

答：只有 MSI 格式的软件包才支持静默安装。而可执行文件和 BAT 类型文件不支持静默安装。

108.新建软件包中的文件获取路径的格式有什么约束？

答：必须符合 http 协议，并且提供下载的软件包必须是 cab 类型的软件包，UEM 的安装包生成器制作生成。

109.问：新建软件包管理中注册表的安装路径格式有什么要求？

答：只需输入注册表的子键的路径，而不需输入注册表键的路径。例如注册表路径：HKEY_LOCAL_MACHINE\ SOFTWARE\MICROSOFT\WINDOWS\... ，只需输入 SOFTWARE\MICROSOFT\WINDOWS\...，而不需输入 HKEY_LOCAL_MACHINE。

我的加密文件夹

110.我的加密文件夹中的文件加密与安全文档加密有什么区别？

答：我的加密文件夹中的文件是用户自愿加密的文件，安全文档策略加密是强制加密，二者加密的途径和技术以及强度都不一样。

111.硬盘有两块硬盘，在主硬盘安装客户端，我的加密文件夹在辅助硬盘中，此时下发禁用辅助硬盘策略，我的加密文件夹也不可用。（R8 以前的版本）

答：客户端在安装时首先查找系统盘，再检查是否有其它盘。如果没有其它盘，我的加密文件夹将创建在系统盘；如果有其它盘，则我的加密文件夹创建在其它盘。如果其它盘只有辅助硬盘，那么我的加密文件夹只能创建在辅助硬盘里。这时，下发禁用辅助硬盘策略，将会导致我的加密文件夹不可使用。

112.win7 操作系统，对本地磁盘或移动硬盘上的主分区根目录下的文件，不能进行安全文件加解密操作。

答：这是因为 win7 系统对上述路径进行了权限保护，只有操作系统管理员权限（Adminstrator）才能进行操作。我们可以在在 win7 系统下避开对下列路径下的文件，直接进行加解密操作。包括：win7 的安装分区根目录（例如 C 盘根目录）；win7 安装路径的 windows 文件夹下所有路径

（例如 C:\windows\...）；移动磁盘的主分区（一般为加载的移动硬盘的第一个分区）。

安全文档

113.为什么安全文档驱动无法启动？

答：因为 Windows 系统的内核进程检测列表只能容纳 8 个不同的进程检测调用，当系统中的其它程序，如杀毒软件、防火墙等，启动后占满该列表，导致安全文档驱动无法启动。遇到安全文档驱动无法启动的问题，请首先确认是否有多余的特殊的防护软件，将其卸载。如果不好定位，请向技术支持人员索取相关工具。

114.为什么有些设置了新建文件不加密策略的进程打开加密文件，修改保存后还是密文?

答：设置新建文件不加密策略后的进程修改加密文件后是否解密，是根据软件的自身写文件机制所决定的，如果软件写文件时，应用程序底层是在新的数据区新建文件之后删除原数据区原文件，再把新建的文件拷贝过来，那么修改之后呈现在我们面前的文件就不加密，如 word；如果软件写文件时，应用程序底层是在原数据区文件上进行修改的话，那么修改之后呈现在我们面前的文件就还是加密文件，如记事本、VSS 中 check out 文件。

115.为什么应用软件升级过后，该应用软件下发签名值策略的加密进程无法访问密文？

答：因为应用软件升级后，进程文件发生变化，导致签名发生变化。建议在进程库中从新添加该应用软件的进程，启用签名值，下发策略即可。

116.为什么压缩类软件在其进程无加密进程策略时压缩加密文件，下发加密进程策略后解压缩导致文件破坏？

答：压缩类软件进程为非加密进程时,将加密文件进行压缩,压缩到压缩包中的文件为密文；对该压缩类软件进程下发加密进程测试后，解压缩上述压缩包,此过程是加密进程再次访问原密文文件，即会导致文件无法打开。建议在对加密文件执行解压缩过程中保持压缩类软件进程策略的一致。

117.为什么利用 Windows 自带的压缩功能压缩加密文件后，再利用其他压缩工具解压缩该压缩包后文件无法打开？

答：windows 自带的压缩功能，是由 explorer.exe 进程访问文件，若 explorer.exe 是非加密进程，压缩包中的文件为原始加密文件；若其他压缩工具的进程是加密进程，解压缩该 zip 包（windows 自带的压缩功能生成 zip 包）时加密进程访问 zip 包中的密文文件，即会导致文件无法打开。

118.为什么通过 Solidworks 应用程序对加密的 solidworks 文件进行打包，之后通过其他解压缩工具对压缩包解压缩后文件无法打开？

答：未打开 solidworks 文件，直接通过右键菜单执行打包操作，该操作时由 explorer.exe 进程执行访问文件，若 explorer.exe 是非加密进程，压缩包中的文件为原始加密文件；通过其他

解压缩工具对压缩包进行解压缩，若其他压缩工具的进程是加密进程，解压缩该压缩包时即是加密进程访问压缩包中的密文文件，即导致文件无法打开。

119.为什么无法从加密的压缩包中将文件拖拽出来？

答：从加密的压缩包中往外拖文件，即是用非加密进程 explorer.exe 去访问加密文件，安全文档禁止非加密进程去访问加密文件，因此会提示访问被拒绝。

120.为什么对解压缩工具进程下发加密策略后，创建的自解压文件无法运行？

答：由于解压缩工具的相关进程是加密进程，所以通过解压缩工具创建的自解压文件(即*.exe)是加密文件，加密的自解压文件无法自动解密运行，所以必须手工解密，然后才能执行自解压步骤。注：加密的 exe 文件均无法自动运行。建议不要对压缩或者解压缩工具下加密进程策略

121.为什么在装有中软安全文档系统的机器上安装有些杀毒软件后，机器异常？

答：第一次安装杀毒软件后机器未重启，所以导致杀毒软件的驱动的状态未知。建议安装杀毒软件后重启机器，机器即可正常运行正常。

122.为什么有些杀毒环境下，访问网络上文件夹较慢？

答：杀毒引擎效率比较低导致。建议对杀毒定期进行升级操作。

123.为什么通过非加密进程（如 Foxmail 发送文件）上传密文到网络中，通过其他加密进程（如 IE）下载网络中的密文，出现文件异常？

答：由于加密进程从网络上下载文件时读的是数据流，安全文档暂不支持对网络数据流的判断，导致文件异常。建议不要将下载文件的进程设置为加密进程。

124.为什么双击打开某些网络服务器（如 ftp）上加密文件，文件无法正常打开？

答：对于一些通过网络数据流来打开加密文件的方式暂时无法支持，因此打开时不会自动解密。对于这种加密文件不建议用加密进程在网络服务器上直接打开。建议将文件复制到本地后可以打开。

125.为什么加密进程打开文件拷贝文件内容到非加密进程打开的文件中未成功后，在非加密进程打开的文件中复制图片就一直提示错误？

答：由于从加密进程打的文件中拷贝内容到非加密进程打开的文件未成功后，剪贴板上的数据一直是从加密进程拷出来的，而在非加密进程打开的文件内部做复制时先去访问剪贴板所以导致复制出错。建议用其他非加密进程（如记事本）打开非加密文件做一次复制，然后在上述非加密进程打开的文件中进行复制，即可恢复正常。

126.为什么卸载了安全文档系统后，有些应用程序不能使用？

答：目前安全文档系统只对进程控制，该进程所有写的文件都会加密，由于加密进程（例如 winword）会读写很多模版文件，这些模版也会自动加密，当安全文档系统卸载后，这些模板因

为加密，所以无法正常调用。建议用灾难恢复工具对相关目录进行恢复，也可以重新安装相应的软件即可解决问题。

127.为什么 Protel 非加密进程打开加密文件，原加密会文件破坏？

答：由于 protel 自身的机制，在打开文件时会修改文件。所以 protel 非加密进程在打开加密文件时会修改密文，造成文件破坏。建议 protel 取消加密进程策略后避免打开加密文件，防止文件破坏 。

128.为什么 PGP 保护区已满保存至该区域的加密文件会出现打不开的现象？

答：PGP 保护区空间已满会导致文件内容无法完全写入，对于加密文件可能会导致数据未被写入，造成文件无法打开。故在进行文件操作的时候请先确认 PGP 盘是否磁盘空间充足。

129.为什么给 word 下发加密进程策略后 Microsoft Office OutLook2003 无法撰写邮件？

答：Outlook2003 默认调用 winword 进行邮件编辑，此时 winword 下发了加密进程策略，而 outlook 是非加密进程，安全文档系统会禁止非加密进程和加密进程之间的操作，所以 outlook 中无法进行邮件编辑。

可通过如下方法配置 OutLook 后解决该问题，具体配置过程如下：

选择 OutLook 菜单栏，选择工具菜单项，在弹出的多页面选项框中界面中选择"邮件格式"，取消邮件格式页中用 MS Word 编辑选项。然后重新启动 OutLook 就可以了

130.为什么对某个文件类型（如 doc）下发强制扫描后，在没有对该文件类型对应的进程下发加密策略的情况下，右键新建该文件类型的文件，仍然是加密文件？

答：全盘扫描加密了该文件类型的模板文件。右键点击新建时，其实是复制相应类型的模板文件到新建文件的位置，所以新建的文件就是加密的，这个问题是相应软件的模板机制导致的。另外全盘扫描之后，需要把相应软件的进程设置为加密进程，否则原来的客户端该软件对应的加密文件就无法正常打开了。

131.为什么将客户端可移动存储介质的控制策略设置为记录自由使用移动介质，记录拷贝文件名；记录拷贝文件的内容后在移动存储介质上用加密进程打开文件时，文件一闪后自动关闭？

答：因为某些应用软件内部机制原因，进程在打开文件过程中，会修改文件数据，而移动存储介质的控制策略为了能够保证记录文件的最新内容，会强制关闭文件。建议在设置了加密策略的前提下，用户不要在移动存储介质上编辑文件；或者选择自由使用移动存储设备的策略。

132. 安全文档的加密扫描会扫描回收站吗？

答：不会。回收站是用户废弃文件的的存放地，不对其进行加密。

安全文档在线审批

133.UEM 客户端新增的“在线申请带出”和原先的“申请带出”之间的区别是什么？

答：“申请带出”是指申请人首先在本地制作审批包，然后通过 U 盘或其他途径将审批包拷贝到审批员机器，审批员再对审批包进行审批操作的过程。而“在线申请带出”是指申请人直接将要带出的文件，通过 UEM 系统在网络上发送给审批员，审批员在审批完毕后，将审批结果再次通过 UEM 系统在网络上告知申请人的过程。

134.如果用户在使用 UEMR6 版本时，在控制台设置了审批规则，当系统从 R6 升级到了 R7 之后审批规则是否继续可用呢？

答：不可使用。因为 UEMR6 的审批规则是要下发到 UEM 客户端的，而 UEMR7 的审批规则是在服务器存放的，由于二者机制的不同，系统升级后 UEM 管理员需重新在 UEM 控制台设置审批规则。

135.在线审批有哪些限制条件？

答：在线审批要求被审批的文件必须是经过安全文档系统加密的文件，同时被审批的文件大小不能超过 100M，且每次申请带出文件的数量不能大于 10 个。

136.为什么审批员的审批任务列表中最多只显示 10 个审批任务？

答：这是 UEM 系统在服务器做了优化处理的结果，这样能限制每次下发任务时的网络数据大小，能够减少系统占有的网络带宽。

137.某 UEM 用户所对应的审批员不在线时，其可否发送在线申请带出？

答：可以。申请人可在审批员不在线时发送审批请求，当审批员上线时 UEM 系统会自动将审批请求发送至审批员机器。

138.UEM 的审批员可否同时审批多个在线申请？

答：可以。审批员只需在审批任务列表中同时选择多条任务，然后点击“同意”或“拒绝”即可。

139.UEM 的审批员可否不查看文件内容，而直接审批在线申请？

答：可以。UEM 系统并没有限制这种操作，审批员在选择审批任务之后可直接点击“同意”或“拒绝”按钮进行审批。

140.为什么 UEM 客户端在发送在线申请带出时，或者 UEM 审批员在下载被审批的文件时，CUP 的占用率会稍有提高？

答：这是因为客户端发起在线申请时，被申请带出的文件会通过网络方式传送到 UEM 服务器，而审批员下载文件时，需将文件从 UEM 服务器下载到本地，所以会占用一定的系统资源，但是这种系统资源的占用只是暂时性的。

141.win7x64 客户端生成的请求包，发到客户端为老版本的审批员处，不能进行正常的审批，怎么办？

答：审批员需要升级老版本客户端，与申请人的客户端同版本即可。8.0.17.269 版本以后的客户端就不存在这个问题。

可信移动介质管理

142.可信移动存储介质提供了几种安全密级？

答：提供了普通、秘密、机密、绝密四种安全密级。

143.可信移动存储介质的安全密级排列顺序是什么？

答：普通 < 秘密 < 机密 < 绝密

144.可信移动存储介质区分的终端类型有几种？

答：有 2 种，可信终端和普通终端。

145.可信移动存储介质存在哪几种状态？

答：可信状态和商旅状态。

146.在授权磁盘的使用范围时，我们可以指定哪些对象？

答：人员范围、计算机范围、组织范围和责任人。

147.可信移动存储系统提供的自我保护机制是什么？

答：（1）不限制，只是当次接入不能加载。　　（2）锁定，禁止使用。
　　（3）自动破坏数据，不可恢复。　　（4）以只读方式加载。

148.密码尝试过多时提供的自我保护机制是什么？

答：（1）不限制，只是当次接入不能加载。（2）锁定，禁止使用。（3）自动破坏数据,不可恢复。

149.达到限定条件时的自我保护机制是什么？

答：（1）锁定，禁止使用。　（2）自动破坏数据，不可恢复。　（3）以只读方式加载。

150.支持商旅模式的可信移动存储介质可以在那种用户权限下使用?

答：Administrator

151.导致可信移动存储介质自毁的原因有哪些？

答：（1）密码尝试次数过多　　（2）超过使用限定次数　　（3）超过使用限定期限

152.为什么商旅状态的可信磁盘拿到普通机器上使用时提示用户权限不够？

答：商旅状态的可信磁盘需要动态加载系统驱动，非管理员没有权限启动驱动，因此，商旅状态的可信磁盘只能在管理员权限下使用。

153.为什么我看不到刚插入主机的 USB 盘？

答：如果在可信磁盘已正常加载后，系统因某种原因异常关机或重新启动，则在启动后可能会看不到移动存储介质的盘符，这时候需要用户到系统的逻辑磁盘管理界面中，手动为设备指定盘符。

操作步骤：

（1）通过“控制面板”----“管理工具”，进入“计算机管理”

（2）选择“存储”中的“磁盘管理”

（3）在窗口右侧列出了系统的所有逻辑磁盘。

（4）在没有盘符的磁盘上点击鼠标右键，选择菜单“更改驱动器名和路径…”

（5）点击新窗口的“添加”按钮，选择“指派驱动器号”，并选择一个盘符，“确定”即可。

（6）关闭窗口，盘符添加成功。

另 Windows2003 系统对于 USB 的管理也存在同样的问题，需要用户手动为磁盘指定盘符。

154.如何使用商旅模式的可信磁盘？

答： 被激活的商旅磁盘上有一个可信磁盘管理程序 WBTSTravel.exe。将激活后的可信磁盘接入普通终端时，如果普通终端允许自动播放功能，操作系统将自动执行文件 WBTSTravel.exe，否则，需用户手动运行该文件。该程序启动后，在操作系统的托盘区新添一图标  。

在图标  上点击鼠标右键，选择“加载可信磁盘”，将弹出口令输入对话框。输入设定口令，点击“确定”按钮即可完成可信磁盘的加载；点击“取消”，放弃加载操作。加载完成后，可以在“我的电脑”中看到新添了一个盘符，对此我们可以进行读写操作。

155.可信磁盘的加载有什么注意事项？

答：当插入可信磁盘时，系统会自动加载该可信磁盘（即弹出密码输入框）；如果本次加载失败或者你想稍后再加载，可通过客户端右键菜单的可信介质管理加载。

156.为什么在资源管理器里有时看不到加载的可信磁盘盘符？

答：加载可信磁盘时，系统不能将磁盘上载消息发送给资源管理器，资源管理不能及时更新磁盘列表。关闭资源管理器，重新打开即可看到加载的可信磁盘的盘符。

157.在向可信磁盘写入数据文件的过程中，非法拔出磁盘，是否会造成数据的丢失？

答：会造成数据丢失，强烈建议用户使用可信盘后，在可信终端上，通过客户端的可信介质管理工具正常卸载；如果是商旅模式的可信盘，在普通终端上使用后，先通过右键菜单卸载已加载的可信磁盘，然后再通过系统托盘区的移动设备管理菜单弹出磁盘，这样才能不造成数据丢失。

158.为什么软盘不支持商旅功能？

答：软盘容量太小，不能存储可信磁盘的自举程序。

159.为什么要将可信磁盘安全卸载？

答：在可信磁盘成功加载后，我们可以随便拷贝文件到可信磁盘上，可以随意编辑磁盘上的文

件。为了提高效率，操作系统在将数据写入磁盘设备时，会先做缓存，将数据保存在系统的内存中，当数据达到一定量时再将数据写入磁盘。因此，为保证数据的完整性，我们需要安全地卸载可信磁盘，可通过客户端图标右键菜单的可信介质管理卸载可信磁盘。否则，如果直接插拔 U 盘，可能会导致数据的丢失，拷贝到磁盘上的文件可能会无法打开或者打开时显示为乱码。

160.可信磁盘是否支持在不同服务器进行磁盘回收、日志查看吗？

答：可信磁盘不支持在不同服务器中进行磁盘回收和日志查看，因为密钥不同。

161.为什么在某些情况下可信磁盘中的文件会比实际文件要大很多？

答：出现该情况可能是磁盘出现坏道，表现出文件大小比实际的文件大，此时通过磁盘的查错工具即可修复。

162.授权时为什么出现 10b 错误？

答：磁盘被设成了只读，所以建议客户端和控制台分开装，不要因为客户端的 U 盘策略导致无法正常授权。

163.磁盘只读时的卷标问题

答：由于我们设置磁盘卷标的时机必须在可信磁盘成功加载到系统后，所以当可信磁盘因某些条件（如机器密级高，时间或使用次数到期）只读加载时，注意卷标有可能无法成功设置！但如果磁盘已经成功加载过，且卷标已经被设成“可信磁盘”，就不会出现此问题！

164.和安全文档共用蓝屏问题

答：安装好的客户端，在第一次使用授权的相对于它是新的可信磁盘时，对文件进行重命名操作会导致蓝屏，重启后恢复正常！
归蔽此问题的方法是：新建一个文件不进行重命名，卸载可信磁盘，重新加载，这样之后都没有问题！

165.策略设置问题

答：UEM 中共有两处关于 U 盘的控制策略，我们这样做的目的是便于单独授权可信功能，对于两处策略采取的是从严控制

166.无法正常回收的问题

答：回收的时候如果弹出错误号是 2 或者 5，说明当前磁盘正在被使用，原因可能有多种，比如杀毒软件正在监控，还有可能当前控制台装有客户端，而对 U 盘有策略，这时停掉杀毒软件的实时监控或者将客户端的策略放开，问题应该可以解决

167.授权范围的问题

答：由于 UEM8.0 的授权分人员、组织和计算机，所以只要有一项符合，就认为其有使用权限

168.更改密码的方法

答：更改密码必须在磁盘未加载的时候进行，加载上的磁盘无法更改密码

网络接入认证

169.在安装安全管理系统客户端的机器上，右击安全管理系统图标有一项菜单项为“网络认证配置”，点击此项菜单时弹出对话框“认证属性设置”请问对话框中的各项都是什么意思？

答：此对话框中的各项功能只有在该网络中启用网络接入认证功能时才有效。“触发认证方式”是指当安全管理系统客户端发起网络认证时，需要将认证开始标志（EAPOL_START）发送到那个地址，其中共有两个可选地址：“广播触发”和“多播触发”，大部分的交换机设备都支持“多播触发”，所以保持默认选择即可。“设备选项”是指安装安全管理系统客户端的计算机连接到什么类型的交换机上，这里只提供了两个可选项“华为 3Com 交换设备”和“CISCO 交换设备”，其他厂商的交换机一般会支持这两种设备的一种，所以根据实际情况选择此项即可。“自动更新网络的 IP 地址（DHCP）”此项功能暂时保留。“上传用户的 IP 地址”是指华为的交换机设备若启用了此项功能，则将该项选中即可。

170.在安装安全管理系统客户端的机器上，右击安全管理系统图标有一项菜单项为“网络认证身份”，点击此项菜单时弹出对话框“网络接入认证”请问这是干什么用的？

答：此功能只有在该网络中启用网络接入认证功能时才有效。当该安全管理系统用户的密码被管理员在安全管理系统控制台更改后，此客户端将无法成功认证网络，此时需要输入更新后的密码，然后点击确定按钮即可。注意：若此处输入无效密码，则此客户端将无法成功认证网络。

171.怎样使用网络认证功能？应注意什么？

答：如果要启动网络接入认证功能，首先需要终端计算机所连接的交换机具备 802.1x 网络认证功能，并将其功能开启。然后，按照 UEM 安装手册中的步骤配置 IAS 服务器。

如果在用户计算机尚未安装 UEM 客户端时，已经启用了网络接入认证功能，则此时用户网络处于未连通状态。在二次打包客户端时，需选中网络接入认证选项，并在配置选项中选择相应的网络设备。安装客户端文件时，需首先选中“启用网络接入认证”复选框，然后输入正确的用户名和密码，再进行安装操作。

如果用户计算机已经安装了 UEM 客户端，当启用了交换机的网络接入认证功能时，UEM 客户端会自动认证网络。若认证网络失败，网络将仍处于未连通状态，此时应确认此计算机所连接的交换机类型，并点击 windows 任务栏中的 UEM 客户端图标，在弹出的菜单中选择“网络认证配置”，在配置对话框中选择正确的“设备选项”，点击“确定”按钮。

如果在 UEM 控制台中更改了用户的密码，则此时 UEM 客户端会自动获取新密码，并自动重新认证网络。若长时间内认证仍然失败，则可尝试客户端菜单中的“网络身份认证”，在弹出的对话框中输入正确的密码，点击“确定”即可。

注意：在 Windows XP 及 Windows 2003 中，客户端启用网络接入认证时，需要把本机的"IEEE 802.1x"功能禁用，具体操作请参考 UEM 安装手册。

172.如果用户不能上网，怎么处理 802.1X?

答：如果用户安装有 UEM 的客户端，若想上网，需要在认证服务器添加客户端的用户名和密码，并保持在 UEM 服务器中用户名和密码和认证服务器中的用户名和密码，客户端注册前需要关闭 windows 自带的认证功能，注册时使用在 UEM 服务器中的用户名和密码。

如果用户没有安装有 UEM 客户端，若想上网，需要使用 windows 自带的认证功能，用户名和密码使用认证服务器中的用户名和密码

策略应用

173. UEM 系统中默认策略、安装客户端二次打包时导入的策略、在控制台给用户下发的策略，它们之间的关系？

答：客户端在安装时没有导入用户策略，就按系统预置的默认策略执行。如果控制台给用户下发了的策略，就以控制台下发的策略为准。它们之间的关系为：控制台下发的策略优先于二次打包时导入的策略，二次打包时导入的策略又优先于系统默认策略。

174. 如何将策略一次下发给多个用户或组织？

答：打开控制台，进入安全管理中心，在策略设置面板中设置好策略后，点击“应用到...”，在弹出的组织结构树对话框选择用户和组织，然后点击“确定”按钮即可。

175. 在主机策略中，如何正确编辑运行状况监控中的文件操作策略？

答：比如您想要监测 c:\Security\下的所有文件，则操作如下：点击“增加”按钮，弹出编辑对话框。第一步选择驱动 c:；第二步编写路径 Security；第三步编写文件名*.*。此时点击“确定”按钮即可监测 c:\Security\下的所有文件。如果您想不监测该目录下的所有 pdf 文件，则进行以下操作：点击对话框中的“添加”按钮，例外列表中会新加一行，然后在此行的“文件名”列中输入“*.pdf”。此时点击“确定”按钮即可监测 c:\Security\下除了 pdf 的所有文件。

176. 安全策略有几种发布方式？

答：每个用户的安全策略的发放可以有两种方式：1、针对某个特定用户发布选定工作策略；2、通过组策略群发的方式进行整个小组的策略更新；

177. 什么是默认策略？

答：默认策略也叫在线基本策略，它是客户端的初始策略。对于刚刚注册成功的客户端，在控制台没有下发指定的策略集之前将执行的策略，其有效时间为每一天的整个时间段。一旦安装了安全管理系统客户端，基本策略就永久存在，不能删除，但可以修改。

178. 什么是在线策略？

答：在线策略是客户端主机和服务器通讯正常情况下运行的有效策略集，它通过控制台配置、修改下发。同时它还支持特定时间段的在线策略的设置，在该时间段内按照时间策略执行。在特定时间段以外，按照在线基本策略执行。

179. 什么是时间策略？

答：时间策略是用户定义的在特定时间段的在线策略，在该时间段内按照时间策略执行。在特定时间段以外，按照在线基本策略执行。

180.什么离线策略？

答：离线策略是客户端的备用策略，可以在控制台配置并下发，正常情况下不会生效。当客户端一旦与服务器之间的网络通讯断开了，则立即启用离线策略。通常离线策略相当严格，以保护客户端主机的安全。

181.什么是策略的生命周期？

答：策略的生命周期，策略生效的一段时间，即从上一安全策略的截止时间起至该策略的截止时间；策略生命周期完结的时间是结束时间。

182.策略的存储和下发是一步完成的吗？

答：策略的存储和下发不是一步完成的，策略保存只是保存策略，策略应用才将策略应用到客户端。

群组策略

183.什么是群组，有何作用？

答：群组是对人员和计算机的逻辑分组，方便管理员对特定人群和特定机群的管理。

184.群组与策略集的策略有何区别?

答：最大的区别在于，策略的应用模式不同：
（1）策略集，是一种以策略为对象的策略编辑和应用模式，管理员可以将所有设置好的策略集放置在策略集列表中统一管理。在需要时，可以方便地将某个策略集的策略下发给多个人员或计算机。
（2）群组，是对人员和计算机的逻辑分组。将人员或者计算机添加至某个群组时，则该群组的策略将被强制下发给该人员或者计算机。

185. 群组中的某个人员或者计算机脱离群组后，该人员或计算机的策略是否发生改变？

答：当某个人员或者计算机脱离群组后，它的策略不会发生改变，仍然为脱离群组前的策略。

186. 群组中的某个人员或者计算机的策略是否可以通过其他方式改变？

答：可以。有两种方式改变该人员或计算机的策略。
（1）在“策略集视图”下，可以将策略集的策略下发给该人员或者计算机；
（2）在“组织结构视图”下，可以直接对该人员或计算机的策略进行编辑和应用。

187.当群组的策略发生改变时，该群组下的人员或计算机的策略是否发生改变？

答：不会。只有将人员或者计算机添加到某个群组的时候，策略才会主动应用到该人员或者计

算机，随后，策略不再随群组的策略变化而变化。

188.管理员如何更改群组下人员的策略？

答：有三种方式可以改变群组下人员的策略：
进入控制台，点击“安全管理中心”，选择一个策略项，例如选择“失泄密防护策略”：
（1）在“群组视图”下，直接编辑并保存群组的策略，将其应用到指定群组。
（2）在“策略集视图”下，将编辑后的某策略集的策略，通过“应用到...”操作，将策略下发给指定群组。
（3）“人员视图”下，将某人员的策略进行编辑后，通过“应用到...”操作，将策略下发给指定群组。

系统角色与用户管理

189.系统内置角色有那些？

答：系统内置角色有四个：

- 管理员：主要管理系统参数设置，同步域帐户、人员视图，计算机视图，增加角色，删除角色，修改角色，查看角色，增加用户，删除用户，修改用户，修改用户密码，查看用户角色等。
- 安全官：主要负责同步域帐户、删除用户管理，审核角色和审核用户状态。
- 操作员：主要进行安全管理中心，响应与知识库，同步域帐户、人员视图，计算机视图等操作。
- 审计员：主要对日志信息和报警信息进行统计审计分析。

190.为什么系统有些角色与用户无法进行修改?

答：系统强制规定内置角色与用户是不能修改的，且不能删除的；
系统强制规定已审核的角色与用户不能进行修改的。

191.为什么用户已经删除，还在组织树上存在?

答：已删除节点目前只改变状态和图标，不从系统中删除。

统计与审计分析

192.统计审计分析面板中，控制台操作日志查询条件中的用户帐号的含义是什么？

答：该用户帐号指的是控制台用户名，而非客户端用户名。

193.控制台的统计审计分析管理界面中，在导出大数据量（大于 5000 条）的日志时，为什么会自动分文件保存？

答：为了避免单个文件过大，UEM 系统在导出日志时，自动以 5000 条作为分段标准，将数据分

别存入多个文件中。

内网安全扫描

194.问：当一个子网跨越了多个交换机时，能否实现阻断非法主机功能？

答：可以，对于跨多个交换机的子网，需要将该子网使用的全部交换机信息输入到配置子网窗口中的交换机列表中，同时要保证输入的交换机数量与实际情况完全相同，并且交换机的 IP 地址、共同体名和类型等信息准确无误。

195.问：当启用 ARP 阻断时，为什么网络数据流量明显增大？

答：这是因为 ARP 阻断时，代理主机要向非法主机频繁发送 ARP 包，如果阻断的强度大时（如选择“阻止其与所有机器的连接”），或者该网段的非法主机数量多时，ARP 包的数量也会增多，故网络数据流量会明显增大，这时建议采用交换机阻断。

196.问：内网安全扫描中的代理主机有什么用途？

答：代理主机是指某子网内的一台合法主机（即安装了 UEM 客户端的机器），该计算机将在其子网范围内进行巡逻扫描，如果该子网启用了 ARP 阻断，则该代理主机还将对符合阻断条件的主机进行 ARP 阻断的功能。

197.问：如果成功启动代理列表以外的合法主机为客户端代理后，为什么每次扫描的客户端代理均为该主机？

答：在“扫描到的计算机列表”中，通过右键菜单启动代理列表以外的合法主机为客户端代理后，UEM 服务器会将该主机加入到代理列表中，并将其设置为第一优先级，然后给新代理下发启动扫描命令。所以在不对代理列表进行修改的情况下，将始终把该主机作为首选客户端代理。

198.问：合法主机在更换网卡后，为什么显示为非法主机，但却可以作为客户端代理正常工作？

答：由于 UEM 服务器在判断主机的合法性时，主要采取检查 IP 和 MAC 地址，并以 MAC 地址为主的原则来进行。所以，合法主机更换网卡后，由于 MAC 地址发生变更，所以服务器即认为其为非法主机，但由于其 IP 地址未变，并且该主机一直是装有 UEM 客户端的，所以仍然可以作为客户端代理进行正常的扫描和阻断工作，但是在“扫描到的计算机列表”中将不会对该代理进行高亮显示。如果需要解决该问题，可以重新安装 UEM 客户端。

199.问：为什么有时在启动客户端代理进行扫描时，代理无法进行扫描，查看日志显示打开网卡失败？

答：该问题主要是由于在作为客户端代理的主机上可能安装有两个不同版本的 WinPcap 软件，造成软件冲突所致。由于 UEM 客户端使用的是 WinPcap3.1 版本，所以为解决该问题只需在该主机上保留此版本的 WinPcap 即可。

200.在某一时刻同时存在正在扫描和停止扫描这两种状态的若干子网，如果更改参数配置，新的参

数能否即刻生效？

答：在这种情况下进行的参数配置更改，对于正在扫描的子网将不会有效，只有在这些子网下一次启动扫描时才会生效。而对于停止扫描的子网，如果启动扫描，这些新的配置参数将即刻生效。

201.为什么计算机 IP 和 MAC 映射表不能进行添加、删除等编辑操作？

答：该表中的数据是从 UEM 服务器组织结构中获取到的，这些数据是判断客户计算机合法性的重要标准，此表数据与 UEM 服务器组织结构保持同步，所以不能对其进行编辑操作。

202.问：对特殊情况下的机器，客户端代理是否会误报、漏报？

答：到目前为止，经过我们测试人员的测试，客户端代理不存在误报的现象。只要您机器的网卡能够应答客户端代理发出的信息，不管是什么条件，客户端代理都可以扫描得到结果，不会漏报。

203.问：为什么使用交换机阻断一台非法主机后，该网段的另外几台合法主机也被阻断了？

答：这是因为这些主机并不是直接连接到交换机端口上的。由于阻断功能控制的是交换机端口，当交换机的端口下连接了集线器，集线器又连接了多台主机时，如果这些主机中的一台非法主机被阻断，则此交换机端口将被关闭，导致这多台主机同时被阻断。

204.问：为什么通过工具栏频繁启动扫描，停止扫描，页面会产生抖动，命令也可能出错？

答：当通过工具栏频繁点击启动扫描和停止扫描时，刷新页面会很频繁，导致页面会产生抖动。由于 UEM 服务器的信号队列不存储重复的信号值，所以当频繁点击启动扫描和停止扫描后，在一个心跳周期内信号队列里可能同时会有开始信号和结束信号，当客户端获取信号后无法判断哪个信号是最新的信号，导致可能是停止扫描命令而执行启动扫描操作，或者是启动扫描命令而执行停止扫描操作。如遇到这种情况请点击停止扫描后，停顿几秒钟再点击启动扫描。

205.问：启用 ARP 阻断或者交换机阻断时，启动扫描并成功阻断某些计算机，此时这些被阻断的计算机将显示在被阻断的计算机列表中，但是停止扫描后，为什么被阻断的计算机列表中有时有信息有时却没有信息？

答：停止扫描后，被 ARP 阻断的计算机列表会清空，但被交换机阻断的计算机信息将仍存在，这些计算机需要被用户手动解除阻断。

206..问：启动扫描后，为什么有的子网显示绿色箭头的图标，有的显示黄色箭头的图标？

答：启动扫描后，能够成功启用代理的子网，显示绿色箭头的图标。暂时没有可用代理的子网显示黄色箭头的图标，表示处于轮询状态，只有出现可用代理时，黄色箭头图标才会变为绿色箭头的图标。

207.问：为什么有的子网可以删除，有的子网不可以删除？

答：只有处于停止扫描状态的子网，才可以被删除，要删除某个子网，需首先停止扫描操作。

208.问：一台代理正在执行扫描，此时，某个优先级较高的代理上线，该优先级高的代理是否会抢占当前代理？

答：不会。启动扫描时，会按优先级由高到低的顺序查看各个代理是否可用，如果优先级最高的代理可用，则启动该代理执行扫描，否则查看下一个代理是否可用，如果所有代理都不可用，则子网处于轮询状态，直到有可用代理出现。当前代理执行扫描时，除非其突然不可用或者用户手动指定其他代理执行扫描，否则即使有优先级较高的代理可用，仍会由当前代理执行扫描。

209.问：成功阻断某台计算机后，这台主机被解除阻断，但过一段时间为什么又会被阻断？

答：因为这台计算机满足阻断条件，故再一次探测到这些计算机时，还是会被阻断。如果不希望这台计算机再次被阻断，可以将其添加到例外计算机列表中。

210.问：内网安全扫描中的例外计算机有什么用途，需要怎样设置？

答：例外计算机是在扫描过程中即使满足阻断条件也不会被阻断的计算机。可以在扫描到的计算机列表中选中某台计算机，然后点击右键选择“加入到例外计算机列表”；或者在被阻断的计算机列表中选中某台计算机，然后右键选择“解除阻断并添加到例外计算机列表”；或者在例外计算机列表页面中，直接添加某台计算机的 IP 和 MAC 地址，将其添加到例外计算机列表中。

211.设置并下发了 ARP 阻断，但为什么仍然无法实现对非法主机的阻断功能？

答：如果主机上安装了 Anti ARP Sniffer 和 360 安全卫士，并开启 ARP 防护，这种情况 ARP 欺骗阻断被当作攻击拦截，UEM 无法实现非法主机阻断功能。解决方法：关闭 Anti ARP Sniffer 和 360 安全卫士的 ARP 防护功能。

212.内网合法主机被扫描报告为非法主机？

答：当主机更换网卡或自行更改Ｍａｃ地址导致ＭＡＣ地址发生变化时，ＵＥＭ扫描会报告为非法主机。

解决方法：将该主机加入例外主机列表即可。

213. 为什么在统计审计分析中，加密带出和记录带出日志有许多源文件名为未知？

答：加密带出和记录带出分别对应失泄密防护策略/存储介质控制/可移动存储介质控制策略中的加密和记录两种控制策略所产生的日志。

为了记录用户的带出操作(将文件从本地硬盘写到移动存储介质中),UEM 系统采用了两种技术：一是直接过滤 Windows 操作系统的 CopyFile 和 CopyFileEx 拷贝函数，通过该函数进行的文件拷贝操作可以获取到所操作的源文件信息；二是监控移动存储设备的文件变化，当检查到有向移动存储设备写操作时依据策略进行相应的控制;该技术可以确保某个应用程序在不通过 Windows 的拷贝函数复制文件到移动存储设备的时候，也可以记录相关的操作，保证策略的有效性，这种情况下产生的日志将无法获取操作的源文件路径。

统计审计分析中显示源文件为未知的日志，即是上述第二种情况下产生的日志。

214. 在内网安全扫描界面中，添加了交换机级联口后为什么在界面上没有显示，并且再次添加

提示该级联口已添加？

答：如果所添加级联口的交换机 IP 未在当前选中的子网范围内，则在交换机级联口列表中将无法看到该级联口，为了看到整个网络所有已添加的交换机级联口，只要选中左侧树中的“全局网络”，然后再选中“交换机级联口”即可。

215. 在已执行用户注册的主机上用其他帐户登录系统，并且该帐户处于未注册状态，为什么进行内网安全扫描时显示该客户端合法，并且在“所属部门”一列中显示的用户为本机已注册的用户？

答：在某主机已存在注册用户的情况下，以未注册用户登录该客户端，由于该主机上已安装有统一终端安全管理系统的客户端，所以认为该客户端是合法的，即：合法性是与主机相关的，在扫描结果“所属部门”一列中所显示的用户为在该主机上已注册的所有用户，而非当前正处于登录状态的用户。

同步域帐户

216.如果在同步时勾选了“监控并同步域帐户”,是否 UEM 的组织结构会跟随域帐户的变化而变化？如果是这样，它的敏感度是怎样的（如果域里加了一个用户，多久 UEM 能同步过来）？

答：如果在同步时勾选了”监控并同步域帐户“，UEM 的组织结构会跟随域帐户的变化而变化(但前提是在 UEM 服务器执行过同步域服务器后，域服务器和 UEM 服务器之间的连接没有断开过，若两台服务器有一方曾经重新启动过或者是二者之间的网络连接曾经断开过，则需要重新同步域服务器，以使二者能够继续保持同步)；二者同步的敏感度很高;若域控制器里增加了一个用户，在 UEM 服务器里马上就能增加该用户。

217.如果在上述情况下，在 UEM 控制台删除了一些组织结构和用户，会不会将再次同步出来？

答：在这种情况下，被删除的组织结构和用户不会重新被同步回来，但这些节点处于删除状态，只有在重新执行 UEM 控制台的“同步域帐户”时，这些被删除的节点才能重新出现。注意，只要某节点曾添加到 UEM 服务器中，则该节点就不会被彻底删除掉，只能被设置成已删除状态。

218.在上述情况下，当我在 UEM 客户端调整了人员的组织归属，在未知的某一时刻，一部分用户将自动回到原来的组织结构下面，而另外一些用户，就不会回到原来的组织。

答：这种情况下，这些被移动的节点不会自动回到原来的组织结构下面，只有在重新执行 UEM 控制台的“同步域帐户”时，这些被移动的节点才能重新回到原组织结构下。早期的 UEM 版本中可能会存在如上面所说的问题，但最新版本的 UEM 版本均已解决。

219.是否可以重复进行同步域用户的操作？重复操作的结果是不是相当于手动更新？

答：可以，这时会将 UEM 服务器中不存在而域服务器中存在的用户添加进来。同步域帐户操作不存在手动更新的说法。

220.能否放弃监视与同步域帐户？

答：可以，只需重新执行 UEM 控制台的“同步域帐户”，且不要勾选“监控并同步域帐户”即可。

服务器操作

221.服务器备份时连接不上 LDAP 数据库。

答：该问题很可能是因为 UEM 服务器安装在域服务器上，域服务使用 389 端口，而 UEM 数据备份时连接 LDAP 数据库的端口默认为 389,从而产生冲突。

解决方法：

1.关闭备份与恢复工具；

2.打开服务器安装目录下的配置文件：\CSS\UEM\WBServer\conf\DBPower.xml；

3.查找<LDAP_Port>（总共两个地方），将其修改为实际的 LDAP 端口，如 390；

4.重新启动备份与恢复工具。

222.为什么登录控制台，输入正确的用户名和口令后，选择了要导入的证书，仍然提示登录失败？

答：出现这种情况首先请检查网络通讯和服务器工作是否正常，如果不存在该问题，有可能证书导入的问题，即通过登录窗口的“选项”功能选择了要导入的证书后，又点击“选项”按钮隐藏了证书路径输入控件，然后点击“确定”出现了该问题。

解决方法：当要第一次导入证书或者需要更新证书时，登录前，选择了证书之后，请不要点击“选项”按钮隐藏证书输入路径。同时，如果还出现登录失败的提示，请关闭该登录窗口，重新启动该窗口，再输入相关信息即可解决

服务器级联

223.什么是服务器级联？

答：随着 UEM 系统的推广，在一些规模较大的企业里，组织内的客户端数量超过一定数量时，单个服务器由于自身的运算速度和能力的限制，需要采用多个服务器进行负载分流。各个服务器之间根据树型结构组成一个服务器群，上级服务器向下级服务器发送策略，下级服务器根据上级要求传输相关数据。这样，上级服务器能够管理以自己为顶点的所有下级服务器以及他们所辖的终端主机情况，上、下多个服务器之间形成了级联关系，这就是我们所谓的“服务器级联”。

224.怎样实现服务器级联？以及它们之间的关系是怎样的？

答：单个服务器首先通过控制台导入上级服务器的证书，然后申请注册到上级服务器，上级服务器审核通过后，即可形成上、下服务器的级联关系。服务器级联不限于两层，在一个规模较大的单位里，可能存在多层级联关系。每层服务器都可以拥有自己的终端主机，且每层服务器与自己所带的客户端、控制台都是一个独立的系统。在服务器没有注册到上级服务器和没有自

己的下级服务器时，整个系统和无级联时一样，服务器级联功能并不启动。

225. 服务器级联中，上、下级服务器之间是怎样通信的？

答：上下级服务器之间采用 HTTPS 协议进行通信。下级服务器作为客户端单向访问上级服务器，上级服务器开设一组专门的 HTTPS 服务用来处理下级服务器的请求。
下级服务器以固定的频率访问上级服务器，从上级服务器的信号队列中获取与自己相关的命令，信号获取成功后，便返回一个销毁信号应答上级服务器，以便上级服务器从相应的信号队列销毁信号。然后解析命令并根据命令执行相关任务，当任务执行成功后，再向上级服务器回复相关应答，使上级服务器知道下达给下级服务器的命令所对应的任务已经成功执行，可以进行相应的处理。

226.怎样断开服务器之间的级联关系？

答：要想断开服务器之间的级联关系，必须从上级服务器做起。上级服务器的管理员有权删除自己的下级服务器，待删除的服务器被审核通过后，正式从上级服务器删除，清空与该服务器相关的数据，并向被删除的下级服务器发送删除信号。下级服务器接到自己被删除的信号，中断所有与上级服务器的通信，清空与上级服务器相关的数据，不再接收上级服务器要求上传的数据，并更改自己的路径，也通知自己的下级服务器更改路径；如审核不通过，下级服务器还原到原来的状态，继续与上级服务器保持通信。

227.上级服务器在没有删除下级服务器的情况下，重新安装后下级服务器连不上上级服务器，这时下级服务器显示已注册，重新导入证书也不行，怎么办？

答：这时需要在下级服务器上强制清除注册信息，然后重新注册。如果自己清除不了，找技术支持。

228.各级服务器之间是怎样实现报警信息上传的？

答：上级服务器向下级服务器下发报警策略，定义下级服务器上传的报警日志类型，那么它以下的所有下级服务器都会根据上级的要求，将报警日志一级一级往上传，一直传到下发策略的上级服务器为至，不再上传。在上传的过程中，每级服务器都会将上传的数据做备份，然后根据用户需要是否显示。

229.各级服务器之间是怎样上传组织结构信息的？

答：服务器注册成功后，依次（部门、人员、计算机、客户端）读取本服务器的组织结构信息，向上级服务器上传。同时，实时监听本级服务器的组织结构变化，并把相应的操作与信息上传给上级服务器，以便上级服务器做相应修改。另外，本级服务器还能将下级服务器上传来的组织结构信息上传到上上级服务器。

230.各级服务器之间是怎样实现日志统计上传的？

答：日志统计上传就是将警报信息、软硬件资产信息按设定的时间段定期上传，支持时报、日报、周报、月报、年报和自定义等多种上传方式。

如果用户选择系统默认设置，日志上传开始时间就是当前系统时间，年报为每年的 1 月，月报为每月的 1 日，周报为每周的星期日，日报为每天的 1 点，时报为每个小时的第 1 分钟。如果用户选择自定义方式，那么就按用户设置定时上传。注意：用户查询的时间段内没有日志上传的时间周期，查询结果可能显示为空。

可信盘跨服务器使用

231.什么是可信盘跨服务器使用？

答：可信磁盘跨服务器访问，简单地说：就是在 A 服务器授权的可信磁盘,在 B 服务器管理的主机上也能使用。但必须满足两个条件：（1）A 服务器和 B 服务器在授权时的用户编号一样，这可以在授权信息中查看；（2）可信磁盘的密级必须和 B 服务器管理的主机密级一致。如果能同时具备这两个条件，就可以实现跨服务器使用。

232.可信盘有几种模式和状态？

答：可信盘分为两种模式，四种状态。

- **可信模式：**这是可信磁盘的一种工作模式，只能在安装 UEM 客户端的环境中使用，在普通环境中无法使用。它分为两种状态：（1）可信模式一般状态。这是可信模式的缺省状态，不能跨服务器使用，只能在授权服务器所管理的主机上使用。访问范围受授权范围、主机密级的限制。可以在控制台通过启用跨服务器标志转换为跨服务器访问状态。（2）可信磁盘跨服务访问状态：允许跨服务器访问，访问范围受服务器授权时用户编号、主机密级的限制。可以在控制台通过关闭跨服务器标志转换为一般状态。
- **商旅模式**：可信磁盘的一种工作模式，用于和外界进行数据交互。它也分为两种状态：（1）商旅未激活状态：在安装 UEM 客户端的环境下能读也能写，在普通环境下不能访问。可以在控制台通过激活操作转换为激活状态。（2）商旅激活状态：在安装 UEM 客户端的环境下只读不能写，在普通环境下能读也能写。可以在控制台通过反激活操作转换为未激活状态。

233.什么样的可信盘不支持跨服务器使用？

答：（1）UEM8.0（Build 8.0.9.91）以前版本系统制作的可信磁盘；（2）一般可信盘在授权时没有加用户密码也不支持跨服务器使用。

234.我在系统升级前制作的可信磁盘能否在升级后正常使用？

答：系统升级前制作的可信磁盘在升级后可以正常使用。升级前如果支持跨服务器使用，那么升级后仍支持服务器使用；如果升级前不支持跨服务器使用，升级后也不支持服务器使用。

密级文件管理

235.密级文件创建时启用了轨迹追踪，为什么看不到轨迹图？

答：轨迹追踪是对密级文件的使用流转过程进行追踪，记录密级文件曾经在哪台机器、哪个路

径下打开使用过，并在什么地方留下了副本。密级文件创建时如果启用了轨迹追踪，必须在本机或者其他机器上移动过（物理路径发生了更改），并且移动后由加密进程打开过，这样才有轨迹记录，才能在统计审计分析中看到轨迹图。当然啦，如果创建时就没有启用轨迹追踪选项，即是密级文件移动过、打开过，也不会产生轨迹追踪记录，更看不到轨迹追踪图。所以，要想看到轨迹追踪图，必须具备两个条件：1．创建密级文件时启用轨迹追踪选项。2．密级文件移动过，并打开过。

236.用户密级、文件密级、计算机密级和可信磁盘密级之间的关系？

答：UEM 现有四种密级：用户密级、文件密级、主机密级和可信磁盘密级。这四种密级都有四个级别：普通、秘密、机密、绝密，他们设置的地方不一样。

用户密级在添加用户时设置，在用户属性中可以查看，通过“更改用户密级”选项可以更改；文件密级在创建密级文件时设置，在密级文件属性中可以查看，通过审批才能修改文件密级；主机密级默认为普通，在计算机属性中可以查看，通过“更改计算机密级”选项可以更改；可信磁盘密级在授权时设置，在授权信息中可以查看。

用户密级和文件密级在使用时有对应关系。如果启用了密级文件访问策略，在控制台设置了“低密级用户不能访问高密级文件”访问规则，那么，客户端低密级用户就不能访问高密级文件。如果没用启用密级文件访问策略，客户端用户可以访问任何密级的文件。另外，密级文件的图标不一样，普通级密级文件为蓝色一个星，秘密级密级文件是黄色两个星，机密级密级文件为橙色三个星，绝密级密级文件为红色四个星，请用户注意区分。

计算机密级和可信磁盘密级之间有一定的对应关系。如果在授权时选中“允许高密级的机器读取磁盘内容”，那么在高密级的主机上也能查看低密级磁盘上的数据，否则将禁止使用。在低密级的主机上，高密级磁盘会自动被禁止使用。同密级的主机和磁盘可以读写，不同密级有限制。

237.操作系统删除功能、安全文件删除、密级文件销毁之间的区别？

答：Windows 操作系统所带的删除功能，只能对文件做删除标志，不能彻底删除文件。文件被删除后大多还能通过恢复工具还原，容易造成机密泄露。UEM 系统开发了一个安全文件删除功能，用户可以设置数据回填次数，重复多次复写，保证被删除文件不可再恢复。一般情况下，我们都利用安全文件删除功能，将本机上的普通文件和普通加密文件做彻底删除。但是，对于密级文件而言，不仅要删除密级文件本身，还要删除它在各个机器、路径下流转的副本，这样才能更安全。UEM 系统的密级文件销毁，就是将不需要的密级文件执行销毁操作的同时，流转的副本文件（控制台轨迹追踪界面追踪到的文件副本）也一并被自动删除，不留安全隐患。

238.密级文件销毁时，对于不在线机器和 U 盘上的副本怎么办？

答：被审批销毁的密级文件，如果在创建时启用了轨迹追踪，那么在销毁自身的同时，也一并销毁在各个机器和各个路径流转留下的副本。但对于不在线机器和 U 盘上的副本，不能一同销毁。当被销毁的副本再次被使用时，会提示用户“非法使用已销毁的文件副本”，并产生一条报警信息。

239.普通加密文件和密级文件的普通密级文件之间的区别？

答：普通加密文件是指启用安全文档的加密进程加密的文件，它没有密级之分，受安全文档策略限制；密级文件是在普通加密文件的基础上，将文件再分为四种级别：普通、秘密、机密、绝密，普通密级文件只是密级文件的一种，它的创建、修改、带出等都要经过审批操作。

240.来源追踪和去向追踪的具体含义？

答：来源追踪和取向追踪的目的是追踪一个密级文件的流转过程。针对与一台计算机，来源追踪的目的是追踪密级文件传播到此计算机之前的传播轨迹。取向追踪的目的是追踪密级文件从此计算机传播出去后的轨迹。简单的说，来源追踪是追踪密级文件以什么轨迹流转到此计算机，去向追踪是追踪密级文件流转出计算机后的流转轨迹。

241.安全文档和密级文件管理之间的有什么关系？

答：安全文档是利用透明加解密技术，用指定的加密算法、指定的密钥，对指定类型的文件进行加解密操作。它是 UEM 系统一个独立的功能模块，其授权通过服务器硬件加密锁控制。

密级文件是基于密级标识的安全文件，与安全文档一样都是以透明加解密技术为基础，同时，密级文件共用了安全文档的加密进程策略管理机制。密级文件策略作为 UEM 系统独立的功能模块，其模块授权方式也是通过 licence 控制的。授权密级标识文件，必须授权安全文档管理；但授权安全文档管理，可不授权密级标识文件。

242.安全文件加解密和安全文档自解密有什么区别？

答：安全文件加解密（我的加密文件夹）是一种主动加密方式。根据用户的意愿，想加密就加密，不想加密就不加密，包括使用范围都可以自己设置。当然啦，用户想解密时就自行解密，解密到什么地方，也可自由设置。所以，安全文件的加解密，是 UEM 系统给客户端用户的一个自我保护工具，完全由用户自由支配。

安全文档是一种被动加密方式，由控制台下发安全文档策略控制，只要客户端用户启用了加密进程，就不知不觉被加密。当然啦，加密文件对用户本身来说是透明，打开、使用都不受限制，但带出时就有麻烦了，必须经过审批，或者通过控制台下发自解密策略，才能将文件解密后带出使用。

243.为什么低密级用户可以访问高密级文件？

答：这可能有两种原因：第一，没有启用密级文件访问策略，对客户端用户来说是自由的，可以访问任意密级的文件，不受限制。第二，客户端用户可能是审批员，对于下载的审批文件，审批员可以任意打开查看，不受密级限制。

244.删除审批规则后，原来审批员遗留的审批任务，还能继续审批吗？

答：将审批任务成功发送给审批员后，在审批管理中将能看到待审批的文件列表。如果审批员还没来得及审批这些文件，这时删除审批规则，也就是取消审批员审批权限，那么审批员还能继续审批那些已经下达的审批任务，对于以后新增的审批任务，他就不能接受和审批了，因为

他已经不是审批员。

245.删除审批规则后，原来审批员还能打开已下载的待审批文件吗？

答：审批员打开已下载的待审批密级文件时，不受密级文件访问策略的限制，可以打开任意级别的密级文件。如果将这些待审批的密级文件通过 U 盘或网络直接发送给审批员，审批员也可能打不开，这时受密级文件访问策略的限制。还有一种情况，删除审批规则后，原来的审批员还能继续打开已下载的待审批密级文件，仍然不受密级文件访问策略的限制。也就是说，通过服务器下载的待审批密级文件，不管他是不是审批员了，依然能够打开。另外，密级文件销毁时，这些已下载的待审批密级文件，因为没有轨迹追踪，不能一同销毁。

246.销毁密级文件时，为什么有的副本销毁不了？

答：销毁密级文件时，只对轨迹追踪能够追踪到的文件进行销毁，追踪不到的副本文件就销毁不了。例如：U 盘上的副本文件，审批员下载待审批文件，这些副本文件不在线，或者没有记录流转轨迹，所以销毁不了。因此，要想销毁密级文件的副本，必须在创建时启用轨迹追踪，这是前提条件。

247.在进程库管理中，复制、粘贴进程类别和创建进程类别有什么不同？

答：不同父节点下，复制粘贴一个与别处同名的类别、进程，这两个类别下的进程会同步更新。即：修改一个类别下的进程，另一个同名类别下的进程也随着更改；删除一个类别下的进程，另一个同名类别下的进程也随着删除。若通过添加类别、进程的方法，创建一个与别处同名的类别、进程，这个两个类别下的进程不会同步更新。

可信计算

248.应用可信计算核心文件检查，为什么有些核心文件会产生报警？

答：因为对核心文件的检查是依据文件的哈希值进行检查的，对于同名文件的不同版本，哈希值是不同的。当核心文件库内不包含对应的待检查的核心文件信息时，可能会有对应的核心文件产生报警，因此，管理员应用核心文件检查策略时，需要先保证核心文件库收集了对应的被应用策略的各个客户端的核心文件信息。

249.可信计算应用程序白名单策略应如何设置？

答：在设置可信计算应用程序白名单时，需要通过控制台先收集各个计算机终端上运行的应用程序信息。在此基础上，将收集到的信息添加到应用程序策略列表中，制定符合组织内部要求的应用程序控制策略。所以，管理员需要注意，在应用策略前，需通过应用程序收集策略将应用程序收集全。

电子文档权限管理

250.已经下发自审批策略（允许用户离线制作主动授权文件），为什么有时仍提示不允许自审批？

答：离线制作主动授权文件时，需要满足如下条件：

1） 自审批策略允许用户将隔离文件或者非隔离文件制作成主动授权文件；

2） 用户选择的文件类型与自审批策略一致；

3） 当前用户对所选择的文件有访问权限，即可以打开文件；当用户选中隔离文件（来自于其他用户）时，如果当前用户无权访问文件，则用户也无权进行离线制作主动授权文件；

4） 文件位于本地，而不是网络磁盘；

5） 文件后缀不可以包含 exe，java，bat，bin，dll，cefsrm，wsd 类型的文件；

6） 文件没有被占用，未被其他软件打开。

7） 文件类型是非加密文件，普通加密文件或者隔离文件，但不能是密级文件。

251.主动授权文件禁止拷贝拖拽，允许拷贝拖拽，截屏控制具有什么含义？

答：主动授权文件禁止拷贝拖拽，是指禁止将主动授权文件的内容拷贝、拖拽到加密进程中；允许拷贝拖拽，则允许将主动授权文件的内容拷贝、拖拽到加密进程中。不管是否允许拷贝拖拽，主动授权文件的内容是不允许流转到非加密进程的。

主动授权文件的截屏控制，是指是否允许将截屏后的内容粘贴到加密进程中。不管是否允许截屏，主动授权文件截屏后的信息，是不允许流转到非加密进程的。

252.通过右键菜单[在线授权]功能，为什么没有成功连接到审批平台？

答：主动授权文件在线授权时，需要事先通过 UEM 控制台配置好审批平台地址，同时将 UEM 组织结构信息导入到审批平台中，初始做完这些配置后，用户即可在客户端通过右键菜单“在线授权”直接进入到审批平台中。

253.通过右键菜单[重新授权]，为什么有时不能重新授权？

答：重新授权功能，是针对主动授权文件再授权，需要满足以下条件：

1） 文件是一个主动授权文件；

2） 制作主动授权文件时，其权限“允许重新授权”是选中的；

3） 当前用户有权限访问该主动授权文件；当文件被限制使用范围时，当前用户必须是使用范围所约定的用户；

4） 主动授权文件位于本地，而不是网络磁盘；

5） 主动授权文件没有被其他软件所占用，如被其他软件打开。

254.取消隔离策略后，隔离文件如何处理？

答：取消隔离策略后，只要用户能访问隔离文件，则另存或者修改隔离文件后，文件会自动变为普通加密文件。用户也可以通过扫描解密工具，将隔离文件批量恢复为普通加密文件或非加密文件。

安全文档隔离管理

255.下发组隔离策略后，组内用户访问隔离文件时是如何控制的？

答：下发组隔离策略后，组内用户可以互相访问隔离文件，包括在组隔离策略下发之前所生成的其他隔离文件。是否可访问隔离文件，不会受到隔离策略中所指定的隔离类型的制约。比如组隔离策略*.xls，则组内用户除了可以互相访问隔离的 xls 文件，也可以访问以前生成的 doc 类型的隔离文件。

256.隔离特殊权限有什么作用？

答：在为用户 A 应用隔离策略（个人隔离或者组隔离）后，隔离范围之外的用户就无法访问用户 A 所产生的隔离文件。在一些特殊情况下，如用户 A 的管理者，需要访问隔离文件。此时，可通过隔离特殊权限的功能，为特殊用户指定强制访问隔离文件的权限。