

SMP.edu

618 19 -22

350002

<http://www.ruijie.com.cn>

<http://support.ruijie.com.cn>

4008-111-000

E-mail: service@ruijie.com.cn

©2009



RGOS® RGNOS®



- _____
- _____
- _____
- _____
- _____

◇

◇

◇

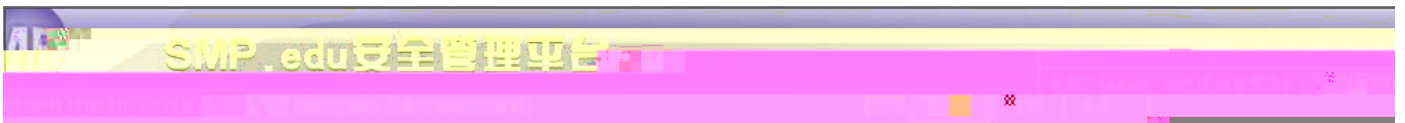
SMP

◇

◇

◇

◇



-
-
-
-

-
-



位置: 系统用户管理 > 添加系统用户

* 用户名: ?

* 所属用户组: ▼

* 密码: ?

* 密码确认:

真实姓名:

Email地址:

电话号码:

-
-



* 用户名: ?

* 所属用户组: ▼

密码: ?

密码确认:

真实姓名:

Email地址:

电话号码:

- _____
- _____
- _____

SMP



位置: 用户管理 > 用户组 > 查询用户组

用户组名称: 用户组描述:

安全策略模板:

操作	<input type="checkbox"/>	用户组名称 ↑	用户组描述	安全策略模板 ↑
修改	<input type="checkbox"/>	第一用户组		default
修改	<input type="checkbox"/>	新建用户组		default



位置: 用户管理 > 用户组 > 添加用户组

* 用户组名称:

* 安全策略模板:

用户组描述:

注意: 如果用户所在的交换机绑定了安全策略模板, 那么这里绑定的安全策略模板将不生效.

添加

重置

返回



位置: 用户管理 > 用户组 > 修改用户组

* 用户组名称:

* 安全策略模板:

用户组描述:

注意: 如果用户所在的交换机绑定了安全策略模板, 那么这里绑定的安全策略模板将不生效.

修改

重置

返回

SMP

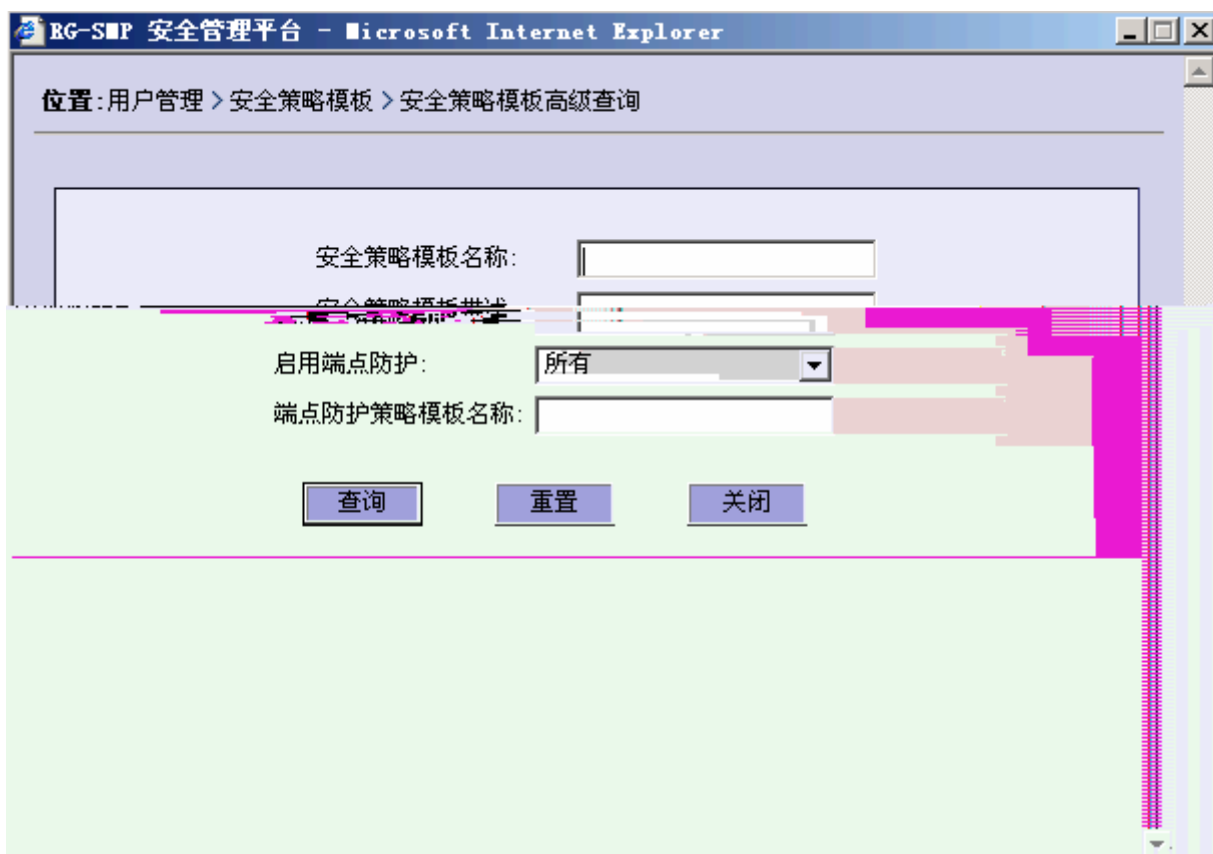


位置: 用户管理 > 安全策略模板 > 查询安全策略模板

安全策略模板名称: 安全策略模板描述: [高级查询](#)

共1条记录 每页20条 第1页/共1页 [GO](#) [首页] [上一页] [下一页] [尾页]

<input type="checkbox"/>	安全策略模板名称 ↑	安全策略模板描述	操作
<input type="checkbox"/>	default	默认安全策略模板, 新学习到的用户组将默认使用该安全策略模板!	查看 修改



-
-
-

端点防护

启用端点防护

端点防护策略模板: 未选择

注意: 如果没有任何端点防护策略模板信息, 请先到“端点防护”中添加!

成功提示信息:

失败提示信息:

桌面接入交换机端点防护模板:

<input type="checkbox"/>	模板名称	描述
<input type="checkbox"/>	端点防护模板	

非桌面接入交换机端点防护模板:

添加 重置 返回

注意: 重置功能将重置所有选项卡中的信息。

-
-
-



基本信息 端点防护

安全策略模板名称:

安全策略模板描述:

*安全策略模板具体信息请查看各标签卡项

注意: 重置功能将重置所有选项卡中的信息。

- _____
- _____
- _____

✧

2008

✧

SMP

✧

端点防护策略模板名称:

用户组:

是否启用微软补丁更新:

共1条记录 每页 20 条 第 1 页/共1页 GO

[\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

<input type="checkbox"/>	端点防护策略模板名称 ↑	描述	是否启用微软补丁更新 ↑	操作
<input type="checkbox"/>	端点_A		否	修改



1)

端点防护策略模板基本信息

杀毒软件联动

微软补丁更新

* 端点防护策略模板名称:

端点防护策略模板描述:



* 端点防护策略模板具体信息请查看各标签卡项

添加

重置

返回

注意: 重置功能将重置所有选项卡中的信息。

端点防护策略模板基本信息

杀毒软件联动

微软补丁更新

启用强联动杀毒软件

启用弱联动杀毒软件

启用实时扫描

启用行为防护

启用勒索软件防护

启用恶意软件防护

启用钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

启用网络钓鱼防护

添加

重置

返回

注意: 重置功能将重置所有选项卡中的信息。

•

- 4) “ ” “ ”
- 5) “ ”
- 6)

SMP



位置: 端点防护 > 杀毒软件联动 > 查询杀毒软件

杀毒软件名称: 联动方式:

是否启用:

[查询](#) [重置](#)

[添加](#) [删除所选](#)

共24条记录 每页20条 第1页/共2页 [GO](#) [\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

<input type="checkbox"/>	杀毒软件名称	联动方式	检查项		检查限制	启用	操作
<input type="checkbox"/>	江民2008及其以后的版本	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	不检查			
<input type="checkbox"/>	江民杀毒软件KV2007	弱联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	卡巴斯基反病毒软件6.0	弱联动	杀毒引擎	不支持		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	卡巴斯基反病毒软件6.0个人版	弱联动	杀毒引擎	不支持		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	卡巴斯基反病毒软件6.0个人版	弱联动	杀毒引擎	不支持		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	卡巴斯基反病毒软件6.0网络版	弱联动	杀毒引擎	不支持		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	卡巴斯基反病毒软件6.0网络版	弱联动	杀毒引擎	不支持		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	AVirus企业版 8	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	AVirus企业版 9	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	AVirus企业版 10	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	检查	自适应顺延天数	7	
<input type="checkbox"/>	AVirus企业版 2005	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	不检查			
<input type="checkbox"/>	AVirus企业版 2010	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	不检查			
<input type="checkbox"/>	AVirus企业版 2011	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	不检查			
<input type="checkbox"/>	AVirus企业版 2012	强联动	杀毒引擎	不检查		<input type="checkbox"/>	查看 修改
			病毒库	不检查			





-
-
-



位置: 端点防护 > 杀毒软件联动 > 添加杀毒软件

基本信息

* 杀毒软件名称:

* 进程名称:

注意: 杀毒软件名称必须与该杀毒软件在“添加删除程序”显示的名称一致, 否则客户端无法识别该杀毒软件是否已安装。

处理方式

* 删除 阻止 阻止并删除 阻止并删除并验证地址

删除

阻止

阻止并删除

-

-

基本信息

* 杀毒软件名称

* 杀毒软件名称:

杀毒软件是否已安装:

注意: 杀毒软件名称必须与该杀毒软件在“添加删除程序”显示的名称一致, 否则客户端无法识别该杀

处理方式

* 杀毒软件安装程序URL:

验证地址

修改

重置

返回

- _____
- _____



位置: 网络攻击防治 > ARP欺骗免疫 > 配置ARP欺骗免疫

启用ARP欺骗免疫功能

共4条记录 每页20条 第1页/共1页 GO

[首页] [上一页] [下一页] [尾页]

网关IP ↑	网关MAC ↑	网关名称 ↑	网关类型 ↑	应用模式	启用ARP欺骗免疫	支持优化模式	操作
192.168.203.150	00D0F82233AD	S3250	S3250-48	网关	<input type="checkbox"/>	<input type="checkbox"/>	查看

S5750S-24GT/12	网关	<input checked="" type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.3	00D0F822A219	AP_JUC_5760	S
S2126G	网关	<input type="checkbox"/>	<input type="checkbox"/>	查看	192.168.203.90	00D0F8BC9556	SMP	

本请参见GSN部署文档。

注意: 优化模式可以提升免疫处理的性能。支持优化模式的交换机软件版

- _____
- _____
- _____
- _____



SMP



位置: 网络访问控制 > 访问控制策略 > 查询访问控制策略

访问控制策略名称: 用户IP:
 用户名: 交换机IP: [高级查询](#)

共1条记录 每页20条 第1页/共1页 [GO](#)

[\[首页\]](#) [\[上一页\]](#) [\[下一页\]](#) [\[尾页\]](#)

<input type="checkbox"/>	访问控制策略名称 ↑	访问控制模板名称	交换机IP ↑	用户IP ↑	安装时间 ↑	操作
<input type="checkbox"/>	HI_端点防护模板_ruijie_19 2.168.203.50	端点防护模板	192.168.203.240	192.168.203.50	2008-07-30 14:44:29	查看

-
-
-
-



设置 - 网络访问控制 > 访问控制模板 > 查询访问控制模板

访问控制模板名称: 目的IP:
 目的MAC: 目的端口:

添加端点防护模板
删除所选

[上一页] [下一页] [尾页]

操作	
查看	修改

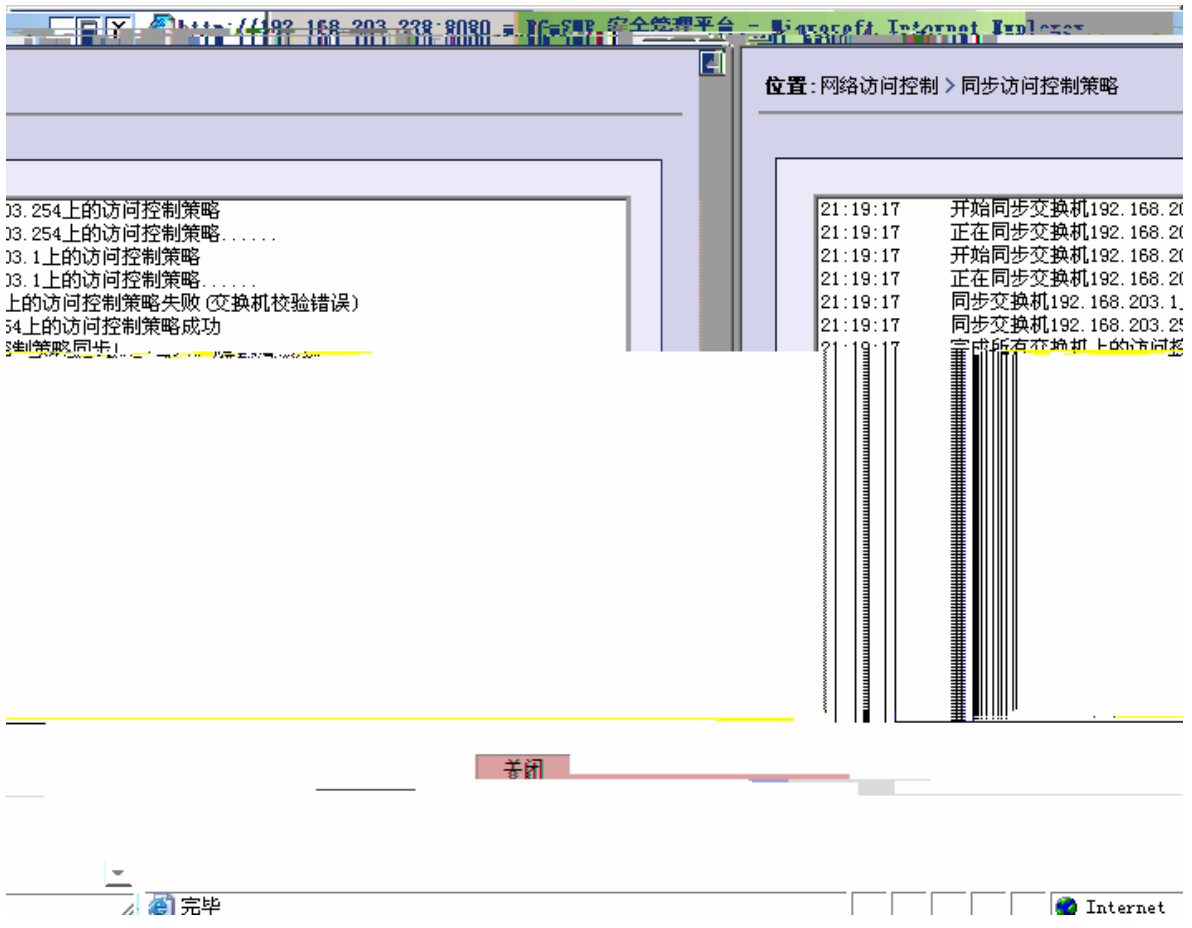
共1条记录 每页20条 第1页/共1页 GO [首页]

	访问控制模板名称 ↑	访问控制模板类型 ↑	访问控制模板描述
<input type="checkbox"/>	端点防护策略模板_A	端点防护模板	



位置: 网络访问控制 > 访问控制模板 > 修改端点防护模板

* 访问控制模板名称:
访问控制模板描述:
* 目的IP:
* 子网掩码:
目的MAC:
目的端口:
协议选择:



- _____
- _____
- _____

- ◇
- ◇
- ◇
- ◇
- ◇
- ◇

- PC
- PC

◇



位置: 设备管理 > 交换机 > 添加交换机

* 交换机IP:	<input type="text"/>
* 是否VRRP部署模式:	否
* 交换机名称:	交换机
* 交换机MAC:	未选择
* 交换机IP:	<input type="text"/>
* 交换机名称:	<input type="text"/>
* 交换机MAC:	<input type="text"/>

- 如果交换机IP是VRRP部署模式下的虚拟IP, 请配置为VRRP部署模式, 这时候获取交换机信息时, 才能获取到正确的虚拟MAC。若获取虚拟MAC失败, 表示交换机软件不支持这种获取方式, 这时请手动输入交换机MAC信息。
- 交换机上的用户将优先应用交换机配置模板绑定的安全策略模板, 只有当交换机配置模板未绑定安全策略模板, 才会应用用户所在用户组绑定的安全策略模板。



位置: 设备管理 > 交换机 > 批量添加交换机

* 开始IP:	<input type="text"/>
* 结束IP:	<input type="text"/>
* 交换机配置模板:	未选择

“ ”

SMP

位置: 设备管理 > 交换机 > 正在搜索

正在搜索，请耐心等待...



7% (搜索到 0 台交换机)

停止搜索

返回

注意：停止搜索功能将中断正在执行的搜索，返回已经搜索到的交换机信息。

位置: 设备管理 > 交换机 > 批量搜索结果

添加选中

重新搜索

返回

注意：在系统中已经存在的交换机信息不可选。

<input type="checkbox"/>	交换机IP	交换机名称	交换机类型	交换机配置模板	操作
<input type="checkbox"/>	192.168.203.2	4F_HJ_5750	S5750S-24GT/12SFP	public	查看
<input type="checkbox"/>	192.168.203.3	4F_HJ_5750	S5750S-24GT/12SFP	public	查看
<input type="checkbox"/>	192.168.203.4	F_2_1_1 (S2628)	S2628G	public	查看

-
-
-



位置: 设备管理 > 交换机 > 修改交换机

* 交换机IP:	<input type="text" value="192.168.203.158"/>
* 是否VRRP部署模式:	<input type="text" value="是"/>
* 交换机配置模板:	<input type="text" value="txx_jieru"/>
* 交换机MAC:	<input type="text" value="001AA9102BCA"/>
交换机名称:	<input type="text" value="S3750"/>
交换机类型:	<input type="text" value="S3750-48"/>
交换机位置:	<input type="text"/>
备注:	<input type="text" value="Ruijie Gigabit Routing S"/>

- 如果交换机IP是VRRP部署模式下的虚拟IP，请配置为VRRP部署模式，这时候获取交换机信息时，才能获取到正确的虚拟MAC。若获取虚拟MAC失败，表示交换机软件不支持这种获取方式，这时请手动输入交换机MAC信息。
- 交换机上的用户将优先应用交换机配置模板绑定的安全策略模板，只有当交换机配置模板未绑定安全策略模板，才会应用用户所在用户组绑定的安全策略模板。

交换机配置模板名称: SNMP协议版本:

安全公共名: 应用模式:

共4条记录 每页20条 第1页/共1页 [GO](#) [首页] [上一页] [下一页] [尾页]

SNMPV2	网关	SNMPV2C	public	安全公共名	接入模式	操作
接入式网关模板	接入	SNMPV1	public	桌面		查看 修改
RG_网关模板	网关	SNMPV1	public			查看 修改
RG_接入模板	接入	SNMPV1	public	桌面		查看 修改

-
-
-
-
-



位置: 设备管理 > 交换机配置模板 > 添加交换机配置模板

* 交换机配置模板名称:

* 应用模式:

* 接入模式:

* SNMP协议版本: ?

* 安全公共名: ?

安全策略模板:

注意: 如果这里绑定了安全策略模板, 相关交换机上的用户将应用这里配置的安全策略模板, 而用户所在设备绑定的安全策略模板将失效。

重置

返回

添加

4)

◇

位置: 设备管理 > 交换机配置模板 > 修改交换机配置模板

* 交换机配置模板名称:

* 应用模式:

* 接入模式:

* SNMP协议版本: ?

public

*

安全策略模板, 相关交换机上的用户将应用这里配置的安全策略模板, 而用户所在设备绑定的安全策略模板将失效。

注意: 如果这里绑定了安全策略模板, 而用户所在设备绑定的安全策略模板将失效。

重置

返回

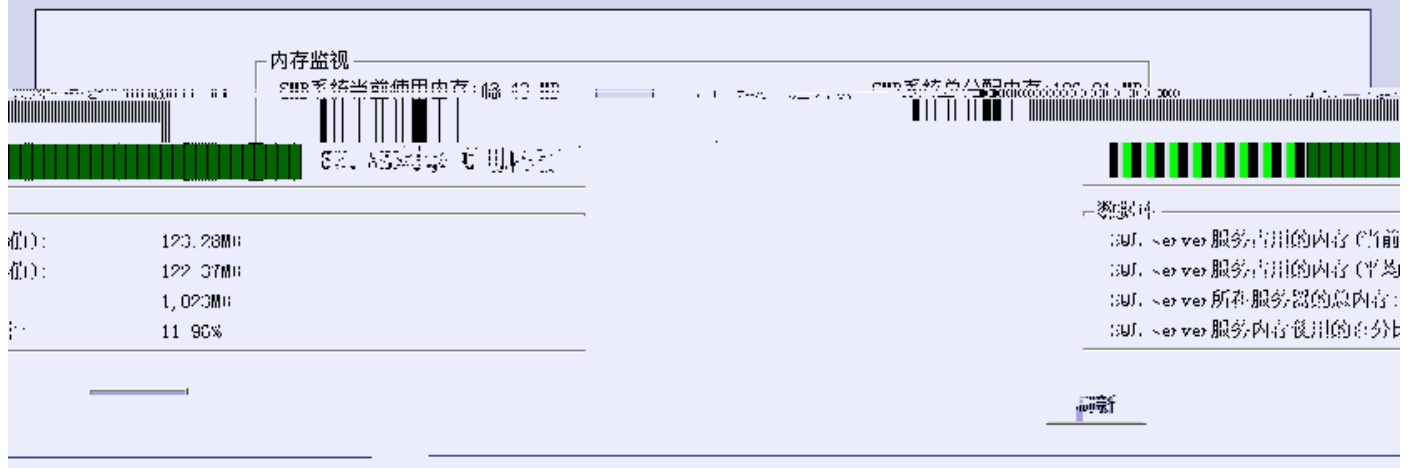
修改

- _____
- _____
- _____
- _____
- _____

◇

◇ ◇

◇



SMP



SMP

删除所选

[建议连接用户数和安装策略数](#)

共6条记录 每页20条 第1页/共1页 GO

[首页] [上一页] [下一页] [尾页]

设备ID	模板名称	设备类型	配置数	应用数	策略数	时间	协议	诊断结果	IP地址
3.240	网关配置模板	网关	0	0	0	2008-01-02 10:17:06	Telnet	诊断结果	192.168.200.1
3.254	S21模板	接入	0	2	0	2008-01-02 10:17:06	Telnet	诊断结果	192.168.200.2
3.80	网关配置模板	网关	0	0	0	2008-01-02 10:16:50	Telnet	诊断结果	192.168.200.3
3.55	S21模板	接入	0	0	0	2008-01-02 10:16:42	Telnet	诊断结果	192.168.200.4
3.233	网关配置模板	网关	0	0	0	2008-01-02 10:16:34	Telnet	诊断结果	192.168.200.5

交换机IP	192.168.203.1
交换机配置模板	网关配置模板
交换机应用模式	网关
交换机软件版本	未知
在线用户数	0
使用策略数	0

关闭

自动删除一周前记录

共1条记录 每页20条 第1页/共1页 GO

[首页] [上一页] [下一页] [尾页]

交换机IP ↑	发送报文数 ↑	最后发送报文时间 ↑	操作
192.168.203.54	1	2008-01-02 10:28:09	Telnet 添加交换机 删除

SMP

- _____
- _____

SMP



位置: 在线用户 > 查询在线用户

重置 高级查询 用户IP: [] 交换机IP: [] 查询

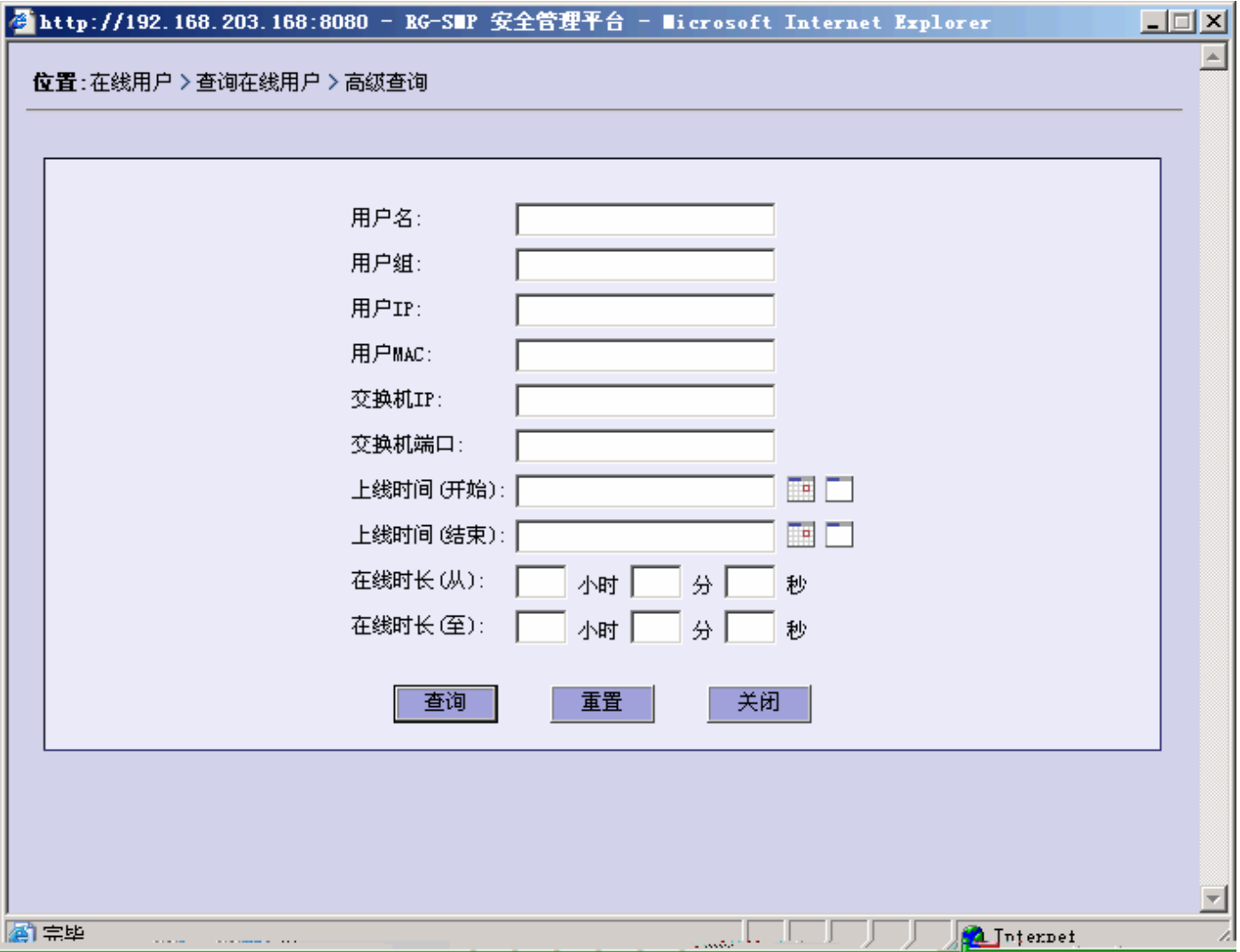
清除在线数据 检测端点防护状态

[首页] [上一页] [下一页] [尾页]

共1条记录 每页20条 第1页/共1页 GO

<input type="checkbox"/>	用户名 ↑	用户IP	用户MAC	交换机IP	交换机端口	上线时间 ↑
<input type="checkbox"/>	ruijie	192.168.203.50	001320498C96	192.168.203.240	4	2008-07-30 14:4

在线时长 ↑	操作
0小时0分29秒	查看



•

接入用户控制

定期检测用户在线状态

192.168.203.60

端点防护

状态检测周期: 1 分钟 (默认为5分钟)

配置文件更新周期: 5 分钟 (默认为60分钟)

配置文件更新服务器: Ftp://smp:smp@192.168.203.32:21

其他功能

设备控制策略同步

修改

重置

- _____
- _____

- ◇
- ◇
- ◇
- ◇
- ◇
- ◇
- ◇
- ◇

◇

系统信息 位置: 日志管理 > 查询日志信息

日志类型: 所有类型 日志的创建时间(开始): 日志的创建时间(结束):

删除所选 删除本次查询所有记录 配置日志参数

共85条记录 每页 条 第 页/共5页 GO [首页] [上一页] [下一页] [尾页]

日志类型	创建时间	创建管理员	日志内容
操作日志	2008-08-04 17:00:31	log	删除本次查询所有日志信息成功!
操作日志	2008-08-04 17:00:22	log	删除本次查询所有日志信息成功!
系统日志	2008-08-04 16:59:42	system	admin(192.168.203.54)成功退出系统!
系统日志	2008-08-04 16:56:44	system	admin(192.168.203.54)登录成功!
系统日志	2008-08-04 16:39:39	system	admin(192.168.203.34)登录成功!
系统日志	2008-08-04 16:20:37	system	admin(192.168.203.44)登录成功!
系统日志	2008-08-04 16:11:59	system	admin(192.168.203.54)登录成功!
系统日志	2008-08-04 16:11:50	system	admin(192.168.203.54)成功退出系统!
系统日志	2008-08-04 15:55:42	system	admin(192.168.203.34)登录成功!
系统日志	2008-08-04 15:52:10	system	admin(192.168.203.22)登录成功!
端点防护日志	2008-08-04 13:40:02	system	用户(192.168.203.34)端点防护检测成功!

-
-
-
-



日志参数配置

- 自动删除 (1~100)* 天以前的端点防护日志
- 自动删除 (1~100)* 天以前的操作日志
- 自动删除 (1~100)* 天以前的系统日志
- 自动删除 (1~100)* 天以前的客户端信息日志

修改

重置

返回



`	~	!	@	#	\$	%	^	&	*
()			[]	{	}		
_	-	=	+	,	.				
;	:	“	”	‘	’	<	>		
					‰				