第1章 移动终端安全

奇安信移动终端安全管理系统是奇安信集团面向政府、金融、运营商、能源、制造等企业推出的新一代企业级移动终端安全管理系统，基于奇安信集团在海量移动终端上的安全技术与运营经验，为客户移动终端在使用企业资源时，提供从硬件、OS、应用、数据到链路等多层次安全防护方案，确保企业数据和应用在移动终端上的安全性。

移动终端安全管理系统采用多层级纵深攻防方法，全面保护高价值数据资产和移动信息的安全性；采用设备准入罚出策略，对移动终端进行准入控制，只有满足准入标准和安全性检查的终端才被准许接入网络，对违规终端第一时间实行违规处罚，有效确保企业网络的安全性；采用数据公私隔离策略，使用动态沙箱技术在移动终端上建立独立工作区，将企业的敏感数据隔离，个人信息进行加密存储，避免企业数据泄漏；构建企业级应用市场，对应用实施安全性检测和加固封装，排除恶意应用和盗版应用风险，避免因应用市场的良莠不齐，使用恶意应用对企业资产和信息造成侵害；对应用进行木马查杀，采用本地查杀和云查杀双核查杀引擎，对移动终端上已安装的应用软件和安装包进行全面扫描，精准查杀，并实时监控正在安装的应用软件，全面保证移动终端运行环境的安全性，避免恶意应用给企业资产和数据信息带来的严重危害。

1.1 用户管理

1.1.1 用户管理实验

【实验目的】

掌握移动终端安全管理系统的用户管理操作。

【知识点】

用户管理、手动添加、批量添加。

【场景描述】

A公司为提高移动办公安全配置了移动终端安全管理系统，在系统上线之前，需要将各部门的用户添加到移动终端安全管理系统中，由于人员较多，运维工程师小李需要将账号批量导入系统中；后期由于又有新的员工入职，需要添加新员工的账号，小李该如何

操作呢？

【实验原理】

管理员可通过移动终端安全管理系统的“用户管理”模块对用户进行管理，包括添加、删除用户。添加用户有两种方式，分别是手动添加和批量添加。

【实验设备】

安全设备：移动终端安全管理系统设备 1 台。

网络设备：无线 AP 1 台。

移动终端：Android 手机 1 台。

主机终端：Windows 7 主机 1 台。

【实验拓扑】

实验拓扑如图 1-1 所示。

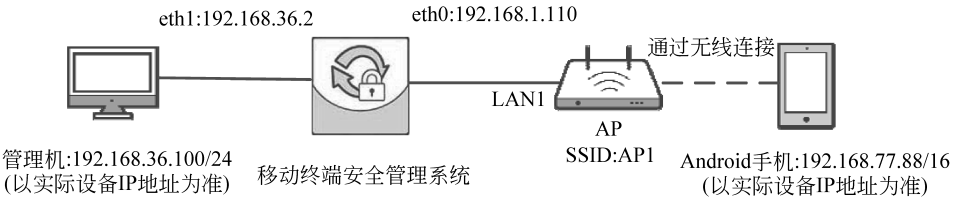

图 1-1　用户管理实验拓扑图

【实验思路】

(1) 进入移动终端安全管理系统。

(2) 在“用户管理”模块中进行手动添加用户操作。

(3) 在“用户管理”模块中进行批量添加用户操作。

【实验步骤】

(1) 在实验平台对应实验拓扑左侧的管理机中打开浏览器，在地址栏中输入移动安全终端设备的地址 https://192.168.36.2，在登录界面中输入对应的管理员账号 admin、密码 tianji 和验证码(以实际的账号和密码为准)，单击“登录”按钮，即可进入控制台管理界面进行相应的管理员操作，如图 1-2 所示。

(2) 选择面板左侧导航栏中的“用户管理”→“用户管理”菜单命令，进入“用户管理”界面，如图 1-3 所示。

(3) 在“用户管理”界面中，单击“添加用户”按钮，共有 3 种添加方式，包括“手动添加”“批量导入”及“LDAP 导入”。选择“手动添加”菜单命令，如图 1-4 所示。

(4) 在“手动添加用户”界面中，输入对应的用户属性信息，输入用户名为“zhang”，输入邮箱为“zhang@gongsi.cn”，输入用户手机号码为“13112345272”，用户所属分组为“未分组”，取消勾选“发送邮件激活”和“发送短信激活”复选框，其他保留默认配置，单击“确认”按钮，如图 1-5 所示。

(5) 返回“用户管理”界面，可见成功添加的 zhang 用户，其“激活码”为 33518288，后

图 1-2　登录 Web 管理界面

图 1-3　进入“用户管理”界面

图 1-4　选择“手动添加”菜单命令

图 1-5　手动添加用户

面注册连接的设备均需要此激活码，如图 1-6 所示。

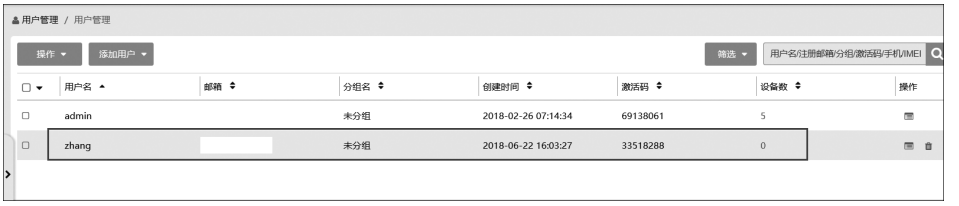

图 1-6　手动添加用户操作结果

（6）选择“添加用户”→“批量导入”菜单命令，如图 1-7 所示。

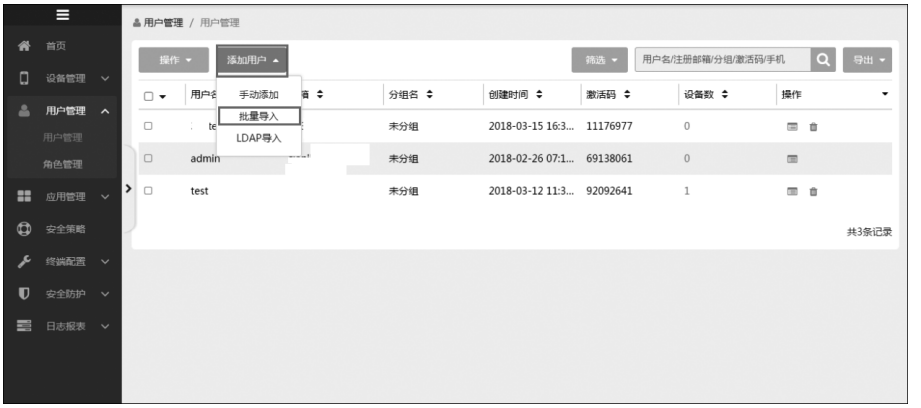

图 1-7　选择“批量导入”菜单命令

（7）在“批量导入用户”界面中，选择“下载 XLS 文件模板”菜单命令，如图 1-8 所示。

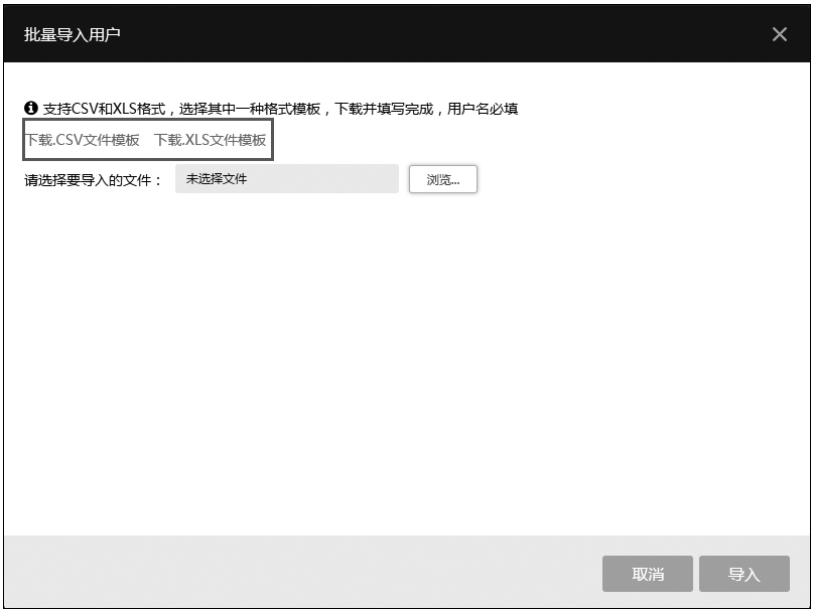

图 1-8　下载模板

（8）将下载好的模板保存至“C:\天机实验”中，如图 1-9 所示。

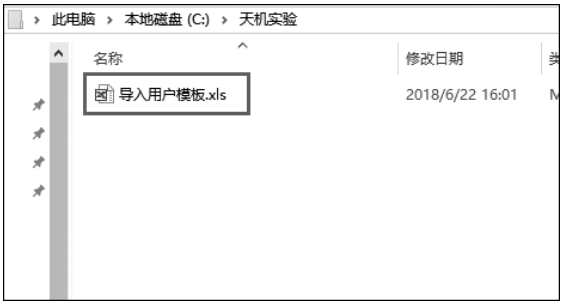

图 1-9　将模板放至指定路径

（9）双击打开“C:\天机实验”下的“导入用户模板.xls”文件，如图 1-10 所示。

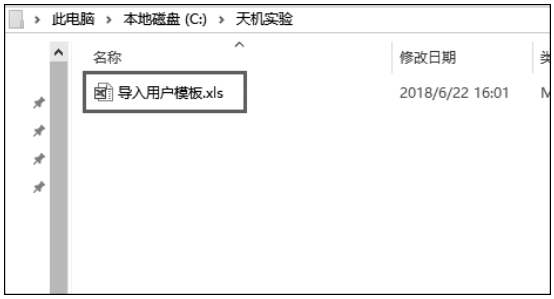

图 1-10　打开文件

（10）发现有两个用户的 IMSI1 相同，如图 1-11 所示。

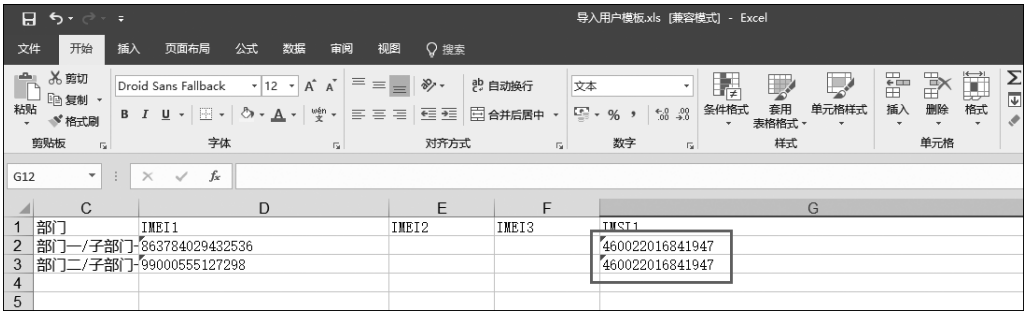

图 1-11　发现格式问题

（11）修改其中一个的 IMSI1 为 460022016841948，使两者不重复，否则无法批量导入至移动终端安全管理系统，如图 1-12 所示。

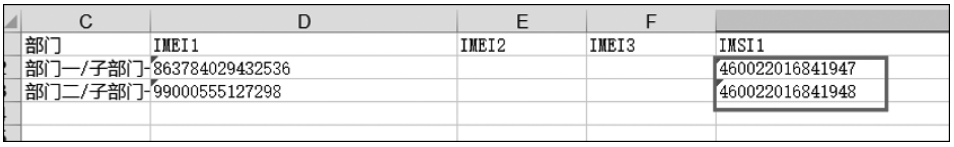

图 1-12　修改格式问题

（12）选择左上角“文件”→“保存”菜单命令，保存此次修改，如图 1-13 所示。

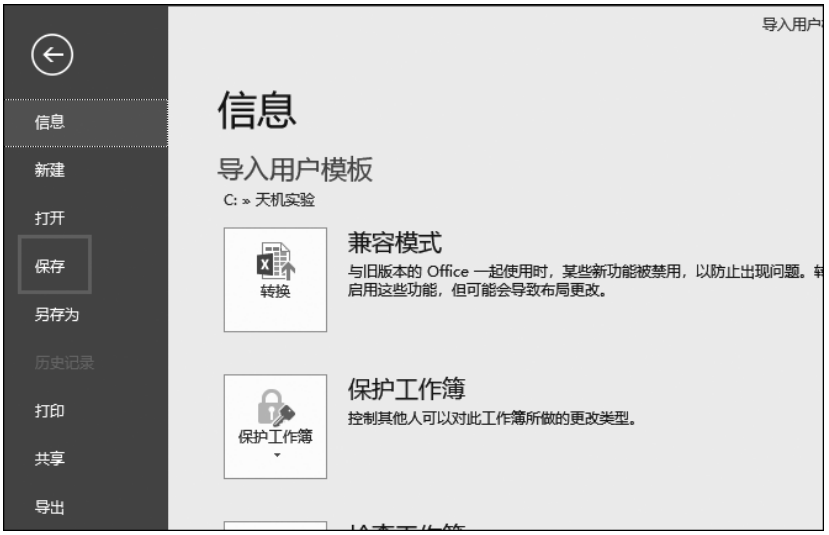

图 1-13　保存修改

（13）返回“批量导入用户”界面中，单击“浏览”按钮，如图 1-14 所示。

（14）选择“C:\天机实验”下的“导入用户模板.xls”，单击“打开”按钮，如图 1-15 所示。

（15）界面显示将要导入的信息，单击“导入”按钮，如图 1-16 所示。

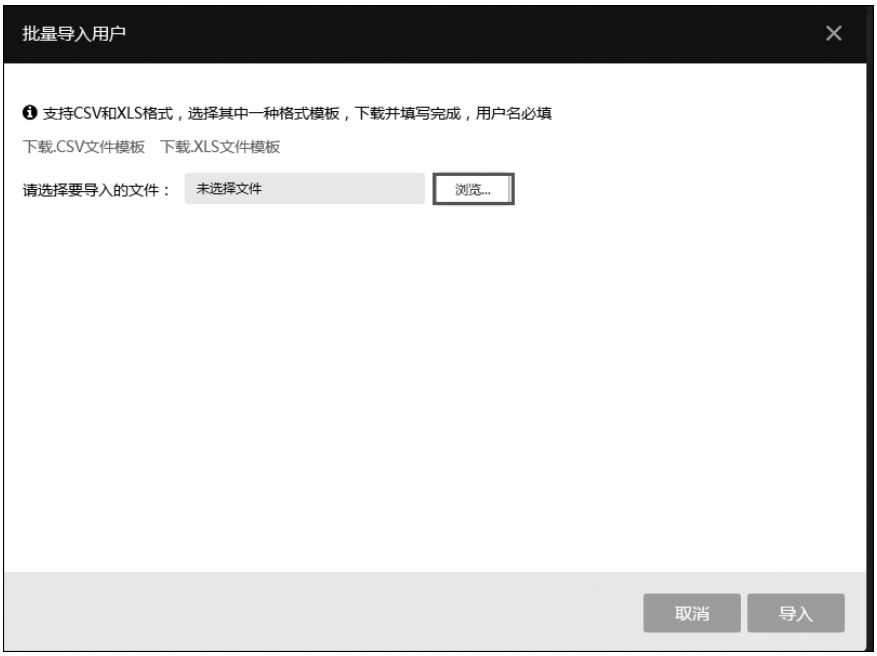

图 1-14　单击“浏览”按钮

图 1-15　选择模板打开

(16) 导入成功,在页面可以找到新导入的用户,如图 1-17 所示。

【实验预期】

(1) 成功执行“手动添加”操作。

(2) 成功执行“批量添加”操作。

图 1-16　单击“导入”按钮

图 1-17　批量添加用户操作结果

【实验结果】

(1)“手动添加”用户信息操作成功，添加的用户信息被保存。

在“用户管理”界面，可以发现通过手动添加的用户 zhang 创建成功，如图 1-18 所示。

图 1-18　“手动添加”创建结果

（2）“批量添加”用户信息操作成功，添加的用户信息被保存。

在“用户管理”界面可以发现通过批量添加的用户“李四”“张三”创建成功，如图 1-19 所示。

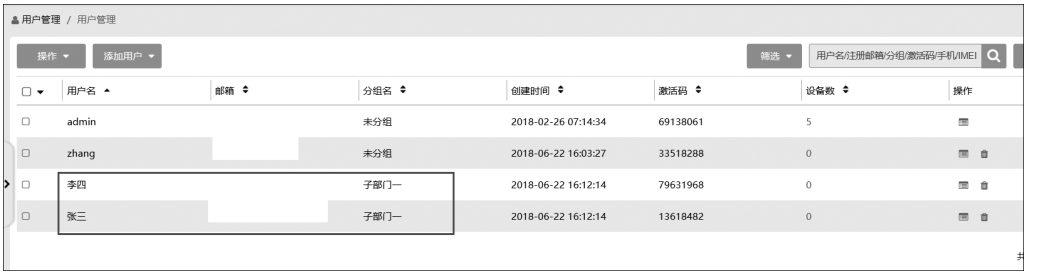

图 1-19　“批量添加”创建结果

【实验思考】

（1）如何为“手动添加”的用户分组？

（2）“批量导入”文件时若出现格式错误提示导致无法导入，如何处理？

1.1.2　角色管理实验

【实验目的】

掌握移动终端安全系统的角色管理操作。

【知识点】

用户管理、角色管理。

【场景描述】

A 公司的移动终端安全管理系统投入使用后，由于不同职能部门管理的权限不同，需要对各职能部门管辖权限进行管理和界定。因此，运维工程师小王需要在移动终端安全管理系统中对各职能部门的角色进行设定和配置，请帮助小王对移动终端安全管理系统的用户权限进行设定。

【实验原理】

管理员可通过移动终端安全管理系统的“用户管理”下的“角色管理”模块，对系统中的角色进行管理，包括创建新角色、设置角色拥有权限、授予用户特定的角色和权限。

【实验设备】

安全设备：移动终端安全管理系统设备 1 台。

网络设备：无线 AP 1 台。

移动终端：Android 手机 1 台。

主机终端：Windows 7 主机 1 台。

【实验拓扑】

实验拓扑如图 1-20 所示。

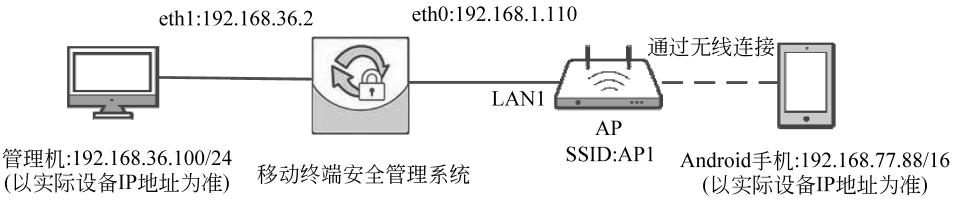

图 1-20　角色管理实验拓扑图

【实验思路】

(1) 进入移动终端安全管理系统。

(2) 在“角色管理”模块中创建角色。

(3) 在“用户管理”模块中创建用户。

(4) 为用户分配角色。

【实验步骤】

(1) 在实验平台对应实验拓扑左侧的管理机中打开浏览器,在地址栏中输入移动安全终端设备的地址 https://192.168.36.2,在登录界面中输入对应的管理员账号 admin、密码 tianji 和验证码(以实际的账号和密码为准),单击“登录”按钮,即可进入控制台管理界面进行相应管理员操作,如图 1-21 所示。

图 1-21　登录 Web 管理界面

(2) 选择面板左侧导航栏中的“用户管理”→“角色管理”菜单命令,如图 1-22 所示。

(3) 在“角色管理”界面中,单击“添加角色”按钮,如图 1-23 所示。

(4) 输入角色名称为“audadmin”,勾选“日志报表”复选框,角色为 audadmin 的用户将拥有查看和管理日志的权限,如图 1-24 所示。

图 1-22　单击“角色管理”按钮

图 1-23　单击“添加角色”按钮

（5）单击“选择管理范围”单选按钮，选择需要编辑的管理范围，勾选“本地”下方的“部门一”复选框，单击“确认”按钮，如图 1-25 所示。

（6）“角色名称”为 audadmin 的角色添加成功，其中“已授权”数为 0，如图 1-26 所示。

（7）选择面板左侧导航栏中的“用户管理”→“用户管理”菜单命令，进入“用户管理”界面，如图 1-27 所示。

（8）在“用户管理”界面中，单击“添加用户”菜单命令，共有 3 种添加方式，包括“手动添加”“批量导入”以及“LDAP 导入”。单击“手动添加”按钮，如图 1-28 所示。

（9）在“手动添加用户”界面中，输入对应的用户属性信息，输入用户名为“zhang”，输入邮箱为“zhang@gongsi.cn”，输入用户手机号码为“13112345272”，用户所属分组为“未分组”，取消勾选“发送邮件激活”和“发送短信激活”复选框，其他保留默认配置，单击“确认”按钮，如图 1-29 所示。

图 1-24　新建角色

图 1-25　设置“选择管理范围”

图 1-26　添加角色结果

图 1-27　“用户管理”界面

图 1-28　单击“手动添加”按钮

(10) 返回“用户管理”界面,可见成功添加的 zhang 用户,如图 1-30 所示。

(11) 单击用户名为 zhang 的新用户右侧的“详情”按钮,如图 1-31 所示。

(12) 在“用户详情”界面中单击“编辑”按钮,如图 1-32 所示。

(13) 单击“角色类型”下拉菜单,选择“管理员”,选择新建的角色 audadmin,设置初始密码为“Tianji”,配置结束后单击“保存”按钮,如图 1-33 所示。

图 1-29　手动添加用户

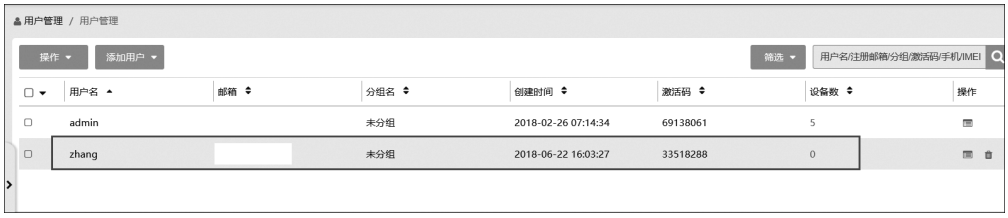

图 1-30　手动添加用户操作结果

图 1-31　单击“详情”按钮

【实验预期】

(1) 在移动终端安全管理系统的“角色管理”模块中成功添加新角色。

(2) 为用户分配新角色。

【实验结果】

1. 成功添加新角色

选择管理界面左侧“用户管理”→“角色管理”菜单命令,可以发现“角色名称”为audadmin 的新角色创建成功,如图 1-34 所示。

图 1-32　单击“编辑”按钮

图 1-33　设置“角色类型”

图 1-34 “角色管理”操作结果

2. 成功为用户分配角色

(1) 在“角色管理”界面中,可以发现新角色 audadmin 的“已授权”由 0 变为 1,单击“已授权”中的 1 图标,如图 1-35 所示。

图 1-35 单击“已授权”1 图标

(2) 可以看到“用户名”为 zhang 的用户已被授权 audadmin 角色,并拥有 audadmin 角色所拥有的管理权限,如图 1-36 所示。

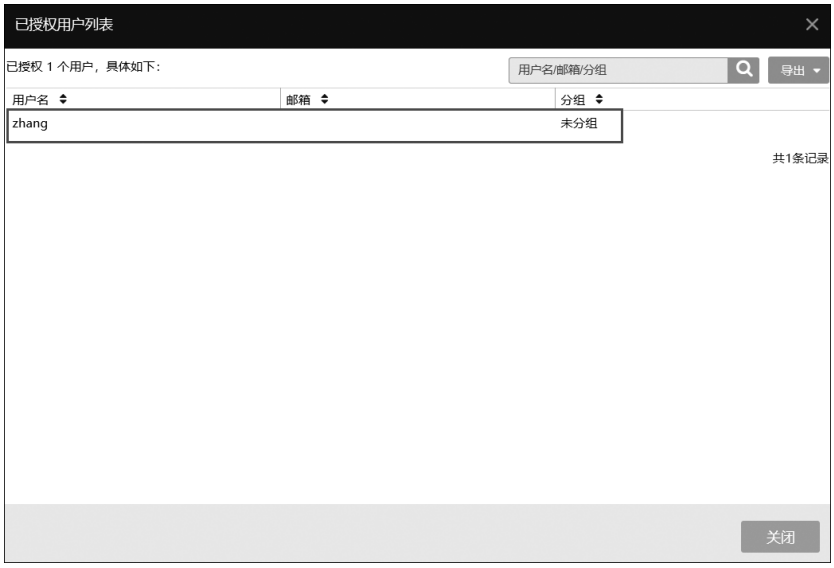

图 1-36 查看新角色授权信息

3. 新建管理员登录

(1) 在管理机中重新打开浏览器,在地址栏中输入移动安全终端设备的地址 https://192.168.36.2,在登录界面中输入对应的新建管理员账号的邮箱"zhang@gongsi.cn"、密码 Tianji 和验证码(以实际的账号和密码为准),单击"登录"按钮,即可进入控制台管理界面进行相应管理员操作,如图 1-37 所示。

图 1-37　新建管理员登录界面

(2) 登录成功,界面显示用户名为 zhang 的管理员拥有的职责和权限,可以看到此管理员拥有日志报表管理功能,如图 1-38 所示。

图 1-38　登录成功

【实验思考】

如何重新修改角色拥有的管理范围?

1.2　设备管理

1.2.1　设备准入管理实验

【实验目的】

使用移动终端安全管理系统设置设备准入条件,管理接入系统的设备。

【知识点】

设备管理、设备准入。

【场景描述】

A公司的运维工程师小李想了解目前公司到底有多少员工接入了移动终端安全系统，了解之后发现公司使用各种型号的手机进行移动办公，为了实现标准、统一化管理，公司要求员工使用指定型号的手机接入移动终端安全管理系统，小李该如何实现这一需求呢？

【实验原理】

管理员可通过移动终端安全管理系统“设备管理”下的“设备准入”模块对接入系统的设备进行管理，通过设置设备准入条件控制设备能否接入终端安全管理系统。

【实验设备】

安全设备：移动终端安全管理系统设备1台。

网络设备：无线AP 1台。

移动终端：Android手机1台。

主机终端：Windows 7主机1台。

【实验拓扑】

实验拓扑如图1-39所示。

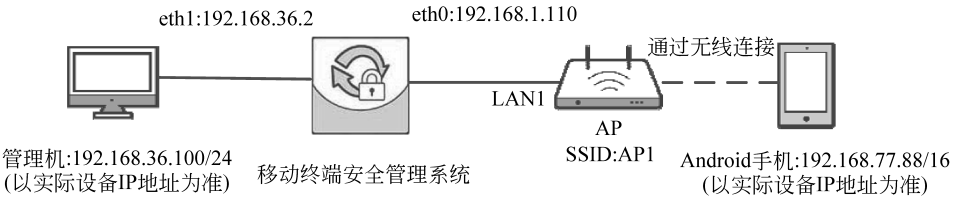

图1-39　设备准入管理实验拓扑图

【实验思路】

(1) 进入移动终端安全管理系统。

(2) 配置Android手机。

(3) 在“设备准入”模块中设置设备准入条件，使得设备允许接入终端。

(4) 更改“设备准入”中的设备准入条件，使得设备禁止接入终端。

【实验步骤】

(1) 在实验平台对应实验拓扑左侧的管理机中打开浏览器，在地址栏中输入移动安全终端设备的地址https://192.168.36.2，在登录界面中输入对应的管理员账号admin、密码tianji和验证码(以实际的账号和密码为准)，单击“登录”按钮，即可进入控制台管理界面进行相应管理员操作，如图1-40所示。

(2) 选择面板左侧导航栏中的“用户管理”→“用户管理”菜单命令，进入“用户管理”

图 1-40　登录 Web 管理界面

界面，可见 admin 用户，它的激活码为 69138061，用于验证可信手机与设备的连接，如图 1-41 所示。

图 1-41　进入用户管理界面

（3）配置 Android 手机的正常连接。首先配置 Android 手机的网络连接，打开 Android 手机的“设置”应用，如图 1-42 所示。

（4）选择 WLAN 菜单命令，设置无线连接，如图 1-43 所示。

（5）开启 WLAN 设置，在 WiFi 列表中连接无线网络，并输入密码（以实际为准），如图 1-44 所示。

（6）单击“连接”按钮，成功连接此无线网络，如图 1-45 所示。

（7）为 Android 手机安装 tianji.apk，此文件负责连接手机和设备。首先通过某个通信软件将此 APK 文件传输至手机终端，接着在手机终端打开 tianji.apk 安装包，单击“安装”按钮，如图 1-46 所示。

（8）安装完毕，单击“打开”按钮，运行程序，如图 1-47 所示。

（9）在界面中单击“确定使用”按钮。

图 1-42　打开“设置”应用

图 1-43　打开 WLAN

图 1-44　打开 WLAN 开关

图 1-45　成功连接无线网络