



惠尔顿网络安全审计功能介绍—如何应对保密检查

深圳市惠尔顿信息技术有限公司

黄章鹏

2021年4月29日



提 纲

1

军工企业上网要求

2

网络安全审计功能介绍

3

应对保密检查注意事项

4

版本升级应对保密新要求



提 纲

1

军工企业上网要求

2

网络安全审计功能介绍

3

应对保密检查注意事项

4

版本升级应对保密新要求



背景

传统企业由于长期从事简单的订单出口业务，注重生产，利润薄负担重，制造业处于水深火热中，2015年国家提出军民融合战略，军方市场逐渐开放，让企业越来越看重这块市场，很多优质的企业趁机转型。

01

国家战略军民融合

部队有保密重任

02

03

民企需要军工订单



军工企业上网规定



《军工保密资格认定工作指导手册(2017年版)》的140、203、204、423、441、458页都有明确规定涉密用户做资格认证时必须要有对应上网防泄密的措施，没有就会扣4-5分;而且现在对于响应军民融合政策的诸多中小企业来讲，大部分人员主要时间都是在非涉密区工作，并需要用到网络，所以上网时不小心泄密成了一个可能泄密的高概率事件。

- 建立互联网接入审批和登记制度，严格控制互联网接入口数量，并采取符合有关规定和标准的监管技术措施。



军工保密资格认定—互联网部分要求

国家保密教育培训丛书

内部资料 注意保管

军工保密资格 认定工作 指导手册

(2017年版)

国家军工保密资格认定办公室 / 编



金城出版社
GOLD WALL PRESS

友善提醒：(摘抄以上手册的第441页，对涉密用户的要求)

1. 未建立互联网接入终端审批和登记制度，或者未设置管理人员的，**第1分**；
2. 单位在一地的互联网接入口多于2个，或者对接入口未采取符合规定的防护监管技术措施的，**第2分**；
3. 未采取管理和技术措施对互联网上网行为进行监控审计的，**第2分**。



军工保密资格认定—互联网部分要求

【原文】

7.6.24 应当建立互联网接入审批和登记制度，严格控制互联网接入数量，并采取符合有关规定和标准的监管技术措施。

【注释】

1. 单位应当选择依法取得经营许可证的互联网接入服务提供商，采取有线局域网的方式接入互联网。每一处独立的科研生产园区，互联网接入不得超过 2 个。

2. 放置在涉密场所的互联网接入终端不得配备、安装和使用摄像头、麦克风等视频、音频输入设备。

3. 集中使用的互联网接入终端应当指定专人负责管理和维护，并对使用情况和信息的导入导出进行监控和记录。分散使用的互联网接入终端也应当明确责任人，责任人对互联网接入终端使用和信息导入导出情况负责管理。

4. 应当采取技术措施对互联网接入终端的使用情况进行监控。使用互联网应当采用实名制方式登录，并通过上网行为监控审计系统，对上网时间、浏览网页、发送邮件、下载信息等进行监控和记录。监控和记录的信息应当至少保存 100 天，在保存期内记录不得修改或者删除。

项目	项目细则	分值	操作方法
互联网接入	202. 未建立互联网接入终端审批和登记制度，或者未设置管理人员的，扣 1 分；	4 分	a) 查验单位是否对设立、管理和使用互联网接入终端，提出了明确的安全保密和控制要求，是否建立了互联网接入终端的审批和登记制度； b) 查验工作区域内是否存在未履行审批程序的互联网接入终端，或者擅自使用的单台互联网计算机； c) 查验互联网接入终端是否明确责任人进行管理和监控； d) 查验相关登记和记录，确认责任人是否履行了监管职责。
	203. 单位在一地的互联网接入口多于 2 个，或对接入口未采取符合规定的监管技术措施的，扣 2 分；		a) 查验单位是否选择依法取得经营许可证的互联网接入服务提供商，采取有线局域网的方式接入互联网；在每一处独立的科研生产园区，互联网的接入口是否多于 2 个； b) 查验是否存在擅自接入或者使用的互联网接入终端（如果使用便携式计算机等信息设备，采取无线方式接入互联网，无论是采用无线网卡，还是 Wi-Fi、蓝牙等，一台接入设备就算一个出口）； c) 查验是否对互联网接入口，采取了防护、监控的管理和技术措施； d) 信息化管理部门、保密工作机构以及相关部门（机构）是否落实了监督检查。



我们的专业服务
使您的工作更轻松

军工保密资格认定—互联网部分要求

项目		项目细则	分值	操作方法
新闻 宣传 管理 (12分)		204. 未采取管理和技术措施对互联网上网行为进行监控审计的,扣1分。		a) 查验体系文件中相关的互联网安全策略和管理要求是否得到落实; b) 查验是否采取技术措施(互联网上网行为监控审计系统)对互联网接入终端的使用情况进行监控审计; c) 查验放置在涉密场所的互联网接入终端是否配备、安装和使用摄像头、麦克风等视频、音频输入设备; d) 查验单位通过互联网的信息发布,是否按要求履行审批程序,审批程序是否合规,审批单以及相关记录是否真实完整,妥善保存(不少于6个月); e) 查验是否对违规上网行为进行教育或者处罚。
		205. 宣传报道未按规定进行保密审查的,扣2分; 206. 举办展览未经保密审查或者主管部门审批的,扣2分; 207. 展品制作未采取严格控制措施的,扣1分; 208. 参观单位涉密展室未经批准的,扣1分; 209. 发表著作和论文未经保密审查的,扣2分; 210. 接受新闻媒体采访未经批准的,扣2分; 211. 参观武器装备科研生产现场未经主管部门审批的,扣2分。	12分	a) 查看单位主要采取哪些新闻宣传形式; b) 查看业务部门工作记载和保管的文件、资料,了解宣传报道、发表的著作和论文等,是否按要求、程序经过了保密审查、审批; c) 查看审查审批记录,了解举办展览、参观涉密展室、接受新闻媒体采访是否按要求、程序经过了保密审查或者主管部门审批;对参观人员是否履行了审批登记手续; d) 通过提问和查看有关资料,检查展品制作过程中是否采取了严格控制措施,对有涉密要求的是否选择具有相应涉密资质单位承担; e) 查看参观武器装备科研生产现场是否经过主管部门审批。



提 纲

1

军工企业上网要求

2

网络安全审计功能介绍

3

应对保密检查注意事项

4

版本升级应对保密新要求



上网也需要安检—泄密风险防范



实名登录有迹可循

- 实名登记并审核，符合规定才上网
- 所有过程有记录可查

审计的目的是防止泄密

- 网页浏览记录
- 邮件收发记录
- 及时通讯的聊天记录
- 详细的上网痕迹报表



审计功能介绍—上网认证模式选择

WEB认证

绿色客户端认证

指纹认证

IC卡认证

网络安全审计 W300NM

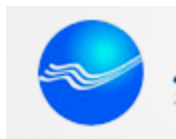


备注：客户可以根据本单位的需求情况选择不同认证的方式



审计功能介绍—军工认证审计内容要求

Baidu 百度



网页审计

邮件审计



文件审计

即时通讯
审计





提 纲

1

军工企业上网要求

2

网络安全审计功能介绍

3

应对保密检查注意事项

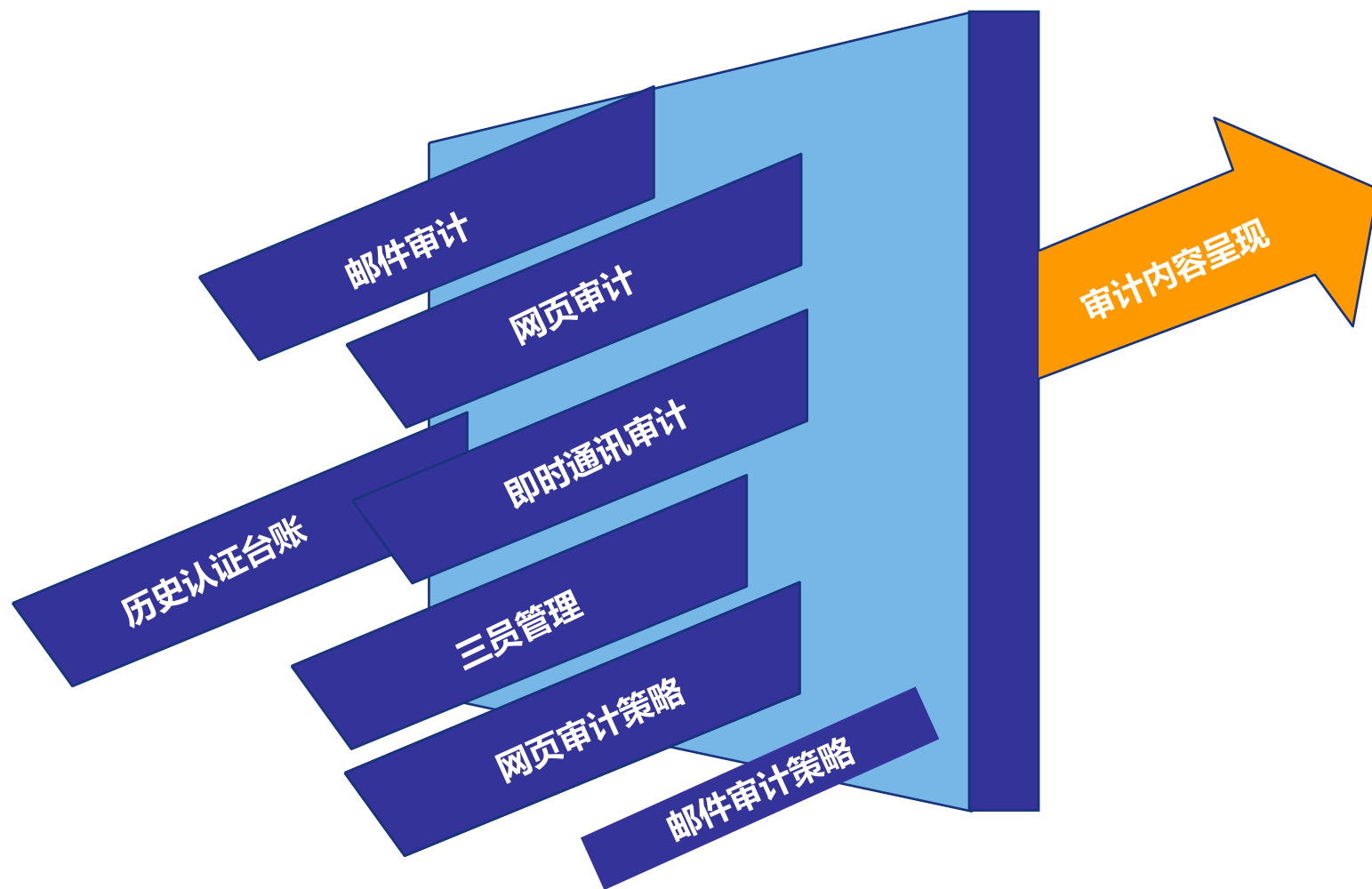
4

版本升级应对保密新要求



我们的专业服务
使您的工作更轻松

保密检查您准备好了吗？





实名认证--上网

 惠尔顿 网络安全审计V10.0

消息通知 修改密码 ? 技术支持 退出系统

导航菜单

实时分析

网络配置

认证配置

组织结构

认证设置

认证策略

认证类型

认证页定制

对象配置

系统状态 组织结构 x

组织结构

搜索组

ROOT

组织成员

添加用户 添加组 删除 清除指纹 备份 恢复 硬件身份管理平台下载

模糊查询

	☐	名称	登录方式	绑定信息	过期时间	状态	修改	操作
1	☐	何三	无限制	无绑定	永不过期	✓		查看截图
2	☐	张六	无限制	无绑定	永不过期	✓		查看截图
3	☐	段九	无限制	无绑定	永不过期	✓		查看截图
4	☐	刘五	无限制	无绑定	永不过期	✓		查看截图
5	☐	测试	指纹登录	无绑定	永不过期	✓		查看截图
6	☐	123	无限制	无绑定	永不过期	✓		查看截图
7	☐	11111	无限制	192.168.0.2 01:02:03:04:05:06	永不过期	✓		查看截图



实名认证--认证设置

系统状态 组织结构 × 认证设置 ×

认证基本设置

认证子网接口:

br0(eth0 <=> eth1)

认证登录页面:

http://192.168.254.6/login.html

验证码设置:

☐ 开启 ☒ 关闭

注销窗口:

☒ 开启 ☐ 关闭

认证成功跳转到:

☒ 用户认证前访问的页面
☐ 指定URL网址

www.baidu.com

WEB认证超时:

600

 分钟后将重新认证

保存

新增用户

☒ 启用该用户

用户名:

批量添加, 例如: 张三,李四,王五

该输入项为:

密码:

.....

(默认密码: 123456)

确认密码:

.....

☐ 首次登录强制修改密码

所属组:

ROOT

用户描述:

登录终端限制

☒ 无限制 ☐ 网页登录 ☐ 客户端登录 ☐ IC卡登录 ☐ 指纹登录 ☐ U盘KEY登录

用户绑定

☒ 无绑定

☐ 禁止重复登录
☒ 允许重复登录, 并踢掉上次登录的IP
☐ 允许重复登录, 并保持其它已登录IP可用, 最大登录数目

1000

☐ 绑定

☐ 绑定IP地址

0.0.0.0

☐ 绑定MAC地址

01:02:03:04:05:06

☐ 绑定计算机名

帐号过期

☒ 永不过期
☐ 指定过期时间

2021-04-26 09:04

保存 取消



上网认证界

当用户打开浏览器时，设备会弹出一个上网认证的登录界面给用户（无法弹出时可以主动访问 设备IP/login进行认证），用户输入我们在组织管理中定义的用户名称和密码即可上网

[←](#) [→](#) [↻](#) ⚠ 不安全 | 192.168.254.6/login [☆](#) [👤](#) [⋮](#)



惠尔顿上网认证系统

用户登录

用户名:

密码:

[登录](#)

[修改密码](#) [下载客户端](#) [保存到本地](#)



网页审计策略

网页审计策略-策略管理-应用层策略-网页管控-网页管控

 惠尔顿 网络安全审计V10.0

消息通知 修改密码 技术支持 退出系统

导航菜单

实时分析

网络配置

认证配置

对象配置

策略管理

防火墙

应用层策略

网页管控

网页标题

网页过滤记录

社交发帖管控

社交发帖记录

URL管控

邮件管控

系统状态

组织结构 ×

认证策略 ×

认证设置 ×

网页管控 ×

+ 新增

✗ 删除

✓ 启用

⊖ 禁用

↑ 上调

↓ 下调

	☐	名称	描述	用户对象	时间对象	网页内容关键字	域名关键字	方向	条件匹配	动作	告警级别	状态	编辑
1	☐	网页防泄密		所有用户	所有时间	保密,秘密,机密,绝密	保密,秘密,机	双向	任意一项匹配	告警	信息	✓	



网页标题审计

网页审计策略-策略管理-应用层策略-网页管控-网页标题-网页标题

 惠尔顿 网络安全审计V10.0

消息通知 修改密码 ? 技术支持 退出系统

导航菜单

实时分析

网络配置

认证配置

对象配置

策略管理

防火墙

应用层策略

网页标题

网页过滤记录

社交发帖记录

URL管控

邮件管控

IM管控

文件管控

系统状态

组织结构 ×

认证策略 ×

认证设置 ×

网页管控 ×

网页标题 ×

详细记录 ×

网站类型(请选择)

所有终端

2021-04-20 00:00:00

2021-04-26 23:59:59

=192.168.254.163

终端	用户名称	地址	URL	标题	语种	网站类型	风险级别	连接信息	时间
1	刘五 / 192.168.254.163	open.weixin.c	/connect/qrconnect?app	微信登录	中文	聊天室或	6	src=192.168.254.163	2021-04-20 1
2	刘五 / 192.168.254.163	g1.crm2.qq.co	/v222/crm2.0/page/cli	客户来源展示	中文	聊天室或	6	src=192.168.254.163	2021-04-20 1
3	刘五 / 192.168.254.163	g1.crm2.qq.co	/v222/crm2.0/cgi/clien	auto verify	中文	聊天室或	6	src=192.168.254.163	2021-04-20 1
4	刘五 / 192.168.254.163	open.weixin.c	/connect/qrconnect?app	微信登录	中文	聊天室或	6	src=192.168.254.163	2021-04-20 1
5	刘五 / 192.168.254.163	open.weixin.c	/connect/qrconnect?app	微信登录	中文	聊天室或	6	src=192.168.254.163	2021-04-20 1
6	刘五 / 192.168.254.163	mail.qq.com	/cgi-bin/readtemplate?	QQ邮箱 - 写信	中文	网页邮件	6	src=192.168.254.163	2021-04-20 1
7	刘五 / 192.168.254.163	mail.qq.com	/cgi-bin/mail_list?sid=	QQ邮箱 - 我的文件夹	中文	网页邮件	6	src=192.168.254.163	2021-04-20 1
8	刘五 / 192.168.254.163	wx.mail.qq.co	/list/readtemplate?nan	QQ邮箱	中文	网页邮件	6	src=192.168.254.163	2021-04-20 1
9	刘五 / 192.168.254.163	mail.qq.com	/cgi-bin/mail_list?sid=	QQ邮箱 - 收件箱	中文	网页邮件	6	src=192.168.254.163	2021-04-20 1
10	刘五 / 192.168.254.163	mail.qq.com	/cgi-bin/laddr_friend?f	QQ邮箱	中文	网页邮件	6	src=192.168.254.163	2021-04-20 1



邮件对象

策略管理-应用层策略-邮件管控-自定义邮件对象，如下图

惠尔顿 网络安全审计V10.0

消息通知 修改密码 技术支持 退出系统

系统状态 组织结构 × 认证策略 × 认证设置 × 网页管控 × 网页标题 × 详细记录 × 自定义邮件对象 ×

+ 新增 - 删除

	名称	描述	发件人	收件人	主题	正文	附件名	附件大小(KB)	条件匹配	方向	编辑
1	☐ 邮件防泄密对				保密,秘密,机	保密,秘密,机	保密,秘密,机	0	任意一项匹配	双向	

策略管理

- 防火墙
- 应用层策略
 - 网页管控
 - URL管控
 - 邮件管控
 - 自定义邮件对象



邮件管控策略

策略管理-应用层策略-邮件管控-邮件管控策略-----如下图

惠尔顿 网络安全审计V10.0

消息通知 修改密码 技术支持 退出系统

导航菜单

实时分析

网络配置

认证配置

对象配置

策略管理

系统管理

追溯系统

数据中心

应用层策略

网页管控

URL管控

邮件管控

自定义邮件对象

邮件管控策略

系统状态 组织结构 × 认证策略 × 认证设置 × 网页管控 × 网页标题 × 详细记录 × 自定义邮件对象 × 邮件管控策略 ×

+ 新增 - 删除 ✓ 启用 - 禁用 ↑ 上调 ↓ 下调

	名称	描述	邮件对象	用户对象	时间对象	动作	状态	告警级别	编辑
1	邮件防泄密		邮件防泄密对象	所有用户	所有时间	告警	✓	信息	

10 第 1 共 1 页

显示1到1,共1记录

当前用户: admin | 登录时间: 2021-04-26 09:12:14 惠尔顿版权所有 © 2021



邮件审计记录

策略管理-应用层策略-邮件管控-网页管控记录，如下图

 惠尔顿 网络安全审计V10.0

消息通知

修改密码

技术支持

退出系统

导航菜单

实时分析

网络配置

认证配置

对象配置

策略管理

- 网页管控
- URL管控
- 邮件管控
 - 自定义邮件对象
 - 邮件管控策略
 - 邮件管控记录
- IM管控

系统管理

追溯系统

数据中心

组织结构 ×

认证策略 ×

认证设置 ×

网页管控 ×

网页标题 ×

自定义邮件对象 ×

邮件管控策略 ×

邮件管控记录 ×

详细记录 ×

所有终端

2021-03-10 00:00:00

2021-04-26 23:59:59

=192.168.254.163

邮件类型

关键字

导出

	用户名称	策略名称	邮件类型	发送	主题	大小	风险级别	动作	时间	操作
1	刘五 / 192.168.	-	WEB发件	755132@qq.com	111	0 B		审计记录	2021-04-20 15:35:	更多
2	刘五 / 192.168.	-	WEB发件	755132@qq.com	111	0 B		审计记录	2021-04-20 15:35:	更多
3	刘五 / 192.168.	-	SMTPTS发件	"huangzhangper	测试报告	14 B		审计记录	2021-04-20 15:33:	更多

10

第 1 共1页

显示1到3,共3记录

当前用户: admin | 登录时间: 2021-04-26 09:12:14

惠尔顿版权所有 © 2021



邮件审计记录

完整内容



[查看邮件原始排版](#)

用户组/用户名/IP地址	刘五 / 192.168.254.163
MAC地址	58:FB:84:4A:59:0C
终端类型	电脑
发件人	"huangzhangpeng8868@163.com" <huangzhangpeng8868@163.com>
收件人	755131 <755131@qq.com>
主题	测试报告
邮件地址	220.181.12.17
文件含有密码	-
文件后缀名被修改	-
文件真实类型描述	-
记录时间	2021-04-20 15:33:02
附件名称	201020测试报告.doc
邮件内容	20200325测试详情 查看附件 huangzhangpeng8868@163.com



导航菜单-数据中心--历史认证台账

 惠尔顿 网络安全审计V10.0

消息通知 修改密码 技术支持 退出系统

导航菜单

实时分析

网络配置

认证配置

对象配置

策略管理

系统管理

追溯系统

数据中心

总体统计

审计报告

分析报告

汇总数据导出

综合审计报告

历史认证台账

数据导出

策略 ×

认证设置 ×

网页管控 ×

网页标题 ×

自定义邮件对象 ×

邮件管控策略 ×

邮件管控记录 ×

详细记录 ×

历史认证台账 ×

所有认证 2021-04-19 09:40 2021-04-26 09:40 请输入用户名或IP 导出

	用户	认证方式	登录时间	退出时间	上行流量	下行流量
1	何三 / 192.168.25	客户端认证	2021-04-25 14:21:56	2021-04-25 14:22:27	0 B	0 B
2	123 / 192.168.25	WEB认证	2021-04-21 16:25:35	2021-04-21 18:05:02	138.23 MB	70.1 MB
3	刘五 / 192.168.25	客户端认证	2021-04-20 15:30:12	2021-04-20 15:52:04	5.32 MB	14.28 MB
4	何三 / 192.168.25	WEB认证	2021-04-19 20:31:10	2021-04-19 22:12:58	2.4 MB	9.91 MB
5	何三 / 192.168.25	WEB认证	2021-04-19 17:06:53	2021-04-19 18:24:45	14.63 MB	49.53 MB

10 第 1 共1页 显示1到5,共5记录

当前用户: admin | 登录时间: 2021-04-26 09:12:14 惠尔顿版权所有 © 2021



导航菜单-数据中心-数据导出

← → ↻ ⚠ 不安全 | 192.168.254.6/# ☆ 👤 ⋮

消息通知 修改密码 ? 技术支持 退出系统

惠尔顿 网络安全审计

🔦 导航菜单

📊 实时分析

🖥️ 网络配置

👤 认证配置

📁 对象配置

📋 策略管理

⚙️ 系统管理

🔍 追溯系统

📁 数据中心

- 📄 审计报告
- 📄 分析报告
 - 📄 汇总数据导出
 - 📄 综合审计报告
 - 📄 历史认证台账
 - 📄 数据导出**
 - 📄 答题记录

⏪ 设置 ×

+ 新增 ×

	☐
1	☐

10 ▾ ⏪

计划时间: 2021-04-26 09:49

任务分类: 导出数据 ▾

任务名称:

时段: 2021-04-01 00:00 至 2021-04-30 00:00

任务描述:

操作内容:

☒ 网页标题审计

☐ URL审计

☐ DNS审计

☒ 邮件审计

☐ FTP审计

☐ SSH审计

☐ WEB文件审计

☐ HTTP协议审计

☐ SNMP审计

☐ NetBIOS审计

☐ NFS审计

☐ Telnet审计

☐ 历史认证台账记录

✓ 保存

✗ 取消

人证台账 ×

数据导出 ×

🔄

创建时间	操作
2021-04-23 00:00	📄

显示1到1,共1记录



三员管理

根据网络安全审计系统的三权分立要求，系统管理添加管理员用户，但是不能设定该用户的管理权限。系统默认有四个权限的角色，每个角色拥有的权限是不一样的。

导航到【系统管理/系统账户】，展示系统三个用户账号的信息，如下图：

系统状态

系统账户 x

+ 新增

✔ 启用

⊘ 禁用

	☐ 用户账号	安全邮箱	绑定IP	描述	状态	编辑
1	☐ admin	service@wholeton.com		内置账号，不可编辑	✔	
2	☐ system	system@wholeton.com		系统管理员	✔	
3	☐ safemanage	safemanage@wholeton.com		安全保密管理员	✔	
4	☐ auditor	auditor@wholeton.com		安全审计管理员	✔	

导航到【系统管理/系统账户】，在【系统账户】界面点击<新增>弹出【新增系统账户】对话框，如下图所示。

新增系统账户

用户名：

绑定IP：

安全邮箱：

描述：

新密码：

确认新密码：

✓ 保存

✗ 取消



有证书，更可靠



使用证书复印件应由产品研制生产单位加盖公章

证书信息核查: WWW.NSSTEC.ORG.CN





提 纲

1

军工企业上网要求

2

网络安全审计功能介绍

3

应对保密检查注意事项

4

版本升级应对保密新要求



版本更新—体现产品价值

- ❖ 一年内4次升级保持产品的持续更新
- ❖ 优化和修复一些已知问题
- ❖ 更好审计加密网页和加密邮件

我们做到：1年4次免费升级！





我们在路上一期待您的意见和建议

合作，多赢





感谢聆听！

www.wholeton.com