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 AP1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。



【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

										-	设置▼ 关于	-▼ 授权▼
	≡		▲ 用户	管理 / 用戶	白管理							
ñ				₽ <i>0</i> = -	法加用户 🚽	1				タ/注册邮箱/分组/激活码/3	£机. O	
۵	设备管理	~			10501107				71022			3.41
	用户管理	~	<u> </u>	用户名	3 🔺	邮箱 ◆	分组名 🗢	创建时间 🗘	激活码 ◆	设备数 💠	操作	
	用户管理			admii	n		未分组	2018-02-26 07:14:	69138061	0		
	角色管理											共1条记录
=	应用管理	~	}									
٥	安全策略		μ									
r	终端配置	~										
U	安全防护	~										
	日志报表	~										

图 1-3 进入"用户管理"界面

	=	â	。用户管理	/ 用户管	理							
*		ľ	操作		添加用户 🔺				筛选 -	用户名/注册邮箱/分组/激活码/手	n Q	●田 ●
۵	设备管理			用户名	手动添加	ā ≜	分组名 ♣	创建时间 🗅	激活码 ✿	设备数 🛔	操作	
4	用户管理		0	admi	批量导入	r	未分组	2018-02-26 07:1	69138061	0		
	用户管理 角色管理			test	LDAP导入 I.	z	未分组	2018-03-12 11:3	92092641	1	□ û	
=	应用管理	>										共2条记录
٥	安全策略	J										
r	终端配置											
U												
101	日志报表											

图 1-4 选择"手动添加"菜单命令

手动添加用户				×
用户名:	zhang			
最大同时活跃设备:	3 •			
邮箱:				
用户所属分组:	未分组			
用户手机号码:		0		
IMSI:		0		
IMEI:		0		
TF ID:		•		
	□ 发送邮件激活 □ 发送短信激活			
		-	取消	确认

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。

4

	▲用户管理 / 用户管理											
	操作 •											
	•	用户名 ▲	±1540 \$	分组名 ◆	创建时间 🕈	激活码 ◆	设备数 ◆	操作				
		admin		未分组	2018-02-26 07:14:34	69138061	5					
	0	zhang		未分组	2018-06-22 16:03:27	33518288	0	= e				
>												

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。

	Ξ		4	用户管理	/ 用户管理									
*				提/E	▼ 逐加月					篩洗 -	用户名/注册邮箱/分组/激活码/手;	印.	0	9# •
۵	设备管理	~		25611				0.00	0/700/1/7					
	用户管理	^		•	用户2 手2	切添加 首	Ŧ	分组名 ▼	创運町间 ▼	激活的 ₹	设置数 ▼	操作		•
					te LDA	AP导入		未分组	2018-03-15 16:3	11176977	0		ΰ.	
					admin			未分组	2018-02-26 07:1	69138061	0			
==	应用管理	~	>		test			未分组	2018-03-12 11:3	92092641	1		÷	
٥	安全策略													共3条记录
æ	终端配置	~												
U		~												
808		~												

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。

批量导入用户	×
 ● 支持CSV和XLS格式,选择其中一种格式模板,下载并填写完成,用户名必填 下载.CSV文件模板 下载.XLS文件模板 请选择要导入的文件: 未选择文件 浏览 	
取消	导入

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。

>	此电脑 > 本地磁盘 (C:) >	天机实验		
	^ 名称	^	修改日期	类
*	國 导入用户模板.xls		2018/6/22 16:01	N
*				
*				
*				

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。

•	此电脑 > 本地磁盘(C:) > 天机实验		
	^ 名称 ^	修改日期	类
*	國 导入用户模板.xls	2018/6/22 16:01	N
*			
*			
7			

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。

- 🖬 ち・♂ - =			:入用户模板.xls [兼容模式] - Excel	
文件开始。插入页面布局公式数据。审阅初	图 ♀ 搜索			
● X 剪切 Droid Sans Fallback v 12 v A A = =	= ≫ - ^{ab} I	自动换行 文本	* *	
お貼・ジ格式刷 Β Ι 旦・ 団・ ひ・ ▲・ 「笑・ 三 三	≡ ≣ ≣ ⊟ 1	合并后居中 👻 🔄	· % , *.8 →.00 条件格式 套用 • 84格式 • 表格格式 •	
剪贴板 🔩 字体 🕵	对齐方式	ra	数字 🔂 样式	单元格
G12 ▼ : × √ f _x				
C D	E	F		G
1 部门 INEI1	IMEI2	IMEI3	INGLI	
2 部门—/子部门-863784029432536			460022016841947	
3 部门二/子部门-99000555127298			460022016841947	
4				
5				

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 人至移动终端安全管理系统,如图 1-12 所示。

	С	D	E	F	
	部门	IMEI1	IMEI2	IMEI3	IMSI1
2	部门—/子部门-	863784029432536			460022016841947
;	部门二/子部门-	99000555127298			460022016841948
Ļ					

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。

7

批量导入用户		×
● 支持CSV和XLS格式,选择其中一种格式模板,下载并填写完成,用户名必填		
下载LSV又件模板 下载.XLS又件模板 请选择要导入的文件: 未选择文件 浏览		
	取消	导入

图 1-14 单击"浏览"按钮

tit#						×
← → • ↑			~ Q	搜索"天机实验"		م
组织 ▼ 新建文件夹				8==	• 💷	0
	修改日期	类型	大小			
3D 对象 國 导入用户模板.xls	2018/6/22 16:05	Microsoft Excel	25 K	В		
副 视频						
■ 图片						
◆ 下载						
• 本地磁盘 (C:)						
→ 本地磁盘 (D:)						
SAMISUNG (F.)						
SAMSUNG (F:) 🗸						
文件名(N): 导入用户模板.xls			~	自定义文件		\sim
					間で光	
					-蚁/月	

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。

■■● 无线网络安全实验指导

批量导入	批量导入用户 ×										
● 支持CSV和XLS格式,选择其中一种格式模板,下载并填写完成,用户名必填 下载.CSV文件模板 下载.XLS文件模板											
	子入的又件: 导入的信息,	: 与八川/模板.Xis 上传成功 , 滚动加载更多信息, 请确认	人格式正确后点击导	<u>5</u> 入。							
原因	用户名	邮箱	部门	IMEI1	IMEI2	IMEI3	IMSI1				
	张三	zhangsan@gongsi.com	部门—/子部门—	863784029432536	-	-	46002201				
	李四	lisi@gongsi.com	部门二/子部门—	99000555127298	-		46002201				
✓	牛激活 🗆	发送短信激活				_	,				
	取消 导入										

图 1-16 单击"导入"按钮

ł	▶ 用户管理 / 用户管理											
	操作	: ▼ 参加用户 ▼	用户名/注册邮箱/分组/激活码/手	RUIMEI Q								
	•	用户名 ▲	邮箱 ◆	分组名 🕈	创建时间 🕈	激活码 ◆	设备数 ♥	操作				
		admin		未分组	2018-02-26 07:14:34	69138061	5					
	0	zhang		未分组	2018-06-22 16:03:27	33518288	0					
>		李四		子部门一	2018-06-22 16:12:14	79631968	0	- ÷				
	0	张三		子部门一	2018-06-22 16:12:14	13618482	0	= i				

图 1-17 批量添加用户操作结果

【实验结果】

8

(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。

4	▲用户管理 / 用户管理										
I	操作	筛选 ▼ 用户名/注册邮箱/:									
		用户名 ▲	邮箱 ◆	分组名 ♥	创建时间 ◆	激活码 ♦	设备数 ◆				
	0	admin		未分组	2018-02-26 07:14:34	69138061	5				
	• [zhang		未分组	2018-06-22 16:03:27	33518288	0				
>		李四		子部门一	2018-06-22 16:12:14	79631968	0				
	0	张三		子部门一	2018-06-22 16:12:14	13618482	0				

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。

	▲用户管理 / 用户管理												
	複作 • 添加用户 • 稍应名注册部输分组成运得手机 Mel Q												
	•	用户名 ▲	邮箱 🗢	分组名 ♥	创建时间 🕈	激活码 ♥	设备数 ◆	操作					
		admin		未分组	2018-02-26 07:14:34	69138061	5						
	0	zhang		未分组	2018-06-22 16:03:27	33518288	0		ı				
>	0	李四		子部门一	2018-06-22 16:12:14	79631968	0	= 6	t				
	0	张三		子部门—	2018-06-22 16:12:14	13618482	0		1				
									ŧ				

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 AP1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。



【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。

	=	_	山 数据统计列表					1
*	首页			0		0		0
۵	设备管理	~		已激活设备		设备合规	×	设备违规
•	用户管理	1						
	用户管理	_	设备违规情况				策略执行情况	
	角色管理							
=	应用管理	~						
٩	安全策略							
r	终端配置	~						
U		~		0 1	皆无数据可以展示		④ 暫无:	敗据可以展示
11		~						

第1章 移动终端安全

图 1-22 单击"角色管理"按钮

	=		▲ 用户管理 / 角色管理						
*			添加角色				角色名称	Q	导出 ▼
۵	设备管理	~	角色名称 ≑	分类 ≑	创建时间 ≑	管理权限	已授权 ◆	操作	_
*	用户管理	^	超級管理员	超级管理员	2018-02-26 07:14:35	全部	1		
									共1条记录
=	应用管理	~							
٩	安全策略								
r	终端配置	~							
U		~							
		~							

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。

新建角色				×
*角色名称: audadmin				
管理范围: 所有人员 	◎ 选择管理	里范围		
权限设置: 🗌 全选				
设备管理		终端配置		
设备管理		Exchange配置		
设备定位		WiFi配置		
自定义属性		书签配置		
设备标签		证书配置		
фШ	0	VPN配置		
应用主场(Andraid)	0	其他邮件配置		
应用市场(Android)		0+42+		
应用市场(IOS)		日志版表		
应用安装统计		设备日志		
安全策略		应用日志		
文上术前		管理员日志		
文王來昭	U	阜出日志		
			取消	确认

图 1-24 新建角色

	新建角色								×
*	角色名称: 管理范围: 分组	audadmi 〇 所有ノ 标签	n 、员 • 选择管理 智能标签	它围]				
	搜索分组			Q		₿ 刷新	展开▼	收起▲	
	□□ 本地								
	⊞ ☑ 部	í)—							
		1)							
		分组							
		∆₽≠分组							
							取消	确	认

图 1-25 设置"选择管理范围"

_						
	▲用户管理 / 角色管理					
	添加角色					
	角色名称 🗘	分类 ♦	创建时间 ◆	管理权限	已授权	÷
	audadmin	管理员	2018-06-22 16:23:00	设备日志、应用日志、管理员日志、	0	
	admin	超级管理员	2018-02-26 07:14:35	全部	1	
1						

图 1-26 添加角色结果

	=		8	用户管理	里 / 用戶	「管理							
ñ				場作		法加田白 🖌				御供 。 用户	乞/注册邮箱/分组/激活码/3	11.0	8.41 -
۵	设备管理			1001						9102 <u>0</u> - 1107 -			
	用户管理			•	用户名	3 🔺	邮箱 ◆	分组名 ♦	创建时间 🕈	激活码 ◆	设备数 ◆	操作	
	用户管理				admi	n		未分组	2018-02-26 07:14:	69138061	0		
	角色管理												共1条记录
==	应用管理												
٥	安全策略		J										
se.	终端配置												
U	安全防护		L										
NU	日志报表	~											

图 1-27 "用户管理"界面

	=		4	。用户管理	/ 用户智	ஊ								
*				操作		添加用户 ▲	1			筛选 -	用户名/注册邮箱/分组/激活码/手	机	Q	导出 -
۵	设备管理	~		0	HD4	毛动添hn]] = =	公泊么 ≜	∂!ஊோர்த் ≜	激活码 ≜	(凸体)数 ≜	揭/5		
۵	用户管理	^			admi	批量导入		≠⇔⁄细	2018-02-26 07:1	69138061	0			
				0	adirin	LDAP导入		777 1 2	2010-02-20 07.1	05150001	0			
	角色管理				test			未分组	2018-03-12 11:3	92092641	1		Û	
==	应用管理	~	>											共2条记录
٩	安全策略													
₽°C	终端配置	~												
U		~												
		ř												

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。

手动添加用户				×
用户名:	zhang			
最大同时活跃设备:	3 •			
邮箱:				
用户所属分组:	未分组			
用户手机号码:		•		
IMSI:		0		
IMEI:		0		
TF ID:		0		
Γ	□ 发送邮件激活 □ 发送短信激活			
_		-	取消	确认

图 1-29 手动添加用户

۵	▲用 户管理 / 用户管理								
操作 ▼ 添加用户 ▼						用户名/注册邮箱/分组/激活码/手			
		用户名 ▲	邮箱 🗢	分组名 🕈	创建时间 🕈	激活码 ◆	设备数 ◆	操作	
	0	admin		未分组	2018-02-26 07:14:34	69138061	5		
1	0	zhang		未分组	2018-06-22 16:03:27	33518288	0	= ±	
>									

图 1-30 手动添加用户操作结果

▲用户	▲用户管理 / 用户管理							
ł	操作 ▼					筛选 ▼ 用户名/注册邮箱/分组/	數活码/手机/IMEI Q	
•	用户名 ▲	邮箱 ◆	分组名 ◆	创建时间 🕈	激活码 ♦	设备数 ◆	操作	
0	admin		未分组	2018-02-26 07:14:34	69138061	5		
0	zhang		未分组	2018-06-22 16:03:27	33518288	0	= ±	
•							详情	

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。

用户详情			×
			í
用户名:	zhang	编辑	
角色类型:	普通用户		
邮箱:			
用户所属分组:	未分组		
分组路径:	本地 / 未分组		
导入时间:	2018-06-22 16:03:27		
激活码:	33518288		
用户手机号码:	13112345272		
IMSI:	无		
IMEI:	无		
		关闭	

图 1-32 单击"编辑"按钮

用户详情			×
			The NH (see 4-2)
用户名:	zhang		取消骗饵
角色类型:	管理员 ▼ audadmin ▼		
初始密码:		隐藏密码	
邮箱:			
用户所属分组:	未分组		
分组路径:	本地 / 未分组		
导入时间:	2018-06-22 16:03:27		
激活码:	33518288		
用户手机号码:	13112345272	Ð	
IMSI:		0	
			保存

图 1-33 设置"角色类型"

无线网络安全实验指导	

		. 田白啓理 / 角色答理			
ñ		ENGA			
۵	设备管理 🖌 🖌	漆加用巴			
	用户管理へ	用巴名称 ▼	分类▼	创建时间 ▼	管埋仪限
	 用户管理	audadmin	管理员	2018-06-22 16:23:00	设备日志、应用日志、管理员日志、…
	角色管理	admin	超级管理员	2018-02-26 07:14:35	全部
==	应用管理・				
٩	安全策略				
se.	终端配置 🖌				
U	安全防护 🗸				

图 1-34 "角色管理"操作结果

2. 成功为用户分配角色

16

(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。

▲ 用户管理 / 角色管理					
添加角色					
角色名称 ◆	分类 ◆	创建时间 ◆	管理权限	已授权	\$
audadmin	管理员	2018-06-22 16:23:00	设备日志、应用日志、管理员日志、…	1	
admin	超级管理员	2018-02-26 07:14:35	全部	1	

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。

已授权用户列表				×
已授权 1 个用户,具体如下:		用户名/邮箱/分组	Q	导出 ▼
用户名 🕈	邮箱 🕈	分组 ♥	_	
zhang		未分组		
				共1条记录
				关闭

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。

nx oge 🎧				zhang@360.cn ▼ 关于 ▼ 援权 ▼
=	LAL 数据统计列表			
☆ 首页 □ 日志报表 >		D.	0 设备会规	 0 Realized
	最新事件			
	时间 设备使用人	设新型号	事件	
		E 1 00	# ㅋ	

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?



1.2.1 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 AP1台。 移动终端:Android 手机1台。 主机终端:Windows7主机1台。

【实验拓扑】

实验拓扑如图 1-39 所示。



【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" — 18 —



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。

									▼ 设置▼ 关	于▼ 授权▼
	=		▲ 用户管理 / 用户管理							
ñ			操作 ▼ 添加用户 ▼				筛选 -	用户名/注册邮箱/分组/激活码	3/手机 Q	──────
۵	设备管理	~		邮箱 ♦	分組名 ♣	创建时间 🗅	激活码 ♦	设备数 ♠	操作	
-	用户管理	^			774H +	60A8431-3 +	MANHED +		19611	
	用户管理		admin		未分组	2018-02-26 07:14:	69138061	0		
	角色管理									共1条记录
==	应用管理	~	`							
0	安全策略									
æ	终端配置	~								
U	安全防护	~								
	日志报表	~								

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

设置	t	
U	设直 	×
	更换壁纸 对屏幕进行个性化设置	×
ł	飞行模式	
	双卡管理	>
	WLAN	已关闭 〉
*	蓝牙	已关闭 〉
1	流量管理	>
	更多	>
	桌面风格	标准风格 >
	显示	>
	声音	>
	\triangleleft O	

٦

图 1-43 打开 WLAN



 \equiv wlan WLAN WLAN+ 已关闭 > 提升网络智能连接体验 可用 WLAN 列表 123 加密 lab **a** 加密 SYS1210 <u></u> 加密 TP-LINK_5A08 **?** 加密 那么 <u></u> 加密 1210-myq -加密 210 扫描/q5 ☆ WLAN 直连 : 更多 71 \triangleleft \bigcirc

图 1-44 打开 WLAN 开关