

天珣内网安全风险管理与审计系统

用户手册

(V6.6.9.4Patch66940000)



启明星辰

Beijing Venustech Cybervision Co., Ltd.

2012 年 11 月

版权声明

北京启明星辰信息安全技术有限公司版权所有，并保留对本手册及本声明的最终解释权和修改权。

本手册中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其他相关权利均属于北京启明星辰信息安全技术有限公司。未经北京启明星辰信息安全技术有限公司书面同意，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。本文档中的信息归北京启明星辰信息安全技术有限公司所有并受著作权法保护。

“天珣”为北京启明星辰信息安全技术有限公司的注册商标，不得仿冒。

信息更新

本文档及其相关计算机软件程序（以下文中称为“文档”）仅用于为最终用户提供信息，并且随时可由北京启明星辰信息安全技术有限公司（下称“启明星辰”）更改或撤回。

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息安全技术有限公司可能已经拥有或正在申请与本文档主题相关的各项专利。提供本文档并不表示授权您使用这些专利。您可将许可权查询资料用书面方式寄往北京启明星辰信息安全技术有限公司。

北京启明星辰信息安全技术有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息安全技术有限公司不对本手册中的遗漏、不准确、或错误导致的损失和损害承担责任。

出版时间

2012 年 12 月 20 日

目 录

(V6.6.9.4PATCH66940000)	1
1. 体系结构	1
1.1. 中心服务器、本地服务器、客户端、以及策略网关的体系结构	1
1.2. 系统中的角色及术语	1
1.2.1. 角色	1
1.2.2. 术语	2
2. WEB 控制台登录	3
2.1. 关于 WEB 控制台登录	3
2.2. WINDOWS 集成认证登录页面	4
2.2.1. 配置介绍	4
2.2.2. 配置要点	4
2.3. 三权分立认证登录页面	5
2.3.1. 配置介绍	5
2.3.2. 配置要点	7
3. 首页	8
4. 基本配置	9
4.1. 关于基本配置	9
4.2. 按需支援操作员	11
4.2.1. 配置介绍	11
4.2.2. 配置要点	12
4.3. 系统管理员	12
4.3.1. 配置介绍	12
4.3.2. 配置要点	15
4.4. 策略服务器	16
4.4.1. 配置介绍	16
4.5. 管理网段	18
4.5.1. 配置介绍	18
4.5.2. 配置要点	20
4.6. IP 组	21
4.6.1. 配置介绍	21
4.7. 部门	26
4.7.1. 配置介绍	26
4.8. 终端注册	28
4.8.1. 配置介绍	28
4.9. 本地用户	30
4.9.1. 配置介绍	30
4.10. 用户组	32
4.10.1. 配置介绍	32
4.10.2. 配置要点（以 AD 域为例）	38

4.11. 可信 MAC	39
4.11.1. 配置介绍.....	39
4.11.2. 配置要点.....	42
4.12. 可信 GUID	43
4.12.1. 配置介绍.....	43
4.12.2. 配置要点.....	45
4.13. 用户、IP、MAC 组合	45
4.13.1. 配置介绍.....	45
4.13.2. 配置要点.....	54
4.14. 网络设备配置.....	55
4.15. 分组信息.....	58
4.15.1. 配置介绍.....	58
4.16. 全局参数.....	58
4.16.1. 配置介绍.....	58
5. 安全基线	64
5.1. 关于安全基线.....	64
5.2. 补丁强制策略.....	66
5.2.1. 配置介绍.....	66
1.1.1. 配置要点.....	69
5.3. 进程运行策略.....	70
5.3.1. 配置介绍.....	70
5.4. 软件安装策略.....	75
5.4.1. 配置介绍.....	75
5.5. WINDOWS 服务管理.....	80
5.5.1. 配置介绍.....	80
5.6. 防病毒软件策略.....	83
5.6.1. 配置介绍.....	83
5.7. WINDOWS 账户策略	85
5.7.1. 配置介绍.....	85
5.8. WINDOWS 本地策略	90
5.8.1. 配置介绍.....	90
5.9. 注册表策略.....	97
5.9.1. 配置介绍.....	97
5.10. 共享资源管理.....	99
5.10.1. 配置介绍.....	99
5.11. WINDOWS 事件日志管理策略	100
5.11.1 配置介绍.....	100
5.12. 用户环境策略.....	102
5.12.1. 配置介绍.....	102
6. 准入控制	110
6.1. 关于准入控制.....	110
6.2. 网络准入.....	111
6.2.1. 关于网络准入.....	111

6.2.2.	RADIUS Server 页面	112
6.2.3.	可信 MAC 认证时授权页面	119
6.2.4.	可信 GUID 认证时授权页面	121
6.2.5.	免认证 MAC 地址列表页面	123
6.2.6.	VLAN 信息页面	123
6.2.7.	网络准入配置要点	124
6.2.8.	网络准入其他组件配置	124
6.3.	应用准入	156
6.3.1.	关于应用准入	156
6.3.2.	策略网关代理设置页面	160
6.3.3.	中性（通用）策略网关安装配置要点	164
6.3.4.	旁路 DNS 准入	167
6.3.5.	IIS 策略网关安装配置要点	169
6.3.6.	ISA 策略网关安装配置要点	170
6.3.7.	Exchange 策略网关安装配置要点	173
6.3.8.	Web 准入安装配置要点	174
6.4.	客户端准入	178
6.4.1.	关于客户端准入	178
6.4.2.	客户端准入页面	179
6.5.	ARP 准入	182
6.5.1.	关于 ARP 准入	182
6.5.2.	ARP 准入页面	183
7.	安全防护	185
7.1.	关于安全防护	185
7.2.	协议端口设定	186
7.2.1.	配置介绍	186
7.3.	防护策略	189
7.3.1.	配置介绍	189
7.3.2.	配置要点	200
7.4.	访客策略	201
7.4.1.	配置介绍	201
8.	补丁管理	205
8.1.	关于补丁管理	205
8.2.	在线补丁源	206
8.2.1.	关于在线补丁源	206
8.2.2.	配置介绍	207
8.2.3.	配置要点	213
8.3.	手工补丁源	214
8.3.1.	关于手工补丁源	214
8.3.2.	配置介绍	214
8.4.	补丁分发	216
8.4.1.	关于补丁分发	216
8.4.2.	配置介绍	217

8.5. WSUS 集成管理	220
8.6. 关于 WSUS 集成管理	220
8.6.1. 配置介绍	221
8.6.2. 配置要点	223
8.7. 补丁查询	224
8.7.1. 关于补丁查询	224
8.7.2. 配置介绍	225
9. 资产管理	226
9.1. 关于资产管理	226
10. 非法外联	229
10.1. 关于非法外联	229
10.2. 非法外联监控	231
10.2.1. 配置介绍	231
10.3. 多网卡限制	234
10.4. 关于多网卡限制	234
10.4.1. 多网卡限制页面	235
10.5. 拨号限制	238
10.5.1. 关于拨号限制	238
10.5.2. 拨号限制页面	238
10.6. 外设管理	241
10.6.1. 关于外设管理	241
10.6.2. 外设管理页面	241
10.7. 异常路由审计	244
10.7.1. 关于异常路由审计	244
10.7.2. 异常路由审计配置页面	244
11. 移动存储	245
11.1. 关于移动存储	245
11.2. 设备认证策略	247
11.2.1. 关于设备认证策略	247
11.2.2. 移动存储设备提交认证相关页面	248
11.3. 移动存储设备管理页面	250
11.4. 设备授权	253
11.4.1. 关于设备授权	253
11.4.2. 移动存储设备授权页面	253
11.5. 可使用未认证设备的计算机	257
11.6. 分区解扰操作说明	259
12. 终端审计	261
12.1. 关于终端审计	261
12.2. 文件审计及控制策略	263
12.2.1. 关于文件审计及控制策略	263
12.3. 文件审计及控制策略	264

13.2.1	关于文件审计及控制策略.....	264
12.2.2	文件操作审计及控制页面.....	265
12.2.3	审计网络拷贝页面.....	268
12.4.	打印审计及控制.....	269
12.3.1	关于打印审计.....	269
12.3.2	打印审计页面.....	269
12.5.	网站审计及控制.....	271
12.4.1	网站审计及控制页面.....	271
12.6.	FTP 审计及控制.....	275
12.5.1	FTP 审计及控制页面.....	275
12.7.	文件涉密信息审计.....	278
12.6.1	文件涉密信息审计页面.....	278
12.6.2	附录 1.....	281
12.8.	应用程序使用审计.....	285
12.7.1	应用程序使用审计页面.....	285
12.9.	刻录审计.....	287
12.8.1	刻录审计策略页面.....	287
12.10.	WINDOWS 事件日志审计.....	290
12.9.1	Windows 事件日志审计页面.....	290
13.	桌面运维.....	291
13.1.	关于桌面运维.....	291
13.2.	软件分发.....	291
13.2.1.	关于软件分发.....	291
13.2.2.	软件分发设置页面.....	292
13.2.3.	软件分发查询页面.....	296
13.2.4.	软件分发默认参数页面.....	297
13.3.	短消息.....	298
13.3.1.	关于短消息.....	298
13.3.2.	关于终端消息推送.....	299
13.4.	计算机名规范.....	301
13.4.1.	关于主机名规范.....	301
13.4.2.	配置要点.....	302
13.4.3.	关于工作组名规范.....	303
13.4.4.	配置要点.....	304
13.5.	远程文件删除.....	305
13.5.1.	关于远程文件删除.....	305
13.6.	自动关机策略.....	306
13.6.1.	关于自动关机策略.....	306
13.7.	WIN 防火墙例外.....	308
13.7.1.	关于 Win 防火墙例外.....	308
13.8.	终端实时操控.....	311
13.8.1.	关于终端实时操控.....	311
13.8.2.	服务页面.....	312
13.8.3.	进程页面.....	313

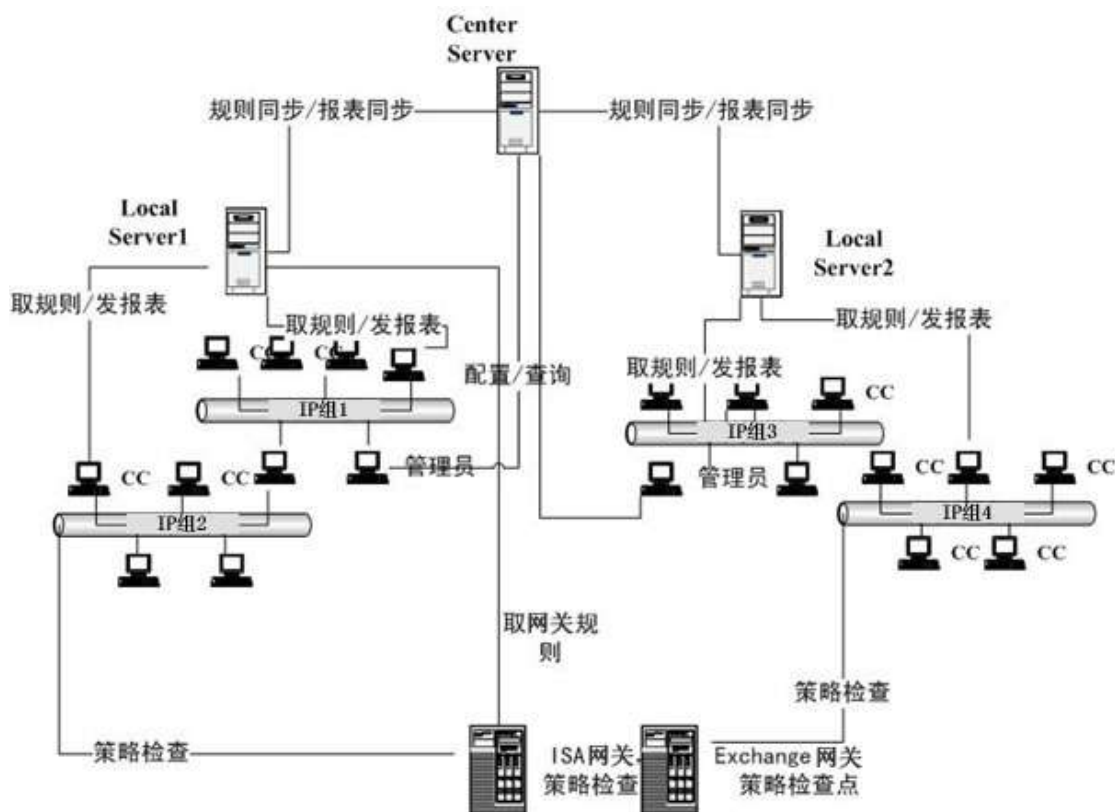
13.8.4.	网络连接页面.....	314
13.8.5.	实时补丁查询页面.....	314
13.8.6.	IE 插件管理页面.....	315
13.8.7.	终端锁屏.....	316
13.8.8.	终端维护.....	317
13.9.	终端资源状况监控.....	317
13.9.1.	关于终端资源状况监控.....	317
14.	认证管理.....	319
14.1.	第三方 CA 机构.....	319
14.2.	天珣 CA 机构.....	320
14.2.1.	天珣 CA 根证书.....	321
14.2.2.	天珣 CA 用户证书.....	322
14.2.3.	天珣 CA 用户证书页面证书及 ActiveX 控件安装.....	325
14.3.	身份认证.....	328
14.3.1.	关于身份认证.....	328
14.3.2.	用户及证书管理配置介绍.....	328
14.3.3.	超级用户.....	331
15.	信息中心.....	333
15.1.	关于信息中心.....	333
15.2.	接入信息.....	334
15.2.1.	配置介绍.....	334
15.3.	资产信息.....	338
15.3.1.	配置介绍.....	338
15.4.	补丁信息.....	355
15.4.1.	配置介绍.....	355
15.5.	审计信息.....	360
15.5.1.	配置介绍.....	360
15.6.	安全基线.....	374
15.6.1.	配置介绍.....	374
15.7.	外联控制.....	398
15.7.1.	配置介绍.....	398
15.8.	攻击告警.....	406
15.8.1.	配置介绍.....	406
15.9.	移动存储.....	411
15.9.1.	配置介绍.....	411
15.10.	桌面运维.....	414
15.10.1.	配置介绍.....	414
15.11.	级联报表.....	420
15.11.1.	配置介绍.....	420
16.	系统维护.....	422
16.1.	关于系统维护.....	422
16.2.	系统维护.....	422

16.2.1.	客户端升级配置页面.....	422
16.2.2.	自动卸载客户端页面.....	425
16.2.3.	数据库自动维护.....	427
16.2.4.	软件分发 IP 组同步	432
16.3.	系统日志.....	432
16.3.1.	管理员操作日志页面.....	432
16.3.2.	按需支援日志页面.....	433
15.2.3	策略服务器日志页面.....	433
15.2.4	告警服务器同步日志页面.....	434
15.2.5	策略网关日志页面.....	434
15.2.6	RADIUS 日志页面.....	435
15.2.7	补丁同步日志页面.....	435
16.4.	LICENSE 管理.....	436
16	系统级联	437
16.1	关于系统级联.....	437
16.2	级联关系.....	438
16.2.1	配置介绍.....	438
16.3	级联策略管理.....	440
16.3.1	配置介绍.....	440
16.4	授权分拆.....	441
16.4.1	配置介绍.....	441
16.5	级联软件分发介质同步	442
16.5.1	配置介绍.....	442
17	更新策略	443
17.1	关于更新策略.....	443
17.2	更新策略的流程.....	443
17.3	SERVER 策略版本页面	444
17.3.1	配置介绍.....	444
17.3.2	本地服务器操作简介.....	445
17.3.3	配置要点.....	446
17.4	更新 CC 策略版本页面.....	447
17.4.1	配置介绍.....	447
17.4.2	配置要点.....	447
17.5	更新策略网关策略页面.....	448
17.5.1	配置介绍.....	448
17.5.2	配置要点.....	448
17.6	更新 RADIUS 策略页面	449
17.6.1	配置介绍.....	449
17.6.2	配置要点.....	450
18.	附录：单点登录配置手册.....	450
18.1	天珣单点登录简介.....	450
18.2	单点登录客户端打包.....	450

18.3	天珣单点登录的两种登录方式.....	452
18.3.1	帐号/密码单点登录.....	452
18.3.2	UKey 单点登录.....	455
18.4	配置利用智能卡进行 WINDOWS 身份验证	458

1. 体系结构

1.1. 中心服务器、本地服务器、客户端、以及策略网关的体系结构



1.2. 系统中的角色及术语

1.2.1. 角色

- “**中心服务器 (Center Server)**”：所有策略规则集中存放的地方，系统中唯一开放了配置用户界面的服务器。管理员从 Web 登录到**中心服务器**，进行策略配置，报表查询。**本地服务器**与**中心服务器**进行策略规则同步，报表同步。
- “**本地服务器 (Local Server)**”：**本地服务器**是客户端 (CC)

日常取规则的地方，也是 CC 发送报表的目的地。**本地服务器**从**中心服务器**同步得到策略。

- **下载服务器：**下载服务器是供客户下载各种运行软件，Windows Service Pack，HotFix，防病毒码以及策略系统本身的安装程序的 Web 服务器，**下载服务器**可以由策略服务器兼作，也可以是单独的服务器。
- **“客户端（CC）”：**安装在每个被策略管理的用户的电脑上的代理程序。执行策略的检查，从**本地服务器**上取规则，向**本地服务器**发送报表，当用户不满足策略规则时，向用户提示相关信息。
- **“策略网关代理(PluginProxy)”：**管理所有关联的**策略网关**，**策略网关代理**从**本地服务器**上取插件规则。当**策略网关**激活时，**策略网关代理**将规则发送给各个关联的**策略网关**。**策略网关代理**的主要作用在于可以将安装在多个应用服务器上的有相同规则的**策略网关**交给同一个**策略网关代理**管理，从而简化管理员的配置；同时，各个**策略网关**可相互共享 CC 的状态，如 CC1 在**策略网关 1** 上通过了认证，那么通过**策略网关 2** 访问时就无需第 2 次认证，提高系统性能。
- **IIS 策略网关、ISA 策略网关、Exchange 策略网关以及中性(通用)策略网关：**策略检查点，与 CC 配合强制用户满足策略规则。**策略网关**从所属的**策略网关代理**上取规则。

1.2.2. 术语

- **管理网段：**管理网段是一个大的网段范围，一个管理网段可以包含多个 IP 组。一个本地服务器可以为多个管理网段服务，每

一个**管理网段**可以由不同的管理员管理。（在当前的版本中，管理员可以管理**本地服务器**上的所有**管理网段**）。一个**管理网段**通常是一个园区网的地址范围。

- **IP 组**：IP 组是设置规则的最小单位，一个管理网段划分为多个 IP 组使配置管理更加灵活。一个主机也可以配置成一个 IP 组。

2. WEB 控制台登录

2.1. 关于 WEB 控制台登录

- 天珣支持两种登录认证模式：“Windows 集成认证登录”和“三权分立认证登录”。在中心服务器安装时可选。在中心服务器上登录时可输入 <http://localhost:8833>，在其他终端上登录时则输入 <http://服务器 IP:8833>。
- “帐号管理员”：天珣系统的帐号创建者，三权分立模式下独有，默认为：**administrator**，只有使用帐号管理员才能创建系统操作员和其他帐号管理员。

注意：Windows 集成模式下 administrator 的默认密码是中心服务器 administrator 的密码，该密码不能为空，同时该管理员登录名称不能更改，如用户环境有更改，需要重新创建 administrator 帐号和密码。

- “系统操作员”：策略配置的制定者，三权分立模式下独有，只能由帐号管理员创建。
- “系统审计员”：只能对告警及审计信息进行查询的管理员，三权分立模式下独有，无法进行策略配置。默认帐号为

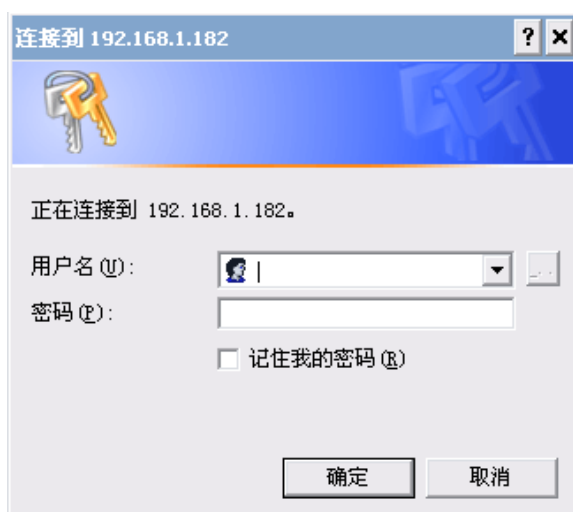
auditor，可使用这个帐号登录再创建其他系统审计员。

- “系统管理员”：默认与 windows 的 administrator 帐号集成，windows 集成认证模式下独有。可进行策略配置，也可进行帐号管理。

2.2. Windows 集成认证登录页面

2.2.1. 配置介绍

此种认证登录模式与安装天珣中心服务器的 windows 的系统帐号集成，第一次登录时默认以“administrator”帐号登录，密码为系统设置的密码。若系统中没有“administrator”帐号，请重新设置一个“administrator”帐号，使用此帐号登录一次 WEB 控制台后再新建其他与系统帐号同名的帐号。



2.2.2. 配置要点

1. 安装完成后，使用“administrator”帐号登录 WEB 界面；
2. 点击“管理员设置”中的“管理员”页面，创建一个系统管理员 stra，点击“保存”；
3. 在 windows 系统中创建一个用户 stra，此时即可使用 stra 帐

号登录天珣 WEB 管理界面进行策略配置。

注意：使用 windows 集成认证登录后直接进入天珣策略配置界面。
具体帐号配置操作请参考“基本配置”-“系统管理员”。

2.3. 三权分立认证登录页面

2.3.1. 配置介绍

“三权分立模式”即帐号管理员，系统操作员及系统审计员三种管理权限。此种认证登录模式使用 **administrator** 和 **auditor** 为默认帐号，默认密码为 **12345678**。



使用 administrator 帐号登录后界面为管理员帐号创建界面

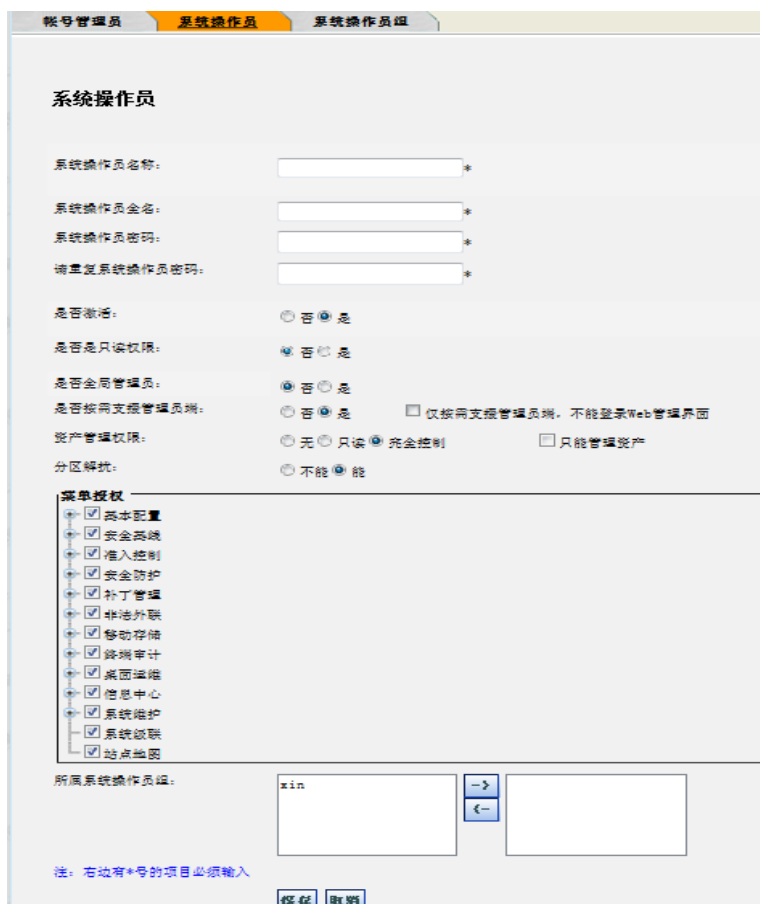


在此界面中可以根据需要创建其他的帐号管理员及系统操作员，只有在创建了一个系统操作员之后，使用系统操作员登录才能正常进入策略配置界面。



系统操作员

点击“系统操作员”菜单，并点击“添加”，进入系统操作员创建界面



系统操作员

系统操作员名称: *

系统操作员全名: *

系统操作员密码: *

请重复系统操作员密码: *

是否激活: ☐ 否 ☒ 是

是否是只读权限: ☒ 否 ☐ 是

是否全局管理员: ☒ 否 ☐ 是

是否按网支管理员: ☐ 否 ☒ 是 ☐ 仅按网支管理员用，不能登录Web管理界面

资产管理权限: ☐ 无 ☐ 只读 ☒ 完全控制 ☐ 只能管理资产

分区授权: ☐ 不能 ☒ 能

菜单授权

- ☒ 基本配置
- ☒ 安全策略
- ☒ 准入控制
- ☒ 安全防护
- ☒ 补丁管理
- ☒ 非法外联
- ☒ 移动存储
- ☒ 终端审计
- ☒ 桌面运维
- ☒ 信息中心
- ☒ 系统维护
- ☒ 系统故障
- ☒ 站点地图

所属系统操作员组:

注: 右边有*号的项目必须输入

创建系统操作员时通过选项给其分配相应的权限。

帐号管理员

在此界面中可创建登录帐号，其作用与默认的 administrator 帐号相同。

系统操作员组

在此界面中可建立操作员组，通过对不同系统操作员分配不同的管理网段来达到分级管理的目的。

系统审计员

使用 auditor 帐号登录后界面为系统审计员界面



在此界面中可以新建其他审计员帐号。

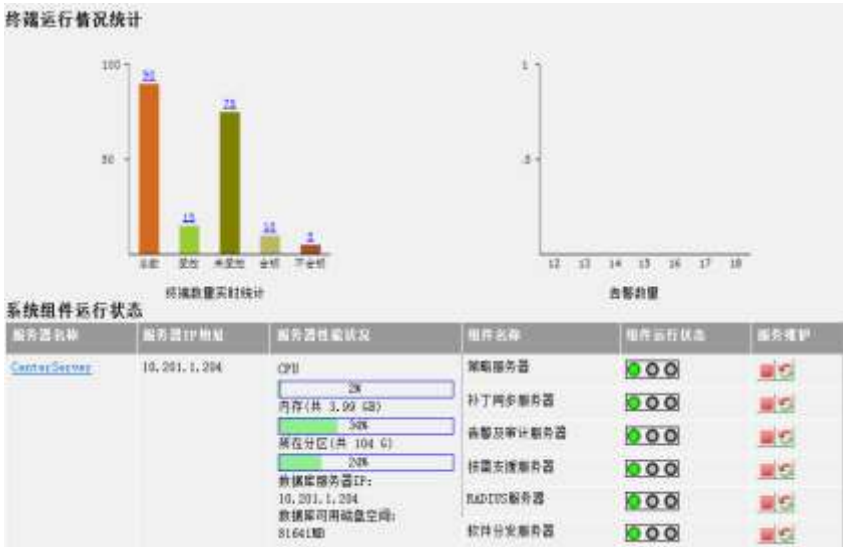
2.3.2. 配置要点

1. 使用“administrator”帐号登录天珣 WEB 控制台；
2. 点击“**管理员设置**”中的“**系统操作员**”菜单，创建一个系统操作员 strb，点击“**保存**”；
3. 使用 strb 帐号登录天珣 WEB 管理界面，此时可进行策略配置；
4. 使用 auditor 帐号登录天珣 WEB 控制台；
5. 点击“**系统审计员设置**”中的“**系统审计员**”菜单，创建一个系统审计员 strc，点击“**保存**”；
6. 使用 strc 帐号登录天珣 WEB 管理界面，此时可进行审计查询。

注意：有审计权限的全局系统操作员也是可以在策略配置界面中看到这些审计信息。而审计员可查看到系统操作员的操作日志，系统操作员也可查看到审计员的操作日志，但均无法查看自身的操作日志，方便各类型管理员之间进行相互监督。

3. 首页

- 在中心服务器上打开浏览器，输入 <http://localhost:8833/>，或在其他机器上输入 <http://服务器 IP:8833/>，然后输入用户密码。首页显示如下内容：



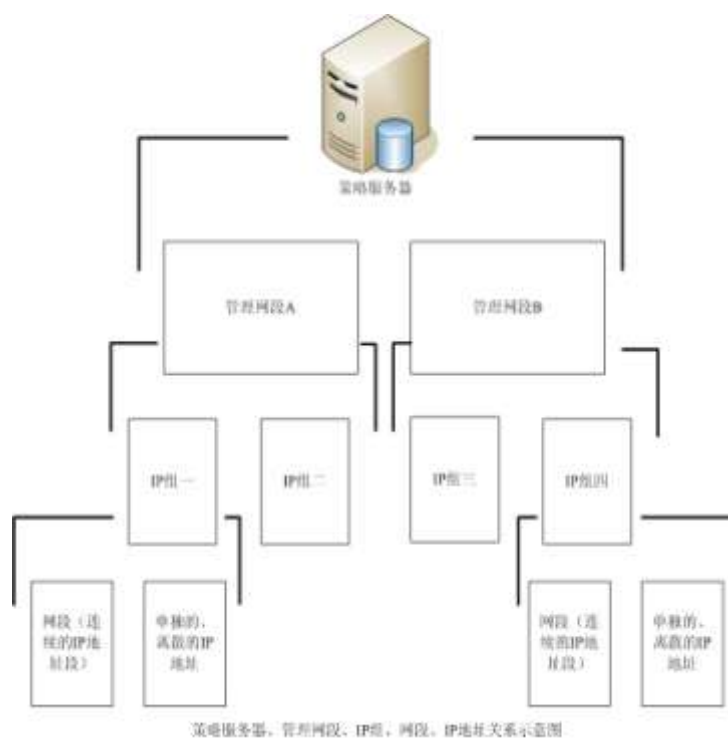
注意：每次点击进入首页或刷新该页面时均可触发终端实时统计，而告警数量则是一天更新一次。若一天中此页面未打开或刷新过，则程序内部在晚上自动执行一次与数据库的同步。

- **终端数量实时统计：**是服务器（包括本地服务器）管理的所有终端数目统计的报表，可以从中查看终端总数、受控/非受控终端，受控终端中合规及不合规的终端数量。
- **告警数量：**是攻击告警统计的报表，横坐标为日期，竖坐标为告警的次数。可以查看到最近一周的安全状态，比如哪天受到的攻击最多，最近安全状况呈上升、下降还是稳定状况等等。
- **系统组件运行状态：**监控各个管理服务器的性能状况和组件状态，同时也可在此界面中直接停止或重启各组件的服务。

4. 基本配置

4.1. 关于基本配置

- 在配置所有的策略之前，您应该先配置策略服务器、管理网段和 IP 组。在您安装中心服务器时，系统已经自动为您配置了一个中心服务器和一个初始的管理网段。在最简单的情况下，您只需再配置一个 IP 组就可以了，IP 组是策略下发和执行的最小单位。下图是策略服务器、管理网段、IP 组、网段、IP 地址关系示意图。在本系统的术语中，IP 组和网段是等同的。



名词解释:

- “按需支援操作员”：三权分立模式下特有，建立系统操作员的同时会建立相同的一个按需支援操作员。
- “系统管理员”：Windows 集成认证模式下特有，默认帐号为 administrator，密码与安装天珣服务器的那台服务器的 Windows 系统下的 administrator 密码相同。

- **“策略服务器”**：策略服务器包括中心服务器及本地服务器，客户端都需要连接到策略服务器来取策略。
- **“管理网段”**：管理网段是策略能够应用的最大的网段范围，也是系统操作员管理权限划分的基本单位。通过添加管理网段，来建立各个策略服务器管理的终端的范围，每个服务器可以管理一个或多个管理网段，只有在管理网段范围内的终端才能根据后续的 IP 组设置来确定是否能从这台策略服务器中获取策略。
- **“IP 组”**：IP 组是系统管理的最小的 IP 策略应用对象单元。IP 组是管理网段下的子网段或单独的 IP 地址，一个 IP 组可包含多个网段或独立 IP 地址。
- **“部门”**：添加部门信息，对上报的终端划分部门类别，客户端在注册时即可自己填写相应的部门，在进行报表查询时可通过选择部门来丰富展现的形式。
- **“终端注册”**：可以在页面上修改已注册终端的部门信息，或者通过管理员手工的方式来注册未注册的客户端。
- **“本地用户”**：本地用户是天珣自带的一种目录服务。本地用户就是用来存储用户信息在服务器本地中，为用户认证或者证书认证提供查找认证信息服务。
- **“用户组”**：用户逻辑组是基于用户设置策略的最小的用户策略应用对象单元。用户逻辑组可以包含 LDAP 中的 Group 和用户还有本地用户。
- **“可信 MAC”**：管理员可以预先设定的终端 MAC 地址列表，在其中列出的 MAC 称之为可信 MAC。可信 MAC 可以作为一项认证条件，与准入控制或安全控制结合对客户端进行合法性认证。
- **“可信 GUID”**：管理员可以预先设定的终端 GUID 列表，在其中列出的 GUID 称之为可信 GUID。可信 GUID 可以作为一项认证条件，与准入控制或安全控制结合对客户端进行合法性认证。

- **“用户、IP、MAC 组合”**：管理员可以预先设置用户、IP、MAC 的组合关系列表，并可作为一项认证条件，与准入控制或安全控制结合对客户端进行合法性认证。
- **“网络设备配置”**：启用准入控制的网络设备的配置，同时可以添加端口绑定，将端口作为一项认证条件，与准入控制或安全控制结合对客户端进行合法性认证。
- **“分组信息”**：已安装客户端的终端并上报了报表信息后，将终端的工作组信息分组展现。
- **“全局参数”**：所有客户端和服务器的全局基本配置参数。

4.2. 按需支援操作员

4.2.1. 配置介绍

此菜单为三权分立模式下特有，在帐号管理员建立系统操作员时，若选择其同时是按需支援操作员的话，在此处将会出现一个同名的按需支援操作员。在系统操作员登录时将无法修改此处的配置。



按需支援操作员配置界面截图，显示了一个表格，列出了已配置的操作员及其状态。

按需支援操作员	操作员全名	是否激活	修改密码
zsf	zsf	是	
jch	jch	是	
jing	jing	是	
liuichang	liuichang	是	
mingyaojingye	mingyaojingye	是	
yyhop	yyhop	是	

点击“添加”，进入“添加按需支援操作员”，可用于添加只有按需支援功能的操作员。

按需支援操作员

按需支援操作员名称:

按需支援操作员全名:

按需支援操作员密码:

请重复按需支援操作员密码:

是否激活: ☐ 否 ☒ 是

注: 右边带*号的项目必须输入

配置项:	说明
按需支援操作员名称	按需支援操作员的登录 ID
按需支援操作员全名	按需支援操作员全名
按需支援操作员密码	输入对应的密码
请重复按需支援操作员密码	重复输入对应的密码
是否激活	如果不激活, 则该管理员将无法登录按需支援管理界面

创建完成后可点击笔形按钮修改密码。

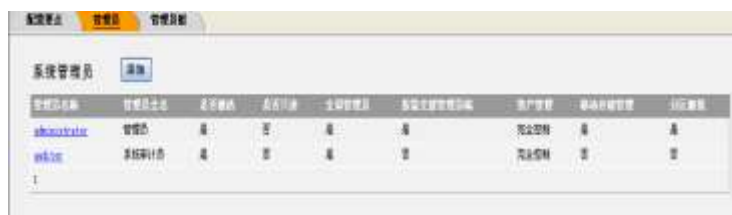
4.2.2. 配置要点

- 1、点击“添加”按钮, 输入“按需支援操作员名称” jch1
- 2、输入“按需支援操作员全名” jch1
- 3、输入“按需支援操作员密码”, 并输入“请重复按需支援操作员密码”
- 4、点击“保存”

4.3. 系统管理员

4.3.1. 配置介绍

此菜单为 windows 集成认证模式下特有。可在此菜单下添加除 administrator 外的其他系统管理员, 并可在管理员组中根据不同的管理网段分配不同权限给非全局管理员。



添加管理员

点击“添加”，进入添加“系统管理员”。



配置项:	说明
管理员名称	管理员的登录 ID，必须与策略服务器操作系统中的用户名相同。
管理员全名	与策略服务器操作系统中用户的全名对应。
是否激活	如果不激活，则该管理员将无法登录获得管理权限。
是否是只读权限	如果选择“只读权限”，则该管理员只能查看其所管理的服务器的配置信息，不能修改。
是否全局管理员	如果管理员为全局管理员，则该管理员具有最大的权限，能查看，修改，删除任何管理员所做的配置。
是否按需支援管理员端	如果管理员为按需支援管理员，则该管理员可为用户提供远程桌面援助。按需

	支援管理员需要安装按需支援监控端程序 hodviewer ，监听客户端发起的远程桌面帮助请求。
资产管理权限	设定管理员对资产模块的管理权限，有只读、完全控制和只能管理资产三种。只读权限只能查看资产信息；完全控制权限可进行查看、修改、删除等操作；只能管理资产权限表示登录 WEB 控制台时，只能管理资产信息，不能查看编辑其他策略。
分区解扰	授权该用户是否有解扰分区加扰后的移动存储设备的权限
菜单授权	对管理能访问的菜单进行授权
所属管理员组	一个管理员可以属于多个管理员组，不同的管理员组管理不同的策略服务器，因而一个管理员可以管理多个策略服务器。

添加管理员组

天珣内网安全风险管理与审计系统以 IP 组为权限管理的单位。不同的管理员组管理不同的管理网段，一个管理员可以同时属于多个组，因而一个管理员可以管理多个管理网段。点击“**管理员组**”设置，系统显示所有现存的组。

点击“**添加**”，进入添加管理员组

管理员组

组名称

组 (192.168.1.1/24) *

组描述

此管理员组的用户具有管理 192.168.1.X/24网段的权限

是否激活

☐ 否
☒ 是

所管理的管理网段

初始管理网段
NAT管理网段 (100)

->-<->

192.168.1.*

注：右边有*号的项目必须输入。

保存

删除

取消

配置项:
[说明](#)

组名称	请输入便于记忆的管理员组名称。
组描述	请输入关于这个管理员组的额外信息。
是否激活	如果不激活,则从属于此组的管理员将无法管理组内的服务器。主要用于测试方便, 建议使用默认值。
所管理的网段	管理员组可管理一个或多个管理网段, 左边的列表是系统中所有的管理网段, 右边的列表是该管理员组所管理的网段。

注意: 当属于某一管理员组的非全局管理员帐号登录时, 其所得到的权限仅限于其管理员组所管理的网段, 无法对所有不属于此网段的 IP 组进行策略配置。

4.3.2. 配置要点

配置前提: 新增一个新的管理员时, 必须确保 windows 系统中有相同名称的用户, 且该用户的密码不为空

1. 以系统管理员登录 Web 控制台, 点击“**管理员组**”中的“**添加**”按钮, 输入“**组名称**”test1, 点击“->”号将“**所管理的网段**”列表中的 miprangel 网段移动到右列中, 点击“**保存**”。
2. 点击“**管理员**”中的“**添加**”按钮, 输入“**管理员名称**”testadmin1, “**管理员全名**”testadmin1, “**是否激活**”选“是”, “**是否只读权限**”选“否”, “**是否全局管理员**”选“否”, “**是否按需支援管理员端**”选“是”, “**资产管理权限**”选“完全控制”, “**分区解扰**”选“能”, 点击“->”将“**所属管理员组**”中的 test1 移动到右列中, 点击“**保存**”。
3. 使用 testadmin1 帐号登录 WEB 管理控制台, 此帐号拥有全部策略配置权限, 但只能对 miprangel 网段所管理的 IP 组生效。

4.4. 策略服务器

4.4.1. 配置介绍

点击“策略服务器”选项，显示系统中所有的服务器，用户可以添加新的服务器，编辑，删除现有的服务器。

策略服务器					
策略服务器 添加					
服务器名称	IP地址	中心服务器IP地址	是否激活	管理端口	资产管理
224的本地服务器	192.168.0.224	192.168.1.16	是	8833	启用
CenterServer	192.168.1.16	192.168.1.16	是	8833	启用

添加服务器

点击“添加”进入添加服务器

策略服务器	
策略服务器	
服务器名称	CenterServer *
服务器描述	中心服务器
IP地址	192.168.1.10 *格式如：10.156.100.18
中心服务器IP地址	192.168.1.10 *
使用中心服务器的数据库连接参数	☒ 是 ☐ 否
SQL Server数据库连接参数	检查数据库连接
数据库服务器IP地址	192.168.1.10
端口	1433
用户名	tx_user
密码	
注：右边有*号的项目必须输入。	
保存 取消	

配置项：	说明
服务器名称	请输入便于识别的服务器名称
服务器描述	请输入此服务器的额外信息，方便管理

IP 地址	安装本策略服务器的电脑的 IP 地址
中心服务器 IP 地址	安装有中心策略服务器的电脑的 IP 地址。如果本策略服务器就是中心服务器，请填写自己的 IP 地址。
使用中心服务器的数据库连接参数	在添加本地服务器时，可选择此项，如果选择“是”，则直接使用与中心服务器相同的数据库，如果选择“否”，则需要配置下面的数据库连接选项
数据库服务器 IP 地址	输入本地服务器所使用的数据库 IP 地址
端口	输入本地服务器所使用的数据库端口地址，默认为 1433
用户名	输入数据库连接用户名
密码	输入数据库连接密码

注意：

- ◆ 天珣使用的登录 WEB 服务器的管理端口为 8833，此端口不可修改。
 - ◆ 资产服务器在中心服务器安装时默认已和中心服务器一起安装，因此无需单独安装。
 - ◆ 在添加本地服务器时必须指定正确的中心服务器 IP 地址，否则该服务器不能与中心服务器同步，因而不能得到最新的策略规则，同时也会影响该服务器所管理的 CC，当 CC 的 Primary Server 和 Secondary Server 都不可用时，中心服务器是 CC 取规则的策略服务器。
-

4.5. 管理网段

4.5.1. 配置介绍

点击管理网段的页面标签，将显示管理员设置的所有服务器的管理网段，通过所属主服务器的不同来区别是中心服务器还是本地服务器的管理网段。

通过添加管理网段，来建立各个策略服务器管理的终端的范围，每个服务器可以管理一个或多个网段，只有在管理网段范围里的终端才能根据后续的 IP 组设置来确定是否能从这台策略服务器中拿取策略。

添加管理网段

点击“管理网段”页面上的“添加”按钮进入添加管理网段界面。

管理网段

管理网段

管理网段名称

172

管理网段描述

管理网段开始IP地址

172.25.0.1

管理网段结束IP地址

172.25.255.255

Primary Server

CenterServer

Secondary Server

CenterServer

是否使用默认的下联服务器

☐ 否 ☒ 是

下联服务器地址

停止客户端服务程序时是否需要验证密码

☐ 否 ☒ 是

卸载客户端时是否需要验证密码

☐ 否 ☒ 是

客户端卸载及停止服务密码

显示明文

注：右边有*号的项目必须输入。

保存 删除 取消

配置项：	说明
管理网段名称	您能记得住的名称。

管理网段描述	您可以输入关于这个网段的额外信息。
管理网段开始 IP 地址	网段不一定是完整的 B 类、C 类或其它完整的子网，可以从任何一个地址开始。
管理网段结束 IP 地址	这个地址也是任意的，但应该大于开始的 IP 地址。注意不同的管理网段的 IP 地址不要有重叠。
Primary Server	本管理网段的主策略服务器。每个网段的客户端首先从主策略服务器取策略，如果失败，则从辅策略服务器取策略，如果失败，则从中心服务器取策略。
Secondary Server	本管理网段的辅策略服务器。
是否使用默认下载服务器	如果选择“是”，则下面的“下载服务器地址”不可填，系统将使用 http://策略服务器 IP:8833/download/ 作为下载服务器地址。如果选择“否”，将使用“下载服务器地址”输入的 URL 作为下载服务器地址。
下载服务器地址	下载服务器供客户端下载红名单中的软件、防病毒软件升级码，补丁程序等。默认的下载服务器地址为 http://策略服务器 IP:8833/download/。如果您使用其他的下载服务器，请在此处输入该服务器的 URL 地址。红名单软件、防病毒软件升级码、补丁程序等的下载 URL 只需输入“下载服务器地址”后面的相对路径部分。比如一个红名单软件的下载地址为 http://策略服务器 IP:8833/download/software/abc.exe，那么，红名单配置中的“下载 URL”只需填

	写 “software/abc.exe”。
停止客户端服务程序时是否需要验证密码	设置停止客户端服务时是否需要输入密码
卸载客户端时是否需要验证密码	设置卸载客户端时是否需要输入密码
客户端卸载及停止服务密码	设置卸载及停止服务的密码

一个管理网段中配置的 IP 地址段可以是整个子网，比如 “192.168.0.1-192.168.1.255”，也可以是一小段连续的 IP，比如 “192.168.0.40-192.168.0.50”，但无法配置为单个 IP 地址。

注意：删除某个管理网段时，将同时删除这个管理网段下建立的所有 IP 组，并且对这些 IP 组生效的策略也将失效（若这些策略关联了其他 IP 组，将不会受影响）。

4.5.2. 配置要点

1. 点击“添加”按钮，进入添加“管理网段”界面
2. 输入“管理网段名称”为本地服务器网段
3. 输入“管理网段开始 IP 地址” 192.168.1.1
4. 输入“管理网段结束 IP 地址” 192.168.1.254
5. 选择“Primary Server”为本地服务器
6. 选择“Secondary Server”为 CenterServer
7. 点击“保存”
8. 此时已为本地服务器定义了管理网段为 192.168.1.1-192.168.1.254 范围，所有这个网段下的客户端均将通过本地服务器连接拿取策略。

4.6. IP 组

4.6.1. 配置介绍

IP 组是设置策略的最小单位，一个管理网段划分为多个 IP 组使配置管理更加灵活，一个主机也可以配置成一个 IP 组。

一台终端的 IP 地址必须属于设定的某个 IP 组才能正常获取到此 IP 组的策略，而这个 IP 组必须属于某个管理网段所管理。

IP 组

点击“IP 组”标签，默认将显示所有服务器的所有管理网段下已建立的所有 IP 组。



通过页面上的查询 IP 组条件，可以分别对某个或某些 IP 组进行查询。



点击管理网段的下拉菜单，可以选择配置好的管理网段；选择好查询条件后，点击“按条件查询 IP 组”按钮，将查询出相应的 IP 组。



如果知道某台客户端的 IP 地址，想查询其所属的 IP 组，那么只需要在“只显示包含指定地址的组”中输入此 IP 地址，然后点击“按

条件查询 IP 组”按钮，即可查询出其所属的 IP 组信息。

点击“添加”按钮进入 IP 组设置界面

IP组

工作时间

IP组名称

test

IP组描述

所属的服务器

Center Server

所属的管理网段

初始管理网段

本IP组中的IP地址

名称	开始地址	结束地址	编辑	删除
192.168.1	192.168.1.1	192.168.1.254		

排除的地址

IP地址	编辑	删除

工作时间

不设置工作时间

本IP组应用的策略

查看及编辑

认证策略

是否启用用户认证

☒ 不启用

☐ 启用

选择启用的目录服务

☐ 本地用户

用户、IP、Mac组合认证

☒ 不启用

可信Mac认证

☒ 不启用

注：右括号*号的项目必须输入。

保存

删除

取消

配置项：	说明
IP 组名称	您能记住的 IP 组名称
IP 组描述	您可以输入关于这个 IP 组的描述信息。
所属的服务器	选择这个 IP 组是被哪个策略服务器管理。这个服务器是 IP 组所在管理网段的主策略服务器（Primary Server）。
所属的管理网段	选择这个 IP 组属于哪个管理网段。这个选项的内容会根据“所属的服务器”的内容变化，如果改变“所属的服务器”，则“所属的管理网段”只出现选择的服务器所管理的管理网段。
排除的地址	IP 组可以包含一个或多个网段，可以对网段中

	的某些 IP 地址进行排除。IP 地址被排除后，这个 IP 地址将不获取策略，系统的应用准入机制也不对这个 IP 地址进行强制策略检查。如果这个排除的 IP 地址在另一个 IP 组中以独立 IP 存在，那么这个 IP 地址对应的策略以那个 IP 组的策略为准。
本 IP 组中的 IP 地址	输入 IP 组名称和具体的 IP 地址范围并添加来定义此 IP 组。添加后可通过笔形按钮进行修改，也可通过 X 形按钮进行删除。
工作时间	选择工作时间选项，工作时间策略的订制可在“工作时间”菜单中添加
本 IP 组应用的策略	通过查看及编辑按钮进行此 IP 组的相应策略配置。若此 IP 组还没有设置策略的话，则会在此处提示用户“还没有应用策略”。
认证策略	在非网络准入的前提下进行的认证选项，可以和“可信 MAC”、“用户、MAC、IP”组合成完善的认证模式。基本认证包括三个选项：不启用时客户端无需进行认证，“仅客户端运行”接入电脑只需运行了客户端即可通过验证。“用户认证”不但需要验证客户端运行，而且需要与第三方认证系统连接，验证用户的有效性。
选择启用的目录服务	启用用户认证后，需要选择一个目录服务的认证系统，这个目录服务需要在“用户组”中建立。通过这个第三方的认证系统，比如 AD 域，客户端需要进行用户密码的认证，只有输入符合 AD 域中的用户和密码才能正常认证。选择其中一个目录服务时，在其前面的方框内打勾即可。同时也可选择进行本地用户认证。

用户、IP、MAC 组合认证	通过用户、IP、MAC 三种条件对客户端进行组合绑定认证。可进行 MAC-IP 和 USER-MAC-IP 认证。在验证输入的用户认证是正确的基础上，再对客户端的 IP 和 MAC 地址进行唯一性认证。在客户端输入用户名和密码后，将对其 MAC 和 IP 进行校验，只有符合这个组合认证里的 IP 和 MAC 才能正常完成认证，否则将会提示客户端不符合安全规范；MAC-IP 组合认证时，客户端无需输入用户名密码，只对本机 MAC 和 IP 进行验证，若 MAC 与 IP 不符合绑定策略的话，将认证不成功，提示客户端不符合安全规范。组合策略需要在“用户、IP、MAC 组合”页面中进行配置。
可信 MAC 认证	对接入认证的机器进行 MAC 地址的检查，属于可信 MAC 范围的将会认证成功，否则将被认为不符合安全规范。策略需要在“可信 MAC”页面中进行配置。

注意：在已定义的工作时间范围内的终端将会显示为在线，非工作时间范围的终端将会显示为离线，并启用离线策略。

注意：此处添加的 IP 组地址范围必须与其管理网段范围一致，否则无法正常保存。

点击本 IP 组应用的策略的“**查看及编辑**”按钮，进入应用策略的编辑界面

IP组 工作时间

工作时间设置

工作时间名称

工作日

工作时间

加班日期及时间

休假日期及时间

注：右这有*号的项目必须输入

保存 取消

配置项：	说明
工作时间名称	输入策略名称
工作日	选择工作时间为几个工作日，通过勾选即可实现
工作时间	添加工作时间段，直接输入时间点如 9：00
加班日期及时间	添加加班日期和时间段
休假日期及时间	添加休假日期和时间段

配置完成后，需在 IP 组配置中应用已经配置好的时间段策略。

4.7. 部门

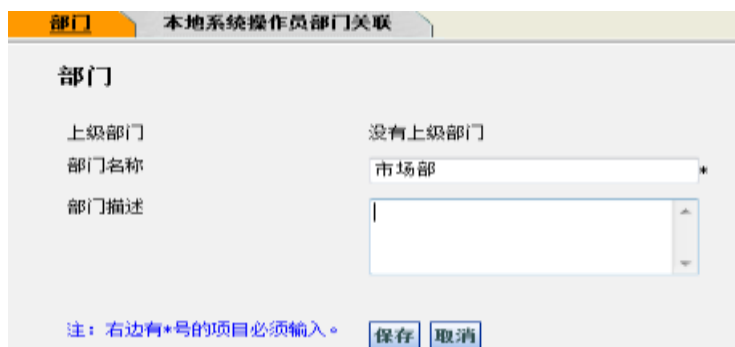
4.7.1. 配置介绍

通过设置各级部门来对客户端进行部门划分，使其在客户端注册时可以选择自己所在的部门，并在报表中体现出不同部门的展现需求。

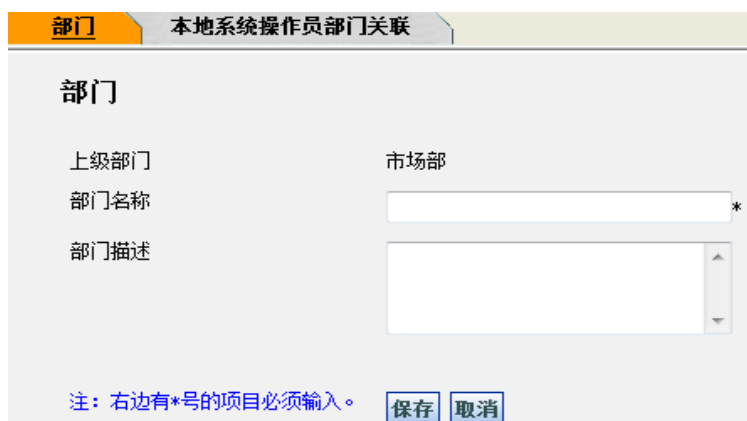
部门



点击“添加顶级部门”对部门进行添加



点击“添加下级部门”对这个顶级部门进行下级部门的设置



调整部门树层次

在创建了很多部门后,如果想将一些部门调整到比较显眼的位置,或者是将比较重要的部门调整到前排,则可以使用部门树右边的上下箭头进行调整,既可以选择上调一级,下调一级;也可以选择置顶或者直接调到最后一行。



注意：部门前后顺序调整只支持同级部门之间的前后顺序调整。

本地系统操作员部门关联

在创建了非全局管理系统操作员之后，使用全局管理员登录管理界面时可以在这个页面看到所有创建的非全局管理系统操作员，并可对其赋予管理个别部门的权限，有此权限的系统操作员即可查看其管理的部门的报表等信息。

部门 本地系统操作员部门关联		
本地系统操作员部门关联		
系统操作员名称	系统操作员全名	所管理的部门
44	444	test5
777	777	support5

点击系统操作员名称链接，进入后对其进行部门权限的分配

部门 本地系统操作员部门关联

本地系统操作员部门关联

系统操作员名称 44

系统操作员全名 444

所属部门

部门管理

☒ test

☐ development

☐ support

☐ HR

☐ 市场部

保存

取消

勾选相应部门后点击“保存”即可。

4.8. 终端注册

4.8.1. 配置介绍

配置完部门后，可在客户端全局参数处启用客户端注册功能，启用注册功能后就能通过终端注册的管理来查看或修改已注册客户端信息，或者页面上手工完成未注册客户端的信息填写。

开启客户端注册功能



在上页面上，管理员还可以增加自己想要的注册项目。

终端手工注册

使用终端手工注册来给客户端进行注册，若已启用进行客户端注册的策略配置，而用户因为疏忽或不想注册的话，则可以在此处由管理员对其进行手工注册，将客户端与部门进行绑定。



通过主机名或 IP 范围可查询出相应已受控的客户端，在方框处打勾后点击“注册选中的终端”进行手工注册，也可直接点击“注册所有的终端”对所有终端进行注册。

修改注册信息

若已启用进行客户端注册的策略配置，那么可以在此处可以查询到正常注册的客户端提交的注册信息以及管理员手工注册的信息，管理员可以对其进行部分调整，手工修改注册信息。



在 mac 地址前的方框中打勾，然后点击“**修改选中终端的部门信息**”，即可修改这些选中终端的部门信息。点击“**修改所有终端的部门信息**”，可以将所有终端部门信息修改。点击“**删除选中终端信息**”即可删除选中的终端注册信息，删除之后客户端会根据策略重新上报。点击“**导出到 Excel**”可以将导出已注册客户端的信息。

注意：客户端注册时支持客户端处于 NAT 环境下，在上报注册信息时会将客户端真实 IP 和 NAT 后的 IP 同时报上来，方便区分。

4.9. 本地用户

4.9.1. 配置介绍

本地用户是天珣自带的一种目录服务。目录服务将有关信息存储为具有描述性属性的对象。人们可以使用该服务按名称查找对象，可使用它们查找服务，同时获得对应的资源或信息。本地用户就是用来存储用户信息在服务器本地中，为用户认证或者证书认证提供查找认证信息服务。

点击“**本地用户**”标签，将显示服务器上现有的本地用户信息



点击添加“添加用户”按钮，进入添加本地用户页面



本地用户

本地用户

登录名

姓名

数字证书用户名

密码 《如果密码为空则不能以用户名/密码方式登录》

确认密码

电话号码

电子邮件

注：右边带*号的原因必须输入

配置项：	说明
登录名（必填）	本地用户认证时的用户登录名
姓名（必填）	用户的姓名
数字证书用户名	证书认证时的证书名（需在用户组-目录服务中的本地用户配置相关信息才能使用）
密码	本地用户认证时的登录密码
确认密码	再次确认登录密码
电话号码	用户的电话
电子邮件	用户的电子邮件

注意：登录名和证书名在本地用户中是唯一的，不能有相同的名字出现；用户密码为空时，必须填上数字证书用户名，认证时只能用证书认证。

“本地用户”标签下，点击“导入用户”按钮，可以批量导入事先储存在本地某个 excel 表中的用户信息。



点击“导出用户”按钮，可以将服务器的本地用户信息导出到一个 excel 表中，此 excel 表就可以作为“导入用户”的信息表。

点击“下载模板”按钮，可下载一个 excel 表的用户信息模板，在表里填入用户信息，就可以作为“导入用户”的信息表。

点击修改密码的笔型按钮，可以修改本地用户的密码。

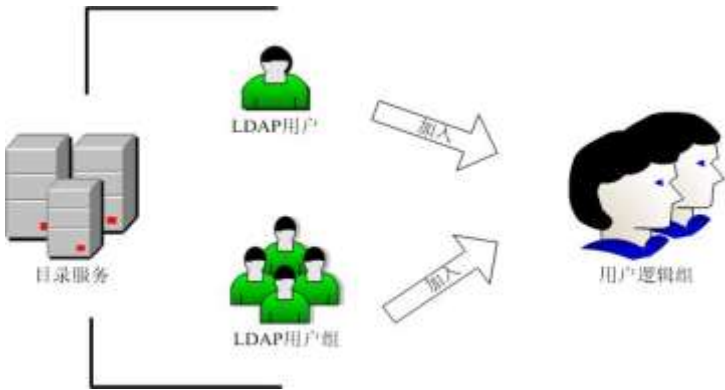
4.10. 用户组

4.10.1. 配置介绍

本系统支持自带的本地用户认证，或者与第三方认证系统联动完成用户认证，采用标准的 LDAP 协议，支持的第三方认证系统包括 AD 域，iPlanet，OpenLDAP 等。这些也称为“目录服务”。如果您的网络中没有认证系统，您可以下载安装免费的 iPlanet 软件，建立一个简单且安全的认证系统。

与 IP 组类似，本系统支持用户逻辑组。用户逻辑组是基于用户设置策略的最小的对象单元。用户逻辑组可以包含 LDAP 中的 Group 和用户。

下图是目录服务、LDAP 用户，逻辑组之间的关系图



下图是通过第三方认证服务器认证过程示意图



目录服务

点击“目录服务”标签，显示服务器现有的目录服务信息。



点击“添加”进入添加目录服务的页面



配置项:	说明
目录名称	设置您企业的目录服务的名称。

目录服务路径	LDAP 管理域的目录服务路径，例如域名为 sample.com，如果目录类型为 AD 域，则填写格式可参考： dc=sample,dc=com；如果目录类型为 SUN 的 iPlanet，则填写格式可参考： OU=People,dc=sample,dc=com。
目录服务类型	本系统支持 AD、iPlanet、OpenLdap 三种目录服务类型。
访问用户名	本系统访问目录服务所用的用户，该用户只需具有读取活动目录的权限即可。输入用户名时建议在用户名前加上域名，例如：sample\administrator。在 iPlanet 环境中，必须输入用户名：CN=Directory Manager。
访问密码	本系统访问目录服务所用的用户的密码。
目录服务器列表	目录服务器列表，可通过输入目录服务器的 IP 或域名来添加，可添加多台服务器。
目录参数	iPlanet 和 OpenLdap 环境中，可建立动态组，此参数用于设置刷新动态组缓存的时间间隔，默认为 24 小时（86400 秒）。

注意：如果是 iPlanet 的话，输入的用户名必须是 CN= Directory Manager，密码也必须是创建 iPlanet 时建立好的 Directory Manager 密码，否则将无法验证成功。

输入完服务器 IP 后，点击“访问密码”右侧的“检验”图标，可

以直接进行模拟验证，如果配置正确的话将验证成功，否则会给出适当提示。

本系统也支持自带的“本地用户”目录服务，在“目录服务”标签的页面下点击“本地用户”，进入本地用户配置页面。

配置项：	说明
目录名称（必填）	设置本地用户的目录服务的名称，默认为“本地用户”
目录服务类型	不能修改，默认为“本地用户”
受信任的证书颁发机构	导入证书颁发机构颁发的根证书，为用户认证时验证用户证书提供信息
证书状态验证	选择“不验证证书状态”，则证书认证时不验证证书是否已被吊销，仅需要认证是否是可信的 ca 颁发的。 选择“先进行在线验证，没有 CA 服务器或 CA 服务器不可用时使用吊销证书列表验证”，则要验证证书是否已被吊销，验证方式为先到 CA 服务器在线验证，没有 CA 服务器或 CA 服务器不可用时则用吊销证书列表验证，需要配置下

	面的配置项
吊销证书列表	添加一个从 CA 服务器发布的一个吊销证书 c1r 列表, 验证证书是否已被吊销
在线验证 CA 服务器列表	添加在线的 CA 服务器, 用于实时在线验证证书状态是否已被吊销

用户组

添加完目录服务之后, 我们就可以在用户组选项里设置用户组了。

用户组是系统设置用户规则的对象单位, 目录服务中的用户组或用户必须加入到这里才能被设置用户规则。一个用户可以属于多个用户组。

点击“用户组”选项, 查看已经存在的用户组列表。



点击“添加”进入添加用户组配置页面



配置项:	说明
用户组名称	您能记住的名称。
描述信息	您可以输入关于这个逻辑组的额外信

	息。
用户组成员	通过查看和编辑选项，连接域服务器添加用户和用户组。
应用的策略	通过查看和编辑选线，对设置好的策略进行应用。

点击用户组成员的“查看及编辑”选项，进入编辑用户组成员界面



选择一个目录服务，点击“添加成员”，系统将从该目录服务读取用户资料，并以列表形式列出，管理员可从列表中选择成员或组加入用户组。

点击“添加成员”按钮后，将连接目录服务进入目录浏览界面：



此时选择你要添加的用户及组，再按“添加选择的项目”按钮，将你所选择的项目添加至用户组。此浏览界面根据目录服务器中的所有用户和组的位置关系，以列表形式展开，每个用户及组都有唯一的目录路径，通过这个路径，在认证时进行定位。

点击应用的策略的“查看及编辑”按钮，进入应用策略的配置界面



在此界面中会显示已经应用到此用户组的策略的列表，要将策略加入此用户组，请点击相应模块的“编辑”按钮，进入策略选择界面



在此界面中会列出已配置的所有对应此模块的策略，需要将某条策略加入此用户组，只需在这条策略前勾选后保存即可。

4.10.2. 配置要点（以 AD 域为例）

添加目录服务

1. 点击“目录服务”中的“添加”按钮，进入目录服务添加页面
2. 输入“目录名称”为企业域服务器
3. 如果 AD 域名称为 testworkl.com，则在目录服务路径中输入“目录服务路径”为“dc=testwork,dc=com”
4. “目录服务类型”选择“Active Directory Server”
5. “访问用户名”为登录 AD 域服务器所在终端的用户名，“访问密码”为该用户名所对应的密码
6. 在“目录服务器列表”栏中输入服务器 IP 地址为 AD 域服务器

的 IP 地址，然后点击“**添加服务器**”按钮，将此 IP 添加到列表中

7. 点击“**验证**”，检查是否配置是否正确，是否能跟目录服务器正常通信
8. 点击“**保存**”，保存此目录服务配置

添加用户组

9. 点击“**用户组**”中的“**添加**”按钮，进入用户组添加页面
10. 输入“**用户组名称**”为财务部
11. 点击“**用户组成员**”的“**查看及编辑**”选项，进入添加用户组成员界面
12. 在“**目录服务**”下拉列表中选择企业域服务器，然后点击“**添加成员**”
13. 进入“**目录浏览**”页面后，选择 OU 中财务部的用户 testuser1，点击“**添加选择的项目**”对所选择的用户加以保存
14. 返回上一级目录，点击“**应用的策略**”的“**查看及编辑**”，进入选择策略界面
15. 选择“**访问控制**”中的“**httpstest**”策略，点击“**保存**”
16. 返回上一级目录后，再次点击“**保存**”按钮，完成“**用户组**”策略的编辑修改

4.11. 可信 MAC

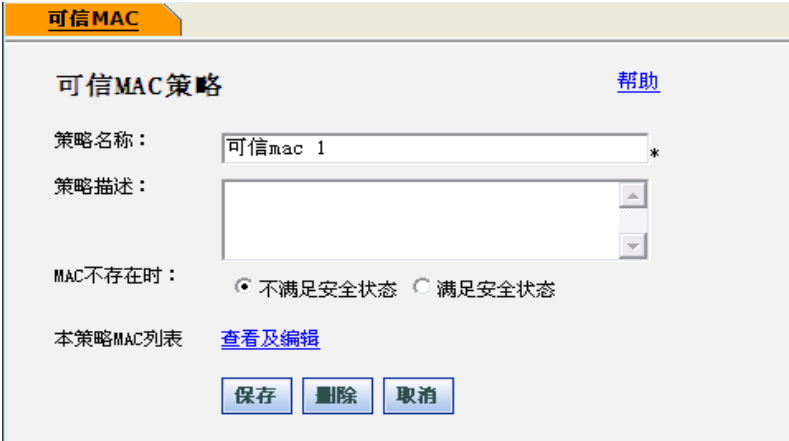
*该章节功能仅适用于高级版和增强身份认证高级版

4.11.1. 配置介绍

可信 MAC 组合认证配置界面。在网络准入中如果启用可信 MAC 认证，那么只有列表内的 MAC 地址才能通过认证；在 IP 组中如果启用可信 MAC 认证，那么只有列表内的 MAC 地址才是符合安全基线要求的。



点击“添加”按钮，进入可信 MAC 策略配置界面



配置项:	说明
策略名称	填写策略名称
策略描述	填写对策略的详细描述
MAC 不存在时	选择客户端 MAC 地址不在此列表内时，客户端是否认为其满足安全基线要求，如果选择不满足则会在客户端给出提示，如果选择满足则会认为此客户端是符合安全基线的。
本策略 MAC 列表	对 MAC 列表进行维护

点击“本策略 MAC 列表”的“查看及编辑”选项，进入添加可信 MAC 地址界面



点击“添加”按钮

可信MAC

添加可信MAC地址

MAC地址

主机名

MAC地址有效期限制

MAC地址有效期起始时间

MAC地址有效期结束时间

802.1X选项 VLANID

EOU选项 ACL

格式: AA-BB-CC-DD-EF-FF

否 是

2000-0-0 00:00:00

2000-0-0 00:00:00

0 (表示不使用此项)

无

注: 右带+号的项目必须输入。

保存 取消

配置项:	说明
MAC 地址	填写可信任的主机 MAC 地址。
主机名	填写主机名，便于查询管理。
MAC 地址有效期限限制	开启 MAC 地址有效期限限制，MAC 地址只能在指定的时间范围内通过认证，超出时间范围将被拒绝。
MAC 地址有效期起始时间	MAC 地址有效期起始时间。
MAC 地址有效期结束时间	MAC 地址有效期结束时间。
802.1X 选项 VLANID	为 MAC 地址分配 VLAN，客户端通过认证后，所接的交换机端口将被自动划分至指定的 VLAN。
EOU 选项 ACL	在 EOU 认证中，以 MAC 地址为目标，向该客户端所接的交换机端口下发动态 ACL。

点击“从报表导入”，通过客户端报表中的主机名和 MAC 地址进行添加



通过选择的 IP 组和是否绑定的条件进行查询，在查询出的列表中对需要的绑定项打勾，然后点击“保存选择的项目”，对这些 MAC 地址进行保存。

注意：绿色显示的 MAC 地址已经添加到了可信 MAC 列表中。

点击“从文件导入”，通过固定格式的 EXCEL 文件，导入到数据库中，对可信 MAC 进行配置。

点击“下载模板”，将固定格式的文件导出至电脑中，通过修改此文件对可信 MAC 列表进行维护，再通过“从文件导入”选项，将维护好的文件导入至数据库中。

4.11.2. 配置要点

1. 点击“添加”按钮，进入可信 MAC 添加页面
2. 输入“策略名称”为认证 MAC 列表
3. “MAC 不存在时”选择“不满足安全基线”
4. 点击“本策略 MAC 列表”的“查看及编辑”按钮进入 MAC 地址编辑页面
5. 点击“从报表导入”，选择服务器为“CenterServer”，所属 IP 组为“所有 IP 组”，点击“查询”
6. 在查询出的列表中选择所需要的 MAC，点击“保存选择的项目”

7. 返回上一级目录，点击“保存”

4.12. 可信 GUID

*该章节功能仅适用于高级版和增强身份认证高级版

4.12.1. 配置介绍

可信 GUID 组合认证配置界面。在网络准入中如果启用可信 GUID 认证，那么只有列表内的 GUID 才能通过认证；

点击“添加”按钮，进入可信 GUID 策略配置界面



可信GUID策略配置界面。包含以下字段：

- 策略名称：输入框，带星号 *
- 策略描述：文本框
- 创建状态：全局
- 创建者：administrator
- 底部按钮：保存、取消

配置项：	说明
策略名称	填写策略名称
策略描述	填写对策略的详细描述

添加完成后的页面如下所示：



可信GUID策略列表界面。包含以下元素：

- 可信GUID策略 添加
- 可信GUID策略列表
- 策略名称：guid
- 描述：guid
- 创建者：administrator
- 设置：铅笔图标
- 帮助

点击“设置”下的“ ”按钮”选项，进入添加可信 GUID 地址界面



点击“从报表导入”，通过客户端报表中的主机名和 GUID 地址进行添加



根据所属 IP 组 和是否绑定的条件进行查询，在查询出的列表中对需要的 GUID 打勾，然后点击“保存选择的项目”，对这些 MAC 地址进行保存。

注意：绿色显示的 GUID 已经添加到了可信 GUID 列表中。

点击“从文件导入”，通过固定格式的 EXCEL 文件，导入到数据库中，对可信 GUID 进行配置。

点击“下载模板”，将固定的 GUID 导入格式的文件导出至电脑中，通过修改此文件对可信 GUID 列表进行维护，再通过“从文件导入”

选项，将维护好的文件导入至数据库中。

注意：GUID 认证仅支持标准 802.1x 与漫游 802.1x

4.12.2. 配置要点

1. 点击“**添加**”按钮，进入可信 GUID 添加页面
2. 输入“**策略名称**”为认证 MAC 列表
3. 点击“**本策略 GUID 列表**”的“**查看及编辑**”按钮进入 GUID 地址编辑页面
4. 点击“**从报表导入**”，选择服务器为“**CenterServer**”，所属 IP 组为“**所有 IP 组**”，点击“**查询**”
5. 在查询出的列表中选择所需要的 GUID，点击“**保存选择的项目**”
6. 返回上一级目录，点击“**保存**”

4.13. 用户、IP、MAC 组合

4.13.1. 配置介绍

通过客户端的 USER-IP-MAC、MAC-IP 的组合绑定，对客户端进行唯一性检查，只有符合绑定要求的客户端才符合安全基线的要求。

USER-IP-MAC 可细分为 User-IP，User-MAC，User-IP-MAC，User4 种组合。

点击“**添加组合策略**”按钮，进入组合管理策略配置界面

用户、IP、MAC组合

组合策略

帮助

组合策略名称

策略描述

组合不存在时

请选择一种组合类型

注：右边有*号的项目必须输入。

保存

取消

配置项：	说明
组合策略名称	填写简单明了的组合策略名称。
策略描述	详细策略描述
组合不存在时	当选择 User-IP-MAC 组合时，登录用户在组合中不存在；或选择 MAC-IP 组合，MAC 在组合中不存在，这两种情况称为组合不存在。在组合不存在的情况下，可以采取“不满足安全基线”和“满足安全基线”两种认证操作。
选择一种组合类型	选择组合类型，包括 User-IP-Mac 以及 MAC-IP 组合两种。User-IP-MAC 以 User 为检测的对象，MAC-IP 组合以 MAC 为检测的对象。

点击“保存”对所配置策略进行保存, 保存后的页面如下图所示：

用户、IP、MAC组合				
组合管理				
组合策略名称	描述	组合类型	创建者	设置组合
010101		USER-IP-MAC组合	luczhaojun	
0102		USER-IP-MAC组合	luczhaojun	
f0efefef		MAC-IP组合	jing	
00		MAC-IP组合	jing	

USER-IP-MAC 组合

点击已保存的策略名称，进入策略修改界面

组合策略

组合策略名称

21212*

策略描述

组合不存在时

☐ 不满足安全状态

☒ 满足安全状态

请选择一种组合类型

USER-IP-MAC组合

注：右边有*号的项目必须输入。

保存

删除

取消

点击“设置”下的“”按钮”选项，进入绑定策略设置界面

设置组合策略“21212”

用户名

IP地址

查询

重置

返回

已设置的用户

用户名	目录服务路径	创建状态	创建者	YLAN	删除
1					

添加用户

从报表添加

从文件导入

导出

下载导入模板

配置项:	说明
添加用户	通过配置页面手工添加组合设置。
从报表添加	系统自动读取客户端报表信息,管理员可从中选择添加组合设置。
从文件导入	使用组合导入工具,将 Excel 文件中的组合信息导入系统数据库。
导出	将组合信息导出至 Excel 文件。
下载导入模板	下载用于文件导入的 Excel 模板。

注意：通过“用户名”或者“IP 地址”的查询，可对所绑定的信息进行快速查询，且在进行绑定设置时，如果出现重复绑定的 IP 地址，程序会自动检测，并给出提示。

点击“添加用户”，进入用户添加界面

启明星辰
http://www.venustech.com.cn

47

用户、IP、MAC绑定

设置组合策略“100”

用户基本信息

用户名:

登录名:

部门:

目录服务路径:

动态VLAN ID:

动态ACL:

帮助

仅在启用802.1x网络准入时生效

仅在启用802.1x网络准入时生效

注：右括号+号的项目必须输入。

保存 取消

配置项:	说明
用户名	填写 LDAP 目录服务中的用户名，可为中文或英文。
登录名	填写 LDAP 目录服务中的登录名，一般为英文。AD 域的登录名在整个域里面都是唯一的，而 IPlanet 和 OpenLDAP 的登录名在域里可以有重名，重名的登录名以目录里的 OU 区分。
部门	填写 LDAP 目录服务中的部门 OU，可不填
目录服务路径	填写此用户的完整 DN 信息，如 test 用户的完整 DN 是： CN=test,CN=Users,DC=Sample,DC=com，那么此处填写的路径 CN=test,CN=Users,DC=Sample,DC=com。注意目录服务认证时对大小写敏感。
忽略目录服务路径	如果目录服务中的登录名是唯一的，不需要通过目录服务路径来区分，您可以选择忽略目录服务路径。（AD 的登录名是唯一的，对其他的目录服务您可以通过规划保证登录名是唯一的）

动态 VLAN ID	为此用户绑定动态 VLANID，用户认证后可自动将交换机端口划分至绑定的 VLAN。此功能仅在启用 802.1x 网络准入时生效。
动态 ACL	为此用户绑定动态 ACL，用户通过 EoU 认证后可自动向交换机下发动态 ACL。此功能仅在启用 EoU 网络准入时生效。

点击“保存”后，对此用户的设置进行保存

注意：如果选择“忽略目录服务路径”，请在输入“用户名和”和“登录名”时与目录服务中的保持完全一致，否则可能出现认证不通过的情况。

点击设置好的用户信息名称，进入后会出现“组合关系”的设置选项

用户、IP、MAC组合

设置组合策略“100”

用户基本信息

用户名: administrator

登录名: administrator

部门:

目录服务路径:

☒ 忽略目录服务路径

动态VLAN ID: 0

动态ACL:

仅在启用802.1x网络准入时生效

仅在启用EoU网络准入时生效

组合关系

查看及编辑

注：右边带+号的项目必须输入。

保存 取消

点击“组合关系”的“查看及编辑”选项，进入 IP-MAC 绑定策略配置界面

用户、IP、MAC组合

设置组合策略“100”

"administrator"的IP及MAC组合关系

手工增加IP及MAC组合关系

查询

MAC地址	IP地址	默认网关	有效期	解除组合关系
002518624120	192.168.0.203	192.168.0.1	不限制	

点击“手工增加 IP 及 MAC 组合关系”按钮

用户、IP、MAC组合

设置组合策略“100”

“administrator”的IP及MAC组合关系

用户名administrator

目录服务路径

MAC地址不限格式：AABBCCDDEEFF

IP地址限制否是

IP地址类型静态IP地址

IP地址

子网掩码255.255.255.0

默认网关

有效期限制否是

有效期起始时间2009-9-14 17:00:58

有效期结束时间2009-9-14 17:00:58

保存删除取消

输入所需绑定的 IP 及 MAC 地址等信息

配置项：	说明
MAC 地址	决定是否将 MAC 地址为组合认证条件。准入认证时客户端的 MAC 地址必须与组合内的 MAC 地址一致才可通过认证。
IP 地址限制	决定是否将 IP 地址为组合认证条件。
IP 地址类型	设置组合认证条件中 IP 地址的类型,包括 DHCP 和静态 IP 两种。
IP 地址	准入认证时客户端的 IP 地址必须与组合内的 IP 地址一致才可通过认证。
子网掩码	子网掩码不作为组合认证条件,仅在系统根据登录用户的 User-IP 组合自动更正客户端 IP 地址时,用于修改子网掩码。
默认网关	默认网关不作为组合认证条件,仅在系统根据登录用户的 User-IP 组合自动更正客户端 IP 地址时,用于修改默认网关地址。

50

启明星辰
http://www.venustech.com.cn

有效期限制	设定组合规则的有效期，如果超过有效期，对网络准入，则认证不通过；对于非网络准入，则此条规则无效。
有效期起始时间	有效期起始时间。
有效期结束时间	有效期结束时间。

点击“保存”，完成 USER-IP-MAC 绑定配置

点击“从报表添加”按钮，可以从已知的客户端报表信息中添加绑定策略



选择需要绑定的主机，并选择对应的目录服务，点击“保存选择的项目”进行绑定操作。

注意：只有向中心策略服务器上报过客户端信息的终端才会出现在列表中，如果“用户”栏是空的，说明这台终端没有登录过目录服务，因此需要在保存后再对其进行手工修改。

MAC-IP 组合

配置 MAC-IP 组合与 USER-IP-MAC 组合类似，点击已保存的策略名称，进入策略修改界面

用户、IP、MAC组合

组合策略

组合策略名称

mac-ip*

策略描述

组合不存在时

☒ 不满足安全状态

☐ 满足安全状态

请选择一种组合类型

MAC-IP组合

IP绑定生效范围

☒ 所有网络环境生效

☐ 仅在所属管理网段生效

☐ 仅在本IP组生效

注：右边有*号的项目必须输入。

保存

删除

取消

点击保存后，出现如下页面：

用户、IP、MAC组合

组合管理

添加组合策略

组合策略名称	描述	组合类型	创建者	设置组合
11111		IP-IP-MAC组合	luczhaojun	
222		IP-IP-MAC组合	luczhaojun	
ffafafaf		MAC-IP组合	jing	
aa		MAC-IP组合	jing	

点击“设置”下的“ ”按钮”选项，进入 MAC-IP 绑定设置界面

用户、IP、MAC组合

设置组合策略“mac/ip”

IP

MAC

查询

重置

返回

已设置的MAC-IP地址组合列表

名称	MAC地址	IP地址	IP地址类型	删除
00221500fc54	00221500fc54	192.168.0.181	静态IP地址	
00242cac1634	00242cac1634	192.168.0.185	静态IP地址	
000c298550d7	000c298550d7	192.168.0.194	静态IP地址	

添加

从报表增加

从文件增加

导出

下载导入模板

配置项：	说明
添加	通过配置页面手工添加组合设置。
从报表增加	系统自动读取客户端报表信息，管理员可从中选择添加组合设置。

从文件增加	使用组合导入工具，将 Excel 文件中的组合信息导入系统数据库。
导出	将组合信息导出至 Excel 文件。
下载导入模板	下载从文件增加功能所使用的导入模板。

点击“添加”按钮，手工添加 MAC-IP 绑定策略



该截图显示了“用户、IP、MAC绑定”配置窗口。窗口左侧为配置项列表，包括名称、MAC地址、IP地址类型、IP地址、子网掩码、网关和描述。右侧为配置区域，包含输入框、下拉菜单和复选框。例如，MAC地址输入框右侧有提示“*这个值和子网掩码不作为认证的条件，仅作为识别固定于MAC的标识”，格式为“AA-BB-CC-DD-EF-FF”。IP地址类型有“静态IP地址”和“动态IP地址”两个选项。IP地址、子网掩码和网关均为必填项。有效期控制部分包含“有效开始时间”和“有效结束时间”两个日期选择器，默认值为2009-9-14 18:00:10。底部有“保存”和“取消”按钮，以及一条提示：“注：右边有*号的项必须输入。”

配置项:	说明
名称	您能记住的名字。一般以主机名或使用者的名字作为名称，名称不作为认证条件。
MAC 地址	系统以这个 MAC 地址为基准，对其对应的 IP 地址进行验证。
IP 地址类型	设置组合认证条件中 IP 地址的类型，包括 DHCP 和静态 IP 两种。
IP 地址	准入认证时客户端的 IP 地址必须与组合内的 IP 地址一致才可通过认证。
子网掩码	地址掩码不作为组合认证条件，仅在系统根据 MAC-IP 组合自动更正客户端 IP 地址时，用于修改地址掩码。
网关	默认网关不作为组合认证条件，仅在系统根据 MAC-IP 组合自动更正客户端 IP 地址时，用于修改默认网关地址。

描述	关于组合规则的进一步描述。
有效期限制	设定组合规则的有效期，如果超过有效期，对网络准入，则认证不通过；对于非网络准入，则此条规则无效。
有效期起始时间	有效期起始时间。
有效期结束时间	有效期结束时间。

点击“保存”，完成 MAC-IP 绑定

也可点击“从报表添加”，从客户端报表中选择需绑定的终端进行 MAC-IP 绑定



4.13.2. 配置要点

- 1. 点击“添加组合策略”，输入“组合策略名称”为 U-I-M 组合策略
- 2. “组合不存在时”选择“不满足安全基线”，并选择“USER-IP-MAC 组合”，并点击“保存”
- 3. 点击策略名称“U-I-M 组合策略”，进入后点击“设置组合”中的“查看及编辑”
- 4. 点击“从报表添加”按钮，选择好所属服务器及 IP 组，点击“查询”
- 5. 在用户列表中找到用户“Darren@ad11”，并勾选此用户，再选

- 择目录服务为“ad11”，点击“保存选择的项目”进行保存
6. 点击用户名“Darren”，进入“用户基本信息配置”界面，并点击“组合关系”的“查看及编辑”，进入组合关系设置界面
 7. 此时这个用户已绑定一个 IP 地址，可点击“手工增加 IP 及 MAC 组合关系”，绑定此用户使用的其他 MAC 和 IP
 8. 取消“MAC 地址”的“不限”的勾选，并输入 MAC 地址为“0026186f4050”
 9. “IP 地址限制”选择“是”，“IP 地址类型”选择“静态 IP 地址”，并输入“IP 地址”192.168.0.18，“子网掩码”为255.255.255.0，默认网关为192.168.0.1，“有效期限限制”选择“否”，并点击“保存”
 10. 此时使用“Darren”用户登录，MAC 地址为“0026186f4050”的客户端的 IP 地址会被绑定为192.168.0.18，而如果用“Darren”用户登录的客户端的 MAC 地址不对，客户端会提示您“不符合安全基线要求”。

4.14. 网络设备配置

*该章节功能仅适用于高级版和增强身份认证高级版

网络设备配置是配置准入控制的交换机或者路由器设备。

在网络准入配置中将已配置好的网络设备关联到 radius 服务器中。

参考《网络准入-》Radius Server》的配置

网络设备配置页面

点击“网络设备配置”中的“添加”可添加新的交换机或者是路由器；

也可点击“网络设备配置”中的“导入”导入交换机或者是路由器的配置信息。

注：右轴为 $\log_{10}$ 的输入。

网络设备类型；LAN 即有线以太网网络设备，如：CISCO 3560；WLAN 即无线以太网网络设备，如 TP-link 无线 AP

SSID	SSID 用来区分不同的无线网络，只需在无线网络中配置此 ID 号。
动态 Vlan 支持	天珣网络准入同时支持基于用户信息、MAC 地址的动态 VLAN 切换。但不同的厂商 VLAN 格式不同，例如 Cisco 交换机的 VLAN 号是字符串形式，而 H3C（原华为）交换机的 VLAN 号是数字形式。请根据具体交换机的厂商选择。 目前版本不支持锐捷交换机的动态 VLAN
LAN 端口绑定	支持对交换机上的端口进行绑定特定的 MAC、IP、GUID 以及登录的用户名。可以手动添加绑定，也可从接入交换机(或者路由器)正在准入的客户端信息中导入。如：对交换机 0/0/3 端口唯一绑定终端 MAC :60EB69F14F53， 终端 GUID： {E0C5B2C8-A61A-4F36-84C3-2DCB9B1EA882}，登录名称为:happy,则只有当接入该端口的客户端满足这三个条件且安全状态满足时，网络才能连通 共有三个选项： “不启动端口绑定，端口使用不受限制”：则不启用端口绑定功能，下面的绑定条目编辑框处于不可编辑状态 “端口仅限绑定的终端使用，未设置绑定的端口不受限制”：绑定的端口只允许被绑定的客户端通过，其他客户端拦截；未设置绑定的端口正常使用，不受限制 “端口仅限绑定的终端使用，未设置绑定的端口禁止使用”：绑定的端口只允许被绑定的客户端

	端通过，其他客户端拦截；未设置绑定的端口 如果开启了 802.1x 认证，则对所有的客户端都 拦截
--	---

4.15. 分组信息

4.15.1. 配置介绍

4.16. 全局参数

4.16.1. 配置介绍

全局参数分为两部分：“客户端全局参数”和“服务器全局参数”。
通过这个配置来确定客户端及服务器的一些开关性质的内容和最基本的参数，此处的参数决定策略系统的运行方式和后台交互的频率，以及全局范围内的默认设置。

客户端全局参数

客户端注册参数： 修改	
是否启用客户端注册	否
对以下日期前注册的客户端，要求重新注册	1970-01-01
客户端注册重复提示周期	不重复提示
客户端注册项目	Email；地址；电话；

配置项：	说明
是否启用客户端注册	设置是否要启用客户端注册
对以下日期前注册的客户端，要求重新注册	对超过一定注册时间的客户端 设置时间要求其重新注册
客户端注册重复提示周期	定时在客户端提示进行注册，若不注册将会在这个周期时间后再一次提示注册

客户端注册项目	设置客户端注册填写的项目,包括其顺序、是否必填项目和是否作为查询条件(在信息中心-资产信息查询作为条件查询),默认项目为 email、地址、电话(这 3 项不能修改或删除)
---------	--

客户端访问控制: 修改	
默认访问控制操作类型	放行
每客户端总带宽限制 (0KB/s表示不限制)	不限制
默认的访问控制日志方式	总是记入日志
配置项:	说明
默认访问控制操作类型	共有 3 种默认操作 放行: 对没有规则匹配的数据包放行。 放行并让用户确定以后的操作: 先放行没有规则匹配的数据包,然后在客户端弹出一个对话框,让用户确定以后将如何处理相同的网络访问。 不放行并让用户确定以后的操作: 先拦截没有规则匹配的数据包,然后在客户端弹出一个对话框,让用户确定以后将如何处理相同的网络访问。
每客户端总带宽限制	客户端防火墙会对每个连入和连出的数据包进行流量统计,但会排除那些注明不计入总流量的网络访问。在一般的设置中,每客户端总带宽限制用来对非业务流量进行一个“封顶”。 可以按照带宽的绝对值 (KB/S) 或

	网卡带宽的相当值(%)来进行设置。
默认的访问控制日志方式	每一条访问控制规则都可以覆盖此处设置的日志方式，也可以使用此处设置的默认日志方式。

注意：在客户端防火墙对客户端的网络数据包进行策略匹配时，如果不能匹配任何访问控制策略，则使用此处设置的默认访问控制操作类型对数据包进行处理。这里的默认访问控制类型是全局的，IP 组或安全防护用户策略组中的默认操作类型可以覆盖这里的设置。

客户端日志参数：

[修改](#)

是否将网络行为日志发送给服务器

是

配置项：

[说明](#)

是否将网络行为日志发送给服务器

设置客户端的网络行为日志即防火墙日志是否发送给服务器，选择是的话，将会在信息中心查询到策略事件的详细信息

客户端运行参数: 修改	
客户端日志缓存文件大小	32768 KB
防火墙日志文件大小限制	100 KB
重新从Server上下载策略的时间间隔	24小时
主动探测非受控终端的在线状态 (建议终端数大于200的VLAN关闭主动探测)	否
客户端DNS设定(不生效)	无
客户端WINS设定(自动修改IP地址时使用)	无
服务中心WEB站点URL	
检测Windows弱密码	否
启用对本系统客户端注册表项的保护(64位系统无效)	否
客户端启用802.1x认证	是
启用Windows自带的802.1x认证	否
是否启用客户端与服务器之间的时钟同步	否
时钟源	无
NTP Server地址	无
禁止用户修改Windows时间	否

配置项:	说明
客户端日志缓存文件大小	客户端 audit.dat 记录了客户端的审计及告警日志信息, 文件默认为 32768 KB, 可以通过该选项修改该文件大小。
防火墙日志文件大小限制	设置客户端的防火墙日志大小; 防火墙日志默认为 100KB,可更改。如: 防火墙日志设为 100KB, 则当防火墙日志大于 100KB 时, 则自动备份, 再重新生成一个客户端防火前日志文件
重新从 Server 上下载策略的时间间隔	如果客户端一直处于运行状态, 客户端将每隔一个固定周期向服务器重新下载策略规则。默认值为 24 小时。客户端每次启动后都会自动下载策略规则。
主动探测非受控终端的在线状态	如果选择了主动探测非受控终端的在线状态的话, 终端会定时发送数据包确认

	非受控终端是否在线，默认为不启用。 但如果用户子网较大或者交换设备性能较差的情况下，可能导致交换机负载过高的问题，此时可以选择取消主动探测非受控终端的在线状态。
客户端 DNS 设定	如果设置了 MAC-IP 绑定和 User-IP 绑定策略，当客户端的 IP 地址与绑定的 IP 地址不符时，系统会自动将客户端的 IP 地址改回到绑定的 IP 地址。并将 DNS 设置为此处输入的 IP 地址。
客户端 WINS 设定	如果设置了 MAC-IP 绑定和 User-IP 绑定策略，当客户端的 IP 地址与绑定的 IP 地址不符时，系统会自动将客户端的 IP 地址改回到绑定的 IP 地址。并将 WINS 设置为此处输入的 IP 地址。
服务中心 WEB 站点 URL	客户端用户界面有一个“服务中心”按钮，当用户点击这个按钮时，会打开一个新浏览器，并自动访问此处设置的 URL。
检测 windows 弱密码	客户端会使用弱密码不断尝试登录 Windows，如果可以登录就说明该用户属于弱密码并上报弱密码。如果 windows 策略中有设置帐号锁定策略，请关闭该功能，即选择为否
启用对本系统客户端注册表项的保护	对本系统在客户端上所注册的注册表项进行保护，防止非法修改和攻击
客户端启用 802.1x 认证	让客户端上的 802.1x 选项默认开启或关

	闭，如果使用网络准入请选择开启
启用 windows 自带的 802.1x 认证	选择是否启用 windows 自带的 802.1x 认证，如果启用了，那么天珣的 802.1x 认证将会受到影响
是否启用时间策略	选择是否启用时间策略
是否启用客户端与服务 器之间的始终同步	选择让客户端是否同步服务器时间
时钟源	选择同步时间的时钟源，可选择直接与中心服务器同步或自定义时钟源
NTPserver 地址	若选择自定义时钟源的话，在此处输入时钟源的服务器地址
禁止用户修改 windows 时间	选择是否禁止用户修改 windows 时间

服务器全局参数

客户端全局参数

服务器全局参数

服务器全局参数

帮助

服务器全局策略：

修改

服务器汇总报表时间	0时0分
报表中的用户名称	未知
当非受控终端的不活动的天数超过以下值时，自动删除该终端信息	2天
当数据库所在硬盘空间少于以下值时，显示字体变为黄色	1024MB

WEB控制台登录参数：

修改

登录失败限制次数	3次
超时退出（注销）的等待空闲时间	20分钟
允许登录 WEB 控制台的 IP 登录列表	0.0.0.0 - 255.255.255.255

企业LOGO：

Web控制台Banner企业LOGO (JPEG或GIF) 标准像素860*57

浏览...

上传文件

企业LOGO (JPEG或GIF) 像素小于500*40

浏览...

上传文件

登录页LOGO (JPEG或GIF) 标准像素350*250

浏览...

上传文件

配置项:	说明
服务器同步报表时间	设定本地服务器与中心策略服务器之间同步客户端信息和部分报表的时间，默认为凌晨 0 点
报表中的用户名称	报表导出成文件时添加这个用户名称，生成企业独特的报表
当非受控终端的不活动的天数超过以下值时，自动删除该终端信息	默认 3 天
当数据库所在硬盘空间少于以下值时，显示字体变为黄色	默认 2048M
登录锁屏的失败限制次数	可手动设置用户输入错误密码时的尝试次数。如:设置为 3，则用户有三次机会尝试输入正确的密码，如果三次都输错，则禁止再次尝试，锁定登录框
登录锁屏的等待空闲时间	设置 锁定登录框后，用户可再次尝试登录的时间间隔；如：设置为 1 分钟，则锁屏一分钟后，用户可再次尝试登录
允许登录 Web 控制台的 IP 登录列表	配置可以访问天珣 Web 控制台的 IP 地址段，默认对 http://localhost:8833 和 http://127.0.0.1:8833 放行
Web 控制台 Banner 企业 LOGO(JPEG 或 GIF) 标准像素 860*57	上传后，在 Web 控制台的顶端会出现该 Logo
企业 LOGO	企业 LOGO，上传后，在导出报表时会将此 LOGO 打上水印
登录页 LOGO	在管理平台登录界面显示的 LOG

5. 安全基线

5.1. 关于安全基线

- 安全基线是每一台受控终端必须满足的最基本的安全规范。

只有满足安全基线的终端才能正常接入网络，才会被认为是

网络内的合格终端，否则，客户端将会给出提示要求修复。

订制安全基线是通过以下几个策略来实现的：补丁策略，进程策略，软件安装策略，windows 服务管理，防病毒软件策略，windows 组策略，屏幕保护策略，共享资源管理，用户环境策略。

- **“补丁强制策略”**：强制要求客户端必须打指定补丁，确保客户端的操作系统的漏洞及时修复。比如打一个比较大的 ServicePack 或单个的补丁。
- **“进程管理策略”**：对客户端运行的软件和进程进行限制。包括红名单，黑名单和白名单。红名单是必须运行的进程列表，黑名单是不能运行的进程列表，白名单是允许运行的进程列表。
- **“软件安装策略”**：软件安装管理可以制定软件安装的红、黑、白名单，确定用户客户端必须安装的软件，禁止非法安装未经许可的应用软件，规定只能安装的软件清单。红名单是必须安装的软件，黑名单是不能安装的软件，白名单是允许安装的软件列表。
- **“Windows 服务管理”** window 服务管理可以禁用或启用客户端运行的服务。禁止不需要的服务，强制启动需要的服务。
- **“防病毒软件策略”**：通过检查客户端安装的杀毒软件的病毒码，对其所安装的防病毒软件的病毒库更新进行监控。目前支持的防病毒软件品牌包括 Symantec，趋势，瑞星，McAfee，微软等。
- **“Windows 账户策略”**：账户策略可以修改 windows 管理员账号、强制禁用 guest 帐号、启用和加强密码复杂度，回收管理员权限等等来保护系统账户安全。
- **“Windows 本地策略”**：通过修改注册表和组策略的方式，强制使不安全的客户端满足加固策略要求。例：开启 IP 协议策略可防止 SYN 攻击。
- **“注册表策略”**：通过检测和保护注册表的方式，保护系

统的注册表不被擅改。

- **“共享资源策略”**：可以检测并上报用户电脑上有哪些共享资源（目录、打印机、IPC），并可设定是否允许开设共享资源（目录、打印机、IPC），如果不允许，可强制取消已经设置了共享资源。
- **“Windows 事件日志管理”**：设置 windows 应用程序、安全和系统的事件日志大小，可查看较长一段时间的日志。
- **“用户环境策略”**：配置安全可靠的用户环境，是否加入域，禁止修改网卡、设置屏幕保护等均可提高计算机使用安全系数。

5.2. 补丁强制策略

5.2.1. 配置介绍

配置补丁强制策略的目的是检查客户端上所打补丁的情况，使每台客户端上安装的系统补丁都相同，如果有某些补丁未安装的话将会给予适当的提示要求其安装补丁。

ServicePack

Service Pack 是操作系统一个比较大的更新，同时也包含了上一个 Service Pack 到这一个 Service Pack 之间的所有的 Hot Fix。通过设置强制补丁，能确保终端操作系统的重要补丁都正常安装。因为 Service Pack 文件很大，而且一般也不需要紧急安装，所以系统不自动下载 Service Pack，需要您手工配置。

点击**“添加”**进入 ServicePack 设置界面

Service PackHotfix

SP 补丁

策略名称

*

策略描述

选择操作系统

Windows 2000 (32位)

ServicePack主编号

没有ServicePack

ServicePack副编号

没有副编号

简体中文下载网址

繁体中文下载网址

英文版下载网址

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30		

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存取消

配置项：	说明
Servicepack 名称	填入补丁的名称，如“Windows XP2”。
选择操作系统	根据不同的补丁，选择相应的操作系统。如选择“WINDOWS XP”。
ServicePack 主编号	根据不同的补丁，选择主编号，如“ServicePack2”。
ServicePack 副编号	选择相应的副编号，若没有，则不用选择。
简体中文下载网址	输入该补丁的简体中文版的下载地址。 输入相对地址“XP/ Windows-XP-serviceXP.exe”，系统将自动在相对地址前补充 http://服务

	器地址:8833/download/。
繁体中文下载网址	配置同“简体中文下载网址”。
英文版下载网址	配置同“简体中文下载网址”。
在线模式	选择在线和离线时此策略是否生效
生效时间	可以根据管理员的需求,灵活配置策略生效的时间范围。
策略应用对象	目前策略应用对象有四种:基于主机名, IP 组, 用户组, 和工作组。
创建状态	全局管理员创建的规则,创建状态为全局。本地管理员创建的规则,创建状态为本地。
创建者	此处为创建者的名称。

Hotfix:

当你对下载后的补丁发布后,就会在此看到相应的系统补丁,并
可对指定的补丁应用到相应的策略组,接收到此规则的终端将强制要求安装这些系统补丁。

下载补丁操作请参照“补丁管理”



1.1.1. 配置要点

1. 点击“ServicePack”标签，并点击“添加”按钮
2. 输入“ServicePack 名称”为 XP SP3
3. “选择操作系统”为 windows XP
4. “ServicePack 主编号”选择 SP3，“ServicePack 副编号”不选
5. “简体中文下载网址”输入 AutoUpdate/XP/winXP-SP3.exe
6. “在线模式”选择为在线时生效
7. 点击“策略应用对象”的“查看及编辑”按钮，选择 IP 组类型及终端，点击“确定”
8. 点击“保存”进行策略保存
9. 点击“hotfix”标签，补丁名栏输入 KB837001 并添加
10. 点击“策略应用对象”的“查看及编辑”按钮，选择 IP 组类型及终端，点击“确定”
11. 客户端必须安装 XP SP3，且必须安装 KB837001 这个补丁。

5.3. 进程运行策略

5.3.1. 配置介绍

此处配置可限制客户端运行的进程，比如哪些进程必须运行（红名单），哪些进程禁止运行（黑名单），以及终端只能运行的进程清单（白名单）。

红名单

点击“红名单”标签中的“添加”按钮



配置项:	说明
进程名称	填写强制运行软件的进程名，如瑞星防病毒软件的 Ravmond. exe 或 Ravmon. exe。
下载地址	该软件的地址链接，当终端没有安装此软件时，可通过此链接下载安装。此地址为相对地址，如果下载的全路径为 http://服务器地址:8833/download/software/abc.exe ，则只需填写 software/abc.exe。前面的

	部分将由系统自动补充。请参考“ 管理网段 ”的“ 下载服务器地址 ”中的说明。可以支持完整的 url，例如将用户现有的杀毒软件 url 输入即可。
MD5 校验码	为防止恶意用户更改程序名逃避红名单检查，可在此处填写 MD5 校验码，MD5 码产生工具在本系统的安装包中。
进程延迟检测时间	设置检测红名单进程的延迟时间
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

黑名单

点击“黑名单”标签中的“添加”按钮

红名单

黑名单

白名单

策略名称

*

策略描述

进程列表

本策略禁止终端运行以下列表中的进程。

进程名称

编辑

添加

源文件列表

本策略禁止终端运行源文件名与以下列表中的值匹配的进程

源文件名

编辑

添加

MDS码列表

本策略禁止终端运行MDS码与以下列表中的值匹配的进程

MDS码

编辑

从样本计算

添加

动作

提示

生效时间

☒ 所有时间

☐ 工作时间

☐ 非工作时间

☐ 以下时间段

开始时间

结束时间

编辑

删除

2012-03-10 9:00

2012-03-10 13:30

添加

在线模式

☒ 在线时生效

☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

配置项:	说明
进程名称	在此添加程序的进程名，如“qq.exe”；或者其调用的 DLL 文件，如“QQBaseClassInDll.dll”。进程调用的 DLL 可从其安装目录查看，或使用专用工具查看。
源文件名	添加程序的源文件名，可在程序的属性，里面的详细信息看到，或使用专业的工具查看。
动作	在黑名单进程运行时，可选择主动的“结束进程”，或“提示”用户，由用户自行去关闭该进程。只有关闭了此进程才满足安全策略。

MD5 校验码	为防止恶意用户更改程序名逃避黑名单检查，可在此处填写 MD5 校验码，MD5 码产生工具在本系统的安装包中。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

白名单

点击“白名单”标签的“添加”按钮



该截图展示了“白名单”配置界面。左侧为配置项列表，包括：名称、描述、操作系统版本、进程列表、非白名单进程动作、生效时间、在线模式、策略应用对象、策略类型、策略范围。右侧为配置详情，包括：名称输入框、描述输入框、操作系统版本下拉菜单（当前选中 Windows 2000 (32位)）、进程列表表格（包含进程名称、进程ID、进程类型、PID等列）、非白名单进程动作选择（提示、结束进程）、生效时间选择（开始时间、结束时间、生效时间、失效时间）、在线模式选择（在线时生效、离线时生效）、策略应用对象选择（按主机名、按IP地址、按用户组、按工作组）、策略类型选择（白名单）、策略范围选择（所有）、以及“添加”、“删除”、“取消”按钮。

配置项:	说明
进程名称	填写此列表的名称。如“qq.exe”。
操作系统版本	选择相应的系统版本，“如 WINDOWS XP”。
非白名单进程动作	对于不在此列表内的进程的默认操作。选择“提示”时，需要手工结束进程。选择“结束进程”时，系统将自动终止非白单进程的运行。 注意：请谨慎使用“结束进程”选项，以免系统将一些不在白名单上的重要的操作系统进程终止，导致 Windows 不能正常工作。
MD5 校验码	为防止恶意用户更改程序名逃避黑名单检查，可在此处填写 MD5 校验码，MD5 码产生

	工具在本系统的安装包中。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

“保存”后，点击创建好的白名单策略名称，点击“从终端取样添加”

终端IP地址: 10.201.222.44 从终端取样添加

终端取样查询结果

保存选择的项目 保存所有的项目 关闭

☐ 进程名称

☐ smss.exe

☐ csrss.exe

☐ winlogon.exe

☐ services.exe

☐ lsass.exe

☐ vmacthlp.exe

☐ svchost.exe

☐ svchost.exe

☐ svchost.exe

☐ svchost.exe

☐ svchost.exe

☐ explorer.exe

☐ spoolsv.exe

☐ VMwareTray.exe

☐ VMwareUser.exe

☐ ctfdmon.exe

☐ vmttoolsd.exe

这时将会到所输 IP 的系统中将正在运行的进程以列表形式展现出来，选择相应的进程，点击“保存选择的项目”，这个进程就被加入到白名单列表中。

注意：白名单策略已经在进程内部将 windows 的系统进程（c:\windows 目录下的文件）以及天珣自身的文件和进程排除掉，因此在添加白名单进程时可忽略这些进程。

5.4. 软件安装策略

5.4.1. 配置介绍

软件安装管理可以制定软件安装的红、黑、白名单，确定用户客户端必须安装的软件，禁止非法安装未经许可的应用软件，规定只能安装的软件清单。

软件红名单（必须安装的软件）

点击“软件红名单”标签中的“添加”按钮



软件红名单配置界面截图。界面顶部有四个标签：红名单、黑名单、白名单、文件规范。当前选中“红名单”。

配置项包括：

- 策略名称：输入框，带星号。
- 策略描述：文本框。
- 软件列表：上方有提示“本策略要求终端必须安装以下软件中的至少一个软件。”。下方是一个表格，包含“软件名称”、“下载地址”、“匹配方式”、“编辑”、“删除”列。当前匹配方式为“模糊匹配”，右侧有“添加”按钮。
- 生效时间：包含“所有时间”、“工作时间”、“非工作时间”、“以下时间段”四个单选按钮。下方是“开始时间”和“结束时间”的输入框，当前分别显示为“2012-03-10 9:00”和“2012-03-10 13:30”，右侧有“添加”按钮。
- 在线模式：包含“在线时生效”和“离线时生效”两个复选框，当前均被选中。
- 策略应用对象：显示为“（还没有应用到任何对象）”，右侧有“查看及编辑”链接。
- 创建类型：显示为“全局”。
- 创建者：显示为“jing”。

底部有“注：右边有*号的项目必须输入。”提示，以及“保存”和“取消”按钮。

配置项：	说明
策略名称	填写此软件安装策略的名称，如“必须安装防病毒软件”

软件名称	填写必须安装的软件名称，如“瑞星” (支持模糊匹配，在控制面板中的增加删除程序中查找匹配名称)
匹配方式	配置上面所填的软件名称是精确匹配还是模糊匹配（在控制面板中的增加删除程序中查找匹配名称）
下载地址	该软件的地址链接，当终端没有安装此软件时，可通过此链接下载安装。此地址为相对地址，如果下载的全路径为 http://服务器地址:8833/download/software/abc.exe ，则只需填写 software/abc.exe。前面的部分将由系统自动补充。请参考“ 管理网段 ”的“ 下载服务器地址 ”中的说明。可以支持完整的 url，例如将用户现有的杀毒软件 url 输入即可。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

软件黑名单（禁止安装的软件）

点击“软件黑名单”标签中的“添加”按钮

红名单

黑名单

白名单

文件规范

软件黑名单

策略名称

*

策略描述

软件列表

本策略禁止终端安装以下列表中的软件。

软件名称	卸载参数	匹配方式	编辑	删除
		模糊匹配		添加

动作

提示

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30		添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

软件白名单（只能安装的软件清单）

点击“软件白名单”标签中的“添加”按钮

红名单黑名单白名单文件规范

软件白名单

策略名称

*

策略描述

操作系统版本

Windows 2000 (32位)

软件列表

终端IP地址:

从终端取样添加

软件名称

卸载参数

匹配方式

编辑

删除

模糊匹配

添加

非白名单软件动作

提示

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

结束时间

编辑

删除

2012-03-10 9:00

2012-03-10 13:30

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注: 右边有*号的项目必须输入。

保存

取消

配置项:	说明
策略名称	填写此软件安装策略的名称，如“部门只能安装的软件清单”
软件名称	填写白名单名称（支持模糊匹配，在控制面板中的增加删除程序中查找匹配名称）
卸载参数	
匹配方式	配置上面所填的名称是精确匹配还是模糊匹配（在控制面板中的增加删除程序中查找匹配名称）
操作系统版本	配置此白名单软件所适用的操作系统
非白名单软件动作	配置对非白名单软件，客户端所采取的

	动作（提示、仅记录、拦截和卸载）
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

在“终端 IP 地址”栏中输入需要取样的终端 IP 地址，然后点“从终端取样添加”，这时将会到所输 IP 的系统中将已安装的软件以列表形式展现出来，选择相应的软件，点击“保存选择的项目”，这个进程就被加入到软件安装白名单列表中。

终端IP地址: 10.201.222.44 从终端取样添加

终端取样查询结果

保存选择的项目 保存所有的项目 关闭

☐ 软件名称

☐ VMware Tools

☐ WebFldrs XP

☐ WinPcap 4.1.1

☐ WinRAR 压缩文件管理器

☐ Wireshark 1.3.3

☐ 傲游浏览器 3

☐ 天珣内网安全风险管理与审计系统客户端

1

文件规范

点击“文件规范”标签中的“添加”按钮

红名单 黑名单 白名单 文件规范

文件规范

策略名称

策略描述

文件列表

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边有+号的项目必须输入。

保存 取消

配置项:	说明
策略名称	填写此软件安装策略的名称，如“部门只能安装的软件清单”
文件路径	填写文件存放的路径，例如 C:\windows
文件名称	填写文件的名称
文件版本	填写文件的版本
递归搜索	配置递归搜索（启用或不启用）
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

5.5. Windows 服务管理

5.5.1. 配置介绍

Windows 服务管理能够对用户客户端的服务进行启用、禁用管理；

对于已经启用的服务可以通过策略使其禁用，对于已经禁用的服务也可以配置相应的策略使其启用。需要注意一点，具有依存关系的两个服务或者是多个服务，若要禁用或启用其中的一个时，必须同时配置其他服务的禁用和启用，策略才能生效。

Windows 服务策略

点击 “Windows 服务管理” 页面中的 “添加” 按钮

Windows服务

SNMP服务

Windows 服务管理

策略名称

*

策略描述

服务列表

服务名称	动作	编辑	删除
	禁用		

添加

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30		

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

配置项:	说明
策略名称	填写此 Windows 服务管理策略的名称，如“管理服务”
策略描述	对该策略进行描述，便于理解
服务名称	填写服务名称
动作	选择需要启用或是禁用服务
生效时间	设置策略生效的时间
在线模式	配置策略在线或离线生效

策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。
--------	----------------------------------

SNMP 服务

点击 “SNMP 服务管理” 页面中的 “添加” 按钮

Windows服务

SNMP服务

SNMP 服务管理

策略名称

*

策略描述

动作

☒ 不配置 ☐ 禁用 ☐ 启用

设置默认Community String

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

2012-03-10 9:00

结束时间

2012-03-10 13:30

编辑

删除

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

配置项:	说明
策略名称	填写此 SNMP 服务管理策略的名称,如“管理服务”
策略描述	对该策略进行描述，便于理解
设置默认 Community String	填写 public 或 private
动作	选择需要启用或是禁用服务
生效时间	设置策略生效的时间
在线模式	配置策略在线或离线生效
策略应用对象	目前策略应用对象有四种：基于主机名，

	IP 组，用户组，和工作组。
--	----------------

5.6. 防病毒软件策略

5.6.1. 配置介绍

防病毒软件策略可以控制流行的防病毒软件的程序版本和病毒码版本。目前系统已经支持 Symantec、趋势防病毒(OfficeScan, ServerProtect)、McAfee、瑞星防病毒、微软防病毒等的版本控制。

如果要强制终端防病毒软件的病毒库版本更新到最新版本时，需在此设定病毒库的强制更新策略。如果要对防病毒软件的程序版本进行管理，请使用进程管理。

点击“添加”按钮配置防病毒软件策略

防病毒软件策略

策略名称

策略描述

防病毒软件类型

防病毒软件进程

进程延迟检测时间

是否检查病毒码版本

要求的病毒码版本

病毒码延迟更新的最长天数

病毒码升级网址

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边有*号的项必须输入。

保存

取消

请选择防病毒软件类型

同一进程可以指定多个PID码，用分号隔开

进程名称PID码编辑删除

从样本计算

添加

分钟

☒ 否 ☐ 是

选择病毒码版本

0为不限制，只有当病毒码版本满足时才会起作用

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间结束时间编辑删除

2012-03-10 0:002012-03-10 13:30添加

☒ 在线时生效 ☐ 离线时生效

还没有应用到任何对象 查看及编辑

全局

ling

配置项：

说明

防病毒软件名称	输入名称如“瑞星防病毒”
防病毒软件类型	选择相应的防病毒厂商，如“瑞星防病毒”。
MD5 校验码	为防止恶意用户更改程序名逃避黑名单检查，可在此处填写 MD5 校验码，MD5 码产生工具在本系统的安装包中。
是否检查病毒码版本	默认为“是”；当不检查时，可选择“否”。
要求的病毒码版本	按照后面的提示，依照正确的格式输入最新的病毒码版本，如“20.49.12”。
病毒码延迟更新的最长天数	最后一次更新病毒码距离今天的天数，如果超过了这个设定值，则被认为安全基线不合格。
病毒码升级网址	对于提供可下载更新包的防病毒软件，可通过此链接下载更新。此地址可填相对地址和绝对地址，如果下载的全路径为 http://服务器地址:8833/download/software/abc.exe ，则可只填写 software/abc.exe，前面的部分将由系统自动补充。请参考“管理网段”的“下载服务器地址”中的说明。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

注意：病毒码延迟更新的最长天数必须在客户端病毒码符合要求的病毒码版本的基础上才能生效。

点击“**选择病毒码版本**”，如果不想每次手工更新病毒码版本，

帐户策略

策略名称

策略描述

Guest 账号

Windows 管理员账号

Windows 管理员缺省账号

帐户锁定

用户权限分配

禁用和删除无用账户

策略执行周期

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边带*号的项必须输入。

保存

取消

策略名称

策略描述

Guest 账号

Windows 管理员账号

Windows 管理员缺省账号

帐户锁定

用户权限分配

禁用和删除无用账户

策略执行周期

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边带*号的项必须输入。

保存

取消

策略名称

策略描述

Guest 账号

Windows 管理员账号

Windows 管理员缺省账号

帐户锁定

用户权限分配

禁用和删除无用账户

策略执行周期

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边带*号的项必须输入。

保存

取消

配置项:	说明
策略名称	输入加固策略的名称，如“加固策略-财务部”。
Guest 账号	可以选择启用或禁用 guest（来宾）账号，注：取消“禁用”后，需配置“启用”才会启用 guest 账号。
Windows 管理员账号	可启用或禁用内置管理员或属于管理员组的账号
Windows 缺省管理员账号	修改管理员缺省帐号名称，默认缺省值为 Administrator。

账户锁定	发生无效登录后锁定使用的登录账户
用户权限分离	为 windows 用户组添加成员或删除某些不在用户组的成员
禁用和删除无用账户	可以删除或者禁用非 windows 内置账户， 注： 可能会删除当前登录的用户，导致下次登录无法进入系统，请安全使用。
策略执行周期	设置执行本条策略的周期时间。 注： 只能是 5 或者 5 的倍数。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

密码策略

密码策略可以对 windows 密码长度，复杂度和使用时间进行配置更改，以达到保护系统的效果。

点击“密码策略”中的“添加”

帐户策略 密码策略 管理员权限回收

密码策略

策略名称

策略备注

密码必须符合复杂性要求 ☒ 不配置 ☐ 禁用 ☐ 启用

密码长度最小值

字符*

密码最长使用期限

天*

密码最短使用期限

天*

强制密码历史 ☒ 不配置 ☐ 取消强制密码历史 ☐ 保留密码历史

个记住的密码

策略执行周期

秒

生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

结束时间

编辑

删除

在线模式 ☒ 在线时生效 ☐ 离线时生效

策略应用对象

还没有应用到任何对象

[查看应用组](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

配置项:	说明
策略名称	输入策略名称。
密码必须符合复杂性要求	本地策略中启用或禁用密码复杂度
密码长度最小值	可以将值设置为介于 1 和 14 个字符之间，或者将字符数设置为 0 以确定不需要密码。
密码最长使用期限	可以将密码设置为在某些天数(介于 1 到 999 之间)后到期，或者将天数设置为 0，指定密码永不过期。安全最佳操作是将密码设置为 30 到 90 天后过期，密码最长使用期限不超过 999 天。
密码最短使用期限	密码最短使用期限必须小于密码最长使用期限，除非将密码最长使用期限设置为 0，指明密码永不过期。如果将密码最长使用期限设置为 0，则可以将密码

	最短使用期限设置为介于 0 和 998 之间的任何值。
强制密码历史	此安全设置确定再次使用某个旧密码之前必须与某个用户帐户关联的唯一新密码数。该值必须介于 0 个和 24 个密码之间。
策略执行周期	默认为 3600 秒，且无法修改
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

管理员权限回收

对注册表的某些项进行保护，以此来防止某些非法程序对注册表进行非法的修改。

点击“管理员权限回收”标签中的“添加”按钮

帐户策略

密码策略

管理员权限回收

管理员权限回收

策略名称 *
策略描述
注：配置有安全基线密码策略时，帐号权限回收策略无效
管理员帐号 *
密码 [显示明文](#)
生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效
策略应用对象 (还没有应用到任何对象) [查看及编辑](#)
创建类型 全局
创建者 jing
注：右边有*号的项目必须输入。
[保存](#) [取消](#)

配置项:	说明
策略名称	输入注册表保护策略的名称。
描述	该策略的详细说明
管理员账号	设置 windows 新的管理员账号，并把 administrator 账号禁用和生成一个 cebuser 普通用户账户。
密码	设置 windows 新的管理员账号密码
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

5.8. Windows 本地策略

5.8.1. 配置介绍

审核策略

点击“审核策略”中的“添加”

审核策略

用户权限分配

安全选项

IP协议安全

数据执行保护

策略名称

策略描述

审核所选项目操作

策略执行周期

生效时间

在线模式

策略应用对象

创建类型

创建者

☒不配置

☐审核策略更改

☒不配置

☐审核登录事件

☒不配置

☐审核对象访问

☒不配置

☐审核过程（进程）追踪

☒不配置

☐审核目录服务访问

☒不配置

☐审核特权使用

☒不配置

☐审核系统事件

☒不配置

☐审核帐户登录事件

☒不配置

☐审核帐户管理

☐成功

☐失败

☐成功

☐失败

☐成功

☐失败

☐成功

☐失败

☐成功

☐失败

☐成功

☐失败

☐成功

☐失败

☐成功

☐失败

☐成功

☐失败

3600秒

☒所有时间

☐工作时间

☐非工作时间

☐以下时间段

开始时间

2012-03-10 9:00

结束时间

2012-03-10 13:30

编辑

删除

添加

☒在线时生效

☒离线时生效

(还没有应用到任何对象)

[查看及编辑](#)

全局

jing

注：右边有*号的项目必须输入。

保存

取消

用户权限分配

点击“用户权限分配”中的“添加”

审核策略

用户权限分配

安全选项

IP协议安全

数据执行保护

用户权限分配

策略名称

*

策略描述

用户权限分配

☒ 不配置

☐ 允许下表中的用户或用户组

☐ 远程关机

☐ 本地关机

☐ 取得文件或其他对象的所有权

名称	用户或用户组	编辑	删除
	☒ 用户组 ☐ 用户		
		添加	

策略执行周期

3600

秒

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30		
		添加	

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

配置项：	说明
策略名称	输入策略的名称。
描述	该策略的详细说明
用户权限分配	名称一项中填写的用户/用户组，将赋予远程关机、本机关机和取得文件或其他对象的所有权的权限。
策略执行周期	默认为 3600 秒并不能修改
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

安全选项

设置针对操作系统所采取的一些加强系统安全性能的策略，例如隐藏登录名，禁止自动播放策略等。

审核策略用户权限分配安全选项IP协议安全数据执行保护

安全选项

策略名称*

策略描述

隐藏上次登录用户名不配置禁用启用

关机时清理虚拟内存页面文件不配置禁用启用

本地帐户的共享和安全模式不配置经典仅来宾

自动播放不配置禁用启用

安全模式不配置禁用启用

策略执行周期3600秒

生效时间所有时间工作时间非工作时间以下时间段

开始时间结束时间编辑删除

2012-03-10 9:002012-03-10 13:30添加

在线模式在线时生效离线时生效

策略应用对象还没有应用到任何对象查看及编辑

创建类型全局

创建者jing

注：右边有*号的项目必须输入。

保存取消

配置项:	说明
策略名称	输入加固策略的名称，如“加固策略-财务部”。
说明	该规则的详细说明
隐藏上次登录用户名	在 windows9x 以上的操作系统中对以前的用户名具有记忆功能，下次重启时，在登录框中会发现上次登录的用户名。为了避免这些信息被非法用户利用，有必要将他隐藏起来。
关机时清理虚拟内存页面文件	解决系统空间不足，电脑关机时清空虚拟内存页面文件将会对系统空间进行优化
本地帐户的共享和安全模式	所谓的经典即访问共享需要输入用户名和密码等，所谓的仅来宾即网络访问的权限仅为 everyone 权限。与 Windows 组策略中“网络访

	问：本地帐户的共享和安全模式”统一。
自动播放	即禁用光盘、USB 设备等的自动播放功能。 注： 取消“禁用”后，需配置“启用”才会启用自动播放功能
安全模式	即系统启动时无法选择下拉列表框。对于双引导系统的电脑有影响，而且无法进入安全模式进行问题恢复。说明：禁止进入安全模式有一定的风险，启用这个选项要谨慎(Vista 和 Win 2008, Win 7 无效)。 注： 取消“禁用”后，需配置“启用”才能进入安全模式。
策略执行周期	默认为 3600 秒并不能修改
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

IP 协议安全

通过加固 TCP/IP 协议栈防范，尽可能的减轻 SYN 攻击的危害

审核策略	用户权限分配	安全选项	IP协议安全	数据执行保护
IP 协议安全				
策略名称		*		
策略描述				
是否启用 SYN 攻击防护		☐ 是 ☒ 否		
设置触发 SYN 洪水攻击保护所必须超过的 TCP 连接请求阈值		(推荐值: 5)		
设置处于 SYN_RCVD 状态的 TCP 连接数的阈值		(推荐值: 500)		
设置处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值		(推荐值: 400)		
策略执行周期		秒		
生效时间		☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段		
		开始时间 2012-03-10 9:00	结束时间 2012-03-10 13:30	编辑 删除 添加
在线模式		☒ 在线时生效 ☒ 离线时生效		
策略应用对象		(还没有应用到任何对象) 查看及编辑		
创建类型		全局		
创建者		jing		
注: 右边有*号的项目必须输入。 保存 取消				

配置项:	说明
策略名称	输入策略的名称。
描述	该策略的详细说明
是否启用 SYN 攻击防护	可选择开启或不启用 SYN
设置触发 SYN 洪水攻击保护所必须超过的 TCP 连接请求阈值	TcpMaxPortsExhausted 是指系统拒绝的 SYN 请求包的数量, 默认是 5。
设置处于 SYN_RCVD 状态的 TCP 连接数的阈值	TcpMaxHalfOpen 表示能同时处理的最大半连接数, 如果超过此值, 系统认为正处于 SYN 攻击中。默认值为 500
设置处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值	TcpMaxHalfOpenRetried 定义了保存在 backlog 队列且重传过的半连接数, 如果超过此值, 系统自动启动

	SynAttackProtect 机制。默认值为 400
策略执行周期	设置执行本条策略的周期时间。 注 ：只能是 5 或者 5 的倍数。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

数据执行保护

DEP (Data Execution Prevention) 即“数据执行保护”，这是 Windows 的一项安全机制，主要用来防止病毒和其他安全威胁对系统造成破坏。

审核策略

用户权限分配

安全选项

IP协议安全

数据执行保护

数据执行保护

策略名称 *

策略描述

设置Windows的DEP (数据执行保护)功能
☒ 不配置
☐ 仅为基本Windows程序和服务启用DEP
☐ 为所有程序和服务启用DEP

注：必须重启系统生效。

策略执行周期 秒

生效时间
☒ 所有时间
☐ 工作时间
☐ 非工作时间
☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式
☒ 在线时生效
☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

配置项：	说明
策略名称	输入策略的名称。
描述	该策略的详细说明

设置 Windows 的 DEP(数据执行保护)功能	为 windows 程序和服务启用 DEP
策略执行周期	设置执行本条策略的周期时间。 注 ：只能是 5 或者 5 的倍数。
生效时间	设置策略生效的时间
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

5.9. 注册表策略

5.9.1. 配置介绍

对注册表的某些项进行检测和保护，以此来防止某些非法程序对注册表进行非法的修改。

点击“注册表策略”标签的“添加”

注册表策略

策略名称

策略描述

注册表检测

注册表保护

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边有*号的返回必须输入。

保存

取消

注册表项

键值名称

键值数据

数据类型

编辑

删除

注：当数据类型为REG_DWORD时，数据必须为十进制整数。

注：当数据类型为REG_DWORD时，数据必须为十进制整数。

所有时间

工作时间

非工作时间

以时间段

开始时间

结束时间

编辑

删除

2012-03-10 00:00

2012-03-10 15:30

添加

在线模式

实时生效

离线时生效

策略应用对象

创建类型

创建者

注：右边有*号的返回必须输入。

保存

取消

配置项:	说明
策略名称	输入策略名称
策略说明:	规则更详细的描述或说明
注册表项	填入需要保护或检测的注册表项，如 “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Run”
键值名称	填入该注册表项下的键值名称，如 “RavTask”，则保护该值不被修改； 若不填写则保护整个 run 项，该项下 禁止删除、更改、创建任意注册表键 值。
键值数据	填入该键准确的数据值
数据类型	根据实际填写的键值的类型选择， REG_SZ 为字符串类型，REG_DWORD 为 整型数字，REG_MULTI_SZ 为多字符串 类型。

启明星辰
http://www.venustech.com.cn

98

策略名称	输入策略名称
策略说明:	规则更详细的描述或说明
共享目录选项	配置允许共享、不允许设立共享（已经共享的目录会被取消），选择允许设立共享目录，在共享录名可填写路径如：C:\windows\share，授权用户可填写用户名如：Administrator，共享权限可组合选择“读取、更改和完全选择三项”
共享打印机选项	配置允许共享打印机、不允许共享打印机
共享 IPC\$	配置允许共享 IPC\$、不允许共享 IPC\$，选择不允许共享 IPC\$后，再选择允许共享 IPC\$时终端需要重启后才能恢复 IPC 共享
策略执行周期	设置执行本条策略的周期时间。 注： 只能是 5 或者 5 的倍数。
生效时间	设置策略生效的时间
在线模式	配置此策略在线和离线是否生效。此处默认在线离线都生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

5.11. Windows 事件日志管理策略

5.11.1 配置介绍

可以通过配置 Windows 事件日志管理策略，管理 windows 应用

程序、安全、系统日志文件大小，可对系统的各项操作有更全面、更长久的详细了解

点击“Windows 事件日志管理”的“添加”

Windows事件日志管理

策略名称

策略描述

Windows事件日志最大日志文件大小

☐ 应用程序

KB

☐ 安全

KB

☐ 系统

KB

当Windows事件日志达到最大的日志大小时

☒ 按需要覆盖事件（旧事件优先）

☐ 当操作系统版本为Vista及以上版本时，日志满时将其存档，不覆盖事件；当操作系统为XP或2003时，存档或改写

改写久于

天的事件

☐ 不覆盖事件（手动清除日志）

策略执行周期

5

秒

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

2012-03-10 9:00

结束时间

2012-03-10 13:30

编辑

删除

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

（还没有应用到任何对象）[查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

配置项：	说明
策略名称	输入策略名称
策略描述：	规则更详细的描述或说明
Windows 事件日志最大日志文件大小	设置应用程序、安全、系统的日志文件大小，最小值为 1024
当 Windows 事件日志达到最大的日志大小时	当 Windows 事件日志达到最大的日志大小时，可选择自动覆盖旧事件或手动清除旧日志文件
策略执行周期	设置执行本条策略的周期时间。 注： 只能是 5 或者 5 的倍数。

	域进行检查。
是否排除 XP HOME 版及 win7 home 版本	选择“是”对 XP HOME 版及 win7 home 版本的操作系统不做检查。
生效时间	设置策略生效的时间段
在线模式	配置此策略在在线和离线时是否生效
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

屏幕保护策略

可以通过定制屏幕保护策略，使接收到策略的终端的自动启用屏幕保护。

点击“屏幕保护策略”标签的“添加”

AD域策略	屏幕保护策略	IE配置	远程桌面管理	禁止修改网卡								
策略名称 * 策略描述 ☒ 不配置（不改变终端现有的屏保设置） ☐ 强制启用屏保（没有设置则选择默认屏保） ☐ 启用屏保的等待时间必须小于 分钟 ☐ 屏保恢复时显示登录界面 ☐ 取消屏保（自动禁用终端屏保） ☐ 禁止使用欢迎界面 注：*仅限于XP或VISTA或Window7系统的客户端 ☐ 禁止使用快速切换用户 注：*仅限于XP或VISTA或Window7系统的客户端 策略执行周期 5 秒 生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段 <table border="1"> <thead> <tr> <th>开始时间</th> <th>结束时间</th> <th>编辑</th> <th>删除</th> </tr> </thead> <tbody> <tr> <td>2012-03-10 9:00</td> <td>2012-03-10 13:30</td> <td>添加</td> <td></td> </tr> </tbody> </table> 在线模式 ☒ 在线时生效 ☒ 离线时生效 策略应用对象 (还没有应用到任何对象) 查看及编辑 创建类型 全局 创建者 jing 注：右边有*号的项目必须输入。 保存 取消					开始时间	结束时间	编辑	删除	2012-03-10 9:00	2012-03-10 13:30	添加	
开始时间	结束时间	编辑	删除									
2012-03-10 9:00	2012-03-10 13:30	添加										
配置项：		说明										

策略名称	输入策略名称
策略说明:	规则更详细的描述或说明
不配置	不改变终端现有的屏幕保护设置
强制启用屏保	如果选中这个选项, 如果客户端原先没有启用屏幕保护, 系统将自动启用一个名为“空白”的屏幕保护程序。 如果选中这个选项, 如果客户端原先已经启用了屏保, 系统将使用该屏保 如果不选中这个选项, 则保留客户端原来的配置。
启用屏保的等待时间必须小于…分钟	如果选中这个选项, 客户端原来的屏保时间大于这个时间时, 系统将自动把客户端的设置改为这里输入的时间; 如果客户端原来的时间小于这个时间时, 系统则保持该时间不变。 如果不选中这个选项, 则保留客户端原来的配置。
取消 屏保	选中这个选项, 如果终端原先没有启动屏保, 则保持原状; 如果中断原先启用了屏保, 系统将自动禁用该屏保。
屏保恢复时显示登陆界面	如果选中这个选项, 系统将自动更改客户端设置使之与管理员设置一致。 如果不选中这个选项, 则保留客户端原来的配置。
禁止使用欢迎界面	如果选中这个选项, Windows 将不显

	示欢迎页让用户点击用户登录，而是要输入用户名进行登录。 如果不选中这个选项，则保留客户端原来的配置。
禁止使用快速切换用户	如果选中这个选项，Windows 将不会出现切换用户界面。 如果不选中这个选项，则保留客户端原来的配置。
Windows 当前登录密码不能为空	如果选中这个选项，当客户端 Windows 当前登录用户密码为空，将提示安全状态不合格。 如果不选中这个选项，则不检查登录用户的密码是否为空。
策略执行周期	设置执行本条策略的周期时间。注：只能是 5 或者 5 的倍数。
生效时间	设置策略生效的时间
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

IE 配置

大多安全隔离要求较高的网络会使用 WEB 代理上网。在这种模式下，需要统一设置很多配置。**IE 策略**可以为所有终端统一添加例外排除的配置信息，大大减轻了管理员的管理工作。

点击“**IE 配置**”中的“**添加**”

AD域策略
屏幕保护策略
IE配置
远程桌面管理

IE配置

策略名称 *

策略描述

是否对所有可信站点都要求用https访问 ☒ 是 ☐ 否

将以下站点添加为可信站点

将以下站点从可信站点中移除

IE代理例外列表

将以下地址添加到IE代理例外列表:

将以下地址从IE代理例外列表中移除:

策略执行周期 5 秒

生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	删除

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注: 右边有*号的项目必须输入。

配置项:	说明
策略名称	输入合适的策略名称, 以方便管理。
策略描述	用以描述该 IE 代理上网的提示信息, 以方便管理。

是否对所有可信站点都要求用 https 访问	选择让 IE 使用 HTTPS 访问可信站点
将以下站点添加为可信站点	在此添加可信站点
将以下站点从可信站点中移除	在此取消可信站点
IE 代理例外列表	输入不通过 Proxy 访问的 By Pass 主机或网段的列表
策略执行周期	设置执行本条策略的周期时间。 注： 只能是 5 或者 5 的倍数。
生效时间	设置策略生效的时间
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

远程桌面管理

通过配置远程桌面管理策略，可以阻止或允许远程计算机对本机的远程操作动作。

AD域策略
屏幕保护策略
IE配置
远程桌面管理
禁止修改网卡

远程桌面管理

策略名称 *

策略描述

远程桌面选项 ☒ 不配置 ☐ 启用 ☐ 禁止

生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

[保存](#) [取消](#)

配置项:	说明
策略名称	输入策略名称
远程桌面选项	选择本机是否开启远程桌面
生效时间	设置策略生效的时间
在线模式	选择该策略生效的网络场景，分为“在线时生效”和“离线时生效”
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

禁止修改网卡

点击“禁止修改网卡”的“添加”

禁止修改网卡功能可以防止使用人擅改网卡 IP 地址，mac 地址等等之类的属性。

AD域策略
屏幕保护策略
IE配置
远程桌面管理
禁止修改网卡

禁止修改网卡

策略名称 *

策略描述

网卡属性 ☒ 不配置 ☐ 不允许修改 ☐ 允许修改

策略执行周期 秒

生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

配置项:	说明
策略名称	输入策略名称

网卡属性	配置是否允许修改网卡属性
策略执行周期	设置执行本条策略的周期时间。 注 ：只能是 5 或者 5 的倍数。
生效时间	设置策略生效的时间
在线模式	选择该策略生效的网络场景，分为“在线时生效”和“离线时生效”
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

“发送到”菜单选项

点击““发送到”菜单选项”的“添加”



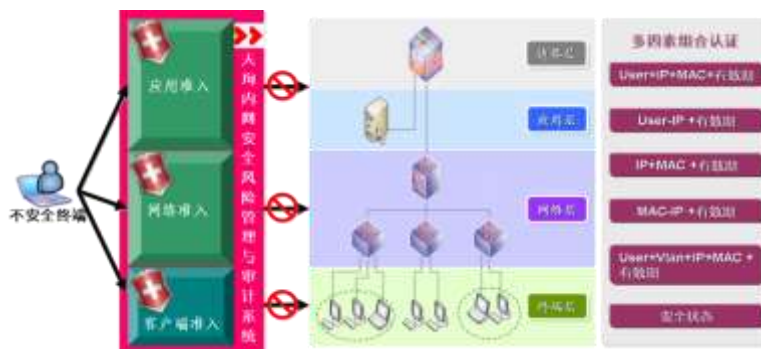
配置项：	说明
策略名称	输入策略名称
“发送到”菜单选项	配置启用或禁止“发送到”菜单选项
策略执行周期	设置执行本条策略的周期时间。 注 ：只能是 5 或者 5 的倍数。

生效时间	设置策略生效的时间
在线模式	选择该策略生效的网络场景，分为“在线时生效”和“离线时生效”
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

6. 准入控制

6.1. 关于准入控制

- 天珣具备业界最完善的计算机终端准入控制机制，从应用层和边界层到客户端，提供了客户端准入和应用准入等多种准入控制手段，确保只有通过身份验证和安全状态检查的计算机终端才能接入内网并进行受控访问，对非法的或存在安全隐患的计算机终端进行隔离和修复，构建出完善的“内网安检系统”，从源头上有效减少内网安全漏洞。
- 天珣支持基于策略网关的应用准入控制及基于计算机终端安全状态的客户端准入控制，更可与启明星辰天清汉马 USG 一体化安全网关进行联动，确保只有通过身份验证和安全状态检查的计算机终端才能接入内网，变被动防御为主动防御，为内网的安全合规提供强制性保障。天珣的多种准入控制手段可灵活组合，有效保护用户投资。
- 天珣的多层准入控制机制，彻底颠覆了传统内网安全管理被动管理的局面，为终端安全合规提供了强制性的保障能力。



天珣多层准入控制逻辑图

6.2. 网络准入

*该章节功能仅适用于高级版和增强身份认证高级版

6.2.1. 关于网络准入

- 网络准入认证支持各种认证策略，包括：支持有线网络准入（标准 802.1x、Eou）和无线网络准入（标准 802.1x），基于仅验证客户端运行，用户认证，用户、IP、MAC 组合认证，可信 MAC 认,可信 GUID 认证和接入设备端口绑定。
- “标准的 802.1x”和“EoU 认证”认证过程中支持组合认证，不支持组合绑定。

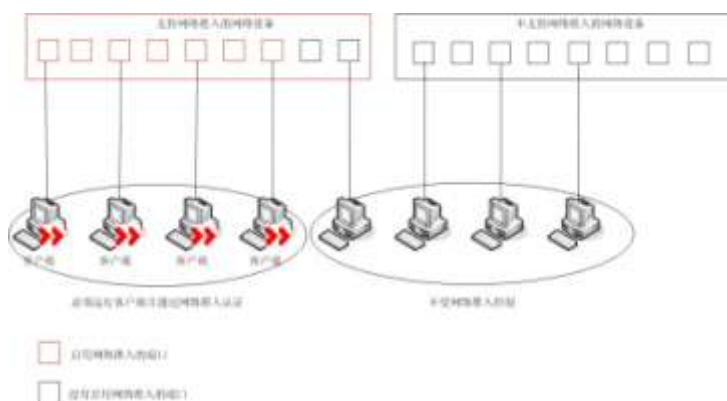
注意：这并不说明标准的 802.1x 不支持 User-IP，MAC-IP 组合自动进行绑定，若网络准入中不配置认证策略，但配置了基于终端的 User-IP 或 MAC-IP 组合，当网络准入认证成功，客户端到策略服务器取策略时，可自动改回指定的 IP 地址。

名词解释

- “RADIUS Server”：网络准入认证的基本选项，包括选用网络准入认证策略、RADIUS 认证服务器 IP 地址和启用网络准入控制的交换机或路由器等。交换机的配置在“基本配置”的“网络设备配置”里面配置。

- **“可信 MAC 认证实时授权”**：如果在认证策略中启用了扩展可信 MAC 认证，那么系统在网络准入认证过程中将会拒绝可信 MAC 列表之外的客户端，管理员可在此对非可信 MAC 地址的客户端进行授权。
- **“可信 GUID 认证实时授权”**：如果在认证策略中启用了扩展可信 GUID 认证，那么系统在网络准入认证过程中将会拒绝可信 GUID 列表之外的客户端，管理员可在此对非可信 GUID 的客户端进行授权。
- **“免认证 MAC 地址列表”**：如果在认证策略中启用了该策略，在免认证 MAC 地址列表里面添加了相应的 MAC 地址，则对在该列表中的 MAC 地址所对应的设备不进行网络准入认证，前提是该设备没有安装客户端，如果该设备安装了客户端，那么接入网络时，还是会对它进行准入认证。
- **“VLAN 信息”**：本系统支持基于用户和 MAC 的动态 VLAN 功能，在此可查看 VLAN 与用户或 MAC 的关联信息。但此处不能用于设置动态 VLAN。

下图是网络准入控制范围示意图。



6.2.2. RADIUS Server 页面

配置介绍

RADIUS Server		可信MAC认证实时授权	可信GUID认证实时授权	免认证MAC地址列表
RADIUS Server				
RADIUS Server名称	初始radius服务器 *			
描述				
IP地址	10.201.1.204 *			
认证策略				
网络准入类型	☒ 标准802.1x ☐ EoU			
基本认证	☐ 仅验证客户端运行 ☒ 用户认证 ☐ 可匿名的用户认证			
选择启用的目录服务	☒ 本地用户			
用户、IP、MAC组合认证	☐ 不启用 ☒ duo			
可信MAC认证	☒ 不启用			
可信GUID认证 (eou认证无效)	☒ 不启用			
MAC免认证 (无线网络认证无效)	☒ 不启用			
是否检查中心服务地址	☐ 是 ☒ 否			

验证客户端是否满足安全状态 (无线网络认证无效)	☒ 不验证 ☐ 安全状态完整时放行，不完整时给出提示后放行 ☐ 安全状态完整时放行，不完整时给出提示后切换到无线MAC地址时指定的VLAN ☐ 安全状态完整时放行，不完整时给出提示后不放行
应用准入控制的交换机或路由器	查看及编辑 *对接入这些交换机或路由器的终端实施准入控制
创建状态	全局
创建者	administrator

ACL 配置	
默认VLANID	☐ 不指定VLAN，使用交换机默认设置
无线MAC地址VLANID	☐ 不指定VLAN，拒绝访问
网络准入策略	
Clientless用户名	
Clientless密码	
Clientless请求ACL	
ClientlessACL	<pre> permit udp any any eq 21802 permit udp any eq bootpc any eq bootpc deny icmp any any </pre>
验证通过时的ACL	<pre> permit ip any any </pre>
无线MAC地址时的ACL	<pre> permit udp any any eq 21802 permit udp any eq bootpc any eq bootpc deny icmp any any </pre>
	重认证时间: 15 秒 重认证时间: 100 秒 重认证时间: 10 秒
重认证时设备有缺省，请使用交换机上的默认值(605~1000秒)	
注：带星号+号的条目必须输入。	
保存 删除 帮助	

配置项:	说明
RADIUS Server 名称	用以标记该 RADIUS 服务器，建议名称能够明确代表该 RADIUS 的真实服务器。
描述	用以对该服务器的角色等详细描述，方便日常管理。
IP 地址	Radius 服务器的 IP 地址
认证策略	
网络准入类型	选择网络准入认证的协议类型。天珣网络准入目前支持“标准 802.1x”，“EoU”（即 Cisco EAP over UDP 类型）。 默认使用标准 802.1x 即可满足大部分用户需求。
基本认证	为了方便管理，可以选择“仅验证客户端运行”，该选项只需安装天珣客户端，终端身份即可认证通过。 “用户认证”用户身份的确认方式，如果该用户没有帐号和密码，则被交换机强制网络阻断。 “可匿名的用户认证”特指在基于用户认证的情况下，允许无用户帐号的终端匿名登录网络。可匿名的用户认证仅在用户认证方式下有效，无用户认证配置就无法使用该模式。
选择启用的目录服务	只有选择了“用户认证”或者“可匿名的用户认证”时，才能应用此选项，默认只有“本地用户”，也可以自己建立其他本地用户认证或 AD 域用户认证，其配置在“基本配置”的“本地用户”和“用户组”里面配置。
用户、IP、MAC 组合认	在网络准入的认证过程中直接对该终端的组合信

证	息确认，若组合条件不满足要求，直接网络阻断并提示。仅在漫游 IP 网段 802.1x 的情况下，可以基于用户绑定信息自动更改终端的 IP 地址。
可信 MAC 认证	此选项与“可信 MAC 认证实时授权”结合使用。选中可信 MAC 认证，若某终端的 MAC 地址不在可信 MAC 列表中，将被网络阻断并提示修复。管理员确认该 MAC 可信后可以在线实时授权。若该 MAC 地址是来访人员，根据其来访的时间，可以分配准入的时间段，如果超过该时间段则网络阻断。
可信 GUID 认证	此选项与“可信 GUID 认证实时授权”结合使用。选中可信 GUID 认证，若某终端的 GUID 地址不在可信 GUID 列表中，将被网络阻断并提示修复。管理员确认该 GUID 可信后可以在线实时授权。若该 GUID 是来访人员，根据其来访的时间，可以分配准入的时间段，如果超过该时间段则网络阻断。
是否检查中心服务器地址	可选择客户端在认证时是否检查其中心服务器 IP 地址是否与 radius 服务器接收策略的中心服务器地址一致，如不一致则认证失败。
验证客户端是否满足安全状态	主要有四种验证方式：（1） 不验证 ；即不对客户端的安全状态做任何验证，就算客户端的安全状态不满足，也不会弹出任何提示；（2） 安全状态完整时放行，不完整时给出提示后放行 ；当客户端的安全状态不完整时，会弹出提示框，但是网络依然是通的；（3） 安全状态完整时放行，不完整时给出提示后切换到无效 MAC 地址时指定的 VLAN ；注意这里要在配置交换机时，让交换机支持动态 VLAN，并且在下面的“无效 MAC 地址 VLANID”里面配

	置 VLANID; (4) 安全状态完整时放行, 不完整时给出提示后不放行; 当客户端安全状态不完整时, 会弹出提示框, 并且阻断网络。
启用准入控制的网络设备	认证策略中最重要的选项, 即勾选 RADIUS 接受认证的网络设备。
创建状态	即该页面创建的权限, 如果是全局管理员创建则状态为全局, 所有管理员均可以看到该配置, 如果是本地管理员, 则其他本地管理员无法看到该页面。
创建者	标记了该策略是由哪个管理员创建。
802.1x 选项	
默认 VLANID	若某终端、用户未被配置 VLAN 信息, 则交换机会将之切换至默认 VLAN 中, 如果不指定 VLAN, 则使用交换机默认设置。
无效 MAC 地址 VLANID	在可信 MAC 认证的前提下, 如果某终端未被授权为可信 MAC, 则将之切换至该 VLAN, 如果指定该 VLAN, 则拒绝访问 (需要管理员授权接入网络)
EOU 选项	
Clientless 用户名	用于在路由器上启用 EoU 认证, 交换机认证可以忽略此选项, 默认值为 Clientless
Clientless 密码	用于在路由器上启用 EoU 认证, 交换机认证可以忽略此选项, 默认值为 Clientless
Clientless 提示 URL	当某终端确认未安装天珣客户端时, 任何 http 访问将被准入交换设备重定向至该 URL。该 URL 可以是任何 URL, 但要确保 Clientless 的 ACL 对此有做明确例外排除, 例如: 如果重定向的 URL 为 http://192.168.0.1/index ,

	那么 Clientless 的 ACL 中需要添加一条 ACE: permit tcp any host 192.168.0.1 eq www。默认值为: http://192.168.0.236:8833/download。(若天珣策略服务器的 IP 地址为 192.168.0.236)
Clientless 的 ACL	即如果终端未安装天珣客户端时, 交换准入设备将分配的 ACL, 如下均为必须 ACE。 <pre>permit tcp any host 192.168.0.236 eq 8833</pre> (若天珣策略服务器的 IP 地址为 192.168.0.236, 该 ACE 允许所有客户端访问客户端下载页面) <pre>permit udp any any eq 21862</pre> <pre>permit udp any eq bootpc any eq bootps</pre> <pre>permit udp any any eq domain</pre> <pre>deny icmp any any</pre> <pre>deny ip any any</pre>
验证通过时的 ACL	如果终端安装有天珣客户端, 并且开启了 EoU 认证选项, 网络准入设备将分别下面的 ACL, 即允许访问任何网络。 <pre>permit ip any any</pre>
无效 MAC 地址时的 ACL	如果 EoU 中有配置可信 MAC 认证, 而该终端 MAC 地址不在可信 MAC 域中, 则走此 ACL。注意: 走此 ACL 的终端必须是已经安装有天珣客户端的 PC。默认值同 Clientless 的 ACL。 <pre>permit tcp any host 192.168.0.236 eq 8833</pre> <pre>permit udp any any eq 21862</pre> <pre>permit udp any eq bootpc any eq bootps</pre> <pre>permit udp any any eq domain</pre> <pre>deny icmp any any</pre> <pre>deny ip any any</pre>

注意：如果网络中有多台 RADIUS 服务器，不同的服务器可仅为指定的那些交换机提供服务,以确定该 RADIUS 服务器的最大负载。但需避免出现某交换机仅在主 RADIUS 服务器上有可信任关系，否则当主 RADIUS 服务器宕机时，该交换机将强制阻断所有接入终端！

当启用“网络准入”的认证策略时，则“基本配置”里面的“IP 组”的用户认证策略则尽可能不要启用，避免发生冲突。

建议：网络中至少部署两台 RADIUS 服务器，而两台 RADIUS 服务器关联的交换机完全相同。

注意：标准的 802.1x 准入下，天珣支持动态 VLAN 功能。如果某用户、终端未分配其 VLAN 号，可以将之切换至默认 VLAN,如果某终端 MAC 地址不在可信 MAC 表中，也可以以将之切换至指定的 VLAN。

注意：clientless 提示 URL 页面建议配置成 http://中心服务器 IP:8833/download 直接给用户一个下载提示页面，并在 clientless 的 ACL 中放开对中心服务器 IP 的 8833 端口限制，假设配置成一个 80 端口的访问页面，那么客户端在弹出页面时将需要花费很长时间。

启用准入控制的网络设备页面

点击“查看及编辑”配置链接可勾选 Radius 接受认证的交换机和路由器：



当配置的交换机或者路由器数量较多时，还可以根据相关的属性对他们进行查找。交换机和路由器的相关配置在“**基本配置**”的“网络设备配置”里面配置。

6.2.3. 可信 MAC 认证实时授权页面

配置介绍

当客户机安装天珣客户端并接入交换机端口(或通过无线连接)时，本系统会自动获取其 MAC 地址并与可信 MAC 列表对比，以确认其是否属于内部终端，若不是则拒绝其接入网络，并将其列入未授权接入列表中。



点击“授权”，管理员可以对其进行设置。

RADIUS Server名称 初始radius服务器

可信MAC策略 * 格式: AABBCDDDEEFF

MAC地址 *

主机名 *

MAC地址有效期限制 ☒ 否 ☐ 是

MAC地址有效期起始时间

MAC地址有效期结束时间

802.1X选项VLANID

802.1X选项ACL

注：右边有*号的项目必须输入。

配置项：	说明
可信 MAC 策略	右边有个下来选项，可以选择对应的策略。
MAC 地址	被拒绝的非可信 MAC 地址。
主机名	填写主机名，便于查询管理。
MAC 地址有效期限制	开启 MAC 地址有效期限制，MAC 地址只能在指定的时间范围内通过认证，超出时间范围将再次被拒绝。
MAC 地址有效期起始时间	MAC 地址有效期起始时间。
MAC 地址有效期结束时间	MAC 地址有效期结束时间。
802.1X 选项 VLANID	为 MAC 地址分配 VLAN，客户端通过认证后，所接的交换机端口将被自动划分至指定的 VLAN，默认值为 0，则表示默认交换机的配置。

授权	给被拒绝的终端授权其进入网络。
----	-----------------

设置完成，点击保存，进入即时更新规则—>更新 Radius 规则，即时更新 Radius 服务器的规则，即可使设置生效。

注意：如果某终端授权时间结束，但其并未关机或与网络断开连接，而且交换机并未出发重认证，该终端仍旧未被阻断，直到 802.1x 触发重认证。

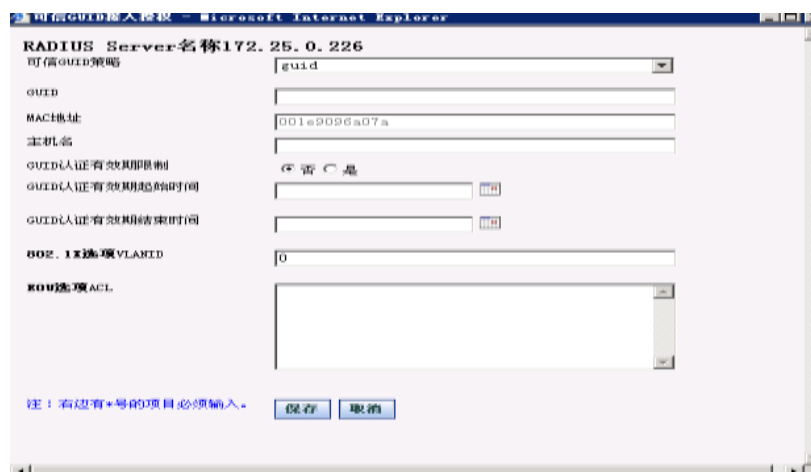
6.2.4. 可信 GUID 认证实时授权页面

配置介绍

当客户机安装天珣客户端并接入交换机端口时，本系统会自动获取其 GUID 地址并与可信 GUID 列表对比，以确认其是否属于内部终端，若不是则拒绝其接入网络，并将其列入未授权接入列表中。



点击“授权”，管理员可以对其进行设置。



配置项:	说明
可信 GUID 策略	选择此 GUID 所属的 GUID 策略
GUID	被拒绝的非可信 GUID
MAC 地址	被拒绝的非可信 MAC 地址。
主机名	填写主机名，便于查询管理。
GUID 地址有效期限制	开启 GUID 地址有效期限制，GUID 地址只能在指定的时间范围内通过认证，超出时间范围将再次被拒绝。
GUID 地址有效期起始时间	GUID 地址有效期起始时间。
GUID 地址有效期结束时间	GUID 地址有效期结束时间。
802.1X 选项 VLANID	为 GUID 分配 VLAN，客户端通过认证后，所接的交换机端口将被自动划分至指定的 VLAN，默认值为 0，则表示默认交换机的配置。
授权	给被拒绝的终端授权其进入网络。

设置完成，点击保存，进入即时更新规则—>更新 Radius 规则，即时更新 Radius 服务器的规则，即可使设置生效。

注意：如果某终端授权时间结束，但其并未关机或与网络断开连接，而且交换机并未出发重认证，该终端仍旧未被阻断，直到 802.1x 触发重认证。

6.2.5. 免认证 MAC 地址列表页面

配置介绍

天珣策略系统支持 MAC 免认证功能，在此处添加免认证 MAC 地址列表，则对在该列表中的 MAC 地址所对应的设备不进行网络准入认证，前提是该设备没有安装客户端，如果该设备安装了客户端，那么接入网络时，还是会对它进行准入认证。

点击“添加”，则可配置策略，策略名称可自定义：



在生成的策略中进行“设置”，点击“添加”，即可填写免认证的 MAC 地址。



注：启用免认证 MAC 功能时，还需要在交换机上面配置相关的命令，具体情况请参考“[网络准入其他组件配置](#)”。

6.2.6. VLAN 信息页面

配置介绍

天珣策略系统支持基于用户和 MAC 的动态 VLAN 功能，如果在可

信 MAC 或用户，IP，MAC 组合中配置了 802.1X VLAN 信息，可以在 VLAN 信息页面查看到该 VLAN。



点击关联用户或关联 MAC 可查看与 vlan 相关联的用户或 MAC 信息，同时也可删除相关联的用户和 MAC。

6.2.7. 网络准入配置要点

- 1、点击 RADIUS Server “添加” 按钮，添加 Radius 服务器；
- 2、输入 “RADIUS Server 名称”、“IP 地址”；
- 3、配置在网络准入过程中的认证策略；
- 4、点击启用准入控制的交换机或路由器“查看及编辑”链接页面；
- 5、在链接页面里面勾选上对应的交换机或者路由器；
- 6、勾选完对应的设备之后，点击“确定”跳转到 RADIUS Server 配置页面，再点击“保存”；
- 7、点击“即时更新策略->更新 RADIUS 策略”，点击“更新 RADIUS 服务器策略”。

将安装有天珣客户端的终端接入启用 802.1x 认证的交换机，即可访问网络。

注意：RADIUS 服务器必须手工更新策略，否则无法获取新的认证策略；更新规则前需确认 RADIUS 服务器 IP 地址存在于 IP 组中。

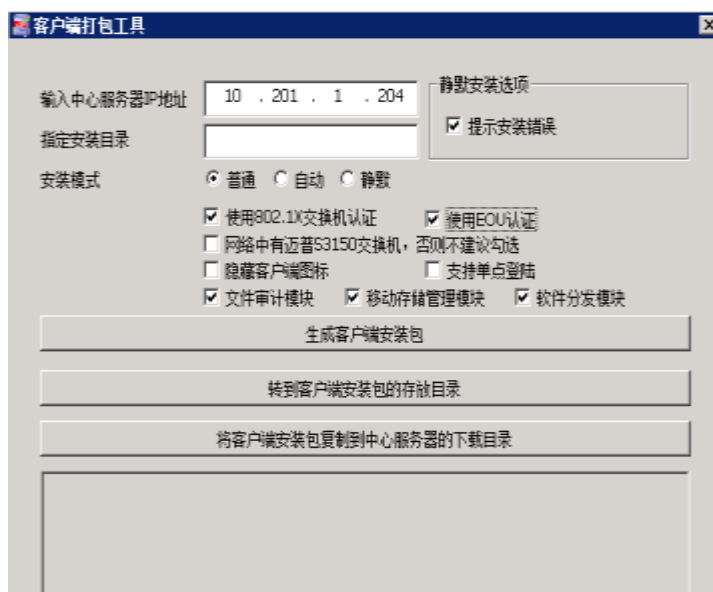
6.2.8. 网络准入其他组件配置

天珣内网安全风险管理与审计系统网络准入控制认证方式包括 802.1x 验证和 Cisco EOU 验证两种。由 3 部分组成：天珣内网安

全风险管理与审计系统 ESCC 客户端, ESRadius 服务器, 提供 802.1x 功能或者 EOU 功能的交换机/路由器。其中 ESCC 客户端和 ESRadius 服务器由启明星辰开发提供。交换机由交换机厂商提供, 不同厂商的 802.1X 配置方法存在较大区别, 对交换机的配置, 下面只介绍配置原理要点, 然后以 Cisco 2950(12.22(EA1))、Cisco3550 和华为交换机为例说明配置过程。

客户端配置

打包客户端: 在服务器使用客户端打包工具生成客户端安装包。打包时必须选择使用 802.1x 交换机认证才能实现 802.1X 认证功能。客户端安装完成重启后, 802.1X 模块即可生效。



如需要启用 EOU 功能, 打包时选择 EoU。或者通过需要修改 ESCC. ini 文件:

[LOG]

LogFile = log\ESCC.log

BakLogFile = log\ESCC.log_bak

MaxLogLine = 100000

Backup = 1

Level = 2

; 1 - DEBUG 2- INFO 3- WARN 4- ERROR 5- FATAL

[Firewall]

PerPacketCheck = 0

[ESCC]

RequestMethodV2 = 1

EnableE0U = 1

将最后一行的 EnableE0U=1 即可。

Radius 服务端配置

Raidus 服务端位于策略系统中心服务器或本地服务器上。要求的操作系统为 Windows2000/2003 Server 版。

如果该计算机已经安装过 IAS 服务，请先卸载该服务，或者停止该服务并设置为已禁用。

运行安装光盘，点击安装 Radius 服务组件，启动安装程序。

安装完成后，请进入 ESRadius 服务器的安装目录，一般默认为 C:\Program Files \ESRadius，打开 ESRadius.ini 文件，文件内容如下所示：

[Radius]

IPAddress = 0.0.0.0

; If a multi-ip host, you need set the listening ipaddress of radius server

; when IPAddress=0.0.0.0, radius server is listening on all ipaddress

EAPMD5Channel = 1

; Some switchs, liking ZTE and Huawei's Product, only support EAP_TYPE_MD5(4), which can't transport other type EAPOL Packages

; Set EAPMD5Channel = 1, Enable set EAP Data Type as MD5's type

[LOG]

LogFile = log\ESRadius.log

BakLogFile = log\ESRadius.log_bak

MaxLogLine = 100000

Backup = 1

Level = 1

; 1 - DEBUG 2- INFO 3- WARN 4- ERROR 5- FATAL

这些选项一般可按照默认设置，按需修改。

IPAddress = 0.0.0.0, 当安装 ESRadius 组件的计算机有多网卡时，需要在此指定 radius server 监听的 IP 地址。

EAPMD5Channel = 1, 如果交换机只支持 EAP_TYPE_MD5(4)，例如中兴、华为交换机，那么此选项设置为 1，如果交换机还支持其他类型的 EAPOL Packages，例如 Cisco 交换机，那么此选项可设置为 0。

文件修改保存后，请重新启动 ESRadius 服务，使配置生效。

天珣内网安全风险管理与审计系统 Radius 服务器组件安装后，会在 iis 默认 web 站点中，新建一个名为 ESRadiusWS 的虚拟目录，这个虚拟目录的运行需要 Dot Net Framework 2.0 的支持。

认证日志

查询客户端接入交换机时，进行 Radius 认证的日志。

管理员可查询指定 Radius 服务器的认证日志。

当日志数据库比较大时，可选择删除指定时间之前的日志，或者一键优化日志数据库。

交换机配置

为使用天珣内网安全风险管理与审计系统的 802.1X 验证功能，需要交换机提供以下功能支持：

- 1 支持 802.1X 功能
- 2 支持 802.1X 的 EAP over Radius 认证功能

3 支持 Radius 协议

为使用天珣内网安全风险管理与审计系统的 EOU 验证功能, 需要交换机/路由器提供以下功能支持:

- 1 支持 EOU 功能
- 2 支持 EAP over UDP 认证功能
- 3 支持 Radius 协议

Cisco2950 的配置 (12.1(14)EA1 以上版本)

以下材料来自于 Cisco 文档: Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide (full book i.pdf

配置前, 做以下设定: 设置 Cisco 交换机 IP 地址为 192.168.0.2, 设置 ESRADIUS 服务器 IP 地址 192.168.0.236, 交换机和 ESRADIUS 服务器通讯的 Radius 密钥为 123456

以下部分是已经完成的配置, 我们在交换机的端口 7 启用了 802.1x 认证。接下来看一下配置步骤。

```
Switch#show running-config
Building configuration...

Current configuration : 1519 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
```

```
aaa new-model

aaa authentication dot1x default group radius

enable secret 5 $1$GyoJ$VX3N1qY0nVH3hXjmVPYB5/

enable password 654321

!

ip subnet-zero

!

!

spanning-tree mode pvst

no spanning-tree optimize bpdu transmission

spanning-tree extend system-id

dot1x system-auth-control

!

!

!

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7
```

```
switchport mode access

dot1x port-control auto

dot1x timeout reauth-period

dot1x reauthentication

spanning-tree portfast

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19
```



```
!  
  
interface FastEthernet0/20  
  
!  
  
interface FastEthernet0/21  
  
!  
  
interface FastEthernet0/22  
  
!  
  
interface FastEthernet0/23  
  
!  
  
interface FastEthernet0/24  
  
!  
  
interface Vlan1  
  
    ip address 192.168.0.2 255.255.255.0  
  
    no ip route-cache  
  
!  
  
ip http server  
  
radius-server host 192.168.0.236 auth-port 1812 acct-port 1813  
key 123456  
  
radius-server retransmit 3  
  
!  
  
line con 0  
  
line vty 0 4  
  
    password 123456  
  
line vty 5 15  
  
    password 123456  
  
!  
  
!  
  
end
```

1. 进入配置命令模式

```
# config terminal
```

2. 配置 Radius 认证服务器

启用认证

```
# aaa new-model
```

设置 802.1X 使用 radius server 组中的所有 radius server 进行认证

```
# aaa authentication dot1x default group radius
```

```
# aaa authorization network default group radius
```

添加 ias 到 radius server，其中 host 后面的 IP 地址为 IAS 服务器地址，auth-port 和 acct-port 为标准的 Radius 端口，key 为交换机和 Radius 服务器通讯密钥

```
# radius-server host 192.168.0.236 auth-port 1812 acct-port 1813 key 123456
```

3. 启用 802.1X

```
# dot1x system-auth-control
```

4. 配置 7 号端口使用 802.1X 认证，若交换机支持 Guest VLAN，那么当认证不通过时，则将其分配至 Guest VLAN

```
# interface FastEthernet0/7
```

```
# switchport mode access
```

```
# dot1x port-control auto
```

```
# dot1x guest-vlan 10 (for example : guest-vlan id =10)
```

```
# dot1x host-mode multi-host ( 启用 交换机 端口 的 multiple-hosts 模式，以使交换机可下接 hub 进行认证)
```

```
# end
```

5. 配置 7 号端口的重认证周期

可选项，配置 802.1X 重认证的周期，以秒为单位，默认为 3600 秒（1 小时），当重认证时，如果网络端口接入其他没有运行天珣内网安全风险管理与审计系统的计算机，端口会立刻封闭。

```
# interface FastEthernet0/7
```

```
# dot1x reauthentication
```

```
# dot1x timeout reauth-period 3600  
# end
```

6. 保存当前配置作为启动配置

```
# copy running-config startup-config
```

7. 如何禁用 dot1x

禁用 AAA: #no aaa new-model

禁用 802.1x 的 AAA 认证: #no aaa authentication dot1x default
group radius

禁用 802.1x 认证 AAA: #no aaa authorization

禁用端口的 802.1x: no dot1x system-auth-control

8. 批量端口配置

对 2-24 端口进行批量配置

```
#interface range FastEthernet0/2 - 24  
  
#switchport mode access  
  
#dot1x port-control auto  
  
#dot1x host-mode multi-host  
  
#dot1x timeout reauth-period 900  
  
#dot1x reauthentication  
  
#spanning-tree portfast  
  
#end
```

注意: CISCO 的交换机如果是远程使用 telnet 登录到交换机进行配置的话, 请千万记得配置 aaa authentication login default line 命令 (不同型号交换机可能命令略有不同)。此命令作用是将 telnet 时进行的认证放在交换机本地, 如果不配置的话, 假如以前 telnet 交换机只需要输入密码的话, 那么在下次进行 telnet 登录时, 交换机将会提示要求输入用户名和密码进行认证。

注意: 如果有多台 radius 服务器进行备份, 要保证主 radius 服务

器出问题时可以正常切换, 需要另外配置 radius-server deadtime 1 命令, 其中 1 表示 radius 服务器认证超时时间。

Cisco EAPoUDP NAD 配置

配置 Radius 服务器

```
aaa new-model

aaa authentication eou default group radius

aaa session-id common

radius-server host 192.168.0.223 auth-port 1812 acct-port
1813 key 123456

radius-server vsa send authentication

路由器中配置 Radius 通讯端口

ip radius source-interface FastEthernet0/0
```

路由器的 EOU 认证

配置 EOU 认证模式

```
ip admission name TEST eapoudp

可以配置只在某些情况下启用 EOU, 通过设置 ACL 实现

ip admission name AVERT eapoudp list 102

access-list 102 deny udp any host 10.10.30.10 eq domain

access-list 102 deny tcp any host 10.10.20.10 eq www

access-list 102 permit ip any any
```

对某些主机的排除设置

```
identity profile eapoudp

device none-authorize ip-address 192.168.0.223 policy
NACless

device none-authorize ip-address 192.168.0.1 policy
NACless

identity policy NACless

access-group clientException
```

```
ip access-list extended clientException  
permit ip any any
```

Clientless 认证设置

```
eou clientless username clientless  
eou clientless password password  
eou allow clientless
```

配置 EOU 通讯端口

```
interface FastEthernet0/0  
ip address 192.168.0.200 255.255.255.0  
ip access-group 101 in  
ip admission TEST  
access-list 101 permit udp any host 192.168.0.200 eq 21862
```

URL-Redirect HTTP Server 配置

```
ip http server  
no ip http secure-server
```

允许 EOU 日志

```
eou logging
```

交换机的 EOU 认证配置

交换机上的 **EOU 认证 (L2 IP Validation)** 通过 EOU 认证协议完成。但 EOU 的认证激活模式与 802.1X 类似。当交换机检测到启用了 L2 IP Validation 的端口上有新的 IP 地址加入时，就会发起 EOU 认证。

只有配置为 switchport mode access 的端口才能启用 EOU。

L2 IP Validation 的启用

1 创建 NAC 规则

```
ip admission name nac eapoudp
```

2 定义 NAC 使用的 accesslist

在认证端口在没有认证的情况下会使用这里定义的 accesslist。

可定义两种 accesslist: Port Access List 和 IP Access List。

如定义 Port Access List, 语法如下: access-list 5 permit any
any

如定义 IP Access List, 则如下:

```
ip access-list extended NAC
  permit udp any any eq 21862          // 允许 EOU 通信
  permit udp any eq bootpc any eq bootps // 允许 DHCP
  permit udp any any eq domain         // 允许域名解析
  deny  icmp any any                   // 拒绝 ICMP
  deny  ip any any                     // 拒绝其他 IP 通信
```

3 对需要进行认证的端口启用 NAC 规则

a、Port Access List

```
interface fa0/1
  ip access-group 5 in
  ip admission nac
```

b、IP Access List

```
interface fa0/1
  ip access-group NAC in
  ip admission nac
```

4 配置 IP Device Tracking

```
ip device tracking probe count 2
ip device tracking probe interval 60
ip device tracking
```

对某些主机的排除设置

```
identity profile eapoudp
  device none-authorize ip-address 192.168.0.223 policy
NACless
  device none-authorize ip-address 192.168.0.1 policy
NACless
```

```
identity policy NACless  
access-group clientException  
ip access-list extended clientException  
permit ip any any
```

EOU 的参数配置

具体指令参考 Cisco 的 NAC 配置指南。需要配置的指令如下

```
eou default  
eou logging  
eou timeout status-query 1800  
eou timeout revalidation 900  
eou revalidate
```

由于天珣内网安全风险管理与审计系统不支持状态查询，需要保证重认证超时<状态查询超时(5s~30min)，上面将重认证超时设置为 15min，状态查询超时设置为 30min

Clientless 的认证设置

交换机和路由器不同，不支持使用 Clientless 用户名密码向 Radius 认证 Clientless 用户，而是通过 Radius 请求的属性辨别是 Clientless 认证还是正常的用户认证。

配置指令

```
eou allow clientless
```

URL 重定向 ACL 的设置

当指定交换机对客户端进行 URL 重定向时，需要事先在交换机上设置用于重定向的 ACL，ACL 名称固定为 url-redirect-acl。当请求与重定向 ACL 匹配时，客户端的 HTTP 请求会被重定向。

下面的 ACL 定义将到 <http://192.168.0.223> 的访问进行重定向。

```
ip http server  
ip access-list extended url-redirect-acl  
permit tcp any host 192.168.0.223 eq www
```

建议将此 URL 设置为中心服务器的客户端下载页面，即提示

<http://服务器 IP:8833/download>

注意：不同的交换机有可能设置 radius 组时的命令不尽相同，不可死搬硬套。例如有时需要定义一个 radius 组让交换机去调用，并在这个组里配置 radius 服务器，aaa group server radius XXX，然后用 aaa authentication eou default group XXX 进行调用。

华为交换机的配置

不同型号的交换机配置步骤可能有所不同，本配置用例仅供参考。

配置前，做以下设定：设置 huawei 交换机 IP 地址为 192.168.0.5，设置 ESRadius 服务器 IP 地址 192.168.0.236，交换机和 ESRadius 服务器通讯的 Radius 密钥为 123456

我们将在交换机的端口 8 启用 802.1x 认证。接下来看一下配置步骤。

设置接入控制方式，该命令可以不配置，因为端口的接入控制在缺省情况下就是基于 MAC 地址的

```
[Quidway] dot1x port-method macbased interface ethernet 0/8
```

设置 802.1x 用户的认证方法，目前提供 3 种认证方法：PAP 认证、CHAP 认证、EAP 中继认证。缺省情况下，华为交换机 802.1x 用户认证方法为 CHAP 认证。此处需要修改设置为 EAP 认证。

```
[Quidway] dot1x authentication-method eap
```

创建 RADIUS 组 dot1x 并进入其视图

```
[Quidway] radius scheme dot1x
```

设置主认证/计费 RADIUS 服务器的 IP 地址

```
[Quidway-radius-dot1x] primary authentication  
192.168.0.236
```



```
# 设置主认证/计费 RADIUS 服务器的 IP 地址

[Quidway-radius-dot1x] primary accounting 192.168.0.236


# 设置系统与认证 RADIUS 服务器交互报文时的加密密码

[Quidway -radius-dot1x] key authentication 123456
[Quidway -radius-dot1x] key accounting 123456


# 指示系统从用户名中去除用户域名后再将之传给 RADIUS 服
器

[Quidway-radius-dot1x] user-name-format without-domain
[Quidway-radius-dot1x] quit


# 创建用户域 dot1x, 并进入其视图

[Quidway] domain dot1x


# 指定 “dot1x” 为该用户域的 Radius 方案

[Quidway-isp-dot1x] radius-scheme dot1x
[Quidway-isp-dot1x]quit


# 指定交换机缺省的用户域为 “dot1x”

[Quidway] domain default enable dot1x


# 开启 E0/8 的 802.1x 认证

[Quidway] dot1x interface Ethernet 0/8


# 开启全局 802.1x 特性

[Quidway] dot1x


# 保存设置
```

```
[Quidway] quit
```

```
<Quidway> save
```

新版 IOS 的 H3C 交换机配置里已经不支持 `scheme radius-scheme` 命令，这条命令被三条命令所取代，这三条命令是：

```
authentication default radius-scheme dot1x
authorization default radius-scheme dot1x
accounting default radius-scheme dot1x
```

注意：华为交换机也存在和思科交换机同样的 telnet 密码认证问题，解决的方法与思科交换机原理相同，将 telnet 密码认证放在本地进行。

```
User-interface vty 0 4
```

```
Authentication-mode password
```

```
Set authen password cipher XXXXXX
```

锐捷交换机的配置

不同型号的交换机配置步骤可能有所不同，本配置用例仅供参考。

配置前，做以下设定：设置锐捷交换机 IP 地址为 192.168.0.249，设置 ESRadius 服务器 IP 地址 192.168.0.191，交换机和 ESRadius 服务器通讯的 Radius 密钥为 123456

我们将在交换机的端口 1 启用 802.1x 认证。

验证通过的交换机软硬件版本：

System hardware version : 3.2

System software version : 1.69 Build Aug 2 2007 Release

System BOOT version : RG-S2126G-B00T 03-03-02

System CTRL version : RG-S2126G-CTRL 03-11-02

Running Switching Image : Layer2

完整的参考配置如下：

```
start#sh run
```

```
System software version : 1.69 Build Aug 2 2007 Release
```

```
Building configuration...
```

```
Current configuration : 731 bytes
```

```
!  
version 1.0  
!  
no enable services web-server  
hostname start  
vlan 1  
!  
vlan 11  
!  
radius-server host 192.168.0.191  
aaa authentication dot1x  
enable secret level 1 5 !,tZ[V/,U+S(\W&-G1X)sv'~H.Y*T7+.  
enable secret level 15 5 $2kE,1u_3hl&-8U04in'.tj9Qjo+/7R:  
!  
interface fastEthernet 0/1  
dot1x port-control auto  
dot1x dynamic-vlan enable  
!  
interface vlan 1  
no shutdown  
ip address 192.168.0.249 255.255.255.0  
!
```

```
no dot1x filter-nonRG-su enable  
  
dot1x auto-req  
  
no dot1x auto-req user-detect  
  
dot1x auto-req req-interval 180  
  
dot1x re-authentication  
  
radius-server key 123456  
  
snmp-server community public ro  
  
line vty  
  
login local  
  
!
```

End

配置步骤:

1、配置 radius 服务器地址，项目部署时请加备用 radius-server。

```
radius-server host 192.168.0.191
```

2、全局启用 dot1x

```
aaa authentication dot1x
```

3、进入接口启用 dot1x

```
interface fastEthernet 0/1
```

```
dot1x port-control auto
```

4、关闭非锐捷客户端的过滤

```
no dot1x filter-nonRG-su enable
```

5、当交换机下接 HUB 时，需打开交换机主动请求认证的功能，并设置发送间隔。

锐捷交换机是以主动发送认证包的方式支持基于 MAC 地址的验

证的。

```
dot1x auto-req
```

```
no dot1x auto-req user-detect
```

```
dot1x auto-req req-interval 180
```

6、打开重认证功能

```
dot1x re-authentication
```

7、设置与 radius server 通讯的密钥

```
radius-server key 123456
```

免认证 MAC 的相关配置

1、思科交换机配置要点：

在正常配置完 802.1X 准入之后，在端口下输入“**mab eap**”或“**dot1x mac-auth-bypass eap**”命令即可开启 mac-auth-bypass。请注意，12.2(55)的 IOS 同时支持这两条命令，但 12.2(25)/12.2(35)只支持 dot1x mac-auth-bypass eap

在实际使用时建议修改 tx-period 的值（思科默认为 30 秒），以缩短交换机重新发起认证的时间，使其尽快使用 mac 地址作为凭证认证。命令是：“dot1x timeout tx-period 5”。

2、H3C 交换机相关配置

与思科交换机不同的是，H3C 交换机配置 mac-auth-bypass 时需要在 system view 和端口模式下分别配置，其余基本一致。

在 system-view 模式下配置：**MAC-authentication** 和 **MAC-authentication domain dot1x**。

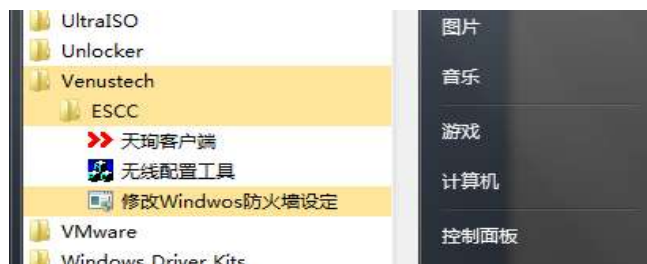
在接口下也要配置：**MAC-authentication**

无线网络准入配置

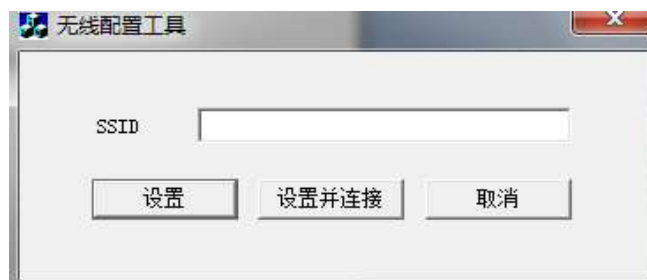
无线网络准入可支持标准 802.1x 用户认证,可信 mac 认证,可信 GUID 认证。

目前市面上大部分的无线路由器和 AP 基本上都支持 802.1x 准入的设置, 流程大致为:

- 1、 客户端设置:在开始菜单的 venustech 目录中,选择无线置工具



并输入 SSID,点击设置并连接



注: XP 系统下需要安装补丁 KB918997

- 2、 在无线路由器或 AP 上启用相应的 WPA/WPA2 认证;
- 3、 在无线路由器或 AP 上配置天珣的 radius 服务器、端口及密码;



注意: radius 服务器的密码与天珣 web 页面上配置的 radius 密码要一致。

- 4、 网络准入配置页面配置网络准入策略, 并添加 radius 客户端设置, ssid 应填写无线路由器或 AP 的正确 ssid;

本页面设置无线工作模式和参数。

SSID : TP-LINK_AP

频段: 5

模式: 54Mbps (802.11g)

交换机配置

交换机配置

交换机名称	wlan *
交换机ip地址	172.25.0.249 *
交换机品牌	D-Link
交换机型号	DGS3200-10
共享密钥	123456 *
交换机类型	☐ LAN ☒ WLAN
SSID	TP-LINK_AP
动态VLAN支持	不支持

- 5、无线信号经过无线路由器或 AP 时，会对其进行 802.1x 认证并将认证信息转发给天珣 radius 服务器；
- 6、天珣 radius 服务器对认证信息进行认证，将认证完成的信息发给无线路由器或 AP，然后决定是否对终端放行。

H3C WX3024 无线局域网的相关配置(瘦 AP)

H3C WX3024 默认情况下 console 进入无线控制模块

无线控制器配置

```
[H3C]display current-configuration
```

```
#
```

```
version 5.20, Release 3110
```

```
#
```

```
sysname H3C
```

```
#
```

```
domain default enable dot1x
```

```
#
```

```
telnet server enable
```

```
#  
  
port-security enable  
  
#  
  
dot1x quiet-period  
dot1x timer reauth-period 60  
dot1x authentication-method eap  
  
#  
  
oap management-ip 192.168.0.101 slot 0  
  
#  
  
vlan 1  
  
#  
  
vlan 2  
  
#  
  
radius scheme dot1x  
primary authentication 10.201.7.1  
primary accounting 10.201.7.1  
key authentication 123456  
key accounting 123456  
user-name-format without-domain  
nas-ip 10.201.0.50  
  
#  
  
domain dot1x  
  
authentication lan-access radius-scheme dot1x  
authorization lan-access radius-scheme dot1x  
access-limit disable  
state active  
idle-cut disable  
self-service-url disable  
domain system
```



```
access-limit disable

state active

idle-cut disable

self-service-url disable

#

user-group system

#

local-user admin

password simple admin

authorization-attribute level 3

service-type telnet

#

wlan rrm

dot11a mandatory-rate 6 12 24

dot11a supported-rate 9 18 36 48 54

dot11b mandatory-rate 1 2

dot11b supported-rate 5.5 11

dot11g mandatory-rate 1 2 5.5 11

dot11g supported-rate 6 9 12 18 24 36 48 54

#

wlan service-template 10 crypto

ssid wlan_dot1x_test

bind WLAN-ESS 10

cipher-suite tkip

security-ie wpa

service-template enable

#

interface NULL0

#
```

```
interface Vlan-interface1

  ip address 10.201.0.50 255.255.0.0
#
interface GigabitEthernet1/0/1

  port link-type trunk
  port trunk permit vlan all
#
interface WLAN-ESS1
#
interface WLAN-ESS10

  port-security port-mode userlogin-secure-ext
  port-security tx-key-type 11key
  undo dot1x handshake
  undo dot1x multicast-trigger
#
wlan ap ap1 model WA2220E-AG
  serial-id 210235A42XB101000025
  radio 1
  radio 2
  service-template 10
  radio enable
#
ip route-static 0.0.0.0 0.0.0.0 10.201.0.1
#
  load xml-configuration
#
user-interface aux 0
user-interface vty 0 4

  authentication-mode scheme
```

```
user privilege level 3

idle-timeout 0 0

#

return
```

无线控制器对应的交换模块配置

<H3C>oap connect slot 0 进入交换模块

```
#

sysname H3C

#

oap management-ip 192.168.0.100 slot 0

#

radius scheme system

#

domain system

#

local-user admin

password simple admin

service-type telnet

level 3

#

vlan 1 to 2

#

interface Vlan-interface1

ip address 172.25.42.200 255.255.0.0

#

interface Aux1/0/0

#

interface GigabitEthernet1/0/1

#
```

```
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
#
interface GigabitEthernet1/0/5
#
interface GigabitEthernet1/0/6
#
interface GigabitEthernet1/0/7
#
interface GigabitEthernet1/0/8
#
interface GigabitEthernet1/0/9
#
interface GigabitEthernet1/0/10
#
interface GigabitEthernet1/0/11
#
interface GigabitEthernet1/0/12
#
interface GigabitEthernet1/0/13
#
interface GigabitEthernet1/0/14
#
interface GigabitEthernet1/0/15
#
interface GigabitEthernet1/0/16
```

```
#  
interface GigabitEthernet1/0/17  
#  
interface GigabitEthernet1/0/18  
#  
interface GigabitEthernet1/0/19  
#  
interface GigabitEthernet1/0/20  
#  
interface GigabitEthernet1/0/21  
#  
interface GigabitEthernet1/0/22  
#  
interface GigabitEthernet1/0/23  
#  
interface GigabitEthernet1/0/24  
#  
interface GigabitEthernet1/0/25  
    shutdown  
#  
interface GigabitEthernet1/0/26  
    shutdown  
#  
interface GigabitEthernet1/0/27  
    shutdown  
#  
interface GigabitEthernet1/0/28  
    shutdown  
#
```

```
interface GigabitEthernet1/0/29
```

```
stp disable
```

```
port link-type trunk
```

```
port trunk permit vlan all
```

```
#
```

```
interface NULL0
```

```
#
```

```
user-interface aux 0
```

```
user-interface vty 0 4
```

```
authentication-mode scheme
```

```
user privilege level 3
```

无线控制器与交换模块之间通信说明:

无线控制器默认采用

```
interface GigabitEthernet1/0/1
```

```
port link-type trunk
```

```
port trunk permit vlan all
```

与交换模块

```
interface GigabitEthernet1/0/29
```

```
stp disable
```

```
port link-type trunk
```

```
port trunk permit vlan all
```

之间进行数据通信

胖 AP : WA2220-AG 配置说明:

```
<WA2220-AG>dis cur
```

```
#
```

```
version 5.20, Release 1113
```

```
#
```

```
sysname WA2220-AG
```

```
#  
  
domain default enable dot1x  
  
#  
  
telnet server enable  
  
#  
  
port-security enable  
  
#  
  
dot1x authentication-method eap  
  
#  
  
undo l2fw wlan-client-isolation enable  
  
#  
  
vlan 1  
  
#  
  
radius scheme system  
  
primary authentication 172.18.18.70  
primary accounting 172.18.18.70  
key authentication 123456  
key accounting 123456  
user-name-format without-domain  
  
radius scheme dot1x  
  
server-type extended  
  
primary authentication 172.18.18.70  
primary accounting 172.18.18.70  
key authentication 123456  
key accounting 123456  
timer realtime-accounting 3  
user-name-format without-domain  
undo stop-accounting-buffer enable  
  
#
```

```
domain dot1x

authentication lan-access radius-scheme dot1x

authorization lan-access radius-scheme dot1x

accounting lan-access radius-scheme dot1x

access-limit disable

state active

idle-cut disable

self-service-url disable

accounting optional

domain system

access-limit disable

state active

idle-cut disable

self-service-url disable

#

user-group system

#

local-user admin

password simple 1231.xmccb

authorization-attribute level 3

service-type telnet

local-user venus

password simple venus

authorization-attribute level 3

service-type telnet

#

wlan rrm

dot11a mandatory-rate 6 12 24

dot11a supported-rate 9 18 36 48 54
```



```
dot11b mandatory-rate 1 2
dot11b supported-rate 5.5 11
dot11g mandatory-rate 1 2 5.5 11
dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 10 crypto
    ssid venustx
    cipher-suite tkip
    security-ie wpa
    service-template enable
#
interface NULL0
#
interface Vlan-interface1
    ip address 172.18.18.249 255.255.255.0
#
interface Ethernet1/0/1
#
interface WLAN-BSS10
    port-security port-mode userlogin-secure-ext
    port-security tx-key-type 11key
    undo dot1x handshake
    undo dot1x multicast-trigger
#
interface WLAN-Radio1/0/1
#
interface WLAN-Radio1/0/2
    service-template 10 interface wlan-bss 10
#
```

```
ip route-static 0.0.0.0 0.0.0.0 172.18.18.254
#
arp-snooping enable
#
load xml-configuration
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme
#
return
```

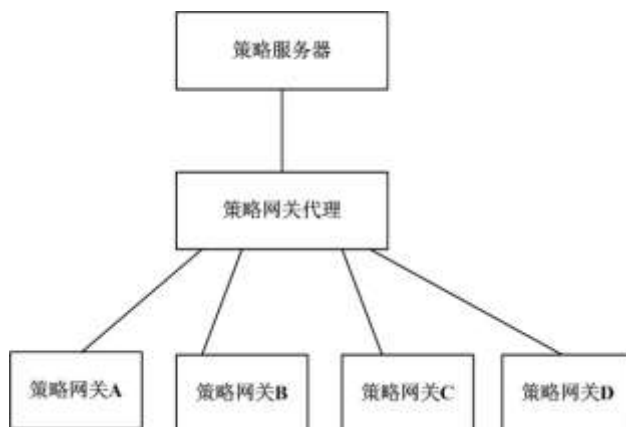
6.3. 应用准入

6.3.1. 关于应用准入

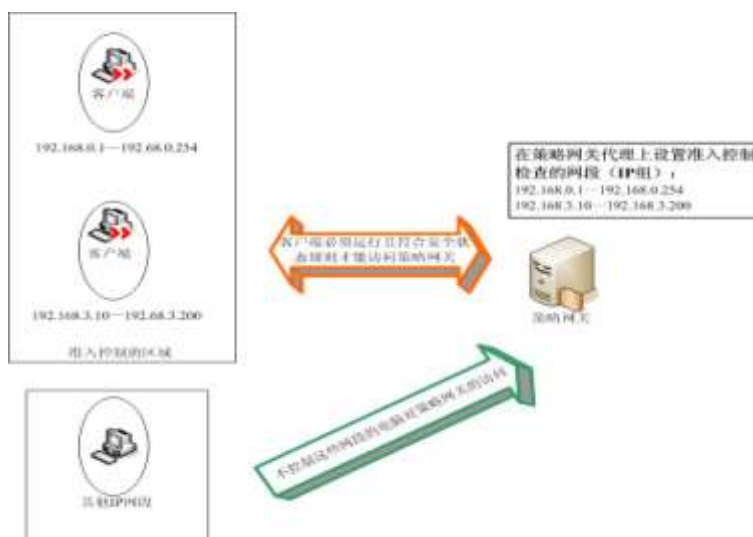
- **“应用准入”**：采用多种策略网关，为企业的关键信息系统和应用提供准入控制手段。只有受天珣管理并且符合安全策略的电脑才允许访问企业的这些系统及应用。应用准入控制为企业关键信息系统提供安全保护，杜绝非授权访问和非安全访问。
- 策略服务器（中心服务器或本地服务器）只与策略网关代理通讯。在有多个策略网关的环境下，这样的机制能极大简化配置。
- 策略网关代理代替策略网关确认终端是否已安装天珣客户端，当客户端主动退出后，策略网关代理负责通知各策略网关及时拦截该终端访问策略网关。
- 这种机制同样可以跨越负载均衡设备，只需负载后面的设备

单向链接到策略网关代理即可，而不需要负载后面的网关与客户端双向通信。

下图是策略服务器、策略网关代理和策略网关的关系示意图：



下图是应用准入控制范围示意图。



下图是应用准入工作流程示例图：



■ 详细流程说明请参考《工作原理和内部机制》文档。

名词解释

策略网关代理：策略网关代理代表一组策略网关对终端安装天珣客户端认证与安全状态确认。这些策略网关应该具有相同的准入控制需求。在策略配置时，将这一组策略网关作为一个管理对象来管理。一般情况下，一个企业需要做准入控制的网段是统一的，即哪些终端需要安装天珣客户端，哪些终端不必须安装天珣客户端。根据公司实际环境，这些准入范围是已知的，只需要配置一个策略网关代理即可。

但也有特殊情况，比如某公司的分支机构有一个专用服务器，该服务器仅需要给该分支机构的几千人提供服务。在此服务器上安装策略网关就不需要连接至总部的策略网关代理了。此时可以新建一个策略网关代理，其准入控制网段仅仅是该分支机构的 IP 组范围。

“策略网关”：即安装在应用服务器上的准入服务程序，策略网关连接至策略网关代理取规则并对访问的终端作安全检查。

天珣支持的应用准入策略网关类型有：

按应用系统分类：Web、Mail、DNS、ISA 代理。

按操作系统分类：Windows、Linux。

下表是天珣具备的针对不同业务应用的策略网关类型列表，用

户总可以从中找到一种或几种适合自己业务应用的应用准入控制解决方案：

表 3 天珣针对不同业务应用的策略网关类型列表

应用类型	不同平台下可选择的策略网关	
	Windows	Linux
Web 应用	IIS 策略网关	中性(通用)策略网关 for Linux
Proxy 应用	ISA 策略网关	中性(通用)策略网关 for Linux
DNS 应用	中性(通用)策略网关 for Windows	中性(通用)策略网关 for Linux
其他应用类型	中性(通用)策略网关 for Windows	中性(通用)策略网关 for Linux

除此之外，天珣能够与启明星辰天清汉马一体化安全网关（简称：天清汉马 USG）联动，实现准入控制互动，由天清汉马 USG 担当准入控制网关，当计算机终端需要通过天清汉马 USG 进行访问时，由天清汉马 USG 和天珣联动，确保只有安装天珣客户端程序、接受天珣管理并且符合企业安全策略的计算机终端才能通过天清汉马 USG 进行访问。

天珣还能针对一些特定的第三方 web 应用来实现 web 准入控制。这种准入控制方式没有特定的操作系统要求，只需将嵌入代码写入 web 登录页面的源代码中，由嵌入式代码检查发起访问的客户端 IE 是否安装了天珣的 IE 控件，并由此 IE 控件和天珣服务器一起决定此客户端是否能够正常访问该 web 页面，从而达到准入的目的，确保只有安装天珣客户端的终端才能安全访问。

天珣应用准入控制可以单独只启用一种平台进行应用准入控制，也可以同时启用多个平台进行应用准入控制，也可以与网络准入控制同时启用，组成“网络准入+应用准入”的复合准入控制体系。更可以与启明星辰天清汉马一体化网关进行准入控制联动，通过多种准入控制手段的组合，全面覆盖企业内网每一个区域和角落，有效保证计算机终端始终安装天珣客户端程序并接受天珣管理。

6.3.2. 策略网关代理设置页面

配置介绍



点击“应用准入”配置页面，将看到策略网关代理设置结果如上图。

策略网关信息页面

点击“连接的策略网关”查看链接，可以看到当前策略网关代理连接的策略网关信息。



注意：如果某策略网关并没有在此页面中显示，说明该策略网关并没有正确连接至策略网关，问题可能出在策略网关端或者是网络端口不通。端口为由策略网关单向连接至策略网关代理的 tcp 7893，请检查网络配置。

配置策略网关代理页面

点击**策略网关代理**名称，可进入策略网关代理添加\配置页面

配置项:	说明
策略网关代理名称	标记该策略网关代理的名称，方便日常管理。
IP 地址	策略网关代理的 IP 地址，告知中心服务器该策略网关代理的 IP 地址，提供策略网关代理的准入策略。
网段描述	方便日常管理，非必填项。
所属的管理网段	即策略网关代理所属的管理网段，此网段决定了策略网关代理如何取策略。
要求对方策略版本	用于强制客户端更新客户端版本。如果某客户端规则版本低于指定的规则版本，策略网关将强制阻断访问。
验证客户端是否满	主要有三种验证方式：（1） 不验证 ：即不对客户端的安

足安全状态	全状态做任何验证，就算客户端的安全状态不满足，也不会弹出任何提示；（2） 安全状态完整时放行，不完整时给出提示后放行 ；当客户端的安全状态不完整时，会弹出提示框，但是网络依然是通的；（3） 安全状态完整时放行，不完整时给出提示后不放行 ；当客户端安全状态不完整时，会弹出提示框，本次连出被拒绝。
客户端下载地址	客户端下载提示页面中客户端的下载地址，默认选项即可。 如果客户端下载 URL 非默认，则可以在此处更改。
管理员姓名	管理员名称，提示页面会有显示。
管理员电话	管理员电话，提示页面会有显示。
管理员邮件地址	管理员邮件地址，提示页面会有显示。
启用个性化客户端提示页面	如果默认提示页面不能满足用户要求，可由用户自定义提示页面。该提示页面可以是独立的 web 站点，甚至是独立的 WEB 服务器。此时需要选择“启用个性化客户端提示页面”。
提示页面 URL	个性化提示页面的 url。该提示页面可以是任意 url，比如：有天珣客户端下载链接的公司门户网站。
客户端 DNS 准入选项	有三个选项：（1）“ 不启用 ”，当不启用 DNS 准入时，则勾选此选项；（2） 对所有 DNS 服务器发送的请求启用 DNS 准入 ；（3） 安全状态完整时放行，不完整时给出提示后不放行 ；当要启用 DNS 准入时，则勾选第二、三选项，还有，要记得在 中性策略网关配置 里面把“启用 DNS 检查”也勾选上，默认是不勾上的。
策略应用对象	即该策略网关代理将对哪些对象做准入控制

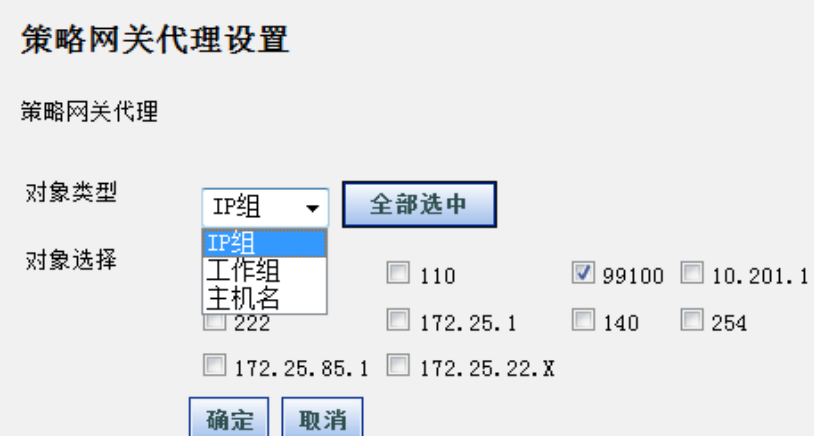
注意：如果策略网关、策略网关代理、中心服务器分别在不同的服

服务器上，此处需要填写的 IP 地址是策略网关代理的 IP 地址。

注意：如果网络中网段很多时，特别注意策略网关代理所在的管理网段，注意选择正确的管理网段。

注意：如果启用了个性化提示页面，天珣策略系统默认提示页面的所有配置信息将失效。

策略应用对象页面



策略网关代理设置

策略网关代理

对象类型

对象选择

☐ IP组
☒ 工作组
☐ 主机名
☐ 222
☐ 172.25.85.1
☐ 172.25.22.X

☐ 110
☐ 172.25.1
☐ 140
☐ 254

☒ 99100
☐ 10.201.1

可以应用到 IP 组，工作组，主机名。

注意：当前版本中若要排除某 IP 地址不做准入控制检查，不能为该 IP 地址添加独立的 IP 组并取消准入控制。而需要在 IP 组中添加该 IP 地址的例外排除。



不建议单独 IP 地址做准入控制检查，否则容易导致配置逻辑混乱。

例如：192.168.0.0/24 网络，测试时仅有一台客户端做测试，建议先添加一个 ip 组，该 IP 组的范围是 192.168.0.0/24，并对该 ip 组做准入控制和 MAC-IP 绑定。而客户端具体功能测试可以单独建立一个单 ip 地址的 IP 组。

配置要点

- 1、点击“添加”策略网关代理设置；
- 2、输入“策略网关代理名称”、策略网关“IP 地址”、配置管理员信息；
- 3、点击“策略应用对象”中“查看及编辑”超链接，选择需要准入的类型并确认；
- 4、保存策略网关代理配置页面后，即时更新策略网关规则。

注意：确认策略网关代理的 IP 地址在管理网段中，否则策略网关代理无法获取准入规则，导致应用准入功能失效。

6.3.3. 中性（通用）策略网关安装配置要点

- 1、请点击“安装中性(通用)策略网关”运行中性(通用)策略网关的 setup 程序，一步步按照提示进行安装。



2、安装结束之前，请注意阅读下面的重要信息。



3、安装完成后，中性(通用)策略网关配置程序启动进行驱动、端口检查、可忽略检查 IP 的配置。

4、配置中性(通用)策略网关驱动程序。首先安装驱动程序，当驱动程序已经安装时，“安装驱动”按钮不可用。安装完驱动程序后，驱动默认对所有的网卡进行监控。如果运行中性(通用)策略网关的机器上有多块网卡，需要将不直接与 CC 客户端通讯的网卡选择状态改为不选中，然后点击“应用网络配置”按钮使配置生效。



5、配置中性(通用)策略网关使用的策略网关代理地址、监控 TCP 端口的范围以及可忽略检查的 IP 地址。程序默认监控 80 和 8080 端口。



6、点击保存，完成中性(通用)策略网关配置。

7、如果需要启用 DNS 准入功能，请将中性(通用)策略网关安装在 DNS 服务器上（旁路 DNS 准入无需安装在 DNS 服务器上），并在中性(通用)策略网关配置界面中，进入 DNS 检查配置选项，勾选启用 DNS 检查，勾选后默认 DNS 服务器将启用准入检查，对所有来访的 DNS 请求进行检查。假设想对某些域名进行例外排除，可以在“例外的域名”栏中填入相应的域名并“添加”即可。



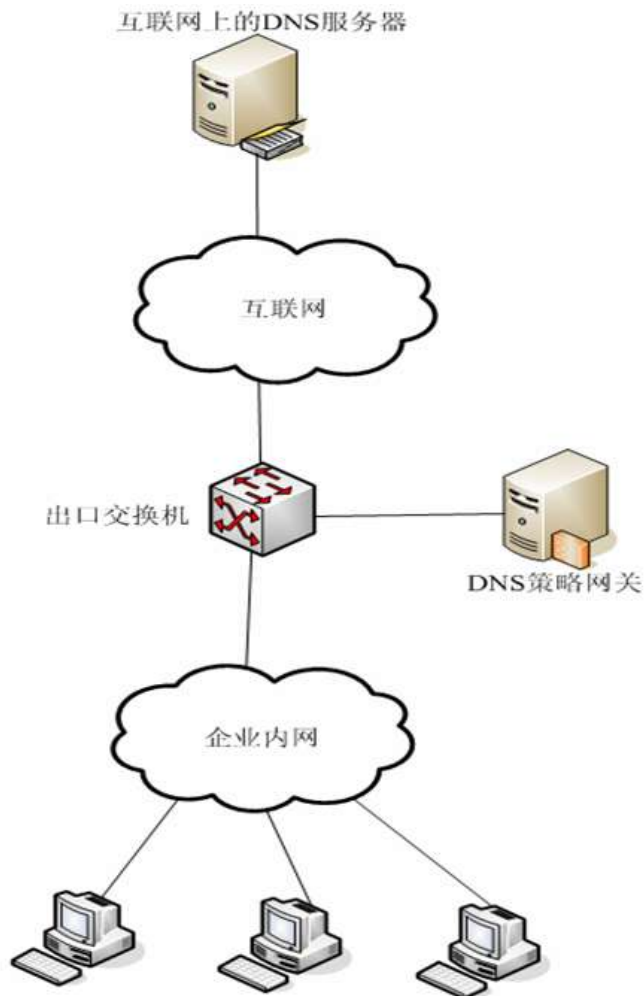
8、安装配置成功后，请进入服务控制器，若系统已经自动添加“ES GatewayPlugin Service”服务，则表明策略网关代理已经安装配置成功。注意此服务第一次需手动启动，以后则可以自动启动。

9、参考 [《应用准入-配置要点》](#)。

6.3.4. 旁路 DNS 准入

DNS 策略网关不单支持在内部 DNS 服务器上安装部署，实现对 DNS 服务器的检查和控制，也支持在没有内部 DNS 服务器的环境中对终端进行 DNS 请求的检查和控制。假如安装在内部 DNS 服务器上策略网关将自动按照在线服务模式（Pass Through）执行 DNS 应用准入，实现旁路侦听和在线服务模式自适应自动切换，满足各种网络环境下，实现基于 DNS 应用的客户端准入控制。

下图为工作在旁路侦听模式的新 DNS 策略网关部署逻辑图：



- a) 在用户使用的 DNS 服务器不统一的情况下, 建议将新 DNS 策略网关连接在互联网出口交换机的镜像监听端口上;
- b) 客户端的 DNS 请求包经过出口交换机时, 会被完整复制一份到镜像监听端口, 并由策略网关检查其是否安装天珣或是是否合规;
- c) 也可以使用 HUB 接入策略网关, HUB 上连接的其他终端都将直接受到监听而无需设置镜像;
- d) 可选择任意一台服务器作为 DNS 应用准入服务器, 此服务器上可以不装任何其他应用服务, 例如 IIS 等等;

在设置交换机端口镜像时, 不要把端口所有的数据都镜像, 这样会造成监听口网络流量巨大, 可能造成网络阻塞, 只需要对 DNS 请求数据镜像就行;

6.3.5. IIS 策略网关安装配置要点

- 1、请点击“安装 IIS 策略网关”运行 IIS 插件策略网关的 Setup 程序，一步步按照提示进行。



- 2、进入策略网关控制面板，设置策略网关代理 IP，点击“保存”。



- 3、打开 Internet 服务管理器，右击“默认 Web 站点”，打开“属性”配置。
- 4、在 ISAPI 筛选器属性页下，增加一个筛选器。



5、为筛选器输入一个名称，可执行文件为

“WINNT\System32\Inetsrv\filter\isawebfilter.dll”。

6、重新启动 IIS 控制服务和 World Wide Web 服务，插件就已经生效。

7、参考 [《应用准入-配置要点》](#)。

6.3.6. ISA 策略网关安装配置要点

- 1、天珣内网安全风险管理与审计系统提供分别适用于 ISA2000 和 ISA2004 的两种策略网关。
- 2、请点击“安装 ISA 策略网关”，进入安装 ISA 策略网关的选择界面。



- 3、运行相应的 ISA 插件策略网关的 Setup 程序，一步步按照提示进行安装。
- 4、点击“安装 ISA 防火墙插件”，注册 ISA 防火墙插件。



- 5、如果插件注册时报告错误，主要可能的原因是注册进程的权限不能满足管理 ISA Server 的需要导致。可先尝试在插件安装目录（ISA 安装目录\Filters）下运行

```
Regsvr32 /i:array ISAAPPFilter.dll
```

- 6、如果还是出现错误，尝试打开 ISA 管理控制台，看当前用户是否可以修改 ISA 配置。
- 7、点击“安装 ISA 代理插件”，注册 ISA 代理插件。



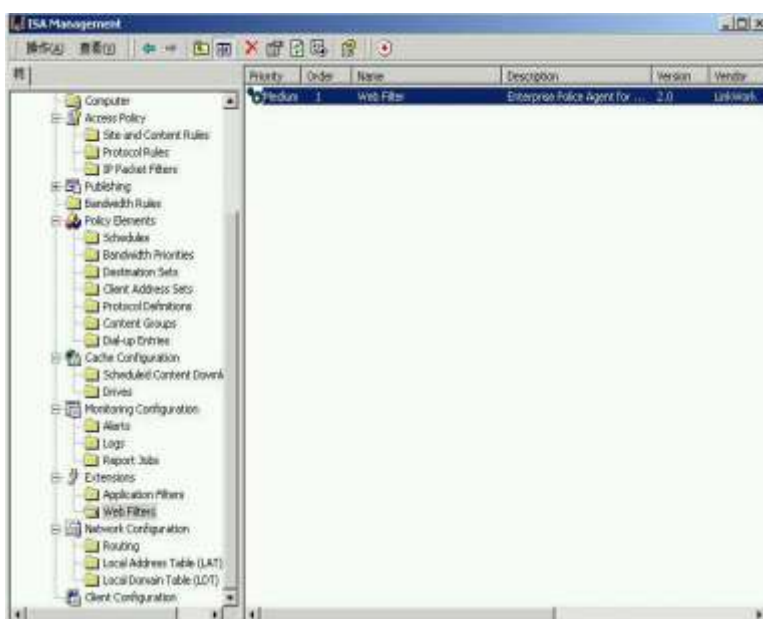
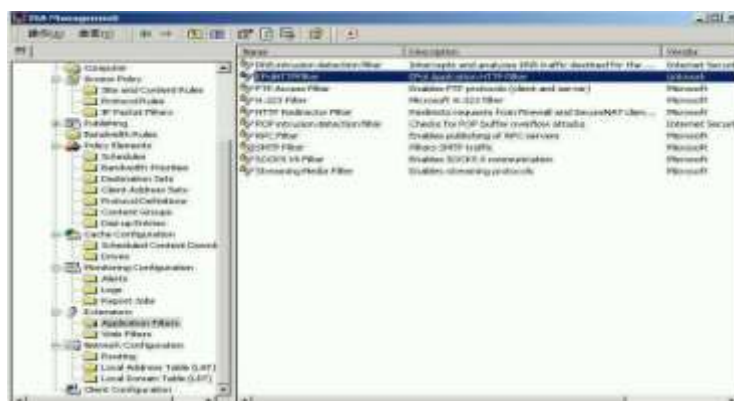
- 8、如果插件注册时报告错误，主要可能的原因是注册进程的权限不能满足管理 ISA Server 的需要导致。可先尝试在插件安装目录（ISA 安装目录\Filters）下运行

```
Regsvr32 ISAWebFilter.dll
```

- 9、如果还是出现错误，尝试打开 ISA 管理控制台，看当前用户是否可以修改 ISA 配置。
- 10、在 ISA 插件安装目录下有一个 ISAWebFilter.ini 文件，通过该文件可以配置当用户通过 WebProxy 访问某些站点时不需

要检查客户端是否满足要求。

- 11、 重新启动 ISA 的 WebProxy 服务和 Firwall 服务，插件就开始运行。如果插件启动时策略网关代理没有运行导致插件取不到规则，插件会每隔 30s 重新连接策略网关代理。
- 12、 完成安装注册后，请进入 ISA 控制器，检查在 Extensions 选项下的 Application Filters 中的 EPolHTTPFilter 以及 Web Filters 中的 Web Filter 是否正常启动，如正常则 ISA 策略网关安装注册成功。



- 13、 如要卸载插件，点击“卸载 ISA 防火墙插件”或“卸载 ISA 代理插件”。
- 14、 参考[《应用准入-配置要点》](#)。

6.3.7. Exchange 策略网关安装配置要点

- 1、请点击“安装 Exchange 策略网关”运行 Exchange 插件策略网关的 Setup 程序，一步步按照提示进行安装。



- 2、安装完成点击进入策略网关控制面板

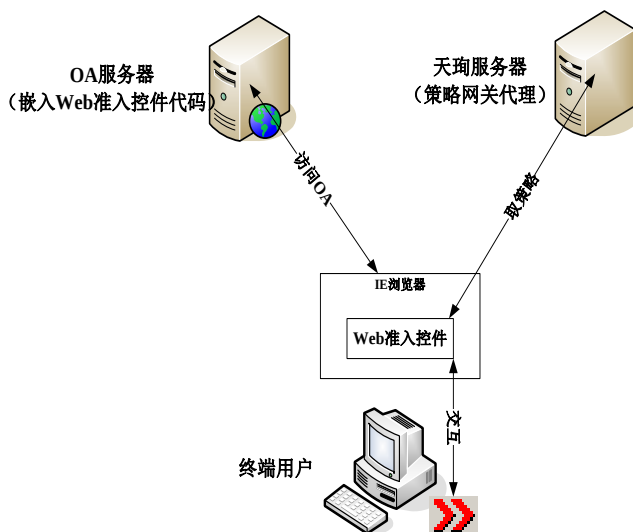


- 3、点击“安装 SMTP 邮件插件”，注册邮件插件。



- 4、为该插件配置合适的插件规则，重新启动 Exchange 服务，插件就已经生效。
- 5、安装注册完成后，请点击“开始”→“程序”→“Venus”→“邮件插件策略网关”→“邮件插件状态查看”，若状态为“激活”则表明 Exchange 策略网关安装配置成功。
- 6、如要卸载插件，点击“卸载 SMTP 邮件插件”即可。
- 7、参考[《应用准入-配置要点》](#)。

6.3.8. Web 准入安装配置要点



- 1、在 web 页面源代码中嵌入天珣 activex 控件代码，以 asp 为例：

```
<form action="index.asp" method="post">
```

```
username:
```

```
<SCRIPT language=javascript>
```

```
function DetectWebCheckerActiveX(){
    try
    {
        var comActiveX = new
ActiveXObject("WebChecker.WebCheckerTextbox.1");
    }
    catch(e)
    {
        return false;
    }
    return true;
};

if(DetectWebCheckerActiveX()==true){
document.write('<OBJECT id=WebCheckerTextbox
codeBase=http://172.25.9.11:8833/Download/WebChecker.cab#versio
n=1,0,0,1
classid=CLSID:51EA9310-CE77-4D0F-99FF-6CD8017AFBC4><PA
RAM NAME="ProxyIP" VALUE="172.25.9.11"><PARAM
NAME="width" VALUE="4000"><PARAM NAME="height"
VALUE="500"></OBJECT>');
}
else{
    document.write('<a
href="http://172.25.9.11:8833/Download/WebChecker.exe">请点此下
载控件</a>');
}

function GetText(){
    var data;
    data=document.getElementById("WebCheckerTextbox").GetTextValue
();
}
```

```
document.getElementById("UserName").value    = data;

}

</SCRIPT>

<br />

usercode:

<input type="text" name="Code"/>

<br />

<input type="hidden" name=wd id="UserName" value="dhhh"/>

<input type="submit" value="提交"  onclick="GetText()"/>

</form>

<%

Response.Write(Request.Form)

%>
```

- 2、 没有安装 web 准入控件的终端访问此服务器时，会提示下载并安装控件：



- 3、 点击“请点此下载控件”，下载安装控件即可：



4、安装完成后将正确显示登录界面：



5、正常登录后，如果终端本身没有运行天珣客户端，则在访问页面时会弹出跳转提示页面要求用户安装天珣客户端；如果安装了天珣客户端但安全基线不满足要求的话，则会在登录框中提示终端不合规：



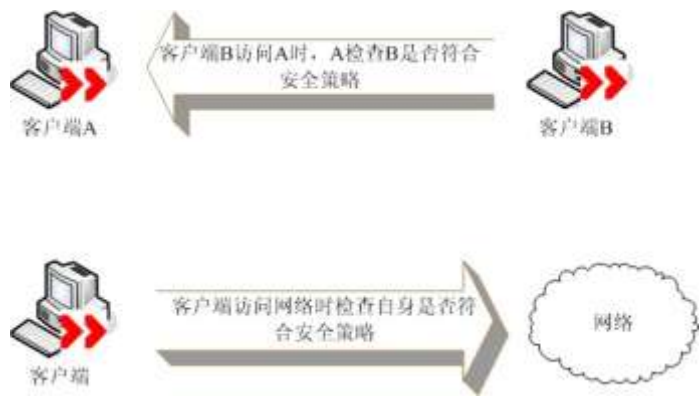
6.4. 客户端准入

6.4.1. 关于客户端准入

- 客户端准入有两层含义：一是接收到访问请求时，检查对方是否安装天珣客户端，同时检查自己是否符合安全策略；二是客户端访问网络时，要检查自己的安全状态是否符合策略。
- 客户端准入启用时注意将无法安装天珣客户端的终端做例外排除。例如：远端网段为同一子网时，同一个子网内的网络打印机、交换机、Linux 服务器等。远端网段为全部管理网段时，全部管理网段内的 web 服务器、dns 服务器、OA 服务器等等。
- 在启用了客户端准入控制的终端上，点击防火墙对话框的“查看全局策略设置”，可以明确查看客户端准入控制策略，而且该策略前有明确的标识为客户端准入策略，以方便管理员日常管理。
- 客户端准入的准入类型为连出时，远端网段为所有地址。启用后的效果为：“满足安全基线时放行，不满足时拒绝并给出提示”。

说明：来访的终端的安全状态是由来访终端自己检查的，如果不符合安全策略客户端将自动拦截访问连出。但实际的效果等同于客户端 A 检查了客户端 B 的安全策略是否满足。

下图是客户端准入控制示意图。



名词解释

客户端准入：安装有天珣客户端的终端发出的 IP 包将具有天珣特征标志。对端客户端接受到该 IP 包时如果发现该 IP 包没有天珣特征标志，则拒绝接受该包。实际的效果为未安装天珣客户端的电脑将无法访问已安装天珣客户端的终端。

建议：客户端准入连入检查的范围一般为同一子网。

6.4.2. 客户端准入页面

配置介绍

客户端准入				
客户端准入				
设备名称	策略描述	回连入是否准入	回连出是否准入	策略网络类型
同一子网内所有设备系统内客户端软件允许访问策略	配置策略：同一子网内所有设备系统内客户端软件允许访问策略。否则本机网络访问将不予响应。注意仅对TCP/UDP协议。	是	否	同一子网
本设备系统内安全策略允许访问策略	配置策略：本机系统内安全策略允许访问策略。系统才允许访问单位内部网络。否则本机网络访问将不予响应。注意仅对TCP/UDP协议。	否	是	全网管理网络

客户端准入

客户端准入

策略名称: 同一子网的其他电脑运行客户端软件才允许*

策略描述: 预置策略。同一子网的其他电脑运行客户端软件才允许访问本机，否则本机将对对方的访问不予响应。注意仅限TCP/UDP协议。

准入类型: ☒ 连入 (远端网段的电脑运行客户端软件且本端满足安全状态才允许连入) ☐ 连出 (本端电脑满足安全状态才允许访问远端网段)

远端网段: ☒ 同一子网 ☐ 全部管理网段

例外的IP地址:

生效时间: ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-02-10 2:00	2012-03-10 13:30		添加

在线模式: ☒ 在线时生效 ☐ 离线时生效

策略应用对象: (还没有应用到任何对象) [查看及编辑](#)

创建类型: 全局

创建者: jing

注: 右边有*号的项目必须输入。

保存 删除 取消

配置项:	说明
策略名称	用以标示策略，方便管理。例如：财务部客户端准入（连入）
策略描述	财务部终端只允许接受安装天珣客户端的终端访问。
准入类型	准入类型分连入和连出两个方向。如果选择连入，则天珣客户端对连入的访问确认是否可信，如果连入终端未安装天珣客户端或者受访终端不满足安全基线时，则将被拒绝访问。如果选择连出，则本地访问网络时客户端检查本机安全基线如果安全基线符合策略，允许访问；如果安全基线不符合策略，拒绝访问并提示。
远端网段	同一子网指天珣客户端仅检查远端网段属于同一子网的终端是否有安装天珣客户端，对于子网外的访问一律放开，例如：服务器区的 dns、dhcp 广播信息等。建议客户端准入选择此模式。该模式下远端网段例外排除的 IP 地址将容易配置；

	全部管理网段指对策略服务器配置的所有管理网段内均启用客户端检查。该种模式的客户端检查需要跨越子网，因此需要例外排除的 IP 地址将需要详细进行配置。 远端网段默认是同一子网。
远端网段例外的 IP 地址	在客户端检查子网范围内对指定的 IP 地址作例外排除，需要排除的 IP 地址包括：网络打印机、无法安装天珣客户端的终端、DNS 服务器等。
在线模式	客户端准入仅在天珣客户端在线时生效，不存在离线模式。此处不可选择。
策略应用对象	选择哪些 IP 组，工作组或主机名的终端需要启用客户端准入。

注意：客户端准入检查的网络访问行为是所有的 tcp/udp 网络行为，但不包括天珣策略系统端口。

注意：另外，天珣防火墙特有的机制决定了启用客户端准入时，对已经建立的网络连接将仍保存放行。

配置要点

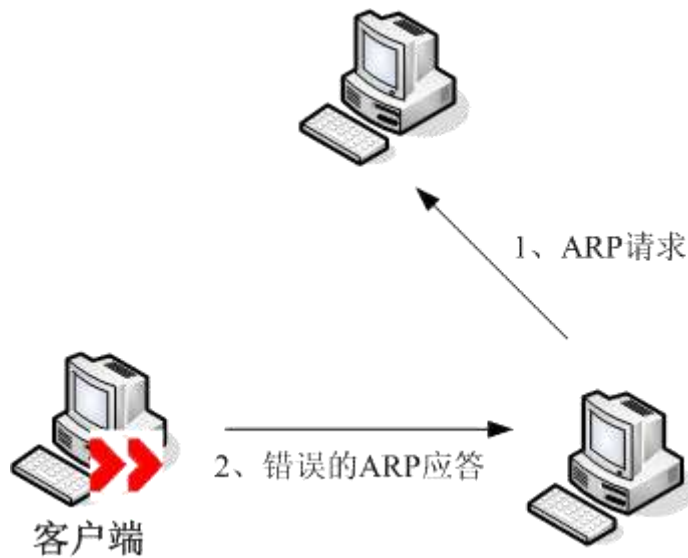
- 1、点击“**添加客户端准入**”建立连入策略；
- 2、准入类型选择“**连入（远端网段的电脑须运行客户端软件才允许连入）**”，“远端网段”选择“**同一子网**”；
- 3、排除该子网内的**网络打印机、网络复印机**等 IP 地址；
- 4、点击“**策略应用对象**”“**查看及编辑**”超链接，选择应用类型及终端，保存退出；
- 5、点击添加“**客户端准入**”，建立连出策略；
- 6、准入类型选择“**连出（远端网段的电脑须运行客户端软件才允**

- 许连出)”，“远端网段”选择“全部管理网段”；
- 7、排除杀毒软件服务器、补丁服务器、安全修复下载服务器等 IP 地址；
 - 8、点击“策略应用对象”“查看及编辑”超链接，选择应用类型及终端，保存退出。

6.5. ARP 准入

6.5.1. 关于 ARP 准入

- ARP 准入，是由受控的终端使用异常的 ARP 数据包，阻断和干扰非受控的终端的网络连接，从而达到终端网络准入控制的目的。
- 为了使 ARP 准入生效，在 1 个 IP 子网内，至少要在 1 台终端上安装天珣客户端（受控终端）。
- 未安装天珣客户端的终端（非受控终端）发出的 ARP 请求，将会收到受控终端发出的异常的 ARP 应答包，从而使非受控终端与其他终端不能正常通信。对于已安装天珣客户端的终端（受控终端）发出的 ARP 包，其他受控终端不发异常 ARP 应答包。
- ARP 准入是基于网段启用的，您必须为每个子网（广播域）配置一条 ARP 准入规则。



6.5.2. ARP 准入页面

配置介绍

ARP准入

ARP准入

子网:
子网掩码:
网关1的IP地址:
网关2的IP地址:
不限制MAC地址:
格式: AA-BB-CC-DD-EF-FF

是否启用ARP准入:
否 是

保存 取消

配置项:	说明
子网	启用 ARP 准入的子网的网络地址，比如 192. 168. 100. 0。
子网掩码	子网对应的子网掩码，比如 255. 255. 255. 0。
网关 1 的 IP 地址	无论网关是否安装了客户端，受控终端始终不对其实施 ARP 欺骗。可以设置两个网关地址。

网关 2 的 IP 地址	无论网关是否安装了客户端，受控终端始终不对其实施 ARP 欺骗。可以设置两个网关地址。
不限制的 MAC 地址	无论这些 MAC 地址对应的终端是否安装了客户端，受控终端始终不对其实施 ARP 欺骗。

注意：因天珣客户端不会对默认网关回应错误的应答，所以不会影响受控终端访问网关。这样也带来了非受控终端在一定的时间段内是可以访问外网的现象。反之，如果发现网络中默认网关有多个 MAC 地址，（而这些 MAC 地址不是网关设备的特殊配置），网络可能存在 ARP 欺骗，这种欺骗行为不属于天珣客户端准入行为。如果某终端被 ARP 欺骗，而该终端没有任何错误应答包，则该欺骗不是天珣客户端的准入行为。

注意：开启 ARP 准入需要特别谨慎，建议仅作为其他准入方式的一种补充。

配置要点

- 1、输入子网号，例如：192.168.0.0；
- 2、输入子网掩码，如：255.255.255.0；
- 3、输入网关 1 的 IP 地址，如：192.168.0.1；
- 4、排除网络打印机的 MAC 地址或其他重要的服务器地址；
- 5、保存，客户端更新策略，ARP 准入策略生效。

7. 安全防护

7.1. 关于安全防护

- 通过天珣内置的进程级访问控制内核,可以实现针对终端基于进程、端口或协议的双向访问的最细粒度的访问控制;有效管理终端带宽,并通过监控 TCP 及 UDP 的连接,对异常流量进行控制,对 ARP 欺骗进行有效的控制。
- **服务:** 服务即终端机器的端口或协议,管理员可针对服务类型(端口和协议)配置有效的访问控制策略。
- **服务组:** 多个服务的集合。
- **服务器地址:** 可以添加一个远端访问的服务器 IP 地址。
- **自定义网段:** 用户可以自定义一个远端访问的 IP 网段。
- **访问控制:** 对客户端的连入和连出访问进行控制,可控制客户端只能访问许可的地址,只能访问许可的服务,只能由指定的程序访问等。可针对进程、端口及协议进行详细的订制。
- **流量控制:** 利用分布式带宽管理每个终端上的每个应用程序,每个端口的流量和带宽。通过合理配置,能有效管理终端的异常流量,即使出现突发状况,也能保证网络正常业务访问。
- **攻击防护:** 通过对终端 TCP 和 UDP 的连接及发包数量的监控,保护终端不受攻击,并通过监控 ARP 请求和应答,防止内网 ARP 欺骗的发生。
- **PING 控制:** 对客户端的 ping 出和被 ping 进行控制
- **访客策略:** 对于任何网络准入类型(标准 802.1X 和漫游网段的 802.1X),如果基本认证的认证方式为可匿名的用户认证,则在登录成功后获取防火墙访客策略。此时可设置访客策略为最小访问权限,保证内网安全。

7.2. 协议端口设定

7.2.1. 配置介绍

协议端口设定是服务、服务组及服务器地址和自定义网段的一个集合。通过这些定义的配置增加策略设置的灵活性。

服务

服务是 TCP/IP 的协议和端口的组合，比如 SMTP 服务是 TCP 协议和 25 端口的组合，DNS (UDP) 协议是 UDP 协议和 53 端口的组合。系统安装时已经配置了最基本的一些服务。

点击“服务”，系统显示目前已经配置的服务（包括预置的服务）。

服务

服务组

服务器地址

自定义网段

Service

添加

名称: 端口:

查询

[帮助](#)

Service名称	协议	端口
不限	不限	不限
echo(7)	不限	7
discard(9)	不限	9
sysstat(11)	不限	11
daytime(13)	不限	13
gotd(17)	不限	17
chargen(19)	不限	19
ftp-data(20)	TCP	20
ftp(21)	TCP	21
ssh(22)	TCP	22
telnet(23)	TCP	23
smtp(25)	TCP	25
time(37)	不限	37
rlp(39)	UDP	39
nameserver(42)	不限	42
nicname(43)	TCP	43
domain(53)	不限	53
bootps(67)	UDP	67
bootpc(68)	UDP	68
tftp(69)	UDP	69

1 2 3 4 5 6 7 8 9

可以通过输入协议名称和端口来进行已配置服务的查询。

点击“添加”

服务

服务组

服务器地址

自定义网段

Service

Service名称

smtp (25) *

协议

TCP *

端口

25

0表示不限端口号 *

所属服务组

网上邻居服务组

->

<-

注：右边有*号的项目必须输入。

保存

删除

取消

配置项:	说明
Service 名称	填入需要保护服务的名称或应用程序的名称。
协议	根据该服务使用的协议来选择。
端口	填写该服务调用的端口号。
所属服务组	如果定义了服务组，可将此服务添加到该服务组。

“服务组”的设置请参照“协议端口设定” – “服务组”

服务组

服务组是服务的组合，比如用户可将上网所需服务加入至一个组合，在配置“访问控制”策略时只需添加一个服务组即可。

点击“服务组”，系统显示目前已经配置的服务组。

服务

服务组

服务器地址

自定义网段

服务组

添加

组名称

已加入的服务

网上邻居服务组

qqsp (135), netbios-ss (137), netbios-dgm (138), netbios-ssn (139), microsoft-ds (445)

点击“添加”

服务

服务组

服务器地址

自定义网段

服务组

服务组名称

服务组描述

服务

注：右边有*号的项目必须输入。

保存

删除

取消

配置项：	说明
服务组名称	自定义服务组的名称。
服务组描述	对该服务组的详细说明，如应用场合、哪些应用系统等。
服务	将此服务组需要用到的服务移到右边的方框中。

服务器地址

定义网络中需要被访问的服务器。在访问控制策略中可以设置对此服务器访问控制。

点击“服务器地址”标签中的“添加”

服务

服务组

服务器地址

自定义网段

服务器地址

帮助

服务器名称

IP地址

描述

注：右边有*号的项目必须输入。

保存

取消

配置项：	说明
服务器名称	填入可区分的服务器名称。
IP 地址	填入该服务器准确的 IP 地址。

描述	填入该服务器的详细信息。
----	--------------

自定义网段

作为 IP 组的补充，定义被访问的网段。

点击“自定义网段”标签的“添加”



自定义网段配置界面。顶部有四个标签：服务、服务组、服务器地址、自定义网段（当前选中）。下方是配置区域，包含以下字段：

- 网段名称：文本输入框，右侧有*号。
- 开始IP地址：文本输入框，右侧有*号。
- 结束IP地址：文本输入框，右侧有*号。
- 描述：多行文本输入框。

底部有提示文字：“注：右边有*号的项目必须输入。”以及两个按钮：“保存”和“取消”。

配置项：	说明
网段名称	填入有别于其他网段的名称。
开始 IP 地址	自定义网段的起始地址。
结束 IP 地址	自定义网段的结束地址。
描述	对网段的具体描述

7.3. 防护策略

7.3.1. 配置介绍

管理员在此集中配置防护策略，包括：访问控制策略、流量控制策略、攻击防护策略和 ping 控制策略。

访问控制

对客户端的连入连出网络访问进行控制，点击“访问控制”，系统显示预设的防火墙规则。

策略名称	策略描述	方向	操作类型	在线状态	策略生效
防止非法地址访问网上资源		流出	放行	✓	✓
防止安全策略阻止访问重要资源地址		流出	安全状态策略放行，不成立时策略提示，然后不放行	✓	✓
防止非法地址访问网上资源		流出	不放行	✓	✓
防止非法地址访问		流出	放行	✓	✓
安全策略阻止访问非法地址	策略描述：安全策略阻止访问非法地址。当安全策略阻止访问非法地址时，系统会提示用户，然后不放行。	流出	安全状态策略放行，不成立时策略提示，然后不放行	✓	
安全策略阻止访问非法地址	策略描述：安全策略阻止访问非法地址。当安全策略阻止访问非法地址时，系统会提示用户，然后不放行。	流出	安全状态策略放行，不成立时策略提示，然后不放行	✓	
安全策略阻止访问非法地址	策略描述：安全策略阻止访问非法地址。当安全策略阻止访问非法地址时，系统会提示用户，然后不放行。	流出	安全状态策略放行，不成立时策略提示，然后不放行	✓	
防止非法地址访问网上资源	策略描述：防止非法地址访问网上资源。当非法地址访问网上资源时，系统会提示用户，然后不放行。	流入	放行	✓	
防止非法地址访问网上资源	策略描述：防止非法地址访问网上资源。当非法地址访问网上资源时，系统会提示用户，然后不放行。	流入	不放行	✓	
防止非法地址访问网上资源	策略描述：防止非法地址访问网上资源。当非法地址访问网上资源时，系统会提示用户，然后不放行。	流入	不放行	✓	✓

点击“添加”按钮，进入添加“访问控制策略”。

访问控制
流量控制
攻击防护
PING控制

访问控制

策略名称:

策略描述:

方向:

远端网段:

子网掩码位数: 24 (有效范围为1~31)

以下网段或服务器:

编辑

服务:

编辑

服务组:

编辑

操作类型: *****选择操作类型*****

访问进程:

不记录完整路径, 多个进程用"/"隔开

记录日志方式:

拒绝访问的个性化提示信息:

(不能超过255个字符)

在线模式: ☒ 在线生效 ☐ 离线生效

策略应用对象: (还没有应用到任何对象) [查看及编辑](#)

所属分组:

创建状态: 全局

创建者: jing

说明: 右边有*号的项目必须输入

保存 取消

配置项:	说明
策略名称	填入策略名称。
策略描述	填入策略的详细描述。
方向	设定此策略控制的访问方向
远端网段	本系统无需设置本端地址,本地地址总是客户端自身的 IP 地址。远端网段可以按以下 3 种方式设置。 1、不限: 远端地址为任意地址 2、同一子网-子网掩码数: 如果填入相应的掩码数,则根据掩码数计算子网地址 3、以下网段或服务器: 选择相应的目标网段或服务器。
服务	选择此策略需要控制的服务。
服务组	选择此策略需要控制的服务组。
操作类型	共有 5 种类型: 1、放行。对匹配本条策略的网络访问放行,对用户没有任何提示。 2、不放行。对匹配本条策略的网络访问不放行,对用户没有任何提示。 3、安全基线完整时放行。对于匹配本条策略的网络访问,如果客户端的安全基线合格就放行,不合格不放行,对用户没有任何提示。 4、安全基线完整时放行,不满足时给出提示,然后放行。对于匹配本条策略的网络访问,无论客户端的安全基线是否合格,都放行,但对安全基线不合格的电脑弹出提示窗口。 5、安全基线完整时放行,不满足时给出提示,然后不放行。对于匹配本条策略的网络访问,如果客

	户端的安全基线合格就放行，不合格不放行，并对安全基线不合格的电脑弹出提示窗口。
访问进程	填入需要匹配的进程名称，不包含完整路径，多个进程用‘ / ’ 隔开，也可从已定义的白名单中获取。若不填，则不对进程进行匹配。
记入日志方式	连接日志记录在客户端防火墙日志里面，可以根据需要选择何种方式记入日志。主要有以下几种方式：“不记入日志”、“被策略允许时记入日志”、“被策略拒绝时记入日志”、“总是记入日志”。
拒绝访问时的个性化信息	当防火墙拦截客户端的数据访问时，给出特别的提示，可自定义。
在线模式	配置在线和离线时是否生效
策略应用对象	将此策略应用到 IP 组，工作组，主机名或用户组
所属分组	在策略浏览时能够按照分组显示。 系统安装时自动创建一个名为“默认分组”的组名。 或可以自行创建分组，名称另行定义

注意:多条访问控制策略应用到同一个 IP 组或用户组时，这些策略的匹配是分先后顺序的，可通过上下箭头来调整顺序，类似路由 ACL。

流量控制

流量控制规则精细控制每个用户电脑中的每个进程访问网络中不同的网段和主机时所能占用的带宽。良好的流量控制规则能在蠕虫病毒爆发时自动遏制其占用的网络带宽，始终保持网络通畅。

点击“添加”

访问控制 流量控制 攻击防护 PING控制

流量控制

策略名称:

策略描述:

控制类型:

协议:

带宽: KB/s ☐ 不限制带宽 ☐ 不记入总流量

远端IP范围:

远端端口:

记入日志方式:

生效时间: ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间: 结束时间:

在线模式: ☒ 在线时生效 ☒ 离线时生效

策略应用对象: [查看及编辑](#)

创建类型: 全局

创建者: jing

注: 右边有*号的项目必须输入。

配置项:	说明
策略名称	填入流量策略的名称。
控制类型	共有 3 种控制类型: 按远端端口, 按本端端口, 按进程。
按远端端口统计	
协议	选择远端端口的协议类型
带宽	填入允许的最大流量值, 单位是 KB/S 或%。KB/S 表示采用带宽绝对值, %表示使用网卡带宽的百分比。 不限制带宽表示对此类流量不进行管理和控制。 不记入总流量, 如果在“基本配置”里设定了客户端总带宽, 而在此设置“不记入总流量”, 则此类流量不统计在总流量中, 即此类流量只

	受此处设置的影响，而不受终端总带宽的影响。
远端 IP 范围	填入远端 IP 的起始和结束地址，若地址不限请点击“ 整个网络 ”。开始和结束地址都为 0 表示整个网络。
描述	填入此规则的详细描述。
远端端口	填入需要控制的远端端口号。
按本地端口统计	
协议	选择本地端口的协议类型
带宽	填入允许的最大流量值，单位是 KB/S 或%。KB/S 表示采用带宽绝对值，%表示使用网卡带宽的百分比。 不限制带宽表示对此类流量不进行管理和控制。 不记入总流量，如果在“基本配置”里设定了客户端总带宽，而在此设置“不记入总流量”，则此类流量不统计在总流量中，即此类流量只受此处设置的影响，而不受终端总带宽的影响。
远端 IP 范围	填入远端 IP 的起始和结束地址，若地址不限请点击“ 整个网络 ”。开始和结束地址都为 0 表示整个网络。
描述	填入此规则的详细描述。
本地端口	填入需要控制的本地端口号
按应用程序统计	
协议	选择本地端口的协议类型
带宽	填入允许的最大流量值，单位是 KB/S 或%。KB/S 表示采用带宽绝对值，%表示使用网卡带宽的百

	分比。 不限制带宽表示对此类流量不进行管理和控制。 不记入总流量，如果在“基本配置”里设定了客户端总带宽，而在此设置“不记入总流量”，则此类流量不统计在总流量中，即此类流量只受此处设置的影响，而不受终端总带宽的影响。
远端 IP 范围	填入远端 IP 的起始和结束地址，若地址不限请点击“整个网络”。开始和结束地址都为 0 表示整个网络。
描述	填入此规则的详细描述。
进程名	填入需要控制流量的进程名，不包含完整路径，多个进程用“/”隔开。也可点击“获取白名单进程”从白名单列表中添加进程。
记入日志方式	主要有两种方式：“不记入日志”和“总是记入日志”。生成的日志记录在客户端防火墙日志里面。
在线模式	配置在线和离线时是否生效
策略应用对象	将此策略应用到 IP 组，工作组，主机名或用户组

攻击防护

攻击防护阻止终端发送欺骗包或攻击包以及未知的流量攻击包，确保内网正常运行。在此可添加防 ARP 欺骗、防 IP 仿冒等功能。

点击“添加”

访问控制

流量控制

攻击防护

PING控制

策略名称

test

启用ARP欺骗防护

同时过滤发送和接收的ARP包

启用ARP请求超时报警

是 否

启用网卡MAC自动绑定

是 否

限制隐藏进程访问网络

是 否

过滤IP伪造数据包

是 否

TCF相关 (0表示不限制)

每进程对外TCF并发连接数限制

高阈值10 限制阈值0

每进程每秒对外TCF并发连接数限制

高阈值10 限制阈值0

无TCF限制的进程

添加进程

删除进程

UDP相关 (0表示不限制)

每进程每秒发送UDP包数

高阈值10 限制阈值0

每进程每秒发送UDP包目标地址数

高阈值10 限制阈值0

每秒发送UDP包总数

高阈值10 限制阈值0

UDP限制时长 (秒)

60 00表示使用默认时间间隔60秒

无UDP限制的进程

添加进程

删除进程

记入日志方式

不记入日志

生效时间

所有时间 工作时间 非工作时间 以下时间段

开始时间 结束时间 编辑 删除

2012-03-10 9:00 2012-03-10 13:30 添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存 取消

配置项:	说明
策略名称	填入攻击防护策略称。
启用 ARP 欺骗防护	共有 4 个选项： 1、不启用。 2、过滤发送的 ARP 包。对发送的 ARP 包进行检查，如果发现欺骗行为，则 ARP 包被丢弃。 3、过滤的 ARP 包。对接收的 ARP 包进行检查，如果发现欺骗行为，则 ARP 包被丢弃。 4、过滤发送和接收的 ARP 包。对发生和接收的 ARP 包都进行检查，如果发现欺骗行为，则

	ARP 包被丢弃。
启用 ARP 请求超时拒答	若选择启用，客户端发送 ARP 请求后如果 5 秒内没有应答包，后面的收到的应答包将被丢弃。
启用网关 MAC 自动绑定	若选择启用，客户端在线状态下自动绑定当前网关的 MAC 地址，而对从网络上接收到的关于网关的 ARP 包不进行处理。客户端在离线状态下自动解除绑定。
限制隐藏进程网络访问	若选择启用，则拦截隐藏进程的网络访问。有些木马程序在 Windows 任务管理器中是看不到的。此选项只有在“访问控制”的日志选项为“记入日志”时才有效。
过滤 IP 仿冒数据包	客户端发包时如果 IP 包的源 IP 地址与自身的 IP 地址不相符，则被认为是 IP 仿冒行为。若选择启用，系统将拦截仿冒的 IP 包。
TCP 相关	设定阈值限制客户端的 TCP 连接行为。在 TCP 相关的设置中，如果数值为 0，则表示对该项目不限制。
每进程对外 TCP 并发连接数限制	系统对每个进程的 TCP 连接进行监控和统计，当一个进程的并发连接数（保持的连接数）超过设定的阈值后，将被限制或告警。建议根据网络的实际情况进行调整、优化。
每进程每秒对外 TCP 并发连接数限制	系统对每个进程的 TCP 连接进行监控和统计，当一个进程的每秒并发连接数（每秒新发起的连接数）超过设定的阈值后，将被限制或告警。建议根据网络的实际情况进行调整、优化。
无 TCP 限制的进程	设置无 TCP 连接数限制的进程，如某些业务进程。

UDP 相关	设定阈值限制客户端的 UDP 发包行为。在 UDP 相关的设置中，如果数值为 0，则表示对该项目不限制。
每进程每秒发送 UDP 包数	系统对每个进程的 UDP 连接进行监控和统计，当一个进程的每秒 UDP 发包数超过设定的阈值后，将被限制或告警。建议根据网络的实际情况进行调整、优化。
每进程每秒发送 UDP 包目标地址数	系统对每个进程的 UDP 连接进行监控和统计，当一个进程的每秒发送 UDP 包的目标地址数超过设定的阈值后，将被限制或告警。建议根据网络的实际情况进行调整、优化。
每秒发送 UDP 包总数	当客户端所有进程发送 UDP 包数超出阈值时，将被限制或告警。建议根据网络的实际情况进行调整、优化。
UDP 限制时长(秒)	当 UDP 发包行为超出限制阈值时，系统将对进程继续发包禁止一段时间，在这里设置这个禁止发包的时间长度。如果是“每秒发送 UDP 包总数”超过限制阈值，则任何进程的 UDP 的发包行为都会被禁止。
无 UDP 限制的进程	设置无 UDP 发送数限制的进程，如某些业务进程。
记入日志方式	主要有两种方式：“不记入日志”和“总是记入日志”。生产的日志记录在客户端防火墙日志里面。
在线模式	配置在线和离线时是否生效
策略应用对象	将此策略应用到 IP 组，工作组，主机名或用户组

注意：当达到告警阈值时，天珣客户端图标将变黄，发出告警，同时在客户端日志中可查看到告警日志。

PING 控制

Ping 控制指的是对客户端的 ICMP 协议进行控制，可控制其 ping 出或者是被 ping。

点击“添加”

访问控制

流量控制

攻击防护

PING控制

PING控制

策略名称

策略描述

允许PING出

允许被PING

记入日志方式

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边有*号的项目必须输入。

保存

取消

配置项：	说明
策略名称	填入策略名称。
策略描述	填入策略的详细描述。
允许 PING 出	设定是否允许 PING 出
允许被 PING	设定是否允许被 PING
记入日志方式	主要有两种方式：“不记入日志”和“总是记入日志”。 生成的日志记录在客户端防火墙日志里面。
在线模式	配置在线和离线时是否生效

策略应用对象	将此策略应用到 IP 组，工作组，主机名或用户组
--------	--------------------------

7.3.2. 配置要点

1. 点击“访问控制”中的“添加”按钮，输入策略名称为“安全基线不满足，http 访问提示并不放行！”
2. “方向”选择为“连出”
3. “远端网段”选择“不限”
4. 点击“服务”的“编辑”按钮，进入后选择“http(80)协议 TCP 端口 80”
5. “操作类型”选择“安全基线完整时放行，不完整时给出提示，然后不放行”
6. “记入日志方式”选择“被策略拒绝时记入日志”
7. “在线模式”选择“在线时生效”
8. 点击“策略应用对象”的“查看及编辑”按钮，选择应用对象类型及终端，“确定”然后“保存”
9. 点击“流量控制”中的“添加”按钮，输入策略名称为“限制 HTTP 带宽”
10. “控制类型”为“按远端端口统计”，协议为“不限”
11. “带宽”设置为 50KB/S，远端 IP 范围选择“整个网络”
12. “远端端口”设为 80
13. 选择“在线时生效”，并点击“策略应用对象”的“查看及编辑”按钮，选择应用对象类型及终端，“确定”然后“保存”
14. 点击“攻击防护”中的“添加”按钮，输入“策略名称”为“攻击防护策略”
15. “启用 ARP 欺骗防护”选择“同时处理发送和接收的 ARP 包”
16. “启用网关 MAC 自动绑定”选择“是”，“过滤 IP 仿冒数据包”选择“是”

17. “每进程对外 TCP 并发连接数限制”中的“告警阈值”设为 70，“限制阈值”为 100
18. “每进程每秒对外 TCP 并发连接数限制”中的“告警阈值”设为 70，“限制阈值”为 100
19. 选择“在线时生效”，点击“策略应用对象”的“查看及编辑”按钮，选择应用对象类型及终端，“确定”然后“保存”
20. 策略配置好后，属于“防火墙组”的终端在安全基线不满足要求的情况下，会被禁止进行 80 端口的访问，而即使能进行 80 端口访问，最大带宽也只有 50KB/S，最大限度限制了终端进行上网操作时所占用的带宽。另外启用了 ARP 欺骗防护，并限制了 TCP 的发包数，可以防止客户端发生 ARP 攻击或被攻击。

7.4. 访客策略

7.4.1. 配置介绍

网络准入中对于外来的安装了客户端的电脑，其只能使用匿名登录，那么可以获取访客策略。此策略一般定义为权限最小的访问策略。

访问控制

对于匿名登录的用户，可以用访问控制规则来限制访客的网络访问行为。一般在此只设置最必要的允许规则，最后以拒绝规则结束。

点击“添加”

访问控制 流量控制

访问控制-访客策略

策略名称

策略描述

协议

端口

远端起始IP地址

远端结束IP地址

操作类型

记入日志方式

生效时间

在线模式

策略应用对象

创建类型

创建者

来源

++++选择操作类型++++

不记入日志

所有时间

工作时间

非工作时间

以下时间段

开始时间

结束时间

编辑

删除

2012-02-10 0:00

2012-02-10 13:30

添加

☒ 在线时生效

☐ 离线时生效

(还没有应用到任何对象) [更改应用对象](#)

全部

jiang

注：右边有*号的项目必须输入。

保存

取消

配置项：	说明
策略名称	填入有别于其他访问控制规则名称。
策略描述	填入该规则的详细信息。
协议	选择访问控制的协议。
端口	访问远程机器的端口号。
远端起始 IP 地址	填入准确的 IP 地址
远端结束 IP 地址	填入准确的 IP 地址
操作类型	选择是否放行以上定义的网络访问
记入日志方式	选是否记入日志。
在线模式	配置在线和离线时是否生效
策略应用对象	将此策略应用到 IP 组，工作组，主机名或用户组

流量控制

对于匿名登录的用户，设置专门的访客流量控制规则，以防止因为它的异常运行而对网络有显著的影响。

点击“添加”

访问控制

流量控制

流量控制-访客策略

策略名称

策略描述

控制类型

按远端端口统计

协议

不限

带宽

KB/s

☐ 不限制带宽

☐ 不记入总流量

远端IP范围

整个网络

远端端口

记入日志方式

不记入日志

生效时间

☒ 所有时间

☐ 工作时间

☐ 非工作时间

☐ 以下时间组

开始时间

结束时间

编辑

删除

2012-03-10 00:00

2012-03-10 13:30

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

<还没有应用到任何对象> [查看总报表](#)

创建类型

全局

创建者

jing

注：右边带*号的项目必须输入。

保存

取消

配置项:	说明
策略名称	填入有别于其他流量控制的策略名称。
控制类型	共有两种控制类型：按远端端口控制和按本端口控制
按远端端口统计	
协议	选择远端端口的协议类型
带宽	填入允许的最大流量值，单位是 KB/S 或%。KB/S 表示采用带宽绝对值，%表示使用网卡带宽的百分比。 不限制带宽表示对此类流量不进行管理和控制。

	不记入总流量，如果在“通用控制”里设定了客户端总带宽，而在此设置“不记入总流量”，则此类流量不统计在总流量中，即此类流量只受此处设置的影响，而不受终端总带宽的影响。
远端 IP 范围	填入远端 IP 的起始和结束地址，若地址不限请点击“整个网络”。开始和结束地址都为 0 表示整个网络。
描述	填入此规则的详细描述。
远端端口	填入需要控制的远端端口号。
创建状态	全局管理员创建的规则，创建状态为全局。本地管理员创建的规则，创建状态为本地。
创建者	创建者管理员的名称
按本地端口统计	
协议	选择本地端口的类型
带宽	填入允许的最大流量值，单位是 KB/S 或%.KB/S 表示采用带宽绝对值，%表示使用网卡带宽的百分比。 不限制带宽表示对此类流量不进行管理和控制。 不记入总流量，如果在“通用控制”里设定了客户端总带宽，而在此设置“不记入总流量”，则此类流量不统计在总流量中，即此类流量只受此处设置的影响，而不受终端总带宽的影响。
远端 IP 范围	填入远端 IP 的起始和结束地址，若地址不限请点击“整个网络”。开始和结束地址都为 0 表示整个网络。

本地端口	填入需要控制的本地端口号
在线模式	配置在线和离线时是否生效
策略应用对象	将此策略应用到 IP 组，工作组，主机名或用户组

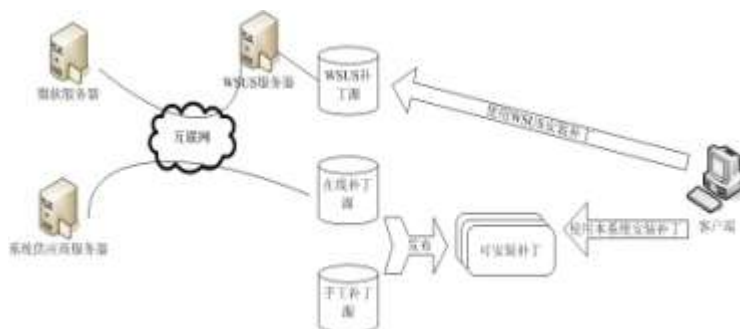
注意：访客策略只对网络准入时使用“匿名登录”的终端生效。

8. 补丁管理

8.1. 关于补丁管理

天珣“补丁管理”：是由天珣策略服务器提供的补丁管理方案，可以通过“在线补丁源”或“WSUS 补丁源”为各终端补丁修复。

三种补丁源及补丁发布安装示意图



- 天珣补丁管理分三种补丁源：在线补丁源、WSUS 补丁源和手工补丁源。
- 内网部署离线补丁是在线补丁源的一种发布模式，请参考[《配置手册-离线补丁》](#)
- 配置完补丁源并发布后，如果不使用本系统的强制安装补丁功能，请到“补丁管理”→“补丁分发”中进行补丁分发其他项目的配置和操作。
- 如果您要使用强制补丁功能，请到“安全基线”→“补丁强

制策略”中进行配置和操作。

- 天珣补丁管理系统维护的 Windows 版本包括：英文版、简体中文版和繁体中文版的操作系统。

名词解释

- **“在线补丁源”**：由天珣研发团队测试维护的补丁库，补丁源地址为：<http://patch.patchsource.cn>，其中的补丁文件来自微软官方网站，并已经经过了天珣研发团队的测试。
- **“WSUS”集成管理**：天珣客户端可代替 WSUS 客户端实现 WSUS 内网补丁分发。
- **“手工补丁源”**：可由管理员自行从微软网站下载、测试并发布到天珣“手工补丁源”，“手工补丁源”补丁发布模式和“在线补丁源”发布模式相同。

8.2. 在线补丁源

8.2.1. 关于在线补丁源

- **“在线补丁源”**按同步方式分“互联网同步”和“离线同步”两种方式。
- **“在线补丁源”**可以和 WSUS 集成管理同时使用。
- **“在线补丁源”**维护了 Windows 系统安全补丁、IE Explorer 安全更新补丁、Outlook 安全更新补丁。
- 涉及到正版验证的补丁并未发布，正版验证补丁需要用户单独确认授权许可并确认更新。
- 补丁分发默认会自动分发，支持分发前对补丁进行测试。

重点：在线补丁是由天珣补丁精灵实现补丁分发，因此支持非系统管理员自动安装补丁，支持 AD 域环境的补丁更新。

名词解释

“补丁列表”：在线补丁源获取的补丁信息和手工补丁创建的补丁信息，都包含在此列表中。列表中的补丁必须经过发布才能通过补丁管理功能向客户端分发。

“系统设置”：系统供应商在互联网上设置在线补丁源，为用户提供 Windows 操作系统安全补丁下载更新。本系统在此处配置与在线补丁源连接的相关参数，包括同步服务 URL、用户许可信息、服务参数等。

“系统控制”：补丁同步服务的控制面板，通过 WEB 与补丁同步服务通讯，执行补丁同步、查询同步状况等任务。

“同步日志”：查看补丁同步服务器的运行日志，若补丁同步任务出现问题可在此查看相关日志。

“同步状态”：查看各个补丁同步服务器同步补丁文件的状态。其中查询中心服务器显示的是从互联网上在线补丁源同步补丁的状态，查询各个本地服务器显示的是本地服务器从中心服务器同步补丁的状态。

8.2.2. 配置介绍

补丁列表页面



补丁列表

搜索：[按补丁名]

名称	来源	描述	安全公告	级别	已同步
KB930952	系统	Windows 网络名称服务 (DNS) 的漏洞可能允许执行程序代码	MS04-008	重要	是
KB930952	系统	微软 (Gasser) 补丁	MS04-011	严重	是
KB930951	系统	Microsoft Jet 数据库引擎中的漏洞可能导致代码执行	MS04-014	重要	是
KB930974	系统	帮助和支持中心的安全漏洞可能允许远程执行代码	MS04-015	重要	是
KB930956	系统	工具管理中的漏洞可能允许执行代码	MS04-019	重要	是
KB930972	系统	任务计划程序中的漏洞可能允许执行代码	MS04-022	严重	是
KB930915	系统	HTML 帮助中的漏洞可能允许执行代码	MS04-020	严重	是
KB930946	系统	Windows Shell 中的漏洞可能允许远程执行代码	MS04-024	重要	是
KB930951	系统	WebDAV 的 Message Handler 中的公告标题漏洞可能导致“拒绝服务”攻击	MS04-030	重要	是
KB930932	系统	WebDAV 中的漏洞可能允许执行代码	MS04-031	重要	是

配置项：

说明

按补丁名	按补丁名称查询某个补丁是否已经存在于天珣的补丁列表中，如查询 KB958644
按安全公告	按补丁的安全公告查询某个补丁是否已经存在于天珣的补丁列表中，如查询 MS04-031

系统设置页面



系统设置

应用配置 帮助

服务器信息

配置项	配置值
同步服务URL	http://patch.patchsource.cn
补丁文件下载根URL	http://192.168.1.16:8833/download/
补丁文件下载相对URL	AutoUpdate/
同步文件到目录 (如不使用默认配置, 输入绝对路径)	Download\AutoUpdate\

配置项:	说明
应用配置	系统下载服务配置项立即重新加载的选项。
同步服务 URL	系统供应商在互联网上设立的在线补丁源的网址，默认为 http://patch.patchsource.cn 。
补丁文件下载根 URL	与补丁文件下载相对 URL 共同组成中心服务器向本地服务器分发补丁文件的完整 URL，其指向默认为中心服务器的下载虚拟目录。
补丁文件下载相对 URL	与补丁文件下载根 URL 共同组成中心服务器向本地服务器分发补丁的完整 URL。其指向一般为中心服务器下载虚拟目录中存放补丁文件的子目录，例如 AutoUpdate。
同步文件到目录 (如不	填写中心服务器从在线补丁源下载补丁

使用默认配置，输入绝对路径)	的存放路径，默认存放于中心服务器安装目录的 Download 目录下的 AutoUpdate 目录中。可参考如下格式：Download\AutoUpdate\。如果不使用默认配置，可输入存放补丁的绝对路径。请注意，当不使用默认配置时，请确保在 IIS 设置中，中心服务器下载虚拟目录所指向的路径与此处输入的绝对路径一致。
----------------	---

服务参数	
配置项	配置值
每天启动同步时间 (HHMM)	2300
信息同步超时时间 (分钟)	30
文件同步超时时间 (分钟)	300
同步文件到所有本地同步服务器超时时间 (分钟)	300

配置项:	说明
每天启动同步时间(HHMM)	设置中心服务器每天启动从在线补丁源获取补丁更新的时间。系统默认值为“2300”，即中心服务器每天晚上 23 时自动从在线补丁源获取更新文件。
信息同步超时时间（分钟）	设置中心服务器从在线补丁源获取补丁更新信息（主要是补丁配置信息等）的超时时间。系统默认值为“30”，即启动同步任务后 30 分钟仍无法获取到补丁更新信息，则表示本次补丁配置信息同步任务超时失败。
文件同步超时时间（分钟）	设置中心服务器从在线补丁源下载补丁文件的超时时间。系统默认值为“300”，即启动同步任务后 300 分钟仍无法完成补丁文件的下载，则表示

	本次补丁文件同步任务超时失败。
同步文件到所有本地同步服务器超时时间（分钟）	设置本地服务器从中心服务器下载补丁文件的超时时间。系统默认值为“300”。

邮件通知信息

配置项	配置值
管理员接收通知邮件地址	
发送邮件服务器	
发送邮件用户名	
发送邮件密码	

配置项:	说明
管理员接收通知邮件地址	填写系统管理员接收通知邮件的地址。配置好后，系统会向该地址发送从在线补丁源更新补丁的情况报告。
发送邮件服务器	填写发送补丁更新报告邮件服务器的 IP 或 URL。系统可通过该邮件服务器，发送报告邮件。
发送邮件用户名	填写用于发送报告邮件的 Email 地址。
发送邮件密码	填写发送报告邮件的 Email 密码。

代理服务器设置

配置项	配置值
使用 HTTP 代理服务访问 Internet	否
HTTP 代理服务地址	
HTTP 代理服务端口	
HTTP 代理服务访问用户名	
HTTP 代理服务访问密码	
HTTP 代理服务认证域	

配置项:	说明
使用 HTTP 代理服务器访问 Internet	在使用 HTTP 代理服务器上上网的网络环境中，中心服务器需要通过 HTTP 代理服务器访问互联网上的在线补丁源，此选项设置为“是”。
HTTP 代理服务器地址	填写 HTTP 代理服务器的 IP 地址。
HTTP 代理服务器端口	填写 HTTP 代理服务器的端口。
HTTP 代理服务器访问用户名	设置通过 HTTP 代理服务器访问互联网的用户名。
HTTP 代理服务器访问密码	设置通过 HTTP 代理服务器访问互

	联网的用户密码。
HTTP 代理服务器认证域	设置通过 HTTP 代理服务器访问互联网所需要的域名。

系统控制页面

系统设置	系统控制	同步日志	同步状态
系统控制 帮助			
启动同步任务		开始	
查询同步任务状况		开始	
查看已连接的本地同步服务器		开始	
清空补丁记录		开始	

配置项:	说明
启动同步任务	系统默认每天 23 时自动启动从在线补丁源同步补丁的任务，管理员也可通过此按钮手工启动补丁同步任务。
查询同步任务状况	查看是否有补丁信息同步任务正在运行。
查看已连接的本地同步服务器	查看已经连接至中心服务器的本地同步服务器。
清空补丁记录	清空补丁发布列表中的所有补丁配置信息。

同步日志页面



页面显示了补丁配置库的同步状态，如果同步失败，日志将打印同步失败的原因。

同步状态页面



页面显示了各服务器补丁文件的同步状态，如果同步失败会多次尝试同步。

8.2.3. 配置要点

1. 点击“补丁管理->在线补丁源->系统控制”中“启动同步任务”的“开始”按钮;
2. 点击“在线补丁源->同步日志”，确认补丁日志中无明显的报错;

同步日志 [清空日志](#)

时间	内容
2009-9-18 15:27:36	找到147条需要删除的热修复
2009-9-18 15:27:33	病毒码更新结束
2009-9-18 15:27:33	病毒码更新文件解释完成
2009-9-18 15:27:33	正在处理病毒软件信息
2009-9-18 15:27:33	病毒码更新数据下载成功,正在处理数据...
2009-9-18 15:27:30	病毒码同步开始...
2009-9-18 15:27:30	收到同步任务启动请求,启动同步任务线程成功!
1	

3. 点击“在线补丁源->同步状态”查看补丁文件是否均“已同步”;

系统设置	系统控制	同步日志	同步状态
2009\MS09-040\Windows2000-KB971032-x86-CHS .exe	1386816	已同步	0
2009\MS09-040\Windows2000-KB971032-x86-ENH .exe	1382136	已同步	0
2009\MS09-040\WindowsXP-KB971032-x86-CHS .exe	1387376	已同步	0
2009\MS09-040\WindowsXP-KB971032-x86-ENH .exe	1391992	已同步	0
2009\MS09-040\WindowsServer2003-KB971032-x86-CHS .exe	1908232	已同步	0
2009\MS09-040\WindowsServer2003-KB971032-x86-ENH .exe	1907696	已同步	0
2009\MS09-041\WindowsXP-KB971657-x86-CHS .exe	962032	已同步	0
2009\MS09-041\WindowsXP-KB971657-x86-ENH .exe	961528	已同步	0
2009\MS09-041\WindowsServer2003-KB971657-x86-CHS .exe	954368	已同步	0
2009\MS09-041\WindowsServer2003-KB971657-x86-ENH .exe	953328	已同步	0
2009\MS09-041\Windows6.0-KB971657-x86 .exe	309563	已同步	0
2009\MS09-041\Windows6.0-KB971657-x86 .exe	308563	已同步	0
2009\MS09-048\WindowsServer2003-KB967723-x86-CHS .exe	845168	正在同步	0
2009\MS09-048\WindowsServer2003-KB967723-x86-ENH .exe	839040	正在同步	0
2009\MS09-048\Windows6.0-KB967723-x86 .exe	4343682	正在同步	0

4. 点击“补丁管理->补丁分发->补丁分发->默认分发任务”，点击应用对象，查看及编辑选择对应的主机名，IP 组，用户组和工作组;
5. 选择补丁安装选项为“自动下载，自动安装”，自动下载前提示用户确认。
6. 保存并更新客户端规则。

注意: 如果同步日志中有报与服务器连接失败等信息，请重复尝试。

并确认中心服务器到 patch.patchsource.cn 的 80、8800 端口均可达。

建议：管理员手工拷贝一份补丁予以备份，方便系统重装或其他测试。

8.3. 手工补丁源

8.3.1. 关于手工补丁源

■ “手工补丁源”作为“在线补丁源”的一种补充，可由管理员自行配置需要安装的补丁，以满足需要。

■ “手工补丁源”发布后补丁分发方式同“在线补丁源”。

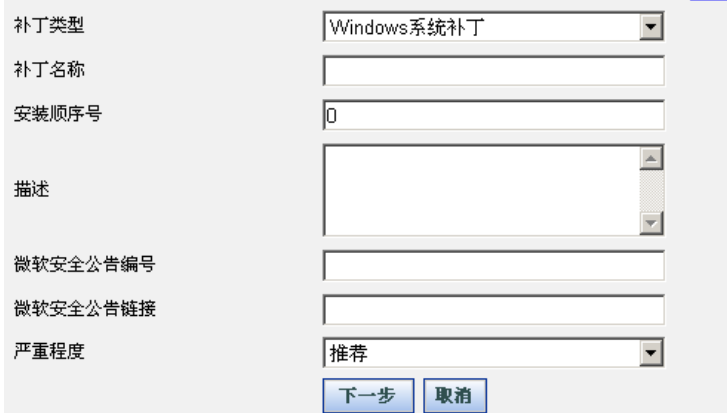
名词解释

“补丁向导”：添加手工补丁的配置向导，管理员可根据向导指引一步步完成手工补丁的配置。

8.3.2. 配置介绍

补丁向导页面

系统补丁配置向导



补丁类型: Windows系统补丁

补丁名称:

安装顺序号: 0

描述:

微软安全公告编号:

微软安全公告链接:

严重程度: 推荐

下一步 取消

帮助

配置项:

说明

补丁类型	本系统目前支持 Windows 系统补丁和 IE/Outlook 补丁两种类型，两种补丁配置的方式不同，请先确认好需要配置的补丁类型，然后再配置其他选项。
补丁名称	输入微软标准的补丁编号，例如 KB824468, Q324567 等，每次只能输入一个。
安装顺序号	本系统在为客户端自动安装补丁时，可设置补丁安装的优先级。此处的安装顺序号数字越小的越优先安装，顺序号的数字不必相连，例如您可以输入 10, 20, 30, 100 这样的数字。
描述	微软安全公告中对于此补丁的描述。
微软安全公告编号	发布此补丁的微软安全公告号，例如 MS08-030。
微软安全公告链接	发布此补丁的微软安全公告的链接，例如 http://www.microsoft.com/china/technet/security/bulletin/ms08-030.msp 。
严重程度	严重程度与微软发布的安全公告的严重等级相对应。
下一步	
文件组名称	每个微软公布的补丁都会包含针对不同操作系统或 IE 版本的补丁文件，在此可以添加多个补丁文件组，每个组适用于一种操作系统版本或 IE 版本，其中包含不同语言版本的补丁文件信息。一般补丁文件组以操作系统版本或者 IE 版本来命名。例如在此填入“WinXP”，表示本组补丁文件适用于 XP 操作系统。
自动安装参数	补丁自动安装参数，设置补丁采用静默安装的模式，在所有补丁安装完成之前不重新启动操作系统。默认设置为 /quiet /norestart，无需修改。
简体中文版文件	填写简体中文版补丁文件存放的相对路径，例如补丁文件存放于服务器安装目录 \$/download/AutoUpdate/2008/MS08-008/中，则此处相对路径应该填写： 2008\MS08-008\Windows2000-KB943055-x86-CHS.EXE。
繁体中文版文件	填写繁体中文版补丁文件存放的相对路径，填写方式与简体中文版类似。
英文版文件	填写英文版补丁文件存放的相对路径，填写方式与简体中文版类似。

下一步 (类型为 Windows 系统 补丁)	
操作系统	选择补丁所适用的操作系统版本。
Service Pack	选择补丁所适用的 ServicePack 版本。
补丁文件组	选择适用的补丁文件组。

8.4. 补丁分发

8.4.1. 关于补丁分发

- “补丁分发”即配置所有终端打补丁的策略。补丁分发可以分为两个阶段，补丁测试与补丁分发。
- 在大规模分发补丁前，可以先在指定的 IP 组中作补丁的测试，如果确认补丁确实不存在问题，可以结束测试任务并分发。
- “补丁测试”以主机名，IP 组，用户组和工作组为单位，对选定的补丁进行小范围分发测试。所有从补丁源发布的补丁初始状态都是未测试，只有经过测试才会被标记为已测试。
- “补丁分发”以主机名，IP 组，用户组和工作组为单位，对选定的补丁在设置时间范围内进行分发。状态为未测试和已测试的补丁都可分发，但建议对所有补丁进行测试后再分发。
- “分发参数”包括“客户端下载补丁流量”和“是否允许在域环境下安装补丁”两个选项。

建议：虽然天珣补丁已经过严格的测试，但 Windows 补丁自身的问题也可能导致部分终端的蓝屏或死机现象，所以建议大型网

络中对所有的补丁测试。

■ “补丁测试”和“补丁分发”可以同时进行，不会出现同一补丁重复安装的现象。

■ 分发参数 设置客户端下载补丁时的带宽和是否允许在域环境下安装补丁。

8.4.2. 配置介绍

补丁测试页面



配置项:	说明
任务名称	即补丁测试的名称，以方便管理。
任务说明	填写测试任务的一些补充说明。
请选择要测试的补丁	即选择需要测试的补丁。

任务状态	补丁测试完成后可结束测试任务，即标记为“已完成”。 相应的补丁状态为“已测试”。
补丁安装选项	即补丁的安装方式，可以手工安装（“不自动下载”），可以“自动下载，手工安装”，可以“自动下载，自动安装”，也可以“静默下载，静默安装”，并且可以根据需要“自动下载前提示用户确认”。
补丁安装前的提示信息	在这里填写提示信息，那么在安装补丁前，就会弹框提示相关文字信息。
补丁安装完成的提示信息	在这里填写提示信息，补丁安装完成之后，则会弹框提示相关文字信息。
应用到 IP 地址	在这里可以输入单个 IP 地址，也可以输入某个 IP 组里面的 IP 地址范围。
应用对象	点击“ 查看及编辑 ”超链接，选择测试补丁的主机名，IP 组，用户组和工作组。

补丁分发页面



客户端下载补丁时间

时间范围	开始时间	结束时间	编辑	删除
	2016-03-01	2016-03-01		

任务状态

补丁安装选项

补丁安装前的提示信息

补丁安装完成的提示信息

应用对象

查看及编辑

保存

取消

配置项：	说明
任务名称	即补丁测试的名称，以方便管理。
任务说明	填写测试任务的一些补充说明。
请选择要测试的补丁	即选择需要测试的补丁。
客户端下载补丁时间	配置补丁分发时间范围。
任务状态	补丁测试完成后可结束测试任务，即标记为“已完成”。 相应的补丁状态为“已测试”。
补丁安装选项	即补丁的安装方式，可以手工安装（“不自动下载”），可以“自动下载，手工安装”，可以“自动下载，自动安装”，也可以“静默下载，静默安装”，并且可以根据需要“自动下载前提示用户确认”。
补丁安装前的提示信息	在这里填写提示信息，那么在安装补丁前，就会弹框提示相关文字信息。
补丁安装完成的提示信息	在这里填写提示信息，补丁安装完成之后，则会弹框提示相关文字信息。
应用对象	点击“查看及编辑”超链接，选择测试补丁的主机名，IP 组，用户组和工作组。

系统“默认分发任务”：自动处理的分发任务，该任务将自动同步所有补丁，管理员仅需将所有 IP 组加入该分发任务即可实现补丁的自动分发。如果需要测试补丁和定期分发补丁，可以将“默认分发任务”的“任务状态”改为“已终止”。

分发参数页面

补丁测试	补丁分发	分发参数						
补丁分发参数 帮助 补丁分发参数： 修改 <table border="1"> <tr> <td>客户端下载补丁流量</td> <td>不限制</td> </tr> <tr> <td>是否允许在域环境下安装补丁</td> <td>不允许</td> </tr> </table>			客户端下载补丁流量	不限制	是否允许在域环境下安装补丁	不允许		
客户端下载补丁流量	不限制							
是否允许在域环境下安装补丁	不允许							
<table border="1"> <thead> <tr> <th>配置项：</th> <th>说明</th> </tr> </thead> <tbody> <tr> <td>客户端下载补丁流量</td> <td>可实现客户端下载补丁的流量限制，也可以不限制带宽。</td> </tr> <tr> <td>是否允许在域环境下安装补丁</td> <td>该参数支持补丁在域环境下安装</td> </tr> </tbody> </table>			配置项：	说明	客户端下载补丁流量	可实现客户端下载补丁的流量限制，也可以不限制带宽。	是否允许在域环境下安装补丁	该参数支持补丁在域环境下安装
配置项：	说明							
客户端下载补丁流量	可实现客户端下载补丁的流量限制，也可以不限制带宽。							
是否允许在域环境下安装补丁	该参数支持补丁在域环境下安装							

8.5. WSUS 集成管理

8.6. 关于 WSUS 集成管理

- “WSUS 集成”在策略服务器端配置 WSUS 补丁更新策略并下发至客户端，由客户端自动修改补丁更新相关的组策略和注册表项，然后利用 WSUS 系统自动分发微软各种补丁。
- 天珣客户端分发 WSUS 补丁是利用 Windows System Update 功能实现，而分发“在线补丁”是利用天珣自身的补丁精灵客户端实现。
- “WSUS 补丁源”利用天珣客户端的部署同时通过策略配置终端的 WSUS 选项，免去了 WSUS 客户端的部署麻烦。
- “WSUS 补丁源”和“在线补丁源”的补丁分发方式不同，

可以一起配置相互作为补充。参见《天珣典型配置示例文档》。

名词解释

"WSUS" 是 Windows Server Update Services 的简称, 可以更新 Windows 补丁, 同时具有报告功能, 管理员还可以控制更新过程。WSUS 是个微软推出的网络化的免费的补丁分发方案, 可以在微软网站上去下载。WSUS 支持微软公司全部产品的更新, 包括 Office、SQL Server、MSDE 和 Exchange Server 等内容。通过 WSUS 这个内部网络中的 Windows 升级服务, 所有 Windows 更新都集中下载到内部网的 WSUS 服务器中, 而网络中的客户机通过 WSUS 服务器来得到更新。这在很大程度上节省了资源, 避免了资源浪费并且提高了效率。

“WSUS 补丁源”: 天珣客户端可以代替 WSUS 客户端负责补丁的分发策略配置。

8.6.1. 配置介绍

WSUS 集成管理页面



WSUS集成管理

策略名称:

策略描述:

Intrasec更新策略URL:

Intrasec计划策略URL:

配置自动更新

通知下载并通知安装 ☒

选择了自动下载并计划安装时, 下载策略设置

计划安装日期: 每天

计划安装时间: 03:00

自定义再次提示执行计划的更新启动前自动更新等待的时间(默认值30分钟) ☐ 分钟(有效值1~1,440分钟)

自定义在继续执行计划的更新启动前自动更新等待的时间(默认值5分钟) ☐ 分钟(有效值1~30分钟)

启用自动更新策略启动后开始处理以前错过的计划安装之前等待的时间 ☐ 分钟(有效值1~60分钟)

自动更新选项

☒ 允许来自Intrasec Microsoft更新服务器位置的匿名内容

☒ 允许非管理员用户接收更新通知

☒ 禁止安装自动更新设置

☒ 允许无警告的自动更新立即安装

☒ 计划的自动更新安装后不自动重新启动

客户端目标

☒ 允许客户端设置

自定义自动更新检测频率(默认值24小时) 小时(有效值1~24小时)

配置项:	说明
------	----

策略名称	建议 WSUS 服务器的名称，以便于管理。
Intranet 更新服务 URL	填写补丁更新服务的 URL，例如安装更新服务的服务器 IP 地址为 192.168.0.11，则更新 URL 为 http://192.168.0.11 。
Intranet 统计服务 URL	填写补丁统计服务的 URL，例如安装统计服务的服务器 IP 地址为 192.168.0.11，则统计 URL 为 http://192.168.0.11 。
配置自动更新	配置客户端补丁自动更新时的下载和安装的方式，此处可以有四种选择：“通知下载并通知安装”、“自动下载并通知安装”、“自动下载并计划安装”、“允许使用本地管理员的设置”，只有在选择“自动下载并计划安装”时，才会激活计划安装相关的详细配置。
自动更新选项	设置 WSUS 客户端获取补丁自动更新的扩展选项，例如允许来自 Intranet Microsoft 更新服务器位置的签名内容，允许非管理员接收更新通知，计划的自动更新安装完成后不自动重新启动等。
客户端目标组	WSUS 可设置客户端目标组，针对不同的组下发不同类型的补丁，选择此项可以将客户端添加至 WSUS 的目标

	组中。
自定义自动更新检测频率(默认值 22 小时)	设置客户端向 WSUS 服务器检测补丁更新的频率。

生效时间

所有时间

工作时间

非工作时间

以下时间段

开始时间

结束时间

编辑

删除

在线模式

☒ 在线时生效

☒ 离线时生效

策略应用对象

(还没有应用到任何对象)

查看及编辑

创建类型

全局

创建者

jing

注：右边带*号的项目必须输入。

保存

取消

配置项：	说明
生效时间	目前策略的生效时间可以灵活配置，可以根据管理员的需求进行配置。
在线模式	策略运行的方式有客户端在线和离线两种模式。
策略应用对象	策略应用对象有四种方式：基于主机名，IP 组，用户组，和工作组。

建议：分发 WSUS 补丁需要管理员对补丁测试，建议不要在生产终端、财务终端 IP 组中启用 WSUS 补丁管理。

8.6.2. 配置要点

- 1、添加“WSUS 补丁策略”输入“策略名称”、“描述”、“Intranet 更新服务 URL”、“Intranet 统计服务 URL”。示例如下图：



WSUS补丁策略

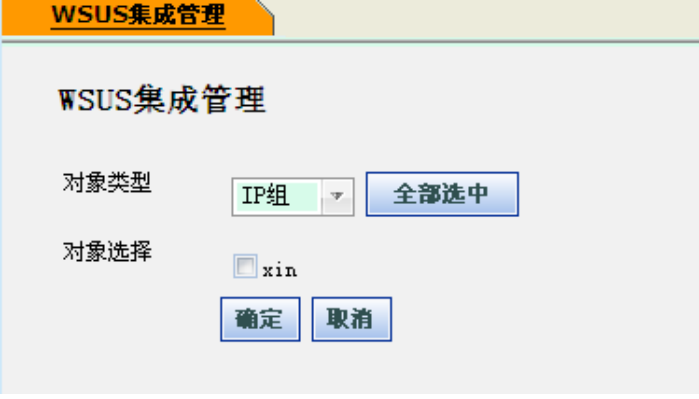
策略名称: 信息中心sus服务器(161) *

描述: 信息中心测试的WSUS服务器, ip地址为 192.168.0.161

Intranet更新服务URL: http://192.168.0.161 *

Intranet统计服务URL: http://192.168.0.161 *

- 2、点击“策略应用对象”的“查看及编辑”超链接，添加需要补丁分发的IP组并“确定”，如下图：



WSUS集成管理

对象类型: IP组 全部选中

对象选择: ☐ xin

确定 取消

- 3、客户端更新规则。

8.7. 补丁查询

8.7.1. 关于补丁查询

- “补丁查询”为管理员提供了补丁分发结果的查询窗口，可以根据补丁查询结果，总结补丁管理的效果并提交补丁管理的报表。
- “从电脑查补丁”确定指定终端上的补丁安装情况。
- “从补丁查电脑”确定指定补丁部署情况。

说明：补丁信息由客户端报表统一上报，补丁上报周期同客户端报表上报周期。

8.7.2. 配置介绍

从电脑查补丁页面

从电脑查补丁

[帮助](#)

请输入要查询的IP地址：

查询

配置项:	说明
请输入要查询的 IP 地址	输入需要查询补丁安装状态的电脑的 IP 地址，此电脑必须已经安装本系统的客户端。

从补丁查电脑页面

从补丁查电脑

[帮助](#)

请输入补丁号

请选择查询类型

要求安装已安装

请选择IP组

信息中心

查询

IP地址

1

配置项:	说明
输入补丁号	输入标准的补丁编号，例如 KB861112。
请选择查询类型	“要求安装”表示该补丁存在于补丁分发任务内，系统会自动向客户端分发。“强制要求安装”表示该补丁存在于安全状态的补丁强制规则内，系统将此补丁作为安全状态选项，强制客户端安装。

请选择 IP 组

选择补丁查询的范围。

9. 资产管理

9.1. 关于资产管理

资产管理依托于天珣客户端，收集内网终端的所有资产信息，包括软、硬件信息。



默认进入页面时会显示所有已经上报过资产的终端的概况。显示为绿色的资产信息为有发生过资产变更的终端。可通过右上角的部门选择栏选择想要查询的部门中的终端资产信息，并可通过“导出到 excel”按钮形成报表。

资产信息

要查看某台终端的资产详细信息，可以点击其 IP 地址进入资产信息明细页面



点击“资产信息明细”按钮，可查看该终端详细的资产信息



点击“查看变更事件”按钮，即可查看该终端变更事件明细表



点击“删除资产信息”按钮，则该终端的资产会被删除.删除后，下一次客户端会重新上报该终端的资产信息



资产变更事件

如果客户端发生了硬件或软件变更，天珣将会自动记录其变更信息，并在此进行查询



管理员可以通过查询变更事件，准确掌握硬件和软件资产的变动情况。

10. 非法外联

10.1. 关于非法外联

非法外联控制示意图



- 天珣防止“非法外联”控制分五个层面：“非法外联监控”、“多网卡限制”、“拨号限制”、“外设管理”与“异常路由审计”。
- 禁用移动存储设备的写入操作包括外设管理中禁用移动设备，移动存储驱动禁止移动设备 IO 流写入（允许读数据）两个层面。禁止移动设备 IO 流写入配置参见《[用户手册-移动存储章节](#)》。

■ 异常路由审计结果在“信息中心->外联监控->异常路由查询”中体现。

■ 非管理手段干预的前提下，非法外联控制的前提是天珣各种准入控制，只有保证网络中所有终端均强制安装天珣客户端才能完全杜绝非法外联行为。

注意：“安全防护->防护策略”的离线禁止网络访问策略经常用于非法外联环境中，但不属非法外联范畴。具体参见《[用户手册-安全防护->防护策略->访问控制章节](#)》。

名词解释

- “非法外联”：指内网终端非法利用各种外设或网络技术连接至其他网络或拷贝数据的行为。这种行为有意或无意的成为了内网安全的漏洞，甚至数据泄密。
- “非法外联监控”：用于实现对终端非法外联行为进行监控，并对非法外连行为进行告警或者是阻止，并告知管理员。
- “多网卡限制”：天珣客户端保护连接至内网的网卡，屏蔽掉其他网卡的数据可防止内网终端通过其他网卡非法外联的行为。
- “拨号限制”：用于对客户端的拨号连接进行限制，主要的限制类型有 PPP 拨号、PPPoE 拨号和 VPN 拨号。
- “外设管理”：用于对终端外设的使用进行控制，禁用或者是启用某个特定或者某些外接设备。
- “异常路由审计”：内网环境特点决定了内网终端路由信息相对无变化。但非法连接其他网络或代理上网将导致路由信息的变化，通过路由信息的变化，可以定位非法外联的网络行为。

10.2. 非法外联监控

10.2.1. 配置介绍

非法外连监控通过监控终端探测网络的两种方式（分别为 ping 和 telnet）来控制终端访问网络的行为，当监控到有非法外联行为产生时，可以记录非法外联行为，向客户端告警、向管理员发送告警信息（非法外联行为上传到服务器/短信/邮件通知等）、断开客户端网络等方式进行告警和阻止。

非法外联监控

点击“非法外联监控”标签中的“添加”按钮



配置项:	说明
策略名称	此处填写策略名称如“test”
策略描述	对策略进行描述，或备注等
探测方式	这里选择检查网络非法外联的方式 (ping 或 telnet)
探测目标列表	此处填写用来检测网络连接的探测目标 ip 或域名。 注: 如选择 telnet 方式，请 先确认探测目标允许 telnet 连接，可以 填写多个探测目标。
动作	此处选择检测到非法外联行为后执行的 动作：1、记录非法外联行为(默认启用)； 2、客户端告警；3、向管理员发送告警； 4、断开网络。
在线模式	配置此策略在在线和离线时是否生效
生效时间	可以根据管理员的需求，灵活配置策略 生效的时间范围。
策略应用对象	目前策略应用对象有四种：基于主机名， IP 组，用户组，和工作组。

非法外联告警设置

非法外联告警设置

非法外联告警设置

非法外联告警设置

非法外联告警设置：

修改

汇总告警时间	0分钟
蜂鸣器告警秒数	0秒
邮箱服务器地址	
用户名	
登录密码	
发送邮箱地址	
SMTP服务器端口	
告警时接收的邮箱地址	
告警时接收的手机号码	

点击非法外联告警设置：“修改”按钮

非法外联监控

非法外联告警设置

非法外联告警设置

汇总告警时间(*若填空或为0则不告警)

0

分钟

蜂鸣器告警长响(*若填空或为0则不启用蜂鸣)

0

秒

邮箱服务器地址(*若填空则不发邮件)

用户名(*若填空则不发邮件)

登录密码

发送邮箱地址

SMTP服务器端口(*若填空则不发邮件)

告警时接收的邮箱地址(*若填空则不发邮件)

告警时接收的手机号码(*若填空则不发短信)

测试邮箱用户

保存

返回

配置项:	说明
汇总告警时间	此处设置汇总告警时间间隔, 填(*若填空或为 0 则不告警);如: 设置汇总时间为 1 分钟, 则一分钟汇总一次告警信息, 然后以信息形式发送到手机或邮箱
蜂鸣器告警长响	此处设置告警时, 蜂鸣器鸣响时间(*若填空或为 0 则不启用蜂鸣器)注: 需硬件支持

邮箱服务器地址	此处填写用来发送告警邮件的邮箱服务器地址(*若填空则不发邮件)
用户名	此处填写用来发送告警邮件的邮箱登录名(*若填空则不发邮件)
登录密码	此处填写邮箱地址对应的密码
发送邮箱地址	此处填写发送告警邮件的邮箱地址，例： mj@163.com
SMTP 服务器端口	Smtp 服务器端口，常见如 25，, 993... (*若填空则不发邮件)
告警时接收的邮箱地址	用来接收告警邮件的邮箱地址，可填写多个，一行一个。(*若填空则不发邮件)
告警时接收的手机号码	用来接收告警短信的手机号码，可填写多个，一行一个。(*若填空则不发短信)注： 需硬件支持

10.3. 多网卡限制

10.4. 关于多网卡限制

- “多网卡限制”用于限制内网终端同时连接多个网络的行为。
- “多网卡限制”分为允许网卡切换和禁止网卡切换两种场景，场景区别在于内网应用场景是否单一。
- “多网卡限制”在禁止使用多网卡的前提下，能够允许使用指定的“非物理网卡”，以满足各种应用场景。
- 存在一种特殊场景，内网中部分用户可以访问指定网络资源，而另一部分用户无法访问该资源。可以访问该网络资源的用户为不能访问该资源的用户提供网络代理。此行为可通过“网站访问控制与审计”中“禁止使用 HTTP 代理服务器上

网”结合非法路由审计功能解决。

说明：Windows 网络共享上网需要多网卡，故与禁止 HTTP 代理上网有别。

重点：网络行为的非法外联控制不仅仅需要多网卡控制，更严格的内网非法外来控制还需要禁止离线客户端访问任何网络，禁止离线客户端使用外设和移动存储设备以及离线审计等策略。

名词解释

“拨号网卡（PPP，VPN，PPPOE）等”：调制解调器、ADSL、VPN 等各种行为，存在各种拨号网卡负责数据发送，而某些场景下这种行为是合法性的外联行为，天珣允许对该设备单独做例外排除。

“虚拟网卡（虚拟机）”：VMware 等虚拟机将创建特殊的虚拟网卡，而这些网卡在宿主终端上属多网卡，因此部分合法应用需要做例外排除。

“物理网卡”：具有硬件实体的网卡，比如有线以太网卡、无线网卡等。

“非物理网卡”：由程序创建的用于特殊环境的虚拟网卡，比如 PPP 拨号、PPPOE 拨号、VPN 拨号，虚拟机虚拟网卡。

说明：Windows 系统不分物理网卡和非物理网卡，其接口完全相同。不同网卡由天珣安全内核驱动识别。

10.4.1. 多网卡限制页面

配置介绍

多网卡限制

策略名称

策略描述

限制多网卡

☐ 允许在所有活动网卡间切换（包括物理网卡和非物理网卡）
☒ 不允许在物理网卡间切换，以下非物理网卡始终可用
☐ 允许在物理网卡间切换，以下非物理网卡始终可用

☐ 拨号网卡（PPP，VPN，PPPOE等）
 ☐ 虚拟网卡（虚拟机）

生效时间

☒ 所有时间
 ☐ 工作时间
 ☐ 非工作时间
 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 8:00	2012-03-10 13:30	添加	

在线模式

☒ 在线时生效
 ☒ 离线时生效

策略应用对象

（还没有应用到任何对象） [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

配置项：	说明
策略名称	输入合适的策略名称，以方便管理。
限制多网卡	默认只有第一个连通到策略服务器的网卡才可以通讯，其他的网卡都不允许通讯。 “允许在所有活动网卡间切换（包括物理网卡和非物理网卡）”：如果选中这个选项，客户端“切换网卡”菜单将激活，用户可在所有可用的网卡中选择一个网卡通信，没有被选中的网卡不能通信。 “不允许在物理网卡间切换，以下物理网卡始终可用”：如果选中这个选项，客户端“切换网卡”菜单不激活，系统只允许第一个连通到策略服务器的物理网卡以及下面选中的非物理网卡通信，其他的网卡不能通信。 “允许在物理网卡间切换，以下非物理网卡始终可用”：如果选中这个选项，客户端“切换网卡”菜单将激活，用户可在可用的物理网卡中选择一个网卡通信，没有被选中的物理网卡不能通信，同时下面选中的非物理网

	卡也可以通信。
生效时间	可以根据管理员的需求，灵活配置策略生效的时间范围。
在线模式	在线时生效，客户端处于在线状态时该规则生效，离线时生效，客户端处理离线状态时该规则生效，默认均选中。
策略应用对象	目前策略应用对象有四种：基于主机名，IP组，用户组，和工作组。

配置要点

1. 点击“添加”多网卡限制策略，如下图：



多网卡限制

策略名称: *

策略描述:

限制多网卡:
☐ 允许在所有活动网卡间切换（包括物理网卡和非物理网卡）
☒ 不允许在物理网卡间切换，以下非物理网卡始终可用
☐ 允许在物理网卡间切换，以下非物理网卡始终可用
☐ 拨号网卡（PPP，VPN，PPPOE等） ☐ 虚拟网卡（虚拟机）

生效时间:
☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	编辑	删除

[添加](#)

在线模式:
☒ 在线时生效 ☒ 离线时生效

策略应用对象:
 （还没有应用到任何对象） [查看及编辑](#)

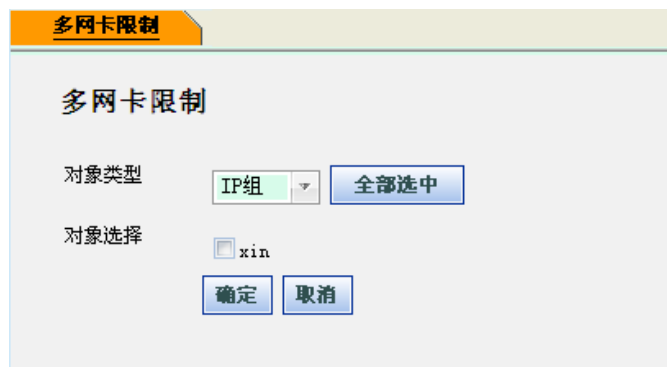
创建类型: 全局

创建者: jing

注：右边有*号的项目必须输入。

[保存](#) [取消](#)

2. 点击“策略应用对象”->“查看及编辑”超链接，关联指定的IP组，如下图。选择指定的IP组，并“确定”：



3. “保存”并更新客户端规则。

10.5. 拨号限制

10.5.1. 关于拨号限制

- “拨号限制”分为禁止 PPP 拨号，禁止 PPPoE 拨号，禁止 VPN 拨号。满足不同环境下对多网卡外联的全面管理。禁止 PPP 拨号不仅能对 PPP 连接进行限制，也能根据需求对指定号码进行限制。

-
- 说明：关于长途号码，如果“区号”或“国家（地区）代码”中有一个不为空就认为是长途号码。
-

10.5.2. 拨号限制页面

配置介绍

策略名称

策略描述

拨号类型限制

☐ 禁止PPP (传统MODEM)拨号
☐ 禁止PPPoE (ADSL、3G等)拨号
☐ 禁止VPN (虚拟专用网)拨号

拨号号码限制
(针对PPP拨号)

☐ 禁止拨打长途号码 (包括国内和国际)
☐ 禁止拨打以下列表中的号码

每个号码一行，可以输入多个号码。

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 8:00	2012-03-10 13:30		

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存 取消

配置项:	说明
策略名称	输入合适的策略名称，以方便管理。
策略描述	对策略的备注，及详细内容描述等
拨号类型限制	◆ 禁止 ppp (传统 modem) 拨号，勾选此项可以禁止所有的 ppp 拨号连接。 ◆ 禁止 PPPoE (ADSL、3G 等) 拨号，勾选此项可以禁止所有的 PPPoE 拨号连接。 ◆ 禁止 VPN (虚拟专用网) 拨号，勾选此项可以禁止所有的 VPN 拨号连接。 注：三个选项可以复选，勾选禁止 ppp 拨号后，拨号号码限制不可选。
拨号号码限制	◆ 禁止拨打长途号码 (包括国内和国际)，

	勾选此项，可以禁止拨所有的国内国外长途号，但允许拨短途或者是内线号。 ◆ 禁止拨打以下列表中的号码，勾选此处，只对列表中的号码进行限制。 注：可以复选，勾选拨以下列表中的号码后，可以对列表进行编辑，每个号码一行，可以输入多个号码。
生效时间	可以根据管理员的需求，灵活配置策略生效的时间范围。
在线模式	在线时生效，客户端处于在线状态时该规则生效，离线时生效，客户端处理离线状态时该规则生效，默认均选中。
策略应用对象	目前策略应用对象有四种：基于主机名，IP组，用户组，和工作组。

配置要点

4. 点击“添加”拨号限制策略，如下图：

拨号限制

策略名称

策略描述

拨号类型限制

☐ 禁止PPP (传统MODEM)拨号
☐ 禁止PPPoE (ADSL、3G等)拨号
☐ 禁止VPN (虚拟专用网)拨号

拨号号码限制
(针对PPP拨号)

☐ 禁止拨长途号码 (包括国内和国际)
☐ 禁止拨以下列表中的号码

每个号码一行，可以输入多个号码。

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

结束时间

编辑

删除

2012-03-10 9:00

2012-03-10 13:30

添加

在线模式	☒ 在线时生效 ☒ 离线时生效
策略应用对象	(还没有应用到任何对象) 查看及编辑
创建类型	全局
创建者	jing
注：右边有*号的项目必须输入。	
保存 取消	

5. 点击“策略应用对象”->“查看及编辑”超链接，关联指定的 IP 组，选择指定的 IP 组，并“确定”。
6. “保存”并更新客户端规则。

10.6. 外设管理

10.6.1. 关于外设管理

- “外设管理”可以最大限度的控制系统外设，杜绝各种非法外联的外设。
- “外设管理”中原有规则禁用外设后，除非将规则更改为启用该外设，否则该外设将保持被禁用状态。

建议：配置设置禁用规则后，相应配置一条外设启用规则，如果需要取消外设禁用则将 IP 组改为启用外设的规则中。详细操作见 [《本节配置要点》](#)

名词解释

“设备采样”：以某个 IP 地址终端的外设为基线，确定需要启用或禁用的外设。

10.6.2. 外设管理页面

配置介绍

外设管理

策略名称

策略描述

禁用内置设备

☐ 软 盘

☐ 并行口 (LPT口)

☐ 1394控制器

☐ 蓝牙设备

☐ 所有USB设备

☐ CDROM/DVD

☐ PCMCIA卡

☐ 红外线设备

☐ USB鼠标/键盘

☐ 移动硬盘 (U盘)

☐ 串行口 (COM口)

☐ 调制解调器

☐ 无线网卡

☐ 鼠标/键盘/U盘之外的USB设备

禁用USB设备

其它需要管理的设备

从终端库中添加

设备名称

识别标志

编辑

删除

生效时间

☒ 所有时间

☐ 工作时间

☐ 非工作时间

☐ 以下时间段

开始时间

结束时间

编辑

删除

在线模式

☒ 在线时生效

☒ 离线时生效

策略应用对象

创建类型

创建者

注：右括号*号的项目必须输入。

保存

取消

配置项：	说明
策略名称	输入规则的名称，以便于管理。
策略描述	对策略的备注，及详细内容描述等
禁用内置设备以及禁用 USB 设备	管理员可以根据需求，勾选上需要禁用的设备。
其他需要管理的设备	通过采样某个终端的外设，在输入框内输入该终端的 IP 地址，选择需要禁用的设备。
注：没有被勾选上的其他设备，默认会被启动	
生效时间	可以根据管理员的需求，灵活配置策略生效的时间范围。
在线模式	在线时生效，客户端处于在线状态时该规则生效，离线时生效，客户端处理离线状态时该规则生效，默认均选

	中。
策略应用对象	目前策略应用对象有四种：基于主机名，IP 组，用户组，和工作组。

“设备采样”，选择需要禁用的终端外设。

在地址框中输入需要采样的 IP 地址，对其进行驱动采样：



勾选设备并确定后即可对其进行采样，并加入到控制的外设列表中：



10.7. 异常路由审计

10.7.1. 关于异常路由审计

- “异常路由审计页面”即异常路由审计配置页面，输入正确的网关用以标记异常的路由信息。只需要将正常的默认网关在此作汇总即可。

10.7.2. 异常路由审计配置页面

配置介绍

异常路由审计

当前管理网段 初始管理网段 添加 批量添加 返回

默认网关地址	网关描述	创建状态	创建者
1			

配置项:	说明
选择服务器	选择需要维护的服务器。
选择管理网段	选择需要维护的管理网段
添加	添加正确的默认网关的 IP 地址
批量添加	如果您的网络中每个子网的网关 IP 非常有规律，您可以通过批量添加的方式，一次添加多个网关 IP 地址。如果您的子网网关分别为 10.0.0.1，10.0.1.1，10.0.3.1……10.0.20.1，您可以通过批量添加，在起始网关地址填 10.0.0.1，在结束网关地址填 10.0.20.1，系统将自动为您添加 21 个网关地址。

11. 移动存储

11.1. 关于移动存储

- “移动存储”管理与“外设管理”共同对移动存储设备进行控制。
- 未启用“移动存储”管理的网段使用移动存储设备不受限制。对启用了“移动存储”管理的网段，设置基本参数。对于每一个移动存储设备的认证和授权，请在“设备授权”→“移动存储设备授权”中设置。

说明：移动存储设备的 GUID 号 是不同的移动存储设备之间相互区分的唯一标识。

- “分区加扰”用于对数据拷贝性能要求高的环境中，设备中的数据并未做加密，但对设备分区表做了加密，导致未授权的终端无法打开该移动存储设备。
- “目录加密”模式中移动设备原理上不需要格式化，但新购买的移动存储设备建议格式化后对其认证并授权。
- “全盘加密”用于对整个磁盘内的数据加密，未授权的移动存储介质无法访问。

注意：天珣未改动移动存储设备硬件的任何信息，原理上不会导致移动设备损坏的现象，但建议对移动存储设备中的**数据做可靠备份**。

- 在“外设管理”对移动存储设备的控制为启用的情况下，设备受移动存储管理策略的控制。下图是移动存储设备使用权限表。

“外设管理” 禁用移动存储	“外设管理”不对移动存储设备进行控制
------------------	--------------------

设备				
1、移动存储设备不能使用 2、移动存储设备策略不能生效	受移动存储策略管理			
	不启用移动存储管理的网段	启用移动存储管理的网段		
		网段被关联到某一个移动存储管理策略		
		设备无需认证	设备需认证	
		任何用户按照“不对移动存储设备进行认证时，对移动存储设备的使用权限”使用	设备使用情况受认证及授权状态决定	
			未认证的设备	已认证的设备
	1、在允许使用未认证设置的电脑上可以使用 2、其他电脑禁止使用	1、授权的登录用户根据授权使用 2、未授权的用户无权使用		

建议：新购移动存储设备确保已格式化，避免设备量产时未设置磁盘卷标。

名词解释

- **“设备认证策略”**：设置移动存储设备的认证策略并关联相应的IP组，使策略生效。
- **“移动存储设备授权”**：用户提交移动存储设备的认证后，该设备出现在此列表中。系统管理员对设备进行认证并授权用户使用该移动存储设备的权限。
- **“未认证设备的使用授权”**：对于某些电脑，可以使用未经认证的移动存储设备。当客户端弹出移动存储设备认证窗口时，用户可点击“不认证”。

11.2. 设备认证策略

11.2.1. 关于设备认证策略

- 同一移动存储设备只能有一种认证策略，即“**移动存储设备管理策略**”认证策略为单选，一个 IP 组只能存在于一种“**移动存储设备管理策略**”。
- 全盘加密时，可以支持多分区大容量移动存储设备，但格式化设备需要较长的时间。

名词解释

“设备认证策略”：即移动存储设备的认证策略，此策略包含对**“移动存储设备管理策略”**的选择，以及该策略应用到的 IP 组范围。

“移动存储设备管理策略”：即移动存储设备的认证方式、是否加密、是否禁用、是否只读、是否读写等。

“专用目录加密认证”：此种认证方式会生成一个名为加密目录的文件夹。加密目录内的数据已加密，但名称未加密；加密目录外的数据未加密。已授权的设备可读取所有数据；未授权的设备无法读取任何目录。未安装天珣客户端的设备只可查看加密目录外的数据；加密目录内的数据呈乱码，不能查看。

“全盘加密认证”：整个磁盘内的数据加密，加密算法为 AES-256。未授权的移动存储介质无法访问，已授权的移动存储介质由天珣客户端格式化已加密分区。磁盘中的数据由天珣客户端负责加密存盘以及解密读入内存。未安装天珣客户端的终端无法打开磁盘，无法读取已加密数据。

注意：尽管已对数据存取做了性能优化，但全盘数据加密必然导致大文件拷贝的速率降低。全盘加密的时耗为 140% 左右。

“分区加扰认证”：磁盘分区被加密，但并未对磁盘数据做加密。未授权的移动存储介质无法访问，已授权的移动存储介质由天珣客户端格式化已加密分区。未安装天珣客户端的终端无法打开磁盘，无法读取数据。

11.2.2. 移动存储设备提交认证相关页面

- 1、未认证的移动存储设备插入受控终端，弹出移动存储认证页面，如下图：



移动存储管理

设备名称：Kingston DT 101 G2 USB Device

责任人：

归属部门：

电话：

Email：

IP地址：192.168.1.152

主机名：winXP3-lizexin

提交认证 不认证 取消

- 2、提交认证但未授权的移动存储设备插入受控终端时，弹出系统提示：“管理员正在处理，移动存储设备***暂时不能使用”，如下图：



- 3、提交认证并仅授予读的权限时，插入移动存储设备，弹出系统提示：“你对移动磁盘***的非加密目录没有写权限，加密目录没有写权限”（此处以专用加密目录认证为例）。



- 4、已提交并授权的移动存储设备插入受控终端，就会去策略服务器查询是否有相应的GUID，如果此时受控终端的网络不通，30秒超时，则会根据离线授权弹出提示；若此时没有离线授权，系统则会根据设备的认证策略弹出提示，如：认证策略是：专用目录加密，弹出的提示“你对移动磁盘 XXX 的加密目录和非加密目录没有访问权限”；如果是全盘加密，提示则相应的变为“你对移动磁盘 XXX 没有访问权限”。专用目录提示如下图：



11.3. 移动存储设备管理页面

配置介绍

移动存储设备管理策略配置页面如下：

移动存储设备认证策略	
移动存储管理	
策略名称	*
策略描述	
移动存储设备使用策略	☐ 禁止使用 ☐ 设备只读 ☐ 设备可读写 ☒ 专用目录加密认证 ☐ 全盘加密认证 ☐ 分区加扰认证
在线模式	☒ 在线时生效 ☒ 离线时生效
策略应用对象	查看及编辑
创建类型	全局
创建者	jing
注：右边有*号的项目必须输入。	
保存 删除 取消	

配置项：	说明
------	----

策略名称	输入合适的策略名称，以方便管理。
移动存储设备使用策略	选择移动存储的使用策略，属单选类型。
在线模式	移动存储设备无离线模式，故默认强制均选中。
策略应用对象	点击“ 查看及编辑 ”超链接，选择指定的 IP 组，工作组，主机名，或者用户组，则这些对象中的电脑启用移动存储设备使用策略。

注意：“禁止使用”、“设备可读”、“设备可读写”、与“外设管理”的区别在于此处是由天珣移动存储驱动控制。“专用目录加密认证”、“全盘加密认证”、“分区加扰认证” 参考 [《本节名词解释》](#)

配置要点

1、专用目录加密认证配置

点击“添加”移动存储设备管理策略，选择“专用目录加密认证”，如下图：

移动存储设备认证策略

移动存储管理

策略名称

专用目录加密认证*

策略描述

移动存储设备使用策略

☐ 禁止使用

☐ 设备只读

☐ 设备可读写

☒ 专用目录加密认证

☐ 全盘加密认证

☐ 分区加扰认证

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

[查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

删除

取消

- 2、点击“策略应用对象”->“查看及编辑”超链接，关联指定的IP 组，如下图。选择指定的 IP 组，并“确定”：

移动存储设备认证策略

移动存储管理
专用目录加密认证

对象类型

IP组

全部选中

对象选择

☒ xin

确定

取消

“保存”并更新客户端规则。

配置要点

- 1、未认证的移动存储设备插入受控终端，弹出移动存储认证页面，如下图：



移动存储管理

设备名称： Kingston DT 101 G2 USB Device

责任人：

归属部门：

电话：

Email：

IP地址： 192.168.1.152

主机名： winXP3-lizexin

提交认证 不认证 取消

- 2、由用户填写标记该移动磁盘的相关信息，包括责任人，部门、IP 地址、主机名等，并以电话等方式申请管理员授权。

注意：每一次提交认证成功，将会触发策略服务器同步策略，不用去手动同步。

- 3、管理员确认该移动存储设备合法性，并授权。如下图：

下图为专用目录加密授权页面：

移动存储设备授权 可使用未认证设备的计算机

移动存储设备授权 (同一个U盘加密模式更改后, 请删除该U盘对应的旧认证及授权信息)

设备编号: Kingston DT 101 G2 USB Device-662 *

部门: * [选择部门](#)

责任人: lzx *

主机名: winXP3-lizexin

IP地址: 192.168.1.152

授权状态: ☐ 未授权 ☒ 授权通过 ☐ 只授权不加密

加密模式: 专用加密目录

非加密目录操作权限: ☐ 读 ☐ 写 ☐ 离线读 ☐ 离线写

加密目录操作权限: ☐ 读 ☐ 写 ☐ 离线读 ☐ 离线写

申请认证时间: 2012-10-30 8:20:21

应用对象授权: [查看及编辑](#)

[保存](#) [删除](#) [取消](#)

下图为全盘加密授权页面:

移动存储设备授权 可使用未认证设备的计算机

移动存储设备授权 (同一个U盘加密模式更改后, 请删除该U盘对应的旧认证及授权信息)

设备编号: Teclast CoolFlash USB Device-996 *

部门: * [选择部门](#)

责任人: abc *

主机名: winXP3-lizexin

IP地址: 192.168.1.152

授权状态: ☐ 未授权 ☒ 授权通过 ☐ 只授权不加密

加密模式: 全盘加密

操作权限: ☐ 读 ☐ 写 ☐ 离线读 ☐ 离线写

申请认证时间: 2012-10-30 8:37:22

应用对象授权: (还没有授权到任何对象) [查看及编辑](#)

[保存](#) [删除](#) [取消](#)

下图为分区加扰授权页面:

移动存储设备授权

可使用未认证设备的计算机

移动存储设备授权

(同一个U盘加密模式更改后，请删除该U盘对应的旧认证及授权信息)

设备编号

Teclast CoolFlash USB Device-424

*

部门

*

选择部门

责任人

abc

*

主机名

winXP3-lirexin

IP地址

192.168.1.152

授权状态

☐ 未授权 ☒ 授权通过 ☐ 只授权不加密

加密模式

分区加扰

操作权限

☐ 读 ☐ 写 ☐ 离线读 ☐ 离线写

申请认证时间

2012-10-30 8:39:33

应用对象授权

(还没有授权到任何对象) [查看及编辑](#)

保存

删除

取消

- 4、将授权信息下发到指定的终端 IP 组，主机名，工作组，或者用户组，例：点击“应用对象授权”后的“查看及编辑”超链接，弹出授权信息，如下图：

移动存储设备授权

可使用未认证设备的计算机

移动存储设备授权

(同一个U盘加密模式更改后，请删除该U盘对应的旧认证及授权信息)

Teclast CoolFlash USB Device-424

对象类型

IP组

全部选中

对象选择

☐ xin

确定

取消

授权信息下发到指定用户组的操作参照上述第 4 点。

“保存”。

说明 1：授权保存后，客户端不用去手动更新策略，也可以获得相应的认证策略信息，但新的认证策略只会对下次接入的移动存储设备生效，对于已接入的移动存储设备必须重新接入才会获得新的认证策略，上述情况只对所属服务器是中心服务器的客户端而言。对于所属服务器是本地服务器的客户端，如果在提交认证开始一分钟之内就授权完成，则自动会将认证信息和授权信息一起同步到本地

服务器；如果提交认证一分钟之后提交授权信息，则必须先同步一下本地服务器的策略，客户端才会自动获取相应的认证策略信息。

说明 2：如果授权信息中有离线授权，则缓存授权信息；如果授权信息中没有离线授权，则删除本地缓存的授权信息。

11.5. 可使用未认证设备的计算机

如果需要对一些受控终端进行特别例外，使其可以使用未认证过的U 盘的话，则可以在此进行配置。

配置介绍



如需要批量添加客户端，可以点击“从文件导入”将大量客户端信息导入进来，省却了单独配置的麻烦。当然也可以将已配置好的信息导出作为备份。

说明：终端识别号是天珣客户端自动注册时，服务器为其分配的唯一序列号。

配置要点

1、点击“添加”可使用未认证设备的计算机，弹出如下图：

客户端查询

组合查询条件： 只从客户端报表查询

所属IP组: **请选择**

IP地址: (可模糊查询)

MAC地址: (可模糊查询)

主机名: (可模糊查询)

每页显示行数: 20

2、选择所属的 IP 组并查询，得到终端的查询结果，如下：

客户端查询

并 21 条记录

操作	IP地址	终端类型	主机名称	IP组别	所属IP组	操作
	192.168.2.117	手工	WCB-C309TVL3078	02411477-9030-4030-8130-P44339333AC	用户终端(192)	
	172.20.84.30	手工	113003030-C3078P	02C48048-8138-8048-8048-6110848PAB79	172.20.84.*	
	172.20.84.30	手工	0140016	02008030-8039-8039-9005-0240P3027489	172.20.84.*	

3、选中需要授权的终端，并点击“保存所选的计算机”。

移动存储设备授权

可使用未认证设备的计算机

设备ID	计算机名	MAC地址	授权状态	创建者	操作
02B118E0-94B9-46E8-9070-0999C092F671	WCB-3F-480310	00-0C-29-3C-14-94	全部	admin	

4、当移动设备接入这些例外的计算机时，会弹出一个认证框：

移动存储管理

设备名称: Fedtest CoolFlash USB Device

责任人:

归属部门:

电话:

Email:

IP地址: 192.168.133.152Fedtest CoolFlash USB Device

主机名: winXP3-62asin

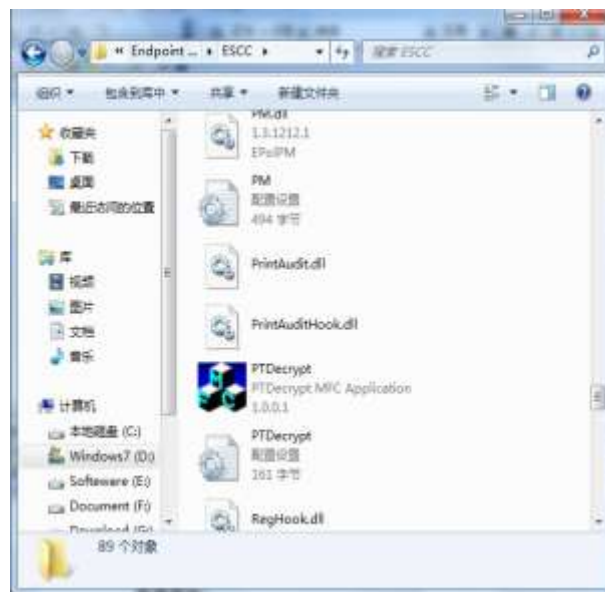
点击“不认证”时，则可以直接使用接入的移动设备，而不需要提交认证授权。

11.6. 分区解扰操作说明

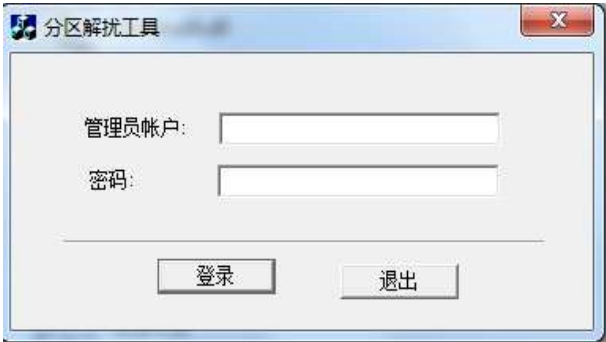
- 天珣客户端可以针对分区加扰的移动存储设备进行解扰。
- 分区解扰需要输入策略服务器帐号和密码确认身份，即仅提供在线解扰。
- 分区解扰后的移动设备为普通移动存储设备。
- 分区解扰操作将提供分区解扰审计。

配置要点

- 1、打开客户端安装目录（%program files%\venustech\endpoint security\esc），如下图：



- 2、打开 PTDecrypt 程序，如下图：

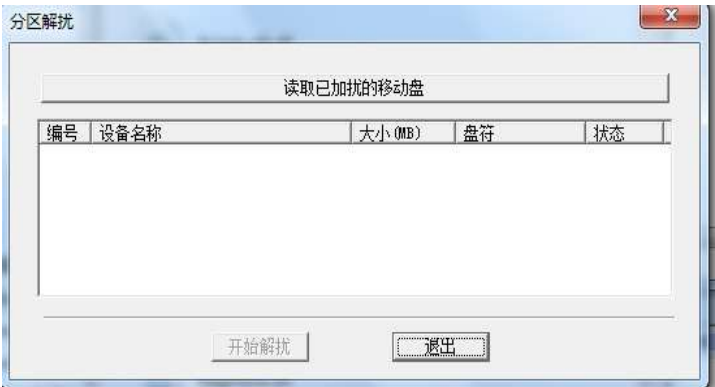


3、输入管理员的帐号和密码，即登录 Web8833 的用户名和密码。

该帐号必须具有分区解扰的权限，如下图：



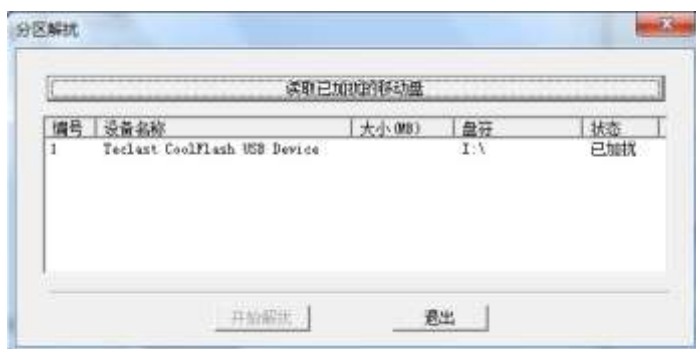
4、输入用户名和密码和进入解扰页面：



5、如果移动盘未加扰，显示状态为未加扰：



6、如果移动盘已加扰，显示状态为已加扰：



7、对于已加扰的移动存储设备，选中后点击“开始解扰”。如图：



12. 终端审计

12.1. 关于终端审计

- 审计信息较多，为减轻审计信息上报对网络的影响，天珣客户端每二十条审计信息上报一次，低于 20 条审计信息，暂时缓存至本地磁盘。
- 同一时间，同一审计信息将拒绝多次插入数据库，仅记录该审计条目的并发次数。

- 因审计数据过多，配置审计策略后建议同时配置数据库维护策略，详见《用户手册-数据库维护章节》。

注意：本章节介绍终端审计策略的配置页面，终端审计信息的查询请查询“[信息中心-审计信息](#)”。

- 因攻击告警服务器的启动依赖于 SQL Server 的启动，故服务器操作系统重启时可能会出现 SQL Server 启动过慢导致攻击告警服务无法启动的现象。

建议：因审计数据内容将占有大量磁盘空间，建议在安装天珣策略服务器前确保 SQL Server 数据库磁盘空间至少有 40G 空间。

名词解释

- **“终端审计”：**关于终端审计策略配置和各审计内容的控制策略的配置。
- **“文件审计及控制”：**关于系统磁盘资源，网络资源相关的审计策略配置和各资源路径及目录控制策略的配置。
- **“打印审计及控制”：**可以对共享打印机、网络打印机等行为控制或审计，但不审计打印内容，审计的信息包括：打印机名称、文档名称、IP 地址、MAC 地址、主机名、用户名、页数和打印时间。
- **“网站审计及控制”：**即基于 HTTP 原语，对 URL 信息做控制与审计。可以对 URL 的关键字控制与审计，但不能对 WEB 页面内容做审计。可以控制 WEB 代理的行为，也可以对合法 WEB 代理做例外排除。
- **“FTP 审计及控制”：**即基于 FTP 协议的基础上，对终端 FTP 传输行为进行审计，并将这些审计信息上传给服务器。可以对 FTP 的关键字控制及审计，也可以限对终端访问 FTP 服务器及

其端口进行控制。

- **“文件涉密信息审计”**：对于系统磁盘资源的内容进行审计，但不对系统磁盘资源的名称或者是目录进行审计，可以添加多个审计关键字。
- **“应用程序使用审计”**：对终端运行程序运行行为进行审计，即可以对指定的某个进程或某些进程进行审计，也可以对终端运行的多有程序进行审计；策略配置后，应用程序开启，关闭后，就会审计下该应用程序运行的状态，包括开始关闭的时间及共运行的时间。
- **“刻录审计”**：支持对终端刻录行为进行控制及审计，并上报审计信息到服务器。
- **“Windows 事件日志审计”**：能够审计到终端用户 windows 应用程序日志、安全日志、系统日志并发送到服务器。

12.2. 文件审计及控制策略

12.2.1 关于文件审计及控制策略

- 文件审计可以针对系统中指定文件夹进行审计，例如：C:\temp 目录。
- 配置控制文件的写入策略时，如果拒绝读取和写入系统关键目录，将导致系统蓝屏或死机。
- 文件目录审计的配置支持系统环境变量，支持的环境变量：%ProgramFiles%，%windir%。

名词解释

- **“审计所有移动盘”**：对 U 盘、USB 移动硬盘等相关 USB 移动磁盘的审计策略配置和控制策略的配置。可以针对“文件名关键字”、“进程名”做审计和控制。
- **“审计所有本地盘”**：关于系统所有分区的审计策略配置和控制

策略的配置。可以针对“文件名关键字”、“进程名”做审计和控制。

- **“审计网络拷贝”**：网络拷贝即拷贝网络中的共享文件，共享文件源于远端共享服务器。“审计网络拷贝”即对拷贝其他终端共享的数据做审计。
- **“审计共享目录”**：共享目录即本机的共享文件夹，共享文件夹中的数据源于本地磁盘。“审计共享目录”即审计其他终端访问本机的共享目录。文件属本地磁盘，可以对共享目录中的数据做操作控制。

注意：注意选择包含子目录，否则审计文件夹下的子目录将无审计。

12.3. 文件审计及控制策略

13.2.1 关于文件审计及控制策略

- 文件审计可以针对系统中指定文件夹进行审计，例如：C:\temp 目录。
- 配置控制文件的写入策略时，如果拒绝读取和写入系统关键目录，将导致系统蓝屏或死机。
- 文件目录审计的配置支持系统环境变量，支持的环境变量：%ProgramFiles%，%windir%。

名词解释

- **“审计所有移动盘”**：对 U 盘、USB 移动硬盘等相关 USB 移动磁盘的审计策略配置和控制策略的配置。可以针对“文件名关键字”、“进程名”做审计和控制。
- **“审计所有本地盘”**：关于系统所有分区的审计策略配置和控制策略的配置。可以针对“文件名关键字”、“进程名”做审计和控制。

制。

- **“审计网络拷贝”**：网络拷贝即拷贝网络中的共享文件，共享文件源于远端共享服务器。“审计网络拷贝”即对拷贝其他终端共享的数据做审计。
- **“审计共享目录”**：共享目录即本机的共享文件夹，共享文件夹中的数据源于本地磁盘。“审计共享目录”即审计其他终端访问本机的共享目录。文件属本地磁盘，可以对共享目录中的数据做操作控制。

注意：注意选择包含子目录，否则审计文件夹下的子目录将无审计。

12.2.2 文件操作审计及控制页面

配置介绍

策略名称	审计所有本地盘 *										
策略描述											
审计目录	ALLDISK		☒ 包含子目录								
	支持的环境变量: %ProgramFiles%, %windir%										
审计内容	☒ 读 ☒ 写 ☒ 创建 ☒ 删除 ☒ 改名/移动 ☒ 文件拷贝										
操作阻止	☐ 读 ☐ 写 ☐ 创建 ☐ 删除 ☐ 改名/移动										
	☐ 仅针对文件名中含有以下关键字的文件 ☒ 文件名中含有以下关键字的文件除外										
文件名关键字	-> <- .dll .com .bat .exe										
	☒ 仅针对以下进程 ☐ 以下进程除外										
进程	-> <-										
生效时间	☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段										
	<table><thead><tr><th>开始时间</th><th>结束时间</th><th>编辑</th><th>删除</th></tr></thead><tbody><tr><td>2012-03-10 9:00</td><td>2012-03-10 13:30</td><td>添加</td><td></td></tr></tbody></table>			开始时间	结束时间	编辑	删除	2012-03-10 9:00	2012-03-10 13:30	添加	
开始时间	结束时间	编辑	删除								
2012-03-10 9:00	2012-03-10 13:30	添加									
在线模式	☒ 在线时生效 ☒ 离线时生效										
策略应用对象	(还没有应用到任何对象) 查看及编辑										

配置项:	说明
策略名称	输入合适的策略名称，以方便管理。
审计目录	即审计的目录范围，系统默认策略无法更改。
审计内容	即对哪些文件操作行为审计。
操作阻止	即对哪些文件操作行为阻止，Windows 系统文件拷贝的控制等同于文件读取和写入。
文件名关键字	即文件的后缀名，可以仅审计 doc,txt 等格式。
进程	可对指定的进程做判断，例如不审计杀毒软件读取的文件名。
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
策略应用对象	点击“查看及编辑”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用文件操作审计及控制策略。

配置要点

- 1、 点击“添加”文件操作审计及控制策略，如下图：

文件操作审计及控制

策略名称

策略描述

审计目录

审计内容

操作阻止

文件名关键字

进程

生效时间

在线模式

策略应用对象

审计“我的文档”

%USERPROFILE%

☒ 包含子目录

支持的环境变量: %ProgramFiles%, %windir%

☒ 读 ☒ 写 ☒ 创建 ☒ 删除 ☒ 改名/移动 ☒ 文件属性

☐ 读 ☐ 写 ☐ 创建 ☐ 删除 ☐ 改名/移动

☒ 仅针对文件名中含有以下关键字的文件 ☐ 文件名中含有以下关键字的文件

☒ 仅针对以下进程 ☐ 以下进程除外

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
00:00-00:10:00/10/10/20	00:10-00:30:00/10/20		

☒ 在线模式 ☒ 离线模式

(还没有应用到任何对象) [查看及编辑](#)

2、 点击“策略应用对象”->“查看及编辑”超链接，关联指定的 IP 组、用户组、工作组、主机名，如下图。选择指定的 IP 组、用户组、工作组、主机名，并“确定”：

文件操作审计及控制

对象类型

对象选择

确定

取消

IP组

全部清除

☒ 140 ☒ 172.25.45 ☒ 99100 ☒ 90

☒ 172.25.90 ☒ 110 ☒ 222 ☒ 20

☒ 172.25.20.123 ☒ 172.25.1.110-210 ☒ 84 ☒ 172.25.22.220

☒ 33 ☒ 254.x ☒ a3主机 ☒ 172.25.85

☒ 99206

3、 “保存”并更新客户端规则。

说明：系统环境变量均提供支持，打开命令行，输入 set 命令即可查看所有环境变量，如下图：

```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator> set
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=LINWORK-JONAS
ConSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\Administrator
LOGONSERVER=\\LINWORK-JONAS
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\Co
mmon Files\Thunder Network\Kankan\Codecs
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0f02
ProgramFiles=C:\Program Files
PROMPT=$PSG
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUMENT1\ADMIN1\1\LOCALS\1\Temp
TMP=C:\DOCUMENT1\ADMIN1\1\LOCALS\1\Temp
USERDOMAIN=LINWORK-JONAS
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS

C:\Documents and Settings\Administrator>
```

12.2.3 审计网络拷贝页面

配置要点

4、点击“添加”文件操作审计及控制策略，如下图：

文件操作审计及控制

策略名称: 审计网络拷贝 *

策略描述:

审计目录: NetworkFolder ☒ 包含子目录

支持的环境变量: %ProgramFiles%, %windir%

审计内容: ☐ 读 ☐ 写 ☐ 创建 ☐ 删除 ☐ 改名/移动 ☒ 文件拷贝

操作阻止: ☐ 读 ☐ 写 ☐ 创建 ☐ 删除 ☐ 改名/移动

文件名关键字:

进程:

生效时间: ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	删除

在线模式: ☒ 在线时生效 ☒ 离线时生效

策略应用对象: (还没有应用到任何对象) [查看及编辑](#)

- 5、点击“策略应用对象”->“查看及编辑”超链接，关联指定的 IP 组、用户组、工作组、主机名，如下图。选择指定的 IP 组、用户组、工作组、主机名，并“确定”：



- 6、“保存”并更新客户端规则。

12.4. 打印审计及控制

12.3.1 关于打印审计

- “打印审计”模块可能会被杀毒软件或防木马软件告警为木马行为，部署前请确认其可信。

12.3.2 打印审计页面

配置介绍

打印审计及控制

策略名称

策略描述

是否允许打印

☐ 禁用 ☒ 允许

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 01:00	2012-03-10 12:30	添加	

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象)

[查看及编辑](#)

创建类型

全部

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

配置项：	说明
策略名称	输入合适的策略名称，以方便管理。
是否允许打印	如果选择“禁用”，则无法打印，无审计记录； 如果选择“允许”则对打印行为审计。
在线模式	如果选择“在线时生效”，则客户端处于在线状态时生效；如果选择“离线时生效”则客户端处于离线时仍生效。如果不选择，则不生效，如不选择“离线时生效”，则客户端离线时不对打印行为审计。
离线策略	即客户端离线时可以选择的动作。如在线时可以审计并控制，离线后可以仅审计不控制。
策略应用对象	点击“查看及编辑”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用打印审计策略。

配置要点

1、 点击“添加”打印审计策略，如下图：



打印审计及控制

策略名称: 财务室打印审计

策略描述: 财务室打印审计策略

是否允许打印: ☐ 禁用 ☒ 允许

生效时间: ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 8:00	2012-03-10 18:00	编辑	删除

在线模式: ☒ 在线时生效 ☒ 离线时生效

策略应用对象: [还没有应用到任何对象](#) [查看及编辑](#)

创建类型: 全局

创建者: jing

注: 右边有*号的项目必须输入。

[保存](#) [取消](#)

2、 点击“应用策略对象”->“查看及编辑”超链接，关联指定的 IP 组、用户组、工作组、主机名，如下图。选择指定的 IP 组、用户组、工作组、主机名，并“确定”：



打印审计及控制

财务室打印审计

对象类型: IP组 [全部清除](#)

对象选择:

☒ 140	☒ 1722545	☒ 99100	☒ 90
☒ 172.25.90	☒ 110	☒ 222	☒ 20
☒ 172.25.20.123	☒ 172.25.1.110-210	☒ 84	☒ 172.25.22.220
☒ 33	☒ 254.x	☒ mj主机	☒ 172.25.85
☒ 99206			

[确定](#) [取消](#)

3、 “保存”并更新客户端规则。

12.5. 网站审计及控制

12.4.1 网站审计及控制页面

配置介绍

网站访问审计及控制

策略名称

策略描述

访问控制

访问审计

关键字列表

HTTP代理

HTTP端口列表

审计选项

生效时间

在线模式

允许访问

允许访问含有下列关键字的网站

禁止访问含有下列关键字的网站

对所有的网站访问进行审计

对网站名称含有下列关键字访问进行审计

对网站名称不含有下列关键字访问进行审计

每个关键字一行，可以输入多个关键字。

允许使用HTTP代理服务器上网（以下列表中的代理服务器除外）

禁止使用HTTP代理服务器上网（以下列表中的代理服务器除外）

例外代理服务器列表（每行一个，必须是IP地址，不能是域名）

添加端口

不添加则对所有端口生效

删除端口

审计详细的访问日志

仅审计所访问的网站

所有时间

工作时间

非工作时间

以下时间段

开始时间

结束时间

编辑

删除

2012-03-10 09:00

2012-03-10 18:00

添加

在线模式

在实时生效

离线时生效

配置项：	说明
策略名称	输入合适的策略名称，以方便管理。
访问控制	如果选择“允许访问”，则可以访问网络； 如果选择“允许访问含有下列关键字的网站”，则 URL 中含有相关关键字时可以访问，否则无法访问；如果选择“禁止访问含有下列关键字的网站”，则 URL 中含有相关关键字时无法访问，否则可以访问；
访问审计	如果选择“对所有的网站访问进行审计”，则客

	户端所有 URL 访问均审计；如果选择“对网站名含有下列关键字访问进行审计”则客户端仅审计 URL 中含有关键字表中的网站访问。如果选择“对网站名不含有下列关键字访问进行审计”则客户端仅审计 URL 中含有关键字表外的其他任何网站访问。
关键字列表	即 URL 中含有的字符串，例如： http://www.baidu.com 中的“.bai”、“idu.co”、“baidu”等等。不审计 html 中的关键字内容。
HTTP 代理	如果选择“允许使用 HTTP 代理服务器上网（以下列表中的代理服务器除外）”，则将禁止使用列表中的代理名称或 IP 地址；如果选择“禁止使用 HTTP 代理服务器上网（以下列表中的代理服务器除外）”，则仅允许使用列表中的代理名称或 IP 地址。
HTTP 端口列表	如果不输入则默认对所有端口的 HTTP 访问均审计，如果添加了 80 端口，则仅审计 80 端口的 HTTP 网站访问。
审计选项	“审计详细的访问日志”能审计到详细的网站访问信息，包括自己访问的网站信息及之后自动访问的网站访问行为； “仅审计所访问的网站”仅审计用户实际访问的网站，而对一些网站后台自动连接的网站访问行为不审计；并且审计周期默认为 10 分钟，即十分钟内的重复数据不上报
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。

在线模式	如果选择“ 在线时生效 ”，则客户端处于在线状态时生效；如果选择“ 离线时生效 ”则客户端处于离线时仍生效。如果不选择，则不生效，如不选择“ 离线时生效 ”，则客户端离线时不对上网行为审计。
策略应用对象	点击“ 查看及编辑 ”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用网站审计及控制策略。

配置要点

- 1、 点击“**添加**”网站访问控制与审计。

网站访问审计及控制

网站访问审计及控制

策略名称

公司员工网络审计 *

策略描述

访问控制

☒ 允许访问
☐ 允许访问含有下列关键字的网站
☐ 禁止访问含有下列关键字的网站

访问审计

☒ 对所有的网站访问进行审计
☐ 对网站名称含有下列关键字访问进行审计
☐ 对网站名称不含有下列关键字访问进行审计

关键字列表

每个关键字一行，可以输入多个关键字。

HTTP代理

☒ 允许使用HTTP代理服务器上网 (以下列表中的代理服务器除外)
☐ 禁止使用HTTP代理服务器上网 (以下列表中的代理服务器除外)
例外代理服务器列表 (每行一个，必须是IP地址，不能是域名):

- 2、 点击策略应用对象的“**查看及编辑**”超链接，选择指定的 IP

组、用户组、工作组、主机名，则这些 IP 组、用户组、工作组、主机名中的电脑启用上网审计或控制策略。

网站访问审计及控制
公司员工网络审计

对象类型 IP组 ▼ 全部清除

对象选择

☒ 140	☒ 172.25.45	☒ 99100	☒ 90
☒ 172.25.90	☒ 110	☒ 222	☒ 20
☒ 172.25.20.123	☒ 172.25.1.110-210	☒ 84	☒ 172.25.22.220
☒ 33	☒ 254.x	☒ mj主机	☒ 172.25.85
☒ 99206			

确定 取消

3、 “保存” 并更新客户端规则。

12.6. FTP 审计及控制

12.5.1 FTP 审计及控制页面

配置介绍

FTP 访问审计及控制

策略名称

策略描述

访问控制

☒ 允许FTP访问

☐ 允许访问含有下列地址的FTP服务器

☐ 禁止访问含有下列地址的FTP服务器

访问审计

☒ 对所有的FTP访问进行审计

☐ 对下列地址中的FTP服务器访问进行审计

☐ 对不在下列地址中的FTP服务器访问进行审计

FTP服务器列表

FTP端口列表

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

结束时间

编辑

删除

2012-03-10 9:00

2012-03-10 13:30

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象)

查看及编辑

配置项:	说明
策略名称	输入合适的策略名称，以方便管理。
访问控制	如果选择“允许 FTP 访问”，则可以访问所有 FTP 服务器；如果选择“允许访问含有下列地址的 FTP 服务器”，则仅 FTP 地址中含有关键字表中的服务器可以访问，否则无法访问；如果选择“禁止访问含有下列地址的 FTP 服务器”，则 FTP 地址中含有关键字表中的服务器无法访问，否则可以访问；
访问审计	如果选择“对所有的 FTP 访问进行审计”，则客户端所有 FTP 访问均审计；如果选择“对下列地址中的 FTP 服务器访问进行审计”则客户端仅审计 FTP 地址中含有关键字表中的 FTP 访

	问。如果选择“对不在下列地址中的 FTP 服务器访问进行审计”则客户端仅审计 FTP 地址中含有关键字表外的其他任何 FTP 访问。
FTP 服务器列表	即 FTP 服务器中的 IP 地址，如：10.201.1.202；如果不输入则默认对所有的 FTP 访问控制并审计。
FTP 端口列表	如果不输入则默认对所有端口的 FTP 访问均控制并审计，如果添加了 21 端口，则仅控制并审计 21 端口的 FTP 访问。
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	如果选择“在线时生效”，则客户端处于在线状态时生效；如果选择“离线时生效”则客户端处于离线时仍生效。如果不选择，则不生效，如不选择“离线时生效”，则客户端离线时不对 FTP 访问行为审计。
策略应用对象	点击“查看及编辑”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用 FTP 审计及控制策略。

配置要点

1、点击“添加”“FTP 访问审计及控制”

FTP 访问审计及控制

策略名称	FTP 访问审计及控制 *								
策略描述									
访问控制	☒ 允许 FTP 访问 ☐ 允许访问含有下列地址的 FTP 服务器 ☐ 禁止访问含有下列地址的 FTP 服务器								
访问审计	☒ 对所有的 FTP 访问进行审计 ☐ 对下列地址中的 FTP 服务器访问进行审计 ☐ 对不在下列地址中的 FTP 服务器访问进行审计								
FTP 服务器列表	>>								
FTP 端口列表	>>								
生效时间	☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段 <table><thead><tr><th>开始时间</th><th>结束时间</th><th>编辑</th><th>删除</th></tr></thead><tbody><tr><td>2012-03-10 9:00</td><td>2012-03-10 13:30</td><td></td><td></td></tr></tbody></table> 添加	开始时间	结束时间	编辑	删除	2012-03-10 9:00	2012-03-10 13:30		
开始时间	结束时间	编辑	删除						
2012-03-10 9:00	2012-03-10 13:30								
在线模式	☒ 在线时生效 ☒ 离线时生效								
策略应用对象	(还没有应用到任何对象) 查看及编辑								

2、点击策略应用对象的“查看及编辑”超链接，选择指定的 IP 组、用户组、工作组、主机名，则这些 IP 组、用户组、工作组、主机名中的电脑启用 FTP 审计及控制策略。

4、“保存”并更新客户端规则。

12.7. 文件涉密信息审计

12.6.1 文件涉密信息审计页面

配置介绍

文件涉密信息审计

策略名称 *

策略描述

关键字列表 *

每个关键字一行，可以输入多个关键字
审计包含任意关键字的文档

关键字之间的关系 ☐ 与 ☒ 或

仅审计以下文档类型 如: ".txt"

生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注: 右边有*号的项目必须输入。

配置项:	说明
策略名称	输入合适的策略名称，以方便管理。
关键字列表	可增加一个或者多个关键字，如果文件内容中包含该关键字，则将被审计出来
关键字之间关系	有‘与’和‘或’两种。‘与’则审计包含所有的关键字，‘或’则审计包含任意关键字
仅审计一下文档类型	可对需要审计的文档类型进行筛选。如“.txt”
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	如果选择“在线时生效”，则客户端处于在线状态时生效；如果选择“离线时生效”则客户端

	处于离线时仍生效。如果不选择，则不生效，如:不选择“ 离线时生效 ”，则客户端离线时不对涉密文档进行审计。
策略应用对象	点击“ 查看及编辑 ”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用文件涉密信息审计策略。

说明

- ◆ 文件涉密信息审计是对文件内容进行审计，而不是文件名。
- ◆ 要使得此策略生效，必须要确保开启终端上的 Windows Search 服务。Windows 7 默认就有该服务，只需确保该服务已启动就可以；但 Windows 7 之前的系统都是默认没有 Windows Search 服务的，必须安装 KB940157 补丁，然后确保启动了 Windows Search 服务。
- ◆ 确保 Windows Search 服务启动后, 还需要手动为需要审计的位置建立索引, 不同系统建立索引的方法见 **附录 1**
- ◆ KB940157 下载链接参考：
<http://www.microsoft.com/windows/products/winfamily/desktopsearch/choose/windowssearch4.msp?tab=Install%20It>
- ◆ 文件涉密信息审计不支持 windows 2000。
- ◆ 文件涉密审计能审计的文档类型与 windows search 支持的类型一致，如：.txt.ini.jpg.cpp.xls.cc.cpp.log.xml Office 文档 电子邮件等。
- ◆ 文件涉密信息审计策略与升级策略存在冲突，管理员可以自行处理避免两种策略同时出现。

配置要点

1、单击“添加”文件涉密信息审计策略

文件涉密信息审计

策略名称

文件涉密信息审计*

策略描述

关键字列表

ad

每个关键字一行，可以输入多个关键字
审计包含任意关键字的文档

关键字之间的关系

☐与☒或

仅审计以下文档类型

如：*.txt

>>

生效时间

☒所有时间☐工作时间☐非工作时间☐以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式

☒在线时生效☒离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

2、点击策略应用对象的“查看及编辑”超链接，选择指定的 IP 组、用户组、工作组、主机名，则这些 IP 组、用户组、工作组、主机名中的电脑启用文件涉密信息审计策略。

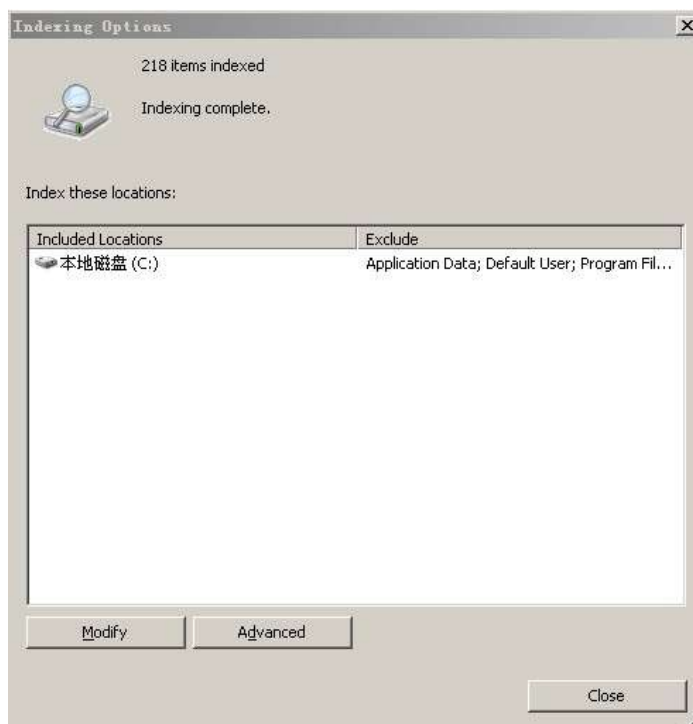
“保存”并更新客户端规则。

12.6.2 附录 1

不同的操作系统在安装完补丁 KB940157 (windows 7 不需要安装此补丁)后，需要手动给需要审计的位置添加索引，如下：

Windows 2003

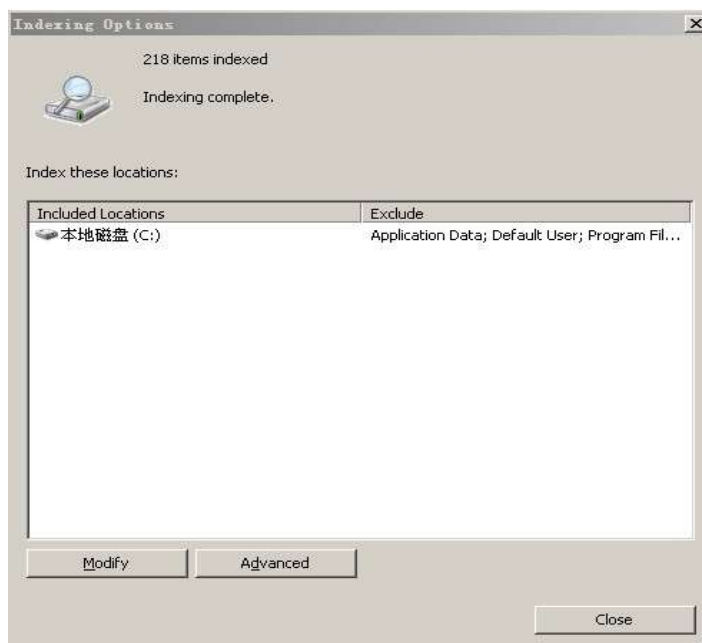
- 1、安装补丁 KB940157 后，确定 Windows Search 服务启动后，点击 “开始—》控制面板—》Indexing Options” 出现如下页面：



2、单击 “Modify”，然后勾选你需要添加索引的位置。然后单击 “确定”

Windows XP

1、安装补丁 KB940157 后，确定 Windows Search 服务启动后，“开始—》控制面板—》性能和维护—》Indexing Options”，然后出现如下页面：



2、单击 “Modify”，然后勾选你需要添加索引的位置。然后单击 “确定”

Windows 2008

1、安装补丁 KB940157 后，确定 Windows Search 服务启动后。“开始—》控制

面板—》索引选项”，点击进入以下页面：



2、单击上图中的“修改”为你所需要的位置建立索引。

Windows Vista

1、安装补丁 KB940157 后，确定 Windows Search 服务启动后。“开始—》控制面板—》系统和维护—》索引选项”点击 如下图：



单击之后进入到如下页面：

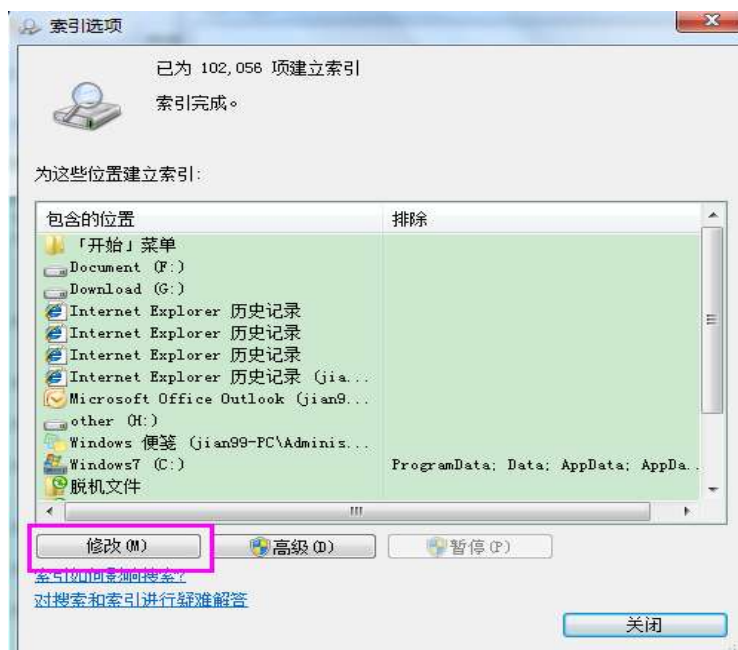


2、单击上图中的“修改”为你所需要的位置建立索引。

Windows 7

1、确定 Windows Search 服务启动后。点击“开始—》控制面板”，然后将查看方式改为“小图标”，单击“索引选项”如下图：





2、单击上图中的“修改”为你所需要的位置建立索引。

12.8. 应用程序使用审计

12.7.1 应用程序使用审计页面

配置介绍

应用程序使用审计

策略名称: 审计进程 *

策略描述: 审计进程

审计行为: ☒ 审计指定进程 ☐ 审计所有进程

进程列表: cmd.exe, notepad.exe, taskmgr.exe, mspaint.exe

生效时间: ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 8:00	2012-03-10 13:30	添加	

在线模式: ☒ 在线时生效 ☒ 离线时生效

策略应用对象: (还没有应用到任何对象) [查看及编辑](#)

创建类型: 全局

创建者: jing

注: 右边有*号的项目必须输入。

保存 取消

配置项:	说明
策略名称	输入合适的策略名称，以方便管理。
审计行为	可以选择是对所有程序进行审计，还是对指定的几个进程进行审计；如果选择“审计指定进程”则由管理员自己确定进程名列表，如果选择“审计所有进程”则任务管理器中的进程列表里面进程全部可以审计出来
进程列表	只有当审计行为 选择为“审计指定进程”，这里才会变为可编写，可以添加一个或多个进程名
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	如果选择“在线时生效”，则只对客户端处于在线状态时的进程运行情况进行审计；如果选择“离线时生效”则只对客户端处于离线状态时的进程运行情况进行审计。如果不选择，则不生效，如:只选择“在线时生效”，则只审计客户端在线时的进程运行情况，而不审计离线状态下的进程运行情况。
策略应用对象	点击“查看及编辑”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用应用程序使用审计策略。

说明：应用程序审计会将程序创建时间、退出时间和连续运行时间审计下来，且只有当程序结束才会上报运行情况，未结束的程序运行情况不立即上报，只记载在客户端。

配置要点

1、 点击“添加”应用程序使用审计 策略

应用程序使用审计

策略名称

策略描述

审计行为 ☒ 审计指定进程 ☐ 审计所有进程

进程列表

cmd.exe
notepad.exe
taskmgr.exe
mspaint.exe

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

2、 点击策略应用对象的“查看及编辑”超链接，选择指定的 IP 组、用户组、工作组、主机名，则这些 IP 组、用户组、工作组、主机名中的电脑启用应用程序使用审计策略。

3、 “保存”并更新客户端规则。

12.9. 刻录审计

12.8.1 刻录审计策略页面

配置介绍

刻录审计

策略名称

策略描述

审计选项

☒ 允许刻录，不审计刻录文件

☐ 允许刻录，审计刻录文件

☐ 禁用刻录

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

策略名称	输入合适的策略名称，以方便管理。
审计选项	“允许刻录，不审计刻录文件”，允许终端刻录且不会审计终端的刻录行为； “允许刻录，审计刻录文件”，允许终端刻录且终端刻录的动作将会被审计； “禁止刻录”，禁止终端的刻录行为
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	如果选择“在线时生效”，则只对客户端处于在线状态时刻录行为进行控制和审计；如果选择“离线时生效”则只对客户端处于离线状态时的刻录行为进行控制和审计。如果不选择，则不生效
策略应用对象	点击“查看及编辑”超链接，对象类型可以选

	择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用刻录审计策略。
--	---

说明

- ◆ 刻录审计只能审计到利用 windows 自带的刻录功能进行的审计，第三方软件的刻录行为审计不到
- ◆ 禁止刻录除了可以禁止 windows 自带的刻录以外，还可以禁止：UltraISO、Magic ISO Maker、IsoBuster、ImgBurn

配置要点

1、 点击“添加” 刻录审计 策略



刻录审计

策略名称 *

策略描述

审计选项
☒ 允许刻录，不审计刻录文件
☐ 允许刻录，审计刻录文件
☐ 禁用刻录

生效时间
☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

2、 点击策略应用对象的“查看及编辑”超链接，选择指定的 IP 组、用户组、工作组、主机名，则这些 IP 组、用户组、工作组、主机名中的电脑启用刻录审计。

3、 “保存”并更新客户端规则。

12.10. Windows 事件日志审计

12.9.1Windows 事件日志审计页面

配置介绍

Windows事件日志审计

Windows事件日志审计

策略名称

Windows事件日志审计*

策略描述

☒ 发送应用程序日志到服务器

☒ 发送安全日志到服务器

☒ 发送系统日志到服务器

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

结束时间

编辑

删除

2012-03-10 9:00

2012-03-10 13:30

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象)

查看及编辑

创建类型

全局

创建者

jing

注：右边有*号的项目必须输入。

保存

取消

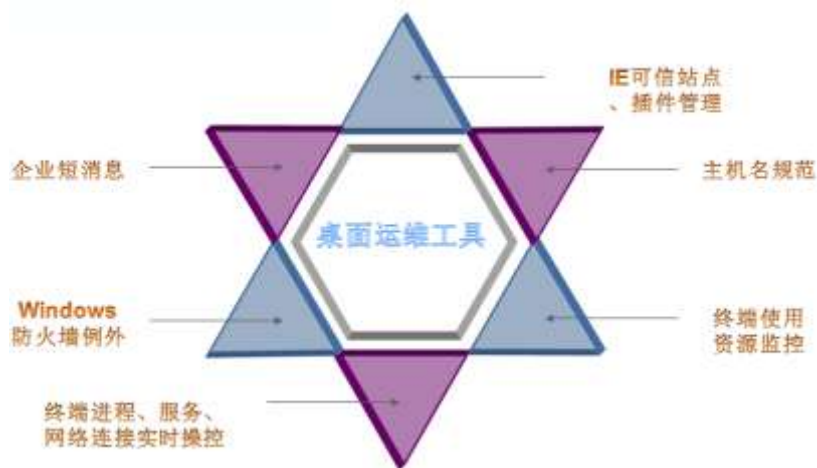
策略名称	输入合适的策略名称，以方便管理。
策略描述	输入适当的描述，以方便管理。选择“发送应用程序日志到服务器”或“发送安全日志到服务器”或“发送系统日志到服务器”，客户端将会把相应的日志上报给服务器。
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	对于 Windows 事件日志审计，在线模式功能无效

策略应用对象	点击“ 查看及编辑 ”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用 Windows 事件日志审计策略。
--------	---

13. 桌面运维

13.1. 关于桌面运维

天珣除了提供资产管理、远程桌面、软件分发等通用的终端运维管理功能模块之外，还提供了多种桌面运维工具，例如主机名规范、企业短消息、终端资源监控、Windows 防火墙例外、终端实时操控等，为管理员提供高效工具，成为管理员终端运维的好帮手。



13.2. 软件分发

13.2.1. 关于软件分发

- 软件分发在天珣产品功能模块中属于相对比较独立一个功能，

- 其主要用于对受控终端进行统一的软件或者文件的分发。
- 软件分发不仅能对可执行文件 exe，标准 msi 等安装程序进行分发，也能直接下发文件或文件夹，并可针对判断条件进行设置，便于对执行过程中的任何问题进行监控。
 - 软件分发可以支持域环境下普通用户帐户对分发的软件进行安装。

13.2.2. 软件分发设置页面

配置介绍

软件分发							
软件分发策略							
任务名称	任务描述	分发条件	已安装	分发失败	任务状态	任务截止时间	操作
test		0	0	1	任务过期	2012-10-17	↓
test_20	test_20	0	1	0	正常	2012-10-24	↓ ↑
test_21		0	0	0	校验失败	2012-10-24	↓ ↑
test_22		0	0	0	校验失败	2012-10-29	↓ ↑
test_23		0	1	0	正常	2012-10-29	↓ ↑
test_24		0	1	0	正常	2012-10-29	↑

点击“添加”按钮设置软件分发策略

软件分发 软件分发查看 软件分发默认帮助

软件分发

任务名称

任务描述

任务类型

分发文件或文件夹

安装包启动程序

安装参数

图标路径

安装选项

任务截止日期

任务执行时段

策略应用对象

是否在所有平台生效

Windows 2000

Windows XP

Windows 2003

Windows Vista

Windows 2008

Windows 7

创建状态

创建者

满足以下条件执行安装

满足以下条件任务完成

配置项:	说明
任务名称	为软件分发的任务命名。
任务描述	用以描述该任务的详细信息。
任务类型	定义分发的文件是何种类型，包括“安装包分发”、“文件分发”和“注册表文件分发”三种。
分发文件或文件夹	选择此次分发的文件所在的路径，点击“选择”

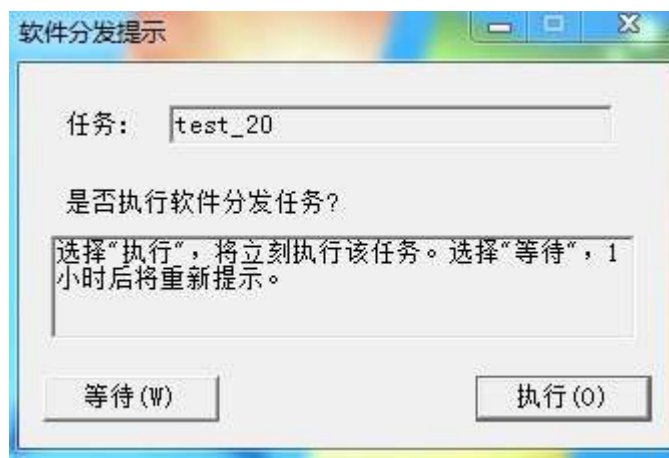
	按钮进行选择。
安装包启动程序	选择分发的安装包启动时调用的安装文件，仅“安装包分发”时可用。
安装参数	对安装的程序包进行参数设置（当需要设置时可参考安装程序的帮助手册了解其特定的安装参数），仅“安装包分发”时可用。
目标路径	设置被分发的文件将被保存在客户端的哪个路径下面，仅“文件分发”时可用。注册表文件分发默认路径为 C 盘，不需要填写目标路径。
安装选项	选项“安装前提示用户”对于软件分发策略下发后在客户端进行提示等待还是执行安装。 选项“以系统身份运行”，支持域环境下以普通用户帐号对分发的软件进行安装。 选项“该任务不需要用户交互”为安装过程不需要用户确认或点“下一步”，后台完全静默安装。 选项“完成任务后 ☐ 分钟关机”支持任务完成后自动关机，增加一个可倒计时关机的参数，可选择 1-999 的参数值，一分钟为单位。 选项“任务执行失败也自动关机”勾选了完成任务后自动关机，才允许勾选“任务失败也执行自动关机”。
任务截止日期	此软件分发任务最终失效时间，默认为当前日期 7 天以后，即默认任务有效期为 7 天。
任务执行时间段	设置此软件分发任务在一天内哪个时间段执行
策略应用对象	关联到 IP 组、工作组、主机名使策略生效
是否在以下平台生效	选择策略生效对应的客户端操作系统平台
满足以下条件执行安装	检查路径或注册表的信息来定义是否让客户端

	执行此次的软件分发策略
满足以下条件任务完成	检查路径或注册表的信息来定义是否此次客户端软件分发的任务完成

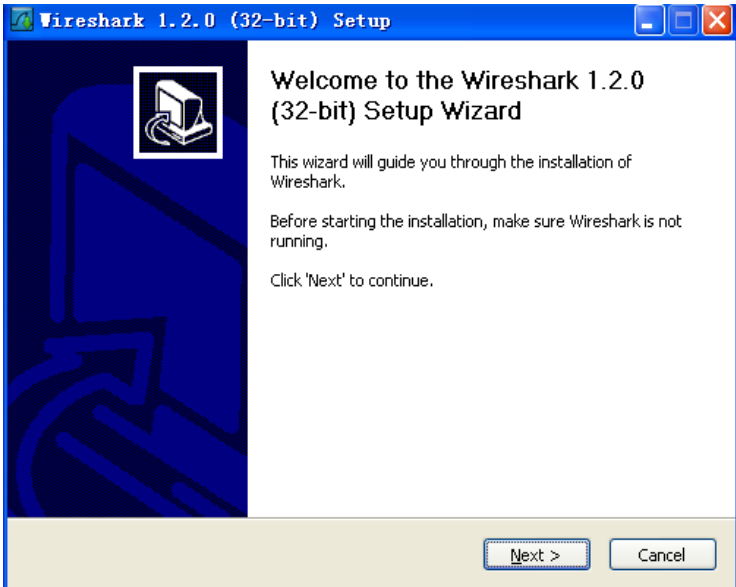
注意：文件分发路径默认设在天珣中心和本地服务器安装目录下的 SDDownload 目录，所有的分发文件请在分发前都复制到此目录中。

配置要点

- 1、点击“添加”按钮设置策略；
- 2、添加一个任务分发 wireshack 抓包软件，并检查路径 c:\program files\abc 存在时完成软件分发任务；
- 3、添加 IP 组对客户端进行分发；
- 4、客户端在接收到策略后，弹出提示页面：



- 5、点击“执行”后，进行软件正常安装：



13.2.3. 软件分发查询页面

配置介绍

软件分发 软件分发查询 软件分发默认参数

软件分发查询 [帮助](#)

任务名称

所有任务

分发状态

所有状态

IP地址

MAC地址

主机名

查询

重置

配置项:	说明
任务名称	选择任务类型，分为“所有任务”、“未过期任务”和“已过期任务”以及每天策略的名称。
分发状态	选择软件分发任务的状态类型，分为“所有状态”、“等待分发”、“正在下载”等。
Ip 地址	输入需要查询分发状态的终端的 IP 地址。
Mac 地址	输入需要查询分发状态的终端的 MAC 地址。

主机名

输入需要查询分发状态的终端的主机名。

可分别根据任务名称和分发状态，以及被分发的客户端的 IP 地址、MAC 地址和主机名等条件进行查询。

点击“查询”进入详细查询页面：

任务名称	任务状态	进行中	已完成	分发数量	任务类型	分发状态	任务截止时间
任务名称	0	1	0	0	安装软件分发	选择	2012-12-29
task_001	1	1	0	0	安装软件分发	选择	2012-11-01
task_002	0	0	0	0	文件分发	选择	2012-12-29
task_003	0	0	0	0	系统补丁分发	选择	2012-12-29
task_004	0	0	0	0	系统补丁分发	选择	2012-12-29
task_005	0	0	0	0	系统补丁分发	选择	2012-12-29
task_006	0	0	0	0	系统补丁分发	选择	2012-12-29
task_007	0	0	0	0	系统补丁分发	选择	2012-12-29
task_008	0	0	0	0	系统补丁分发	选择	2012-12-29
task_009	0	0	0	0	系统补丁分发	选择	2012-12-29

此页面显示的是该任务的分发状态及是否已完成。

再次点击“任务名称”进入详细任务状态查询页面：

任务名称	任务状态	进行中	已完成	分发数量	任务类型	分发状态	任务截止时间	任务备注
task_001	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_002	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_003	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_004	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_005	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_006	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_007	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_008	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	
task_009	安装软件分发	10.10.10.1	10.10.10.1	10.10.10.1	安装软件分发	选择	2012-12-29	

此页面可查询某台客户端进行此次软件分发的状态。

13.2.4. 软件分发默认参数页面

配置介绍

软件分发	软件分发查询	软件分发默认参数
服务器带宽 2000 KB/S 最大值为102400KB 客户端带宽 512 KB/S 最大值为102400KB 客户端上报时间间隔 10 分钟 保存		

配置项:	说明
服务器带宽	输入用于软件分发的全局服务器最大带宽流量，默认为 2000KB/S
客户端带宽	输入用于软件分发的全局单台客户端最大带宽流量，默认为 512KB/S
客户端上报时间间隔	设置客户端分发状态上报时间，默认为 10 分钟

13.3. 短消息

13.3.1. 关于短消息

- 短消息功能使管理员可以统一向客户端发送文字短消息，以行使通知、提醒等功能。

配置介绍

短消息

终端消息推送

短消息

短消息标题

短消息编辑框

是否要求确认

授权发布单位

正式发布日期

重复发布周期

生效截止日期

策略应用对象

创建类型

创建者

注：右边有*号的项目必须输入。
短消息保存后将不能再修改。

保存

取消

*

☒ 否 ☐ 是

天 * (0为不重复提示)

(还没有应用到任何对象) [查看及编辑](#)

全局

jing

配置项:	说明
短消息标题	输入该条短消息的标题以便进行管理
短消息编辑框	短消息的内容，注意只能是文字内容
是否要求确认	要求用户是否需要阅读的短消息进行确认； 选择“是”，则客户端更新策略拿到短消息后，会弹出消息阅读框，并且置顶显示，直到用户点击确认，消息框才会消失； 选择“否”，则客户端更新策略拿到短消息后，电脑桌面右下角，会弹出消息提示，点击阅读； 无论选择“是”还是“否”，短消息的阅读记录都会从历史短消息中查询出来
授权发布单位	短消息发布的单位
正式发布时间	短消息发布的时间
重复发布周期	短消息重复发布的周期
生效截止日期	短消息生效的截止日期
策略应用对象	设置接收该短消息的 IP 组、工作组、主机名

13.3.2. 关于终端消息推送

- 终端短消息推送能使管理员精确的向一个或多个客户端实时推送文字短消息，以行使通知、提醒等功能。

配置介绍

点击“客户端实时短消息”的“添加”按钮

短消息

终端消息推送

客户端实时短消息

短消息标题

中秋快乐！*

短消息编辑框

(最大字数限制100个汉字，禁止发布不正当言论！)

月到中秋分外明，节日喜气伴你行。人逢喜事精神爽，人团圆事业旺。节日愉快身体健，心想事成您准赢。

保存

删除

取消

配置项:	说明
短消息标题	输入该条短消息的标题以便进行管理
短消息编辑框	短消息的内容，注意只能是文字内容

保存后如图

短消息

终端消息推送

客户端实时短消息

消息

内容

短消息标题

中秋快乐！

发送到

选择需要发送的实时短消息点击“发送到”按钮

短消息

终端消息推送

客户端实时短消息

客户端IP地址

起端IP地址

使用人

部门

选择部门

主机名

过滤

复选框	IP地址	主机名	使用人	部门	MAC地址
☐	10.201.110.22	albjia-774c3165			00-0C-29-52-52-30
☐	10.201.254.10	352-PC			0C-62-8D-46-82-T2
☐	10.201.100.123	W38-TLTXKJ00FL			00-0C-29-04-47-FA
☐	10.201.140.45	dao-PC			00-24-81-58-33-3F
☐	10.201.139.1	zywans-mj			00-1C-25-6B-0A-5A
☐	10.201.202.44	win-844	zshsp	测试部-%	00-0C-29-52-T3-79
☐	10.201.202.68	win-844	asd	测试部-%	00-0C-29-AC-56-3E
☐	10.201.99.208	jia209-PC	dcf	测试部-%	00-28-18-6E-40-50
☐	172.28.89.101	vaosaz			00-28-C6-81-57-34
☐	10.201.99.199	jia2003			000C29C7D8E

发送

取消

勾选接收短消息的终端，然后点击发送就可以了。

13.4. 计算机名规范

13.4.1. 关于主机名规范

- **主机名规范：**为管理员提供了一种便利的手段管理整个网络中的主机名，使统一命名网络中的主机名成为可能。

配置介绍



主机名规范配置界面截图。界面顶部有“主机名规范”和“工作主机规范”两个标签。左侧是配置项列表，包括“主机名规范名称”、“描述”、“选项”、“创建类型”和“创建者”。右侧是配置内容区域，包含三个单选按钮：“不启用主机名绑定，允许修改主机名”（当前选中）、“不启用主机名绑定，禁止修改主机名”和“启用主机名绑定，禁止修改主机名”。下方是一个表格，列出了终端ID、IP地址、MAC地址和主机名。表格下方有“从文件导入”、“导出”和“下载导入模板”按钮。底部有“保存”和“取消”按钮。

配置项：	说明
主机名规范名称	输入该策略的名称
描述	对该策略的描述
选项	选择“不启用主机名绑定，允许修改主机名”，则该客户端不启用主机名绑定，但可以任意修改主机名。选择“不启用主机名绑定，禁止修改主机名”则该客户端不启用主机名绑定，但也不能修改主机名。选择“启用主机名绑定，禁止修改主机名”则该客户端启用了主机名绑定，不能修改主机名。可以点击“从报表添加”按钮获得相应的终端 ID、IP 地址、MAC 地址、主机名。

13.4.2. 配置要点

1、点击“添加”新建一个主机名规范，如下图所示：



2、点击“从报表添加”以添加绑定项。如下图所示：



5、选择想要绑定的终端项，点击“保存选择的项目”以保存，或点击“保存所有的项目”。如下图所示：



7、点击某客户端主机名修改主机并保存。

8、更新客户端规则以使策略生效。

13.4.3. 关于工作组名规范

- **工作组名规范:** 为管理员提供了一种便利的手段管理整个网络中的工作组名，使统一命名网络中的工作组名成为可能。

配置介绍



配置项:	说明
主机名规范名称	输入该策略的名称
描述	对该策略的描述
选项	选择“不启用工作组名绑定，允许修改工作组名”，则该客户端不启用工作组名绑定，但可以任意修改工作组名。选择“不启用工作组名绑定，禁止修改工作组名”则该客户端不启用工作组名绑定，但也不能修改工作组名。选择“启用工作组名绑定，禁止修改工作组名”则该客户端启用了工作组名绑定，不能修改工作组名。可以点击“从报表添加”按钮获得相应的终端 ID、IP 地址、MAC 地址、工作组名。

13.4.4. 配置要点

1、点击“添加”新建一个主机名规范，如下图所示：



2、点击“从报表添加”以添加绑定项。如下图所示：



5、选择想要绑定的终端项，点击“保存选择的项目”以保存，或点击“保存所有的项目”。如下图所示：



7、点击设置绑定的笔形编辑按钮修改某客户端的工作组名并点绿色钩保存，再保存整个策略。

	间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	选择该策略生效的网络场景，分为“在线时生效”和“离线时生效”
策略应用对象	关联到 IP 组、工作组、主机名使策略生效

配置要点

- 1、 点击“添加”远程文件删除策略，如下图：



- 2、 填写要删除的文件路径及文件名称，添加到删除文件列表
- 3、 点击“策略应用对象”->“查看及编辑”超链接，关联指定的 IP 组、工作组、主机名
- 4、 保存，更新策略。

13.6. 自动关机策略

13.6.1. 关于自动关机策略

- 自动关机策略能指定客户端的关机，同时可以指定客户端系统空闲时的等待关机时间，有效解决人离开了计算机没有关闭带来的管理弊端及风险。

自动关机策略

策略名称

策略描述

自动关机时间

系统空闲关机时间

生效时间

在线模式

策略应用对象

创建类型

创建者

注：右边有*号的项目必须输入。

保存

取消

策略名称 *

策略描述

自动关机时间 (24小时制, 格式 hh:mm)

系统空闲关机时间 分钟 (注：系统空闲指鼠标, 键盘都不操作的时间)

生效时间

☒ 所有时间
 ☐ 工作时间
 ☐ 非工作时间
 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式

☒ 在线时生效
 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

配置项:	说明
策略名称	为该策略命名
策略描述	该策略的详细说明
自动关机时间	指定终端计算机的关机时间 (24 小时制, 格式 hh:mm)
系统空闲关机时间	系统空闲时间指鼠标键盘没有输入操作的空闲时间
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效, “开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	选择该策略生效的网络场景, 分为“在线时生效”和“离线时生效”
策略应用对象	点击“查看及编辑”超链接, 对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”

	四种类型，选择相应的应用对象则启用自动关机策略。
--	--------------------------

配置要点

- 1、点击“添加”远程自动关机策略，如下图：



自动关机策略配置界面截图。界面标题为“自动关机策略”。

策略名称：test *

策略描述：test if this rule can control auto shutdown.

自动关机时间：23:30 (24小时制, 格式: hh:mm)

系统空闲关机时间：60 分钟 (注：系统空闲指鼠标、键盘都不操作的时间)

生效时间：
☐ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☒ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式：
☒ 在线时生效 ☒ 离线时生效

策略应用对象：(还没有应用到任何对象) [查看及编辑](#)

创建类型：全局

创建者：jing

注：右边有*号的项目必须输入。

保存 取消

- 2、填写自动关机时间或系统空闲关机时间
- 3、点击“策略应用对象”->“查看及编辑”超链接，关联指定的 IP 组、工作组、主机名。
- 4、保存，更新策略。

13.7. Win 防火墙例外

13.7.1. 关于 Win 防火墙例外

- Win 防火墙例外可以设定指定应用程序进程，自动添加到 Windows 防火墙的例外列表中。

配置介绍

Win防火墙例外

Win防火墙例外

策略名称 *

策略描述

例外进程列表

进程名称	编辑	删除
	添加	

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

[保存](#) [取消](#)

配置项：	说明
策略名称	为该策略命名
策略描述	该策略的详细说明
例外进程列表	填写 Windows 防火墙例外的进程名
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	选择该策略生效的网络场景，分为“在线时生效”和“离线时生效”
策略应用对象	点击“查看及编辑”超链接，对象类型可以选择“IP 组”、“用户组”、“工作组”、“主机名”四种类型，选择相应的应用对象则启用 Win 防火墙例外策略。

配置要点：

- 1、点击“添加”Win 防火墙例外策略，如下图：

Win防火墙例外

Win防火墙例外

策略名称: qq.exe *

策略描述: QQ

例外进程列表:

进程名称	编辑	删除
qq.exe		

生效时间:

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30		

在线模式: ☒ 在线时生效 ☒ 离线时生效

策略应用对象: (还没有应用到任何对象) [查看及编辑](#)

创建类型: 全局

创建者: jing

注: 右边有*号的项目必须输入。

- 2、点击“策略应用对象”->“**查看及编辑**”超链接，关联指定的 IP 组、工作组、主机名，如下图。选择指定的 IP 组、工作组、主机名，并“确定”：

Win防火墙例外

qq.exe

对象类型: IP组

对象选择:

☒ 140	☒ 1722545	☒ 99100	☒ 90
☒ 110	☒ 222	☒ 20	☒ 172.25.20.123
☒ 172.25.1.110-111	☒ 84	☒ 172.25.22.220	☒ 33
☒ 254.x	☒ mj主机	☒ 172.25.85	☒ 99206
☒ 42	☒ 10.201.251		

- 3、“保存”并更新客户端规则。
- 4、点击“开始”→“控制面板”→“Windows 防火墙”→“例外”，确认 QQ 已经被成功添加到 Windows 防火墙例外中，如下图：



13.8. 终端实时操控

13.8.1. 关于终端实时操控

方便管理员主动连接至指定客户端查看和管理客户端服务、进程、网络连接、补丁信息等情况，以方便桌面运维。可以远程停止终端的服务、进程，可以更改远程终端相关服务器的启动方式，可以关闭远程终端的网络连接行为。也可以使用终端实时操作启用、禁用或删除指定终端的 IE 插件，管理员也可以用它来将指定的终端锁屏解锁，以及实时卸载客户端程序。

注意：“终端实时操控”的端口（UDP 7891）与应用准入端口相同。如果安装天珣客户端但仍然无法验证通过，可以在“终端实时操控”中输入该终端 IP 地址，如果无法查询则说明至客户端网络（UDP 7891）不通。

13.8.2. 服务页面

配置介绍



配置项:	说明
客户端 IP 地址	输入需查询客户端的 ip 地址。
更改启动方式	选中指定的服务，点击“更改启动方式”下拉列表框，即可更改该服务的启动方式。
操作	选中指定的服务，点击“操作”下拉列表框，即可更改该服务的状态。
服务名	输入“服务名”即可对指定的服务查询(过滤)。

说明：如果查询中提示“获取指定服务列表失败”，有可能是网络超时所导致，请多次尝试。多次尝试失败说明至天珣客户端网络不通。

配置要点

1、输入客户端 IP 地址，点击“查询”，如下图：



2、获得该客户端的服务列表如下：



3、选中需要更改启动方式的服务，并在下拉列表框中更改原服务启动方式，即可成功更改服务的启动方式：



4、选中需要操作的服务名称，下拉列表框中选择服务的操作类型，并点击确定，即可停止指定的服务。

13.8.3. 进程页面

配置介绍



配置项:	说明
客户端 IP 地址	输入需查询客户端的 ip 地址。
进程名	输入“进程名”即可对指定的进程查询（过滤）。

说明：如果查询中提示“获取指定进程列表失败”，有可能是网络超

时所导致，请多次尝试。多次尝试失败说明至天珣客户端网络不通，请检查客户端防火墙。

重要：强行杀除系统进程存在系统蓝屏、死机或数据丢失的现象，建议慎重处理！

13.8.4. 网络连接页面

配置介绍

服务 进程 网络连接 实时补丁查询 IE插件管理 终端故障 终端维护										
查看客户端连接信息										
注：*本功能只通过XXT连接服务器端的客户端无效										
客户端IP地址 10.201.90.203 查询										
序号	协议	本地IP	本地端口	远端IP	远端端口	状态	进程	操作	结束进程	
1	TCP	10.201.90.203	82908	104.172.245.35	118	ESTABLISHED	C:\Program Files (x86)\Wangsheng\Hadoop\Security\SECURITY.exe	结束	结束进程	
2	TCP	10.201.90.203	82907	10.201.1.204	8080	ESTABLISHED	C:\Program Files (x86)\Internet Explorer\iexplore.exe	结束	结束进程	
3	TCP	10.201.90.203	82908	10.201.1.204	8080	ESTABLISHED	C:\Program Files (x86)\Internet Explorer\iexplore.exe	结束	结束进程	
4	TCP	10.201.90.203	52418	10.201.1.204	8080	ESTABLISHED	C:\Program Files (x86)\Internet Explorer\iexplore.exe	结束	结束进程	
5	TCP	10.201.90.203	52420	10.201.1.204	8080	ESTABLISHED	C:\Program Files (x86)\Internet Explorer\iexplore.exe	结束	结束进程	

配置项：	说明
客户端 IP 地址	输入客户端的 IP 地址，点击“查询”，即可查询到该终端的网络连接情况。

说明：如果查询中提示“获取指定网络连接失败”，有可能是网络超时所导致，请多次尝试。多次尝试失败说明至天珣客户端网络不通。

13.8.5. 实时补丁查询页面

配置介绍

服务 进程 网络连接 实时补丁查询 IE插件管理 终端故障 终端维护					
查询客户端实时补丁信息					
注：*本功能只通过XXT连接服务器端的客户端无效					
客户端IP地址 10.201.90.203 查询					
序号	补丁名	用户名	安装日期	备注	
1	KB2032270			Security Update	
2	KB2079403			Security Update	
3	KB2207966			Security Update	

配置项:	说明
客户端 IP 地址	输入客户端的 IP 地址，点击“查询”即可查询到当前系统的补丁安装情况。

13.8.6. IE 插件管理页面

配置介绍



配置项:	说明
客户端 IP 地址	输入客户端的 IP 地址，点击“查询”即可查询到当前系统的 IE 插件安装情况。

配置要点

- 1、输入目标主机的 IP 地址，点击查询即可查看该终端的 IE 插件安装情况。如下图所示：



- 2、选择需要处理的插件，点击“启用选中的控件”“禁用选中的控件”“删除选中的控件”可对选择的插件做相应的操作。同时，“操作”项中将显示目前该插件的状态。如下图所示：



13.8.7. 终端锁屏

- **终端锁屏**: 对终端进行实时的屏幕锁定，管理员若发现某终端非法接入或做出影响网络和其他终端安全行为时可对其进行及时控制。

配置介绍



配置项:	说明
客户端 IP 地址	输入客户端的 IP 地址，或“从终端发现里选择”需要锁屏的终端，点击“锁屏”可以将终端锁屏。

配置要点

- 1、输入目标主机的 IP 地址，或者从终端发现里选择相应的主机，如下图所示：



- 2、选择相应的客户端之后点击“锁屏”将该终端的屏幕锁定。同时，被配置的条目将出现在本策略的配置页面上。管理员可以本页中

选择对终端解锁。



13.8.8. 终端维护

配置介绍



配置项:	说明
客户端 IP 地址	输入客户端的 IP 地址，或“卸载”将该客户端程序卸载。
操作	卸载客户端，重启客户端，重启终端电脑，关闭终端电脑

13.9. 终端资源状况监控

13.9.1. 关于终端资源状况监控

- 终端资源监控为管理员提供了一种资源使用率监控手段，可使管理员及时了解终端的 CPU、内存、硬盘、网络的使用情况。

配置介绍

终端资源状况监控

终端资源状态监控

策略名称

*

策略描述

CPU使用率

☒ 监控 高于 0 %时告警 (0为不告警)

内存使用率

☒ 监控 高于 0 %时告警 (0为不告警)

硬盘剩余空间

☒ 监控 少于 0 GB时告警 (0为不告警)

网络数据包

☒ 监控 高于 0 时告警 (0为不告警)

网络字节数

☒ 监控 高于 0 KB时告警 (0为不告警)

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间

2012-03-10 9:00

结束时间

2012-03-10 13:30

添加

在线模式

☒ 在线时生效 ☒ 离线时生效

策略应用对象

(还没有应用到任何对象) [查看及编辑](#)

创建类型

全局

创建者

jing

注: 右边有*号的项目必须输入。

保存

取消

配置项:	说明
策略名称	为该策略命名
策略描述	用于描述该策略的详细信息
CPU 使用率	设置 CPU 使用率的告警值
内存使用率	设置内存使用率的告警值
硬盘剩余空间	设置硬盘剩余空间的告警值
网络数据包	设置网络数据包的告警值
网络字节数	设置网络字节数的告警值
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效,“开始时间”以及“结束时间”仅对“以下时间段”有效。
在线模式	生效时的网络场景,分为“在线时生效”和“离

	线时生效”
策略应用对象	点击“查看及编辑”超链接，对象类型可以选择“IP 组”、“工作组”、“主机名”三种类型，选择相应的应用对象则启用终端资源状况监控策略。

在“信息中心”>“桌面运维”->“终端资源使用状况告警”查看告警信息，如下图所示：

终端资源使用状况告警查询						
策略统计 导出图表 设为首页						
主机名称	IP地址	上报时间	报警内容	报警类型	部门名称	
JTAR	172.25.100.206	2010-7-26 22:21:33	网络数据包: 51 KB	网络数据包告警	科技部	
JTAR	172.25.100.206	2010-7-26 22:21:33	网络字节数: 10.3M	网络字节数告警	科技部	
JTAR	172.25.100.206	2010-7-26 22:21:33	内存使用率: 24%	内存使用率告警	科技部	
JTAR	172.25.100.206	2010-7-26 22:21:33	内存使用率: 24%	内存使用率告警	科技部	
JTAR	172.25.100.206	2010-7-26 22:21:33	网络数据包: 42 KB	网络数据包告警	科技部	
JTAR	172.25.100.206	2010-7-26 22:21:33	网络字节数: 8.3M	网络字节数告警	科技部	
JTAR	172.25.100.206	2010-7-26 21:21:33	内存使用率: 24%	内存使用率告警	科技部	
JTAR	172.25.100.206	2010-7-26 21:21:33	网络数据包: 42 KB	网络数据包告警	科技部	
JTAR	172.25.100.206	2010-7-26 21:21:33	网络字节数: 8.3M	网络字节数告警	科技部	
JTAR	172.25.100.206	2010-7-26 20:21:33	内存使用率: 23%	内存使用率告警	科技部	
第1页/共112页1123条数据						

14. 认证管理

14.1. 第三方 CA 机构

第三方 CA 机构页面用于实现导入第三方 CA 机构根证书即其相关信息的功能，可用于在登录天珣用户控制的时候验证该 CA 机构颁发的用户证书。点击“第三方 CA 机构”页面上的“添加”

第三方CA机构

CA名称	第三方CA机构
CA描述	
数字证书	上传证书
吊销证书列表	上传吊销证书列表
OCSP服务路径	
证书状态验证	☒ 不验证证书状态 ☐ 先进行在线验证，没有CA服务器或CA服务器不可用时使用吊销证书列表验证
是否启用	☒ 启用 ☐ 禁用

注：右边有*号的项目必须输入

配置项：	说明
CA 名称	填写易区别的名称
CA 描述	详细描述 CA 的相关属性
数字证书	点击右边的“上传证书”可以上传第三方根证书
吊销证书列表	上传被吊销用户名的列表
OCSP 服务路径	填写 OCSP 服务路径，用于在线验证证书状态
证书状态验证	可选择是否要验证证书状态
是否启用	配置启用还是禁用此根证书

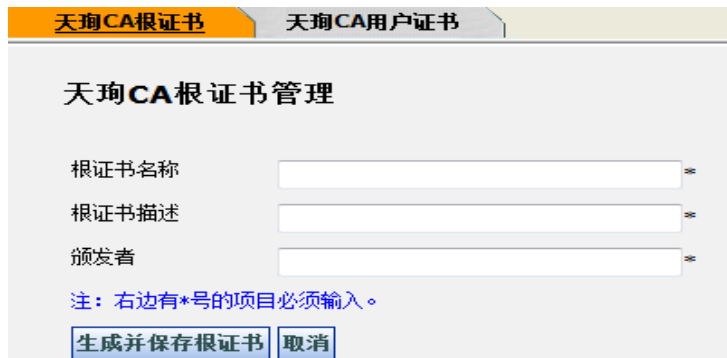
14.2. 天珣 CA 机构

*该章节功能仅适用于增强身份认证基础版和增强身份认证高级版

天珣系统自带轻量级的 CA，支持证书的生成、颁发，并且可以将证书颁发到 UKEY 介质中。

14.2.1. 天珣 CA 根证书

点击“天珣 CA 根证书管理”页面上“添加”按钮



天珣CA根证书管理

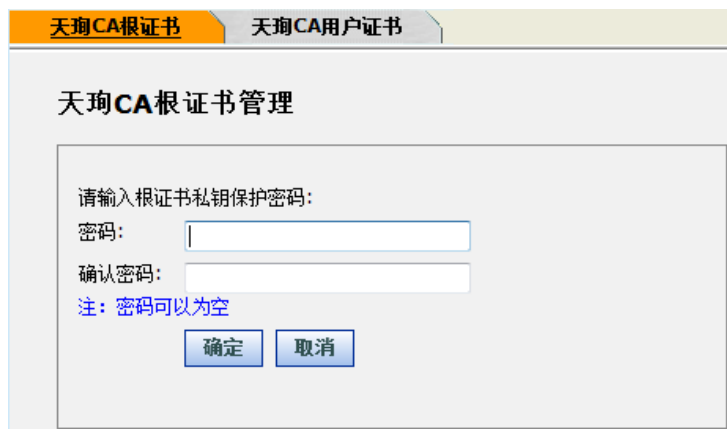
根证书名称

根证书描述

颁发者

注：右边有*号的项目必须输入。

“根证书名称”、“根证书描述”同“颁发者”都是必填项，可根据自身要求填写；点击“生成并保存根证书”时，弹出私钥保护密码输入框，校验一致后对证书的私钥部分进行加密。



天珣CA根证书管理

请输入根证书私钥保护密码：

密码：

确认密码：

注：密码可以为空



天珣CA根证书

天珣CA用户证书

天珣CA根证书管理

根证书名称

test

*

根证书描述

test

*

颁发者

test

*

注：右边有*号的项目必须输入。

导出公钥证书

备份

删除

取消

说明

- 天珣根证书页面仅可以创建一个根证书，根证书创建完成后，不可修改，但可以删除或者备份；
- 天珣根证书私钥保护密码，管理员务必牢记，服务器不保存该密码；
- “备份”出来的根证书不能为第三方应用系统使用；若要使用此根证书，请使用“导出公钥证书”功能，可导出 cer 格式的根证书

14.2.2.天珣 CA 用户证书

天珣CA根证书

天珣CA用户证书

天珣CA用户证书

生成新证书

生成吊销列表

显示未吊销的证书

显示已吊销的证书

帮助

证书用户名	部门	邮件地址	颁发者	是否吊销	有效期
test	AAA	test@test.com	test	否	2012-03-13 至 2012-03-30

点击“天珣 CA 用户证书”页面上的“生成新证书”按钮

天珣CA根证书
天珣CA用户证书

生成新证书

证书用户名 *

部门 选择部门

邮件地址

有效期

三月, 2012

周	日	一	二	三	四	五	六
8						1	2
9	4	5	6	7	8	9	10
10	11	12	13	14	15	16	17
11	18	19	20	21	22	23	24
12	25	26	27	28	29	30	31

时间: 11:48

三, 三 7

注: 右边有*号的项

生成新证书

点击“生成新证书”时，弹出根证书私钥保护密码输入框，校验一致后生成新的用户证书。

天珣CA根证书
天珣CA用户证书

请输入根证书私钥保护密码

密码:

确定
关闭

说明： 点击“生成新证书”时，如果是本地登录第一次点击，则会弹出根证书私钥保护密码的输入框，如果不是本地登录第一次点击，则不要求输入根证书私钥保护密码

插入 UKEY，点击颁发到 UKEY，弹出 pin 码校验框。



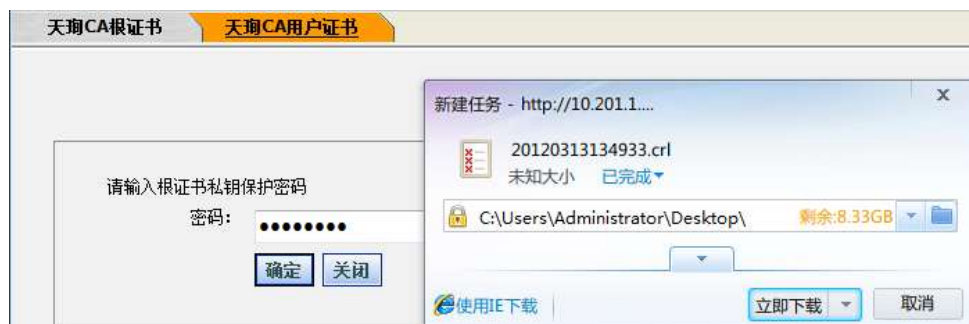
证书颁发到 UKey 成功，如下：



说明：

- ◆ 第一次进入“天珣 CA 用户证书”页面时页面会提示安装 ActiveX 控件及启明星辰安全证书。
- ◆ 天珣自带 CA 是轻量级的 CA，因此不单独提供和维护吊销列表。仅提供生成导出功能。
- ◆ Vista 以上系统运行该功能，须以管理员身份运行 IE。

天珣 CA 用户证书页面，点击“生成吊销列表”按钮，



14.2.3.天珣 CA 用户证书页面证书及 ActiveX 控件安装

第一次点击“天珣 CA 用户证书”页面时，页面会弹出需要安装 ActiveX 控件的提示，用于实现颁发证书到 UKey，现在详述 ActiveX 控件及证书的安装步骤，如下：

第一次去到“天珣 CA 用户证书”页面后，页面上弹出需要安装 ActiveX 控件的提示

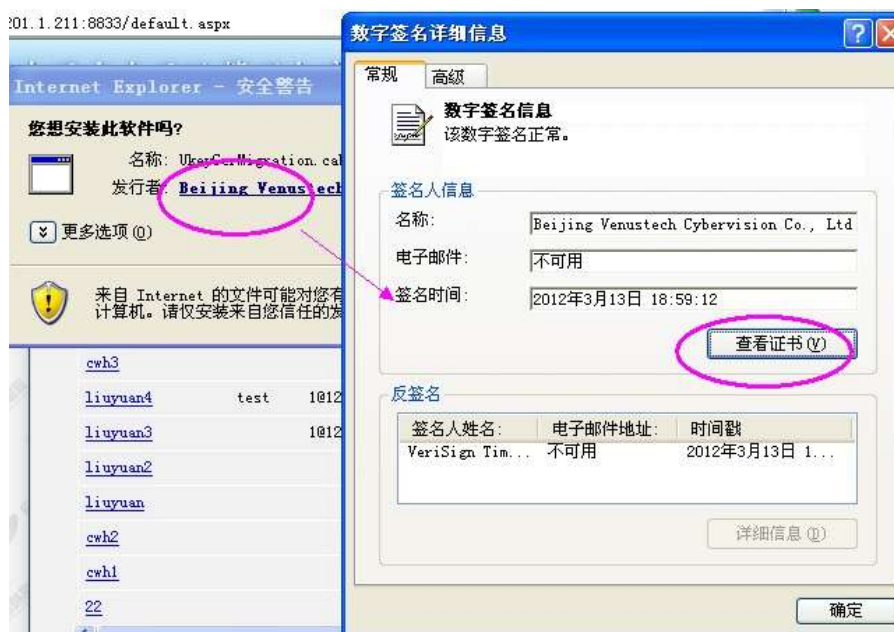


右键点击弹出框并选择“安装 ActiveX 控件”，注意名称



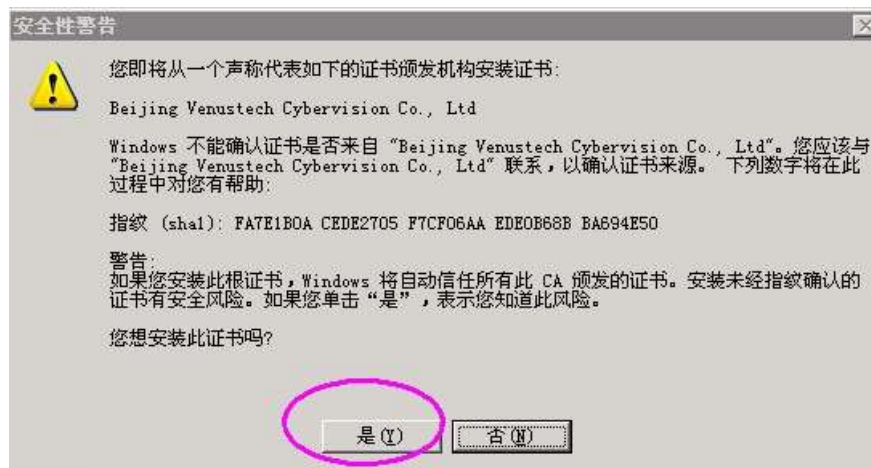
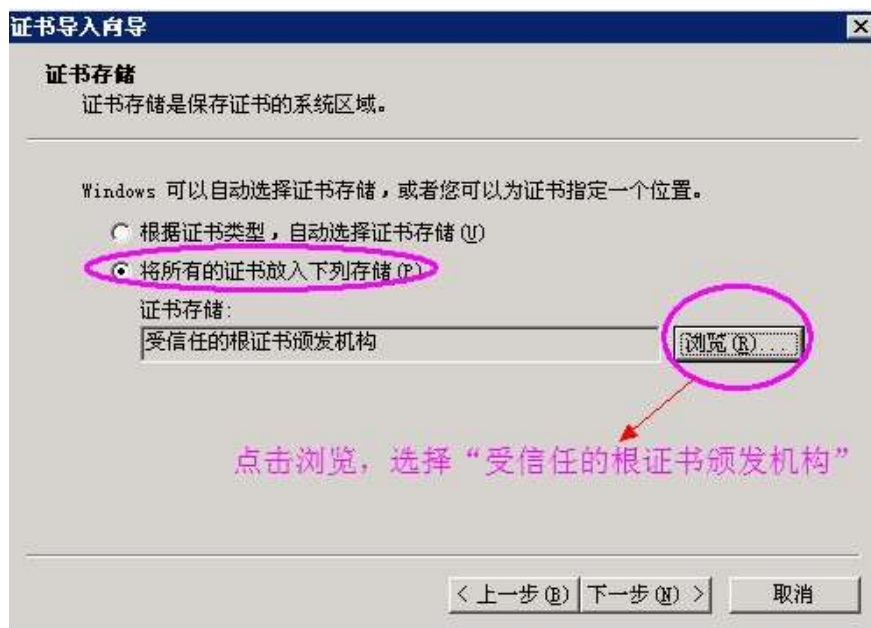
点击“Beijing Venustech Cybercision Co.,Ltd”进入“数字签名详细信息”页面，

再点击“查看证书”



跳到“证书”页面，点击“安装证书”





点击“是”后，会弹出证书安装成功的提示，这是说明证书已经安装成功了。

现在接着安装 ActiveX 控件，接着上述步骤，刷新该页面，然后再进入“天珣 CA 用户证书”页面，就会弹出一个安装插件的提示，



点击“安装”，安装成功后，刷新该页面，就可以开始颁发天珣用户证书了。

14.3. 身份认证

*该章节功能仅适用于增强身份认证基础版和增强身份认证高级版

14.3.1. 关于身份认证

身份认证包括用户及证书信息管理和超级用户, 用户及证书管理用于将用户及证书关联起来, 此处的用户可以为天珣本地用户、AD 域用户及第三方 LDAP 用户; 超级用户页面用于规定网络认证的用户是否以名称为 TXAdmin 的超级管理员登录 windows 系统。

14.3.2. 用户及证书管理配置介绍

以添加 AD 域用户为例。

(1) 先到“基本配置”的“用户组”里面配置相关的目录服务, 详细配置请参考 [4.10.2](#)

(2) 回到“用户及证书信息管理”配置页面, 点击“第三方系统导入”



选择目录服务



选择对应的目录服务之后, 点击“添加成员”按钮:



点击“users”，选择用户，勾选需要添加的用户，然后点击“添加选择的项目”的按钮：



接着点击“目录浏览”旁边的“返回”按钮，跳转到此界面，再点击“保存”按钮，即可添加成功



(3) 将用户名称同证书名称进行绑定。点击对应的登录名：

用户及证书					
第三方系统导入 从文件导入 下载文件导入模板					
登录名	用户类型	目录服务	姓名	证书用户名	绑定终端
link		linkworkad	link		
link		linkworkad	link		

用户及证书信息管理 超级用户

用户信息编辑

用户登录名

姓名

用户类型Active Directory Server

目录服务dc=linkworkad, dc=net

目录服务路径linkworkad

部门

选择部门

电子邮件

证书用户名venus

保存

删除

取消

例如填写证书用户名 venus，然后保存。

(4) 如果需要为该证书绑定终端，点击下图按钮

用户及证书					
第三方系统导入 从文件导入 下载文件导入模板					
登录名	用户类型	目录服务	姓名	证书用户名	绑定终端
link		linkworkad	link	venus	
link		linkworkad	link		

点击“添加绑定终端”列的图标

用户及证书信息管理 超级用户

证书详细信息

登录名link

证书用户名dc=linkworkad

添加绑定终端

删除选中终端

GUID	终端名	MAC地址	主姓名	使用人	部门

保存

取消

勾选想要绑定的终端 GUID，点击“确定”按钮：



然后在点击“保存”按钮，即成功绑定终端：

配置项：	说明
登录名	用于天珣用户认证取策略的帐号
用户类型	用来表示该登录名是哪种用户类型，比如“本地用户”，“AD 域”或者“LDAP”。
目录服务	显示的是目录服务的名称。
姓名	仅是一个标记，其配置不影响功能的使用。
证书用户名	证书用户名是颁发到 Ukey 里面的证书用户名称。
添加绑定终端	某证书绑定了对应的终端之后，该证书只能在绑定的终端上使用，其他终端不可使用该证书。
删除绑定终端	可以删除已经绑定的终端

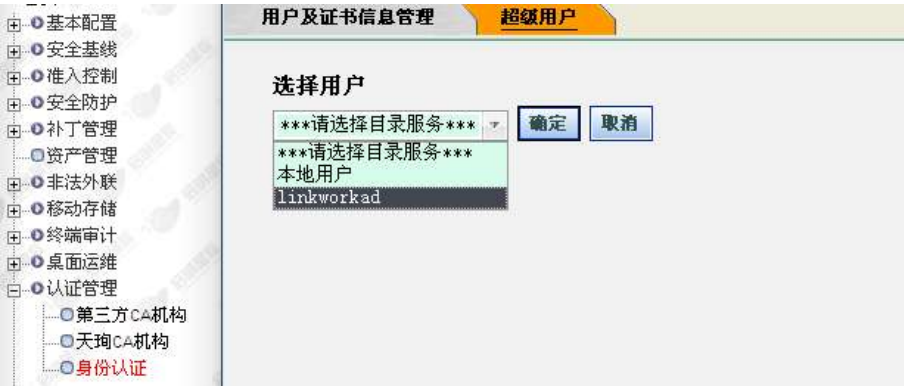
注意：

- 天珣本地用户不用另外导入，只需要在[基本配置→本地用户](#)页面添加完之后，就会自动出现在用户及证书页面；
- 天珣本地用户绑定证书可以按照上述方法绑定，也可以在[基本配置→本地用户](#)页面进行绑定。

14.3.3.超级用户

超级用户，即启用单点登录功能时，总是以管理员 TXAdmin 身份登录 Windows 系统的网络认证用户。用户可为天珣本地用户、AD 域用户和第三方 LDAP 用户。

添加超级用户的步骤如下：
在“超级用户”页面点击“选择用户”，跳转到如下页面：



比如添加本地用户，选择对应的登录名之后，点击“确定”按钮：



配置项：	说明
用户帐号	此处的用户帐号就是登录名。
目录服务	包括本地用户或者第三方系统目录服务。
操作	当点击“取消”时，则此条策略将被删除。

添加成功。
单点登录时，如果以该帐号或者该帐号关联的证书登录系统时，Windows 系统则会以 TXAdmin 登录，并且该 TXAdmin 帐号具备管理员权限。

注意：如果你打包[单点登录客户端安装包](#)的时候，选择“Windows 本地登录帐号”为“与网络认证相同的 AD 域帐号”时，就不会以 TXAdmin 帐号登录了，而只会以该 AD 域帐号登录。

15. 信息中心

15.1. 关于信息中心

- 信息中心集中展现了终端的分布及受控状态、终端的资产报表、攻击告警及审计数据等重要信息，管理员可以在此处对终端的基本状况和策略配置后终端的执行状态进行详细查询，以便对策略运行的效果进行监督并根据报表进行改进。
- 在信息中心我们预置了超过 70 种不同的查询或统计报表，并通过各种条件的组合查询来满足不同用户的不同需求。在报表生成之后可以通过导出到 excel 方便对比和存档，每个报表在生成后都可将其设置为报表的首页，方便管理员实时查看。
- **接入信息：**对终端设备运行状态统计，包括终端数量、在线数量、受控数量、非受控数量和不合规数量等，以便于管理员实时查看终端运行状况。
- **资产信息：**显示上报的所有受控终端的资产信息，可详细查询终端的硬件资产，也可查询安装的软件信息等。包括终端品牌, CPU, 主板, 硬盘, 内存, 显卡, 声卡, 操作系统, 指定软件, 防病毒软件等进行查询统计。
- **补丁信息：**对客户端补丁安装情况进行查询统计
- **审计信息：**详细审计终端的各种行为，例如上网 URL、文件操作、打印, 主机名, IP, MAC 变更, 等审计信息。
- **安全基线：**详细审计终端所有安全基线违规的行为，例如强制补丁, 进程管理, 软件安装, 防病毒软件, 安全加固
- **外联控制：**详细审计终端设备非法外联，例如外设违规, 多网卡

使用, 异常路由

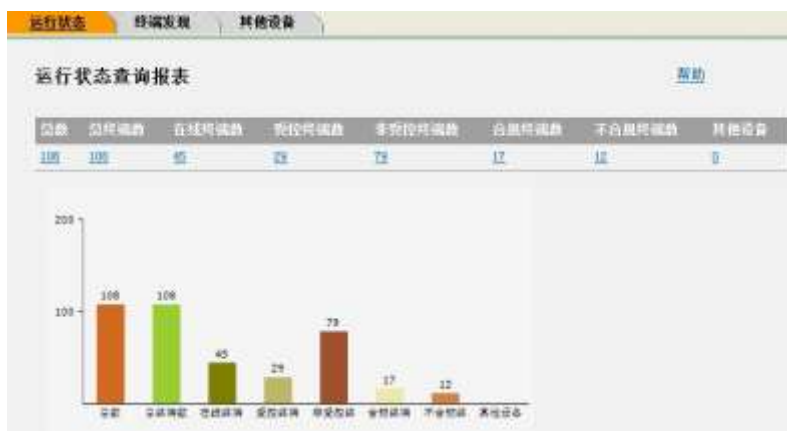
- **攻击告警:** 记录一段时间内终端的 TCP/UDP 异常、流量异常、ARP 欺骗发生情况等, 并能详细记录终端的防火墙日志。通过这些日志, 管理员能轻松发现终端存在的问题并及时加以改进。
- **移动存储:** 审计终端移动存储设备的操作行为
- **桌面运维:** 详细查询统计到终端资源使用状况和短消息阅读情况
- **级联报表:** 详细查询统计到所在单位的终端发现、补丁安装信息、补丁安装信息、安全基线违规终端、策略分发统计、资产信息操作系统以及主机类型统计的级联报表。

15.2. 接入信息

15.2.1. 配置介绍

对终端设备运行状态统计, 包括终端数量、在线数量、受控数量、非受控数量和不合规数量等, 以便于管理员实时查看终端运行状况。受控终端即已安装天珣客户端的终端。

接入信息



配置项:	说明
总终端数	所有子网中受控与非受控终端数合计
在线数量	目前在线的终端数，同时包括受控与非受控终端
受控数量	已安装天珣客户端的终端数量
非受控数量	未安装天珣客户端的终端数量
合规数量	受控终端中安全基线满足要求的终端数量
不合规数量	受控终端中安全基线不满足要求的终端数量
其他设备	网关,打印机,交换机,路由器,IP 电话等其他类型的非受控终端

注意: 一个子网中至少要有一台已安装天珣客户端的终端存在才能发现这个子网中所有的其他终端的情况，

比如点击“**受控数量**”的数字链接，可以查看到所有受控的终端



IP地址	MAC地址	设备名称	状态	备注	更新时间
10.10.10.1	08-00-2D-0A-00-01	10.10.10.1	受控	10.10.10.1	2010/10/10 11:10:10
10.10.10.2	08-00-2D-0A-00-02	10.10.10.2	受控	10.10.10.2	2010/10/10 11:10:10
10.10.10.3	08-00-2D-0A-00-03	10.10.10.3	受控	10.10.10.3	2010/10/10 11:10:10
10.10.10.4	08-00-2D-0A-00-04	10.10.10.4	受控	10.10.10.4	2010/10/10 11:10:10
10.10.10.5	08-00-2D-0A-00-05	10.10.10.5	受控	10.10.10.5	2010/10/10 11:10:10

再点击其中某台受控终端的 IP 地址链接，进入查看此台终端详细信息的界面，即客户端报表



客户端报表显示了客户端的一些常见信息如部门信息、使用人、ip地址等，对于同一个 MAC 地址，系统最多纪录最近 3 次的主机名和 IP 地址。还有客户端安全基线快照等信息。

页面中的“资产信息”请参照“资产管理”，页面中的“进程”，“服务”，“网络连接”请参照“桌面运维”-“终端实时操控”。

终端发现

通过组合条件查询终端信息



配置项:	说明
部门	选择需要查询的部门信息，如果有设置部门的话
子网号	所有已发现的终端的子网号都将会显示出来，选择其中一个进行查询
IP 地址	输入要查询的终端 IP 地址
MAC 地址	输入要查询的终端 MAC 地址
主机名	输入要查询的终端的主机名
是否受控	选择查询受控终端还是非受控终端
是否合规	选择查询合规终端还是不合规终端
是否活动	选择查询是否活动的终端
客户端版本	输入客户端版本号来查询特定版本的已受控终端（只有选择了查询受控终端时此处才能激活）

选择特定条件，例如“所有受控终端”



子网号	IP地址	MAC地址	主机名	是否受控	是否合规	是否活动	客户端版本
10.10.10.1	10.10.10.1	00-00-00-00-00-00	adstar77k033de	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.2	10.10.10.2	00-00-00-00-00-00	jiashu000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.3	10.10.10.3	00-00-00-00-00-00	server	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.4	10.10.10.4	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.5	10.10.10.5	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.6	10.10.10.6	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.7	10.10.10.7	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.8	10.10.10.8	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.9	10.10.10.9	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.10	10.10.10.10	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.11	10.10.10.11	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.12	10.10.10.12	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.13	10.10.10.13	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.14	10.10.10.14	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.15	10.10.10.15	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.16	10.10.10.16	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.17	10.10.10.17	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.18	10.10.10.18	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.19	10.10.10.19	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.20	10.10.10.20	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.21	10.10.10.21	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.22	10.10.10.22	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.23	10.10.10.23	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.24	10.10.10.24	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.25	10.10.10.25	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.26	10.10.10.26	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.27	10.10.10.27	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.28	10.10.10.28	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.29	10.10.10.29	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1
10.10.10.30	10.10.10.30	00-00-00-00-00-00	server000	是	是	是	10.10.10.10.1.1.1.1.1

点击其中的 IP 地址链接，同样可进入客户端报表查询界面

15.3. 资产信息

15.3.1. 配置介绍

查询统计终端资产信息的详细情况，包括终端的硬件资产和软件信息



资产信息

请选择查询统计图表类型：

- ☐ 资产信息查询
- ☐ 按终端厂商品牌统计
- ☐ 按CPU型号统计
- ☐ 按内存大小统计
- ☐ 按内存大小查询
- ☐ 按硬盘大小统计
- ☐ 按硬盘大小查询
- ☐ 按硬盘型号统计
- ☐ 按网卡型号统计
- ☐ 按主板型号
- ☐ 按显卡型号统计
- ☐ 按声卡型号统计
- ☐ 按modem型号统计
- ☐ 按CD-ROM型号统计
- ☐ 操作系统类型统计
- ☐ 指定软件安装统计
- ☐ 防病毒软件统计
- ☐ 按主机类型统计
- ☐ 终端操作系统安装时间查询

按主板型号



资产信息

报表类型：按主板型号

报表名称：按主板型号

所属部门：所有部门

主板型号：(可模糊查询)

图表类型：☒ 无图 ☐ 饼状图 ☐ 纵向柱状图

创建状态：全部

创建者：administrator

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
主板型号	输入要查询的终端的主板型号
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

点击“执行”后



点击数字链接，可以查看到具体客户端



The screenshot shows the '资产统计' (Asset Statistics) interface with a table of asset details. The table has columns for IP address, hostname, system name, MAC address, service name, and creation time.

IP地址	主机名	系统名称	MAC地址	服务名称	创建时间
172.25.80.202	ly	LIIYUW-PC	60920000	Microsoft Windows 7 旗舰版	2012-10-18 11:53:31

注意：此处可导出图表到 excel

点击 IP 地址链接，可以查看该终端详细的资产信息。如：

资产ID: {A38D90C0-1E9F-4E2C-B8F7-B212CF9CEFC8} 固定资产号: 导出到Excel

资产信息	项目	值
	名称	主机名测试1
	域	WORKGROUP
	制造商	ASUSTek Computer INC.
	型号	P5GZ-MX
	名称	主机名测试1
	CPU数量	1
	物理内存	2138222592
	用户名	主机名测试1\Administrator
	项目	值
	名称	Microsoft Windows XP Professional
	版本	5.1.2600
	服务包版本	Service Pack 3
	空闲物理内存	130180
	空闲页面空间	3421048
空闲虚拟内存	2039452	

按终端厂商品牌统计

资产信息

报表类型

按终端厂商品牌统计

报表名称

按终端厂商品牌统计

所属部门

所有部门

选择部门

厂商品牌名称

模糊查询

图表类型

无图

饼状图

横向柱状图

创建状态

全局

创建者

administrator

保存并执行

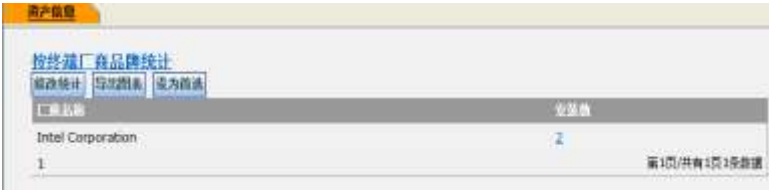
保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
厂商品牌名称	输入要查询的厂商品牌名称，可模糊查询
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



按 CPU 型号统计

资产信息

报表类型: 按CPU型号统计

报表名称: 按CPU型号统计

所属部门: 所有部门 选择部门

CPU型号: (可模糊查询)

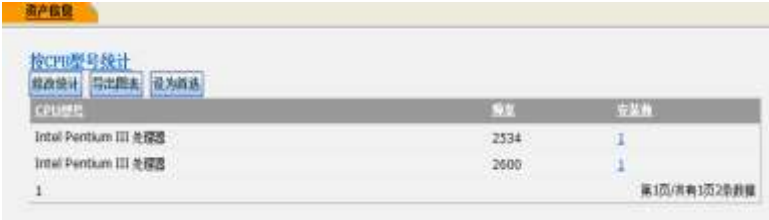
图表类型: ☒ 无图 ☐ 饼状图 ☐ 横向柱状图

创建状态: 全图

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
CPU 型号	输入要查询的 CPU 型号，可模糊查询
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



按内存大小统计

资产信息

报表类型

按内存大小统计

报表名称

按内存大小统计

所属部门

所有部门

选择部门

图表类型

☒ 无图

☐ 饼状图

☐ 横向柱状图

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

资产信息

按内存大小统计

统计描述

导出图表

设为默认

内存大小

资产数量

512M~1G

↓

512M以下

↑

1

第1页/共有1页2条数据

按内存大小查询

资产信息

报表类型

按内存大小查询

报表名称

按内存大小查询

所属部门

所有部门

选择部门

内存大小

☐ 小于

☐ 大于

☒ 介于

MB至

MB

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
内存大小	可直接输入小于或大于某个值的内存大小，也可在一个内存大小区间查询



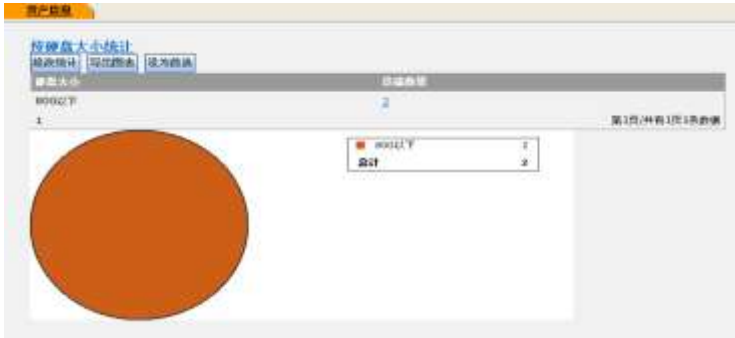
注意: 按内存大小统计和按内存大小查询的区别在于前者只按照实际上报内存的大小从数据库中读取出来并展现，而后者可以通过定义大小区间来展现，满足不同用户的需求。

按硬盘大小统计



配置项:	说明
报表类型	此报表的类型

报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



按硬盘大小查询

资产信息

报表类型: 按硬盘大小查询

报表名称: 按硬盘大小查询

所属部门: 所有部门 [选择部门]

硬盘大小: ☐ 小于 ☐ 大于 ☒ 介于 G6至 GB

全局: administrator

[保存并执行] [保存] [执行] [删除] [取消]

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
硬盘大小	可直接输入小于或大于某个值的硬盘大小，也可在一个硬盘大小区间查询

资产信息

按硬盘大小查询

快速统计 导出报表 设为默认

IP地址	主机名称	操作系统	部门名称	硬盘大小 (GB)
172.25.42.111	CLIENT2	Microsoft Windows XP Professional		5
192.168.1.4	THINKPAD-1F7F8F	Microsoft Windows XP Professional		5

1

第1页/共有1页2条数据

资产信息查询

资产信息

报表类型: 资产信息查询

报表名称: 资产信息查询

所属部门: 所有部门 [选择部门]

主机名: [可模糊查询]

主机类型: 不限

IP地址范围: [可模糊查询]

计算机序列号 (SN): [可模糊查询]

固态硬盘号: [可模糊查询]

CPU型号: [可模糊查询]

网卡型号: [可模糊查询]

网卡MAC地址: [格式AA-BB-CC-DD-EF-FF, 可模糊查询]

内存大小: ☐ 小于 ☐ 大于 ☐ 介于 [MB] 和 [MB]

硬盘大小: ☐ 小于 ☐ 大于 ☐ 介于 [GB] 和 [GB]

资产报表更新时间: ☐ 早于 ☐ 晚于 ☐ 介于 [日] 和 [日]

操作系统类型: 不指定

固定软件名称: [可模糊查询, 支持多个关键词使用 / 分隔查询]

使用人: [可模糊查询]

创建状态: 全部

创建者: administrator

[保存并执行] [保存] [执行] [删除] [取消]

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
主机名	输入需要查询的主机名，可模糊查询
主机类型	输入需要查询的主机类型，如“台式机”和“笔记本”
IP 地址范围	输入要查询的 IP 地址范围

计算机序列号	输入要查询的计算机序列号，可模糊查询
固定资产号	输入要查询的固定资产号，可模糊查询
CPU 型号	输入要查询的 CPU 型号，可模糊查询
网卡型号	输入要查询的网卡型号，可模糊查询
网卡 MAC 地址	输入要查询的 MAC 地址，可模糊查询
内存大小	输入要查询的内存大小，可选择区间
硬盘大小	输入要查询的硬盘大小，可选择区间
资产报表更新时间	选择资产报表更新的时间
操作系统类型	选择操作系统类型
指定软件名称	输入要查询的软件名称，多个软件通过“/”来间隔
使用人	输入使用人，客户端注册后才有此信息



注意：此处的查询属于一个综合报表自定义查询，通过各种不同的组合条件，查询出符合用户需要的资产报表。

按网卡型号统计



配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
网卡型号	输入要查询的网卡型号
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



按主机类型统计

资产信息

报表类型: 按主机类型统计

报表名称: 按主机类型统计

所属部门: 所有部门 选择部门

图表类型: ☒ 无图 ☐ 饼状图 ☐ 横向柱状图

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择

图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”
------	-------------------------



按显卡型号统计

资产信息

报表类型: 按显卡型号统计

报表名称: 按显卡型号统计

所属部门: 所有部门 选择部门

显卡型号: (可模糊查询)

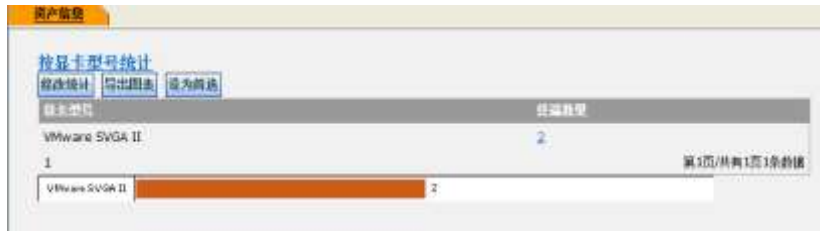
图表类型: ☒ 无图 ☐ 饼状图 ☐ 横向柱状图

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
显卡型号	输入需要查询的显卡型号，可模糊查询
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



按声卡型号统计

资产信息

报表类型

按声卡型号统计

报表名称

按声卡型号统计

所属部门

所有部门

选择部门

声卡型号

(可模糊查询)

图表类型

无图

饼状图

横向柱状图

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
声卡型号	输入需要查询的声卡型号，可模糊查询
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

资产信息

按声卡型号统计

删除统计

导出图表

设为默认

资产名称	创建数量
Creative AudioPCI (ES1371,ES1373) (WDM)	2
1	

第1页/共有1页1条数据

按 modem 型号统计

资产信息

报表类型

按modem型号统计

报表名称

按modem型号统计

所属部门

所有部门

选择部门

Modem型号

向模糊查询

图表类型

无图

饼状图

横向柱状图

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
Modem 型号	输入需要查询的 modem 型号，可模糊查询
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

资产信息

按modem型号统计

修改统计

统计图表

设为默认

modem型号

按值查询

1

第1页/共2页0条数据

按 CD-ROM 型号统计

资产信息

报表类型

按CD-ROM型号统计

报表名称

按CD-ROM型号统计

所属部门

所有部门

选择部门

CD-ROM型号

(可模糊查询)

图表类型

无图

饼状图

横向柱状图

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
CD-ROM 型号	输入需要查询的 CD-ROM 型号，可模糊查询
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

资产信息

按CD-ROM型号统计

修改统计

导出图表

设为筛选

CD-ROM型号

按值排序

MATSHITA DVD-RAM UJ862A

NECMWar VMware IDE CDR10

1

第1页/共有1页2条数据

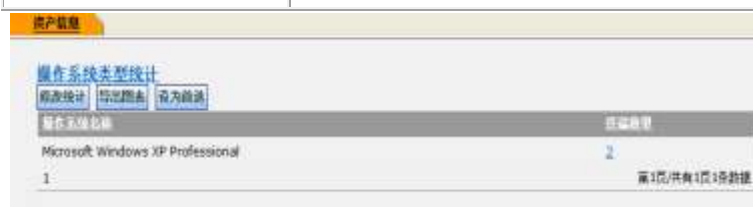
操作系统类型统计

资产信息

报表类型	操作系统类型统计
报表名称	操作系统类型统计
所属部门	所有部门 选择部门
图表类型	☒ 无图 ☐ 饼状图 ☐ 纵向柱状图
创建状态	全局
创建者	administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
图表类型	选择图表类型，可选择“饼状图”和“纵向柱状图”



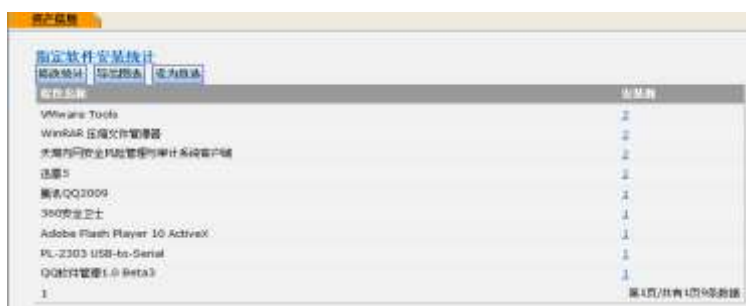
指定软件安装统计

资产信息

报表类型	指定软件安装统计
报表名称	指定软件安装统计
所属部门	所有部门 选择部门
指定软件名称	(可模糊查询, 支持:)
图表类型	☒ 无图 ☐ 饼状图 ☐ 纵向柱状图
创建状态	全局
创建者	administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
指定软件名称	输入要查询的软件名称，可模糊查询
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



防病毒软件统计

资产信息

报表类型: 防病毒软件统计

报表名称: 防病毒软件统计

所属部门: 所有部门 选择部门

允许延迟更新天数:

图表类型: ☒ 无图 ☐ 饼状图 ☐ 横向柱状图

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称

所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
允许延迟更新天数	输入允许延迟更新的天数
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



按硬盘型号统计



配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
硬盘型号	输入要查询的硬盘型号，可模糊查询

图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”
------	-------------------------



15.4. 补丁信息

15.4.1. 配置介绍

补丁信息可以查询统计终端补丁安装状态

补丁信息查询与统计

请选择查询统计图表类型：

- ☐ 指定终端补丁安装状态查询
- ☐ 终端安装指定补丁状态查询
- ☐ 指定日期内客户端补丁安装状态查询
- ☐ 指定日期内未安装补丁的客户端查询
- ☐ 客户端补丁安装状态统计
- ☐ 补丁安装状态统计
- ☐ 安装失败补丁查询
- ☐ 部门补丁安装状态统计

下一步 **取消**

客户端补丁安装状态查询

补丁信息查询与统计

报表类型：客户端补丁安装状态统计

报表名称：客户端补丁安装状态统计

所属部门：所有部门 **选择部门**

创建状态：全部

创建者：administrator

保存并执行 **保存** **执行** **删除** **取消**

配置项：	说明
------	----

报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

补丁信息查询与统计

客户端补丁安装状态统计

机选 网选 网选

IP地址	主机名称	工作组	部门名称	已安装补丁数	待安装补丁数	待安装补丁数	待安装补丁数	待安装补丁数	待安装补丁数
172.25.25.4.77	dkd-PC	WORKGR OUP	牛晓部门	1	0	0	0	100%	100%
10.201.33.1.17	WIFI-HS377D 596M	WORKGR OUP	mj张南	27	2	1	2	67%	33%
10.201.10.0.77	jingjun-X64sp		mj张南	0	0	35	35	0%	100%
10.201.22.2.88	duo-PC	WORKGR OUP	mj	22	0	0	0	100%	100%
10.201.90.2.13	Buyuan-PC	ly	一级	23	0	0	0	100%	100%
10.201.99.2.06	jian99-PC	WORKGR OUP	牛晓部门	21	0	0	0	100%	100%
172.25.25.4.501	venus-638F96 b45	season.co st	ly张南	22	0	0	0	100%	100%
10.201.11.0.8	XP64测试组	XP64	mj张南	130	0	0	0	100%	100%
172.25.1.20.4	t222	WORKGR OUP	牛晓部门	1	0	0	0	100%	100%
10.201.11.0.20	sin-PC	WORKGR OUP	牛晓部门	1	0	0	0	100%	100%

第1页/共有2页15条数据

点击数量链接，可以查看到具体补丁。

终端安装指定补丁状态查询

补丁信息查询与统计

报表类型: 终端安装指定补丁状态查询

报表名称: 终端安装指定补丁状态查询

所属部门: 所有部门 [选择部门](#)

请输入补丁号:

请选择查询类型: 要求安装已安装

创建状态: 全局

创建者: administrator

[保存并执行](#) [保存](#) [执行](#) [删除](#) [取消](#)

配置项:	说明
报表类型	此报表的类型

报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
请输入补丁号	输入补丁的 KB 号
请选择查询类型	选择“要求安装已安装”“要求安装未安装”等查询条件

指定终端补丁安装状态查询

补丁信息查询与统计

报表类型: 指定终端补丁安装状态查询

报表名称: 指定终端补丁安装状态查询

IP地址: 0.0.0.0

所属部门: 所有部门 选择部门

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
IP 地址	输入要查询的 IP 地址

补丁信息查询与统计

指定终端补丁安装状态查询

数据列表 数据图表 数据导出

补丁名称	是否已安装	要求安装	强制要求安装
KB22229593	是	否	否
KB8873330	是	否	否
KB885835	是	否	否
KB885836	是	否	否
KB886185	是	否	否
KB886113	是	否	否
KB886302	是	否	否
KB886850	是	否	否
KB8861781	是	否	否
KB8863756	是	否	否

显示 12345678910 条记录

第 1 页 / 共有 95 页 3 条数据

补丁安装状态统计

补丁信息查询与统计

报表类型

补丁安装状态统计

报表名称

补丁安装状态统计

所属部门

所有部门

时间范围

☒最近 7 天

☐从 到

图表类型

☒无图

☐饼状图

☐横向柱状图

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择统计的补丁安装时间范围
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

补丁安装状态统计

导出报表

导出图表

设为默认

补丁名称	本型系统安装量	已有系统安装量
KB2229593	0	1
KB2393882	1	0
KB2412687	1	0
KB2425227	0	1
KB2478968	1	0
KB2478971	1	0
KB2479943	1	1
KB2483185	1	0
KB2485376	1	1
KB2485863	1	0

1 2 3 4 5 6 7 8 9 10 ... 全部

第 1 页 / 共 14 页 132 条数据

注意：补丁安装状态统计和客户端补丁安装状态统计的区别在于前者是以补丁为关键字，后者是以客户端为关键字来查询。

指定日期内未安装补丁的客户端查询

补丁信息查询与统计

报表类型: 指定日期内未安装补丁的客户端查询

报表名称: 指定日期内未安装补丁的客户端查询

所属部门: 所有部门

统计的天数: 10 内 0表示不限

创建状态: 全局

创建者: administrator

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
统计的天数	选择要查询的时间点距离今天的天数

补丁信息查询与统计

指定日期内未安装补丁的客户端查询

IP地址	主机名称	部门名称	MAC地址
10.201.33.2	venus-538c9d044	网络部	00-0c-29-e1-ab-09
10.201.33.27	WIN-QU8E8K13EQ	网络部	00-0c-29-0d-7d-83
10.201.33.117	WIN-45337D99804	网络部	00-0c-29-3a-9b-2b
10.201.100.77	JHX2J4F-364rp	网络部	00-0c-29-0e-13-a3

1 第1页/共1页4条数据

指定日期内客户端补丁安装状态查询

补丁信息查询与统计

报表类型: 指定日期内客户端补丁安装状态查询

报表名称: 指定日期内客户端补丁安装状态查询

所属部门: 所有部门

统计的天数: 10 内 0表示不限

创建状态: 全局

创建者: administrator

配置项:	说明
------	----

报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
统计的天数	选择要查询的时间点距离今天的天数

补丁安装成功统计

指定日期内客户端补丁安装状态查询

刷新数据 导出数据 返回数据

IP地址	主机名称	部门名称	已安装补丁数
10.201.33.117	Win7-451137089M	mj常用	20
10.201.30.213	Buyuan-PC	一般	2
172.23.234.101	venus-038f96b45	lv常用	22
10.201.140.1	admin-yangweie	一般	81
10.201.33.27	Win7-QJ8BE8K1EQ	mj常用	2
10.201.33.2	venus-518c94b44	mj常用	2
10.201.140.27	Win-yangweie	mj	1

1

第 4 页 / 共有 4 页 2 条数据

15.5. 审计信息

15.5.1. 配置介绍

对文件操作、网站访问、打印，windows 登录，主机名、IP、MAC 变更等进行审计，围绕内网合规管理要求，为内网安全状况持续改善提供保证。

审计信息查询与统计

请选择查询统计图表类型：

☐ 统计访问次数最多的网站TopN

☐ 统计访问网站次数最多的电脑TopN

☐ 网站访问审计

☐ 文件操作审计

☐ windows登录与注销审计

☐ 主机名、IP、MAC变更审计

☐ 打印审计

☐ windows事件日志查询

☐ 客户端卸载审计

☐ windows开关机审计

☐ 客户端运行审计

☐ 涉密信息审计查询

☐ 应用程序运行审计

☐ FTP审计查询

☐ 刻录审计

下一步

取消

主机名，IP，MAC 变更审计

审计信息查询与统计

报表类型

主机名、IP、MAC变更审计

报表名称

主机名、IP、MAC变更审计

所属部门

所有部门

选择部门

时间范围

最近 7 天

☐ 从

10.201.140.1

 到

IP地址

10.201.140.1

主机名

MAC地址

创建状态

全部

创建者

jing

保存并执行

保存

执行

取消

配置项：	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择

时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址	输入需要查询的 IP 地址，不填默认查询所有终端
主机名	输入需要查询的主机名
MAC 地址	输入需要查询的 MAC 地址

点击“执行”

审计信息查看与统计						
主机名、IP、MAC变更审计						
IP地址	主机名称	部门名称	上次IP/MAC	变更前内容	变更后内容	变更时间
172.25.10.5	ZH400E	生物工程研究所	00-1C-25-7C-19-FA	主机名:ZH400E 网卡:Intel(R) 82566MM Gigabit Network Connection MAC:00-1C-25-7C-19-FA IP:172.25.108.5 网卡:Intel(R) 无线 WiFi 适配器 4965AGN MAC:00-1F-38-02-02-89 IP:172.25.108.8	主机名:ZH400E 网卡:Intel(R) 82566MM Gigabit Network Connection MAC:00-1C-25-7C-19-FA IP:0.0.0.0 网卡:Intel(R) 无线 WiFi 适配器 4965AGN MAC:00-1F-38-02-02-89 IP:0.0.0.0	2010-7-28 19:07:59

点击 IP 地址链接，进入查看此终端详细信息的界面，即客户端报表。

windows 事件日志查询

审计信息查询与统计	
报表类型	windows事件日志查询
报表名称	windows事件日志查询
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
事件类型	不限
IP地址范围	-
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点

	击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
事件类型	选择 windows 系统日志中的事件类型
IP 地址范围	输入要查询的 IP 地址范围

windows事件日志表						
IP地址	主机名称	部门名称	类型	事件内容	时间	
10.201.140.27	WIN-yangwei		系统	ES-SCAgent Service 服务处于 正在运行 状态。	2012/10/25 15:56:37	
10.201.140.27	WIN-yangwei		系统	Interactive Services Detection 服务处于 正在运行 状态。	2012/10/25 15:59:09	
10.201.140.27	WIN-yangwei		系统	ES-SCAgent Service 服务处于 停止 状态。	2012/10/25 16:09:13	
10.201.140.27	WIN-yangwei		系统	ES-SCAgent Service 服务处于 正在运行 状态。	2012/10/25 16:09:25	
10.201.140.27	WIN-yangwei		系统	Windows Error Reporting Service 服务处于 正在运行 状态。	2012/10/25 16:09:30	

打印审计

审计信息查询与统计

报表类型

打印审计

报表名称

打印审计

所属部门

所有部门

选择部门

时间范围

最近 7 天

从 到

IP地址范围

创建状态

全部

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的 IP 地址范围



windows 登录审计

审计信息查询与统计

报表类型: windows登录与注销审计

报表名称: windows登录与注销审计

所属部门: 所有部门 选择部门

时间范围: ☒ 最近 7 天 ☐ 从 到

IP地址范围:

创建状态: 全局

创建者: jing

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的 IP 地址范围



文件操作审计

审计信息查询与统计

报表类型

文件操作审计

报表名称

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

IP地址范围

源文件名称

目标文件名称

操作类型

不指定

创建状态

全部

创建者

jing

保存并执行

保存

执行

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的 IP 地址范围
文件审计筛选	选择文件操作的种类，如创建、修改、删除等

文件操作审计

IP地址	主机名	端口	源文件名称	目标文件名称	操作	源文件大小	操作时间
10.20.1.20	huayu-an-P	445	C:\Users\huayu\AppData\Local\Microsoft\OneDrive\OneDrive\LearnL.DA	C:\Users\huayu\AppData\Local\Microsoft\OneDrive\OneDrive\LearnL.DA	读	255.25	2012/10/31 13:23:11
10.20.1.20	huayu-an-P	445	C:\Users\huayu\AppData\Local\Microsoft\OneDrive\OneDrive\LearnS.DA	C:\Users\huayu\AppData\Local\Microsoft\OneDrive\OneDrive\LearnS.DA	读	255.25	2012/10/31 13:23:11
10.20.1.20	huayu-an-P	445	C:\Users\huayu\AppData\Local\Microsoft\Windows\History\History.IE5\PMHnuto12012103120121101\index.dat	C:\Users\huayu\AppData\Local\Microsoft\Windows\History\History.IE5\PMHnuto12012103120121101\index.dat	读	255.25	2012/10/31 13:23:11
10.20.1.20	huayu-an-P	445	C:\Users\huayu\AppData\Local\Microsoft\OneDrive\OneDrive\LearnL.DA	C:\Users\huayu\AppData\Local\Microsoft\OneDrive\OneDrive\LearnL.DA	读	255.25	2012/10/31 13:23:11

网站访问审计

审计信息查询与统计

报表类型

网站访问审计

报表名称

所属部门

所有部门

选择部门

主机名

时间范围

最近8天

从到

IP地址范围

网站审计是否允许

全部

允许

不允许

网站域名

创建状态

全部

创建者

jing

保存并执行

保存

执行

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
主机名	输入要查询的主机名
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的 IP 地址范围
网站审计是否允许	选择是否允许网站审计的条件

网站访问审计

数据列表

统计图表

IP地址	主机名称	部门名称	网站地址	时间
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:29
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:28
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27
10.201.33.2	venust-518c94044	二部B	www.sina.com.cn/	2012/10/30 15:30:27

第1页/共有39页307条数据

统计访问次数最多的电脑 Top10

审计信息查询与统计

报表类型

统计访问网站次数最多的电脑TopN

报表名称

统计访问网站次数最多的电脑TopN

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

TopN

10

图表类型

☒ 无图

☐ 饼状图

☐ 横向往柱状图

创建状态

全部

创建者

jing

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择统计时间范围
TOPN	输入要统计的最大终端数
图表类型	选择图表类型，可选择“饼状图”和“横向往柱状图”

审计信息查询与统计

统计访问次数最多的网站Top10

报表统计

导出图表

名为自选

IP地址

主机名称

部门名称

访问次数

1

第1页/共1页0条数据

统计访问次数最多的网站 Top10

审计信息查询与统计

报表类型

统计访问次数最多的网站TopN

报表名称

所属部门

所有部门

选择部门

时间范围

最近 7 天

从 到

TopN

10

图表类型

无图

饼状图

纵向柱状图

创建状态

全局

创建者

jmg

保存并执行

保存

执行

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择统计时间范围
TOPN	输入要统计的最大终端数
图表类型	选择图表类型，可选择“饼状图”和“纵向柱状图”

统计访问次数最多的网站TopN

统计时间

统计次数

www.soso.com	38
tiandy.cn	30
www.tiandy.cn	28
download.windowsupdate.com	20
man.aliya.com	17
masterconn.qq.com	13
qqnews2-item.qq.com	14
static.tiandyui.com	12
www.sina.com.cn	12
qqnews2-item.qq.com/	10
1	

第1页/共1页 10条数据

客户端卸载审计

审计信息查询与统计

报表类型

客户端卸载审计

报表名称

所属部门

所有部门

选择部门

时间范围

最近 7 天

从 到

IP地址范围

创建状态

全局

创建者

jing

保存并执行

保存

执行

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择查询的时间范围
IP 地址范围	选择查询的 IP 范围

客户端卸载审计				
修改报表	导出图表	设为首页		
IP地址	主机名称	部门名称	事件内容	上报时间
10.201.222.66	admin-774c3ef09		卸载客户端	2011/9/14 9:46:14
10.201.99.23	jian-win2K3X64	C	卸载客户端	2011/9/14 10:07:30

windows 开关机审计

审计信息查询与统计

报表类型

windows开关机审计

报表名称

所属部门

所有部门

选择部门

时间范围

最近 7 天

从 到

IP地址范围

创建状态

全局

创建者

jing

保存并执行

保存

执行

取消

配置项:	说明
------	----

报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择查询的时间范围
IP 地址范围	选择查询的 IP 范围

Windows 开关机审计

修改报表 导出图表

IP地址	部门名称	用户名	主机名	域名	类型	时间
10.201.20.21			WIN-HACLF04CSLU		开机	2011/9/14 13:25:24
10.201.20.21			WIN-HACLF04CSLU		开机	2011/9/14 13:31:12
10.201.20.21		Administrator	WIN-HACLF04CSLU		开机	2011/9/14 14:01:46
10.201.20.21			WIN-HACLF04CSLU		开机	2011/9/14 14:08:41
10.201.88.3		闫发江		damen.com	关机	2011/9/14 14:34:45
10.201.88.3		闫发江		damen.com	关机	2011/9/14 14:39:12
10.201.222.20			WIN-9EVL8RP96OC		开机	2011/9/13 23:46:13
10.201.222.65			WIN-zsdzsd		开机	2011/9/14 15:03:20
10.201.222.66		Administrator	ADMIN-774C3EFD9		开机	2011/9/14 15:03:26
10.201.222.20			WIN-9EVL8RP96OC		开机	2011/9/14 0:03:32

第2页/共24页237条数据

客户端运行审计

审计信息查询与统计

报表类型: 客户端运行审计

报表名称:

所属部门: 所有部门 选择部门

时间范围: ☒ 最近 7 天 ☐ 从 到

IP地址范围: -

事件类型: 不选

创建状态: 全部

创建者: jing

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择

时间范围	选择查询的时间范围
IP 地址范围	选择查询的 IP 范围

审计信息查询与统计						
客户端运行审计						
修改报表	导出图表					
IP地址	主机名称	部门名称	windows用户名	操作系统用户名	事件类型	时间
10.201.140.1	admin-yangweie	二级B	administrator		更新策略	2012/10/25 15:48:41
10.201.140.27	WIN-yangweie	二级A	Administrator		更新策略	2012/10/25 15:48:02
前页 ... 82 83 84 85 86 87 88 89 90 91 末页						
						第91页/共有91页902条数据

涉密信息审计查询

审计信息查询与统计	
报表类型	涉密信息审计查询
报表名称	涉密信息审计查询
所属部门	所有部门 选择部门
主机名	
时间范围	☒ 最近 7 天 ☐ 从 到
IP地址范围	-
涉密关键字	☒ 包含下列所有关键字 ☐ 包含下列任意关键字 (多关键字以"/"分隔)
创建状态	全局
创建者	jing
保存并执行 保存 执行 取消	

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
主机名	输入需要查询的主机名
时间范围	选择查询的时间范围

IP 地址范围	选择查询的 IP 范围
涉密关键字	输入查询的关键字,多关键字以/分隔

审计信息查询与统计					
审计信息审计查询					
修改报表	导出报表	设为筛选			
IP地址	主机名称	部门名称	文件名称	关键字	查询时间
10.201.90.203	LIUYUAN-PC		C:\用户\liuyuan\桌面\DNS - 测试 - 进入网络攻击数据设计3.doc		2011/9/26 15:12:25
10.201.90.203	LIUYUAN-PC		C:\Program Files (x86)\WinRAR\WinRAR.exe	测试	2011/9/26 15:12:25
10.201.90.203	LIUYUAN-PC		C:\Program Files (x86)\WinRAR\WinRAR.exe	测试	2011/9/26 15:12:25

FTP 审计查询

审计信息查询与统计	
报表类型	FTP审计查询
报表名称	
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
IP地址范围	
传输文件名称	
操作类型	不指定
创建状态	全部
创建者	jing
保存并执行 保存 执行 取消	

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择查询的时间范围
IP 地址范围	选择查询的 IP 范围
传输文件名称	选择查询的 FTP 文件名
操作类型	

FTP审计查询

返回列表

导出列表

IP地址	主机名称	端口名称	FTP服务器地址	设备	源文件名称	目标
1						

第 1 页 / 共 1 页 0 条数据

刻录审计

报表类型

刻录审计

报表名称

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

IP地址范围

源文件名称

目标文件名称

创建状态

全部

创建者

jing

保存并执行

保存

执行

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择查询的时间范围
IP 地址范围	选择查询的 IP 范围
源文件名称	选择查询的刻录源文件名称
目标文件名称	选择查询的刻录的目标文件名

应用程序运行审计

报表类型

应用程序运行审计

报表名称

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

IP地址范围

创建状态

全局

创建者

jmg

保存并执行

保存

执行

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择查询的时间范围
IP 地址范围	选择查询的 IP 范围

应用程序运行审计							
修改配置		历史数据					
IP地址	主机名称	部门名称	进程名称	创建时间	退出时间	运行时间	上传时间
10.201.90.203	kuysan-PC	一研	dlhost.exe	2012/10/26 14:08:25	2012/10/26 14:08:33	8秒	2012/10/26 14:09:44
10.201.90.203	kuysan-PC	一研	mobsync.exe	2012/10/26 14:09:34	2012/10/26 14:09:53	19秒	2012/10/26 14:10:43
10.201.90.203	kuysan-PC	一研	dlhost.exe	2012/10/26 14:10:25	2012/10/26 14:10:38	13秒	2012/10/26 14:11:43
10.201.90.203	kuysan-PC	一研	worfaul.exe	2012/10/26 14:10:40	2012/10/26 14:10:58	9秒	2012/10/26 14:12:46
10.201.90.203	kuysan-PC	一研	dlhost.exe	2012/10/26 14:12:31	2012/10/26 14:12:58	7秒	2012/10/26 14:14:47
10.201.90.203	kuysan-PC	一研	svchost.exe	2012/10/26 14:10:27	2012/10/26 14:12:58	3分31秒	2012/10/26 14:14:47
10.201.90.203	kuysan-PC	一研	dlhost.exe	2012/10/26 14:13:13	2012/10/26 14:13:18	5秒	2012/10/26 14:14:47
10.201.90.203	kuysan-PC	一研	dlhost.exe	2012/10/26 14:13:15	2012/10/26 14:13:23	8秒	2012/10/26 14:14:47
10.201.90.203	kuysan-PC	一研	dlhost.exe	2012/10/26 14:13:20	2012/10/26 14:13:28	8秒	2012/10/26 14:14:47
10.201.90.203	kuysan-PC	一研	ssanchedlhost.exe	2012/10/26 14:12:24	2012/10/26 14:13:28	1分04秒	2012/10/26 14:14:47
第1页/共有28页273条数据							

15.6. 安全基线

15.6.1. 配置介绍

受控终端安全基线状态和历史记录，包括进程违规，软件安装违规，病毒码违规，强制补丁违规，安全加固等。

安全基线查询与统计

请选择查询统计图表类型：

- ☐ 终端安全基线违规TopN
- ☐ 进程违规状态查询
- ☐ 强制补丁违规状态查询
- ☐ 病毒码违规状态查询
- ☐ 安全加固-加入和登录域统计
- ☐ 安全加固-域策略违规状态查询
- ☐ 软件安装违规状态查询
- ☐ 进程违规历史查询
- ☐ 强制补丁违规历史查询
- ☐ 病毒码违规历史查询
- ☐ 安全加固-域策略违规历史查询
- ☐ 软件安装违规历史查询
- ☐ 计算机帐号查询
- ☐ ServicePack违规状态查询
- ☐ ServicePack违规历史查询
- ☐ 终端共享资源查询

下一步 **取消**

安全基线查询与统计

请选择查询统计图表类型：

- ☐ 终端安全基线违规TopN
- ☐ 进程违规状态查询
- ☐ 强制补丁违规状态查询
- ☐ 病毒码违规状态查询
- ☐ 安全加固-自定义安全策略违规状态查询
- ☐ 安全加固-加入和登录域统计
- ☐ 安全加固-域策略违规状态查询
- ☐ 软件安装违规状态查询
- ☐ 进程违规历史查询
- ☐ 强制补丁违规历史查询
- ☐ 病毒码违规历史查询
- ☐ 安全加固-自定义安全策略违规历史查询
- ☐ 安全加固-域策略违规历史查询
- ☐ 软件安装违规历史查询
- ☐ 计算机帐号查询
- ☐ ServicePack违规状态查询
- ☐ ServicePack违规历史查询
- ☒ 终端共享资源控制和管理

终端安全基线违规 TOPN

安全基线查询与统计

报表类型: 终端安全基线违规TopN

报表名称: 终端安全基线违规Top10

所属部门: 所有部门

时间范围: ☒ 最近 7 天 ☐ 从 到

TopN: 10

图表类型: ☒ 无图 ☐ 饼状图 ☐ 横向往柱状图

创建状态: 全局

创建者: administrator

配置项:	说明
查询类型	此查询的类型

查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
TOPN	输入需要查询出的统计最大数量
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

点击执行



红名单进程违规历史查询

报表类型	进程违规历史查询
报表名称	红名单进程违规历史查询
查询条件	红名单
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
操作系统	不指定
IP地址	
主机名	
创建状态	全部
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询类型
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择

时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

红名单进程违规历史查询

修改报表 导出图表 设为默认

IP地址	主机名称	端口名称	进程名称	所在系统	上报时间
10.201.140.1	admin-yangweie	一级	cmd.exe	Windows XP	2012/10/25 16:54:53
10.201.140.1	admin-yangweie	一级	cmd.exe	Windows XP	2012/10/25 17:05:54
10.201.140.1	admin-yangweie	一级	cmd.exe	Windows XP	2012/10/25 17:05:54
10.201.140.1	admin-yangweie	一级	cmd.exe	Windows XP	2012/10/25 17:07:56
10.201.140.1	admin-yangweie	一级	cmd.exe	Windows XP	2012/10/25 17:45:04
10.201.140.1	admin-yangweie	一级	文件审计与目录加密启动检测测试工具.exe	Windows XP	2012/10/25 17:45:04
10.201.140.1	admin-yangweie	一级	cmd.exe	Windows XP	2012/10/25 17:46:05
10.201.140.1	admin-yangweie	一级	文件审计与目录加密启动检测测试工具.exe	Windows XP	2012/10/25 17:46:05
10.201.140.1	admin-yangweie	一级	cmd.exe	Windows XP	2012/10/25 17:47:05
10.201.140.1	admin-yangweie	一级	文件审计与目录加密启动检测测试工具.exe	Windows XP	2012/10/25 17:47:05

首页 1 2 末页

第1页/共有2页13条数据

红名单进程违规状态查询

报表类型: 进程违规状态查询

报表名称: 红名单进程违规状态查询

查询条件: 红名单

所属部门: 所有部门 [选择部门](#)

时间范围: ☒ 最近 7 天 ☐ 从 到

操作系统: 不指定

IP地址:

主机名:

创建状态: 全量

创建者: administrator

[保存并执行](#) [保存](#) [执行](#) [删除](#) [取消](#)

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询类型
所属部门	选择需要查询的终端所属的部门，也可点

	击“ 选择部门 ”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名



黑名单进程违规状态查询

报表类型	进程违规状态查询
报表名称	黑名单进程违规状态查询
查询条件	黑名单
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
操作系统	不指定
IP地址	
主机名	
创建状态	全部
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询类型
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统

IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名



白名单进程违规状态查询

安全基线查询与统计

报表类型: 进程违规状态查询

报表名称: 白名单进程违规状态查询

查询条件: 白名单

所属部门: 所有部门 选择部门

时间范围: ☒ 最近 7 天 ☐ 从 到

操作系统: 不指定

IP地址:

主机名:

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询类型
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名



强制补丁违规状态查询

安全基线查询与统计

报表类型: 强制补丁违规状态查询

报表名称: 强制补丁违规状态查询

所属部门: 所有部门 选择部门

时间范围: ☒ 最近 7 天 ☐ 从 到

操作系统: 不指定

IP地址:

主机名:

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名



病毒码违规状态查询

报表类型

病毒码违规状态查询

报表名称

病毒码违规状态查询

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

病毒码违规状态查询

刷新数据

导出数据

设为默认

IP地址	主机名	部门名称	违规类型	最后更新时间
10.201.145.22	WDR-ywt	网	安装安装360杀毒软件	2012/11/1 10:41:04
1				

第1页/共4页4条数据

安全加固-加入和登录域统计

报表类型

安全加固-加入和登录域统计

报表名称

安全加固-加入和登录域统计

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

图表类型

☒ 无图

☐ 饼状图

☐ 横向柱状图

创建状态

全局

创建者

administrator

保存并执行

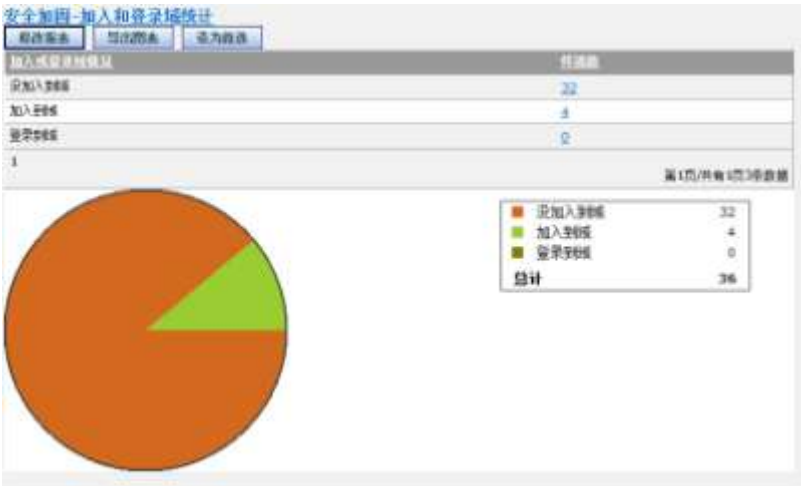
保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



安全加固-域策略违规状态查询

报表类型	安全加固-域策略违规状态查询	
报表名称	安全加固-域策略违规状态查询	
所属部门	所有部门	选择部门
时间范围	☒ 最近 7 天 ☐ 从 到	
操作系统	不指定	
IP地址		
主机名		
创建状态	全局	
创建者	administrator	
保存并执行 保存 执行 删除 取消		

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

安全加固-域策略违规状态查询

1

第 1 页 / 共 1 页 0 条数据

白名单软件安装违规状态查询

报表类型

软件安装违规状态查询

报表名称

白名单软件安装违规状态查询

查询条件

白名单

时间范围

最近 7 天

从 到

所属部门

所有部门

选择部门

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
查询条件	选择进程查询条件
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

白名单软件安装违规状态查询

操作列表

新增列表

高级筛选

IP地址	主机名	部门名称	软件名称	操作系统	更新时间
10.201.140.22	WIN-ywe	mq	360安全卫士	Windows 7	2012/11/1 10:41:44
10.201.140.22	WIN-ywe	mq	QQProtect	Windows 7	2012/11/1 10:41:44
10.201.140.22	WIN-ywe	mq	QQ软件管家1.0 Beta3	Windows 7	2012/11/1 10:41:44
10.201.140.22	WIN-ywe	mq	腾讯QQ2012(安全防IP)	Windows 7	2012/11/1 10:41:44
3					

第1页/共有3页4条数据

黑名单软件安装违规状态查询

报表类型

软件安装违规状态查询

报表名称

黑名单软件安装违规状态查询

查询条件

黑名单

时间范围

☒ 最近 7 天

☐ 从 到

所属部门

所有部门

选择部门

操作系统

不指定

IP地址

主机名

创建状态

全部

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
查询条件	选择进程查询条件
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

黑名单软件安装违规状态查询

操作报表

打印报表

导出数据

IP地址	主机名	部门名称	进程名称	操作系统	更新时间
10.201.180.1	admin-vsnpcie	一般	360	Windows XP	2012/10/29 10:51:21
10.201.185.27	WIN-ywa	mj	360	Windows 7	2012/11/1 10:41:44
1					

第1页/共有1页2条数据

计算机帐号查询

报表类型

计算机帐号查询

报表名称

计算机帐号查询

所属部门

所有部门

选择部门

IP地址范围

查询组合条件

☐弱密码 ☐被锁定 ☐密码过期 (密码过期仅对winXP以上系统生效)

指定计算机名

帐号可用性

不指定

帐号类型

所有

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
IP 地址范围	选择进程查询条件
查询组合条件	选择帐号查询组合条件
指定计算机名	输入要查询的计算机名
帐号可用性	选择帐号属性
帐号类型	选择帐号类型

计算机帐号查询

IP/M	主机名	端口名	用户名	权限	是否	是否	是否	是否	备注
172.25.254.101	venus-638f96b45	mq服务	ASPNET	普通用户	是	是	是	是	Account used for running the ASP.NET worker processes (aspnet_wp.exe)
172.25.254.101	venus-638f96b45	mq服务	USR_VENUS-RSKEBRL6	普通用户	是	是	是	是	警告访问 Internet 连接服务的用户
172.25.254.101	venus-638f96b45	mq服务	USAM_VENUS-RSKEBRL6	普通用户	是	是	是	是	用于自动进程分应用程序的 Internet 连接服务的用户
172.25.254.101	venus-638f96b45	mq服务	krb5g	普通用户	是	是	是	是	互联网信息中心服务用户
172.25.254.101	venus-638f96b45	mq服务	test101	普通用户	是	是	是	是	
172.25.254.101	venus-638f96b45	mq服务	SUPPORT_388945a0	普通用户	是	是	是	是	这是一个帮助和故障排除的帐户
172.25.254.101	venus-638f96b45		ASPNET	普通用户	是	是	是	是	Account used for running the ASP.NET worker processes (aspnet_wp.exe)

黑名单进程违规历史查询

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
查询条件	选择进程查询条件
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

未名年课程注册历史查询						
动态列表	历史列表	注册列表				
IP地址	注册名称	用户名	密码名称	操作名称	注册时间	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:36:19	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:36:19	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:36:19	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:36:19	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:36:19	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:36:01	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:39:01	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:39:01	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:39:01	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:39:01	
172.29.1.200	中文主帐号	6C-62-6D-46-E2-71	notepad.exe	Windows 7 x64	2012/10/23 19:39:01	

388
stech.com.cn

报表类型

进程违规历史查询

报表名称

白名单进程违规历史查询

查询条件

白名单

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

白名单进程违规历史查询

数据列表

导出列表

帮助指南

IP地址

主机名称

部门名称

操作系统

违规类型

所在系统

注册时间

1

第1页/共有2页0条数据

强制补丁违规历史查询

报表类型

强制补丁违规历史查询

报表名称

强制补丁违规历史查询

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

操作系统

不指定

IP地址

主机名

创建状态

全部

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

强制补丁违规历史查询

取消筛选

清除筛选

重置筛选

IP地址	主机名称	端口名称	补丁名称	操作系统	更新时间
10.201.169.27	WIN-yangwei	一服	KB2731847	Windows 7	2012/10/30 15:43:26
10.201.169.27	WIN-yangwei	一服	KB2731847	Windows 7	2012/10/30 15:44:23
10.201.169.27	WIN-yangwei	一服	KB2731847	Windows 7	2012/11/1 9:47:34
1					

第1页/共有1页3条数据

病毒码违规历史查询

报表类型

病毒码违规历史查询

报表名称

病毒码违规历史查询

所属部门

所有部门

选择部门

时间范围

最近 7 天

从 到

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

病毒码违规历史查询

报表类型

报表名称

选择部门

IP地址	主机名称	部门名称	操作系统	违规内容	更新时间
10.201.100.27	jingjun-XS4xp	IT部		防病毒未安装	2012/10/29 17:32:46
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:34:04
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:44:24
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:44:25
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:46:26
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:47:00
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:48:30
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:49:00
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:51:01
10.201.185.27	WiFi-yangweie	一服	Windows 7	防病毒未安装	2012/10/30 15:56:32

共1页/共96页53条数据

安全加固-域策略违规历史查询

报表类型

安全加固-域策略违规历史查询

报表名称

安全加固-域策略违规历史查询

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

安全加固-域策略违规历史查询

操作指南

导出报表

添加筛选

IP地址	主机名称	操作系统	未加入信任的域名称	登录系统	上次时间
1					

第1页/共有2页0条数据

白名单软件安装违规历史查询

报表类型

软件安装违规历史查询

报表名称

白名单软件安装违规历史查询

查询条件

白名单

时间范围

最近 7 天

从

到

所属部门

所有部门

选择部门

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询条件
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

白名单软件安装违规历史查询

IP地址	主机名	部门名称	软件名称	操作类型	注册时间
10.201.180.27	WIN-yangwei	一切	360安全卫士	Windows 7	2012/10/26 12:02:42
10.201.180.27	WIN-yangwei	一切	QQProtect	Windows 7	2012/10/26 12:02:42
10.201.180.27	WIN-yangwei	一切	QQ软件管理1.0 Beta3	Windows 7	2012/10/26 12:02:43
10.201.180.27	WIN-yangwei	一切	腾讯QQ2012(安全防护)	Windows 7	2012/10/26 12:02:43
10.201.180.27	WIN-yangwei	一切	360安全卫士	Windows 7	2012/10/26 13:57:45
10.201.180.27	WIN-yangwei	一切	QQProtect	Windows 7	2012/10/26 13:57:45
10.201.180.27	WIN-yangwei	一切	QQ软件管理1.0 Beta2	Windows 7	2012/10/26 13:57:45
10.201.180.27	WIN-yangwei	一切	腾讯QQ2012(安全防护)	Windows 7	2012/10/26 13:57:45
10.201.180.27	WIN-yangwei	一切	360安全卫士	Windows 7	2012/10/26 13:58:45
10.201.180.27	WIN-yangwei	一切	QQProtect	Windows 7	2012/10/26 13:58:45
第1页/共有46页454条数据					

红名单软件安装违规历史查询

报表类型

软件安装违规历史查询

报表名称

红名单软件安装违规历史查询

查询条件

红名单

时间范围

最近 7 天

从 到

所属部门

所有部门

选择部门

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询条件
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

安全基线检测与统计

红名单软件安装违规历史查询

修改统计

导出图表

设为默认

主机名称	操作系统	IP地址	软件名称	操作系统	上报时间	部门名称
1						

第1页/共有1页0条数据

黑名单软件安装违规历史查询

报表类型

软件安装违规历史查询

报表名称

红名单软件安装违规历史查询

查询条件

红名单

时间范围

最近 7 天

从 到

所属部门

所有部门

选择部门

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询条件
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

红名单软件安装违规历史查询

综合列表

导出列表

查看详情

IP地址	主机名称	部门名称	软件名称	操作系统	更新时间
10.201.110.8	XP64测试机		style	Windows XP x64	2012/10/26 15:48:13
10.201.140.27	WIN-yangweic	一研	腾讯	Windows 7	2012/10/26 9:52:43
10.201.140.27	WIN-yangweic	一研	腾讯	Windows 7	2012/10/26 9:53:43
10.201.140.27	WIN-yangweic	一研	飞流	Windows 7	2012/10/26 10:04:04
10.201.140.27	WIN-yangweic	一研	腾讯	Windows 7	2012/10/26 10:04:05
10.201.140.27	WIN-yangweic	一研	360	Windows 7	2012/10/26 10:17:03
10.201.140.27	WIN-yangweic	一研	360	Windows 7	2012/10/26 10:17:05
10.201.33.27	WIN-QUMESK11EQ	一研	360	Windows 7	2012/10/26 10:17:43
10.201.33.117	WIN-MSJ3TD50EM	一研	360	Windows 7 x64	2012/10/26 10:17:55
10.201.33.2	venust-518c94044	一研	360	Windows XP	2012/10/26 10:18:03

1

2

3

4

5

6

7

8

9

10

...

末页

页码/共页30页168条数据

红名单软件安装违规状态查询

报表类型

软件安装违规状态查询

报表名称

红名单软件安装违规状态查询

查询条件

红名单

时间范围

最近 7 天

从 到

所属部门

所有部门

选择部门

操作系统

不指定

IP地址

主机名

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
查询条件	选择进程查询条件
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
操作系统	选择操作系统
IP 地址	输入要查询的 IP 地址
主机名	输入要查询的主机名

红名单软件安装违规状态查询

报告列表

报告列表

报告列表

IP地址	主机名	部门名称	软件名称	操作系统	更新时间
172.25.29.123	carl	一服	QQ	Windows 2003	2012/10/31 15:28:58
10.201.140.1	admin-clangsuo	一服	abc	Windows XP	2012/10/29 10:51:31
10.201.140.22	WDN-gmcc	mj	abc	Windows 7	2012/11/1 10:41:44

1

第 4 页 / 共有 1 页 3 条数据

终端共享资源查询

报表类型	终端共享资源查询		
报表名称	终端共享资源查询		
所属部门	所有部门		选择部门
IP地址范围			
共享资源类型	不指定		
创建状态	全局		
创建者	administrator		
保存并执行保存执行删除取消			

配置项：	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
共享资源类型	可以"不指定"类型,或选择文件共享,打印机共享, IPC\$共享进行查询

终端共享资源查询						
IP地址	主机名	端口	mac地址	共享资源	操作系统	更新时间
10.201.100.205	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享F:\03	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.208	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享C:\Windows	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.205	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享C:\	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.208	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享F:\	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.205	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享F:\	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.208	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享G:\	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.205	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享G:\	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.208	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享H:\	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.205	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享F:\OS DV	Windows 2008 x64	2012/10/31 17:06:43
10.201.100.208	win2008R5-4testworkse-rver20222222222	—	6C-62-6D-07-61-AF	文件共享F:\soft	Windows 2008 x64	2012/10/31 17:06:43
首页 1 2 3 4 5 6 7 8 9 10						第1页/共有9090条数据

15.7. 外联控制

15.7.1. 配置介绍

外联控制记录了外设违规，多网卡，异常路由。

请选择查询统计图表类型：

☐ 终端非法外联违规TopN

☐ 非法外联不合规网段统计TopN

☐ 曾经发生多网卡外联行为终端统计

☐ 客户端多网卡外联历史查询

☐ 客户端多网卡外联快照查询

☐ 终端多网卡违规查询

☐ 外设违规查询

☐ 异常路由查询

☐ USB设备使用历史查询

☐ 非法外联告警查询

☐ 终端违规拨号查询

下一步

取消

外设违规查询

报表类型	外设违规查询
报表名称	外设违规查询
所属部门	所有部门 选择部门
操作系统	不指定
IP地址	
主机名	
创建状态	全部
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项：	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择

操作系统	选择操作系统类型
IP 地址	输入需要查询的终端 IP 地址
主机名	输入需要查询的终端主机名

点击执行

外设连接查询

IP地址	主机名称	部门名称	操作系统	连接类型	连接次数	连接时间
10.201.33.2	venus-518c94044		Windows XP	CIDRCH	4	2012/10/30 13:30:40
10.201.33.2	venus-518c94044		Windows XP	CIDRCH	2	2012/10/30 15:44:46
10.201.33.2	venus-518c94044		Windows XP	CIDRCH	2	2012/10/30 15:45:07
10.201.33.2	venus-518c94044		Windows XP	CIDRCH	4	2012/10/30 15:52:45
10.201.33.27	WIN-QUBBEK1IEQ		Windows 7	CIDRCH	1	2012/10/26 13:05:59
10.201.33.27	WIN-QUBBEK1IEQ	mj网络	Windows 7	CIDRCH	2	2012/10/26 15:38:26
10.201.33.27	WIN-QUBBEK1IEQ	mj网络	Windows 7	CIDRCH	1	2012/10/26 20:16:03
10.201.33.27	WIN-QUBBEK1IEQ	mj网络	Windows 7	CIDRCH	1	2012/10/26 21:22:57
10.201.33.27	WIN-QUBBEK1IEQ	mj网络	Windows 7	CIDRCH	1	2012/10/26 22:09:34
10.201.33.27	WIN-QUBBEK1IEQ	mj网络	Windows 7	CIDRCH	1	2012/10/26 22:28:10

第1页/共有6页38条数据

点击 IP 地址连接，可以查看该客户端详细报表。

异常路由查询

报表类型: 异常路由查询

报表名称: 异常路由查询

所属部门: 所有部门 选择部门

路由信息查询类型: 查询所有路由信息

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
路由信息查询类型	选择查询的路由信息类型

异常路由查询

IP地址	主机名称	部门名称	路由地址	Interface	首次使用	最后使用
208.73.41.166	LENOVO-V7YGH14T		172.25.0.1	172.25.85.254	2012-10-30 17:41:24	2012-10-30 17:41:24
1						

第1页/共有1页1条数据

终端多网卡违规查询

报表类型	终端多网卡违规查询
报表名称	终端多网卡违规查询
所属部门	所有部门 选择部门
操作系统	不指定
IP地址	
主机名	
时间范围	☒ 最近 7 天 ☐ 从 到
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
操作系统	选择操作系统类型
IP 地址	输入需要查询的终端 IP 地址
主机名	输入需要查询的终端主机名
时间范围	选择时间范围

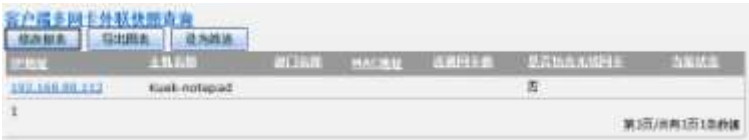
终端多网卡违规查询				
综合报表	导出图表	设为默认		
IP地址	主机名称	操作系统	网卡名称	连接次数
192.168.88.112	kusk-notepad			1
				2012/10/27 14:13:33
1				

客户端多网卡外联快照查询

报表类型	客户端多网卡外联快照查询
报表名称	客户端多网卡外联快照查询
所属部门	所有部门 选择部门
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
查询类型	此查询的类型

查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择



客户端多网卡外联历史查询

按表类型 客户端多网卡外联历史查询

按表名称 客户端多网卡外联历史查询

所属部门 所有部门 选择部门

主机名

时间范围 ☒ 最近 7 天 ☐ 从 到

IP地址范围

创建状态 全部

创建者 administrator

保存并执行 保存 执行 删除 取消

配置项：	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
IP 地址范围	输入需要查询的终端 IP 地址范围
主机名	输入需要查询的终端主机名
时间范围	选择时间范围



曾经发生多网卡外联行为终端统计

报表类型

曾经发生多网卡外联行为终端统计

报表名称

曾经发生多网卡外联行为终端统计

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

是否排除网卡数为2且有WLAN网卡的电脑

☒ 否 ☐ 是

创建状态

全部

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择时间范围
是否排除网卡数为2且有WLAN网卡的电脑	选择是否排除掉有两块网卡，且有无线网卡的电脑

曾经发生多网卡外联行为终端统计

IP地址	主机名称	部门名称	网卡地址	是否排除网卡数为2且有WLAN网卡的电脑	当前状态	数据更新时间	选择操作
192.168.88.112	Kuok-notepad			否		2012/10/27 14:13:33	
1							

第1页/共1页1条数据

非法外联不合规网段统计 Top10

报表类型

非法外联不合规网段统计TopN

报表名称

非法外联不合规网段统计Top10

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

TOP N

10

图表类型

☒ 无图

☐ 饼状图

☐ 柱状图

创建状态

全部

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	选择时间范围
TOPN	输入要统计的终端最大数量
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

非法外联不合规网段统计 Top10

网段	所属终端	违规次数	非法外联违规网段
10.201.33.2	0	0	09
10.201.33.27	0	0	24
192.168.88.112	0	0	1

1 第1页/共1页3条数据

终端非法外联违规 Top10

报表类型	终端非法外联违规TopN
报表名称	终端非法外联违规Top10
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
TOP N	10
图表类型	☒ 无图 ☐ 饼状图 ☐ 横向柱状图
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点

	击“ 选择部门 ”来进行选择
时间范围	选择时间范围
TOPN	输入要统计的终端最大数量
图表类型	选择图表类型，可选择“ 饼状图 ”和“ 横向柱状图 ”

终端非法外联记录Top10

IP地址	主机名称	部门名称	连接次数
10.201.33.27	WIN-QUS8E9K1IEQ	研发部	124
10.201.33.2	venus-S18C94044	一部	120
10.201.33.117	WIN-NS133TD99EM	研发部	101
10.201.33.27	WIN-QUS8E9K1IEQ	一部	82
10.201.33.117	WIN-NS133TD99EM	一部	72
10.201.33.2	venus-S18C94044	研发部	50
172.25.1.110	818K-PC	进出口	27
10.201.33.2	venus-S18C94044	市场部	18
10.201.33.117	WIN-NS133TD99EM	市场部	10
172.25.1.110	818K-PC	市场部	8

第1页/共有1页10条数据

非法外联告警查询

报表类型	非法外联告警查询
报表名称	非法外联告警查询
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
IP地址范围	
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
查询类型	此查询的类型
查询名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
时间范围	选择时间范围
IP 地址范围	选择查询的 IP 地址范围

USB 设备使用历史查询

报表类型	USB设备使用历史查询
报表名称	USB设备使用历史查询
所属部门	所有部门 选择部门
IP地址范围	-
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
IP 地址范围	选择查询的 IP 地址范围

USB设备使用历史查询						
IP地址	主机名称	部门名称	设备名称	接口	设备ID	操作时间
10.201.10.200	win2008x64testworkse-rvr2022222222	一	Port_#0001.Hub_#0004	HP v230p USB Device	USB\VID_03F0&PID_5F07\0000000000004A	2012/10/31 8:06:17
10.201.10.200	win2008x64testworkse-rvr2022222222	一	Port_#0004.Hub_#0003	USB Mass Storage Device	USB\VID_03F0&PID_5F07\6E3B832873&0&4	2012/10/31 8:06:17
10.201.10.200	win2008x64testworkse-rvr2022222222	一	Port_#0001.Hub_#0004	USB Human Interface Device	USB\VID_0483&PID_3100\0&12&1b0a480&1	2012/10/31 8:06:17
10.201.10.200	win2008x64testworkse-rvr2022222222	一	Port_#0002.Hub_#0004	USB Human Interface Device	USB\VID_0483&PID_3100\0&12&1b0a480&2	2012/10/31 8:06:17
10.201.10.200	win2008x64testworkse-rvr2022222222	一	Port_#0002.Hub_#0004	SONY DVD RW DRU-V200A USB Device	USB\VID_0484&PID_0830\0&1&1000110&0&1	2012/10/31 8:06:17
10.201.10.200	win2008x64testworkse-rvr2022222222	一	Port_#0004.Hub_#0003	Generic Flash Disk USB Device	USB\VID_058F&PID_6387\0&0&1A&11	2012/10/31 8:06:17
10.201.10.200	win2008x64testworkse-rvr2022222222	一	Port_#0001.Hub_#0004	SAMSUNG G1 Portable USB Device	USB\VID_058F&PID_6387\0&0&1A&11	2012/10/31 8:06:17

15.8. 攻击告警

15.8.1. 配置介绍

攻击告警查询与统计

请选择查询统计图表类型：

☐ 告警次数历史统计

☐ 统计告警事件最多TopN

☐ 告警事件查询

☐ ARP欺骗次数统计

☐ 客户端防火墙日志查询

下一步

取消

告警事件查询

通过对指定的告警事件类型，日期，IP 等的组合查询特定的告警事件。

报表类型

告警事件查询

报表名称

告警事件查询

所属部门

所有部门

选择部门

主机名

时间范围

☒ 最近 7 天

☐ 从 到

IP地址范围

告警类型

ARP欺骗

告警子类型

所有

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项：	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择

主机名	输入要查询的终端主机名
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的终端 IP 地址范围
告警类型	选择告警类型
告警子类型	选择告警子类型

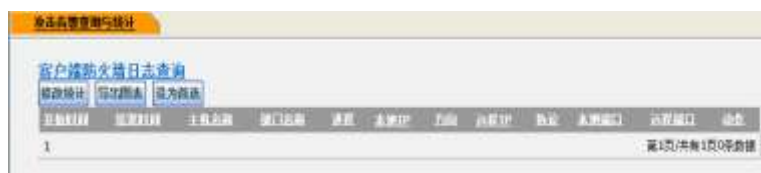


客户端防火墙日志查询

报表类型	客户端防火墙日志查询
报表名称	客户端防火墙日志查询
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
IP地址	
端口	
方向	所有
协议	所有
动作	所有
创建状态	全部
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址	输入要查询的终端 IP 地址

端口	输入要查询的日志中匹配的端口号
方向	选择连入或连出
协议	选择协议
动作	选择防火墙的动作类型



ARP 欺骗次数统计

攻击告警查询与统计

报表类型: ARP欺骗次数统计

报表名称: ARP欺骗次数统计

所属部门: 所有部门 选择部门

时间范围: ☒ 最近 7 天 ☐ 从 到

图表类型: ☒ 无图 ☐ 饼图 ☐ 横向柱状图

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围

图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”
------	-------------------------



统计告警事件最多 Top10

攻击告警查询与统计

报表类型: 统计告警事件最多TopN

报表名称: 统计告警事件最多Top10

所属部门: 所有部门 选择部门

时间范围: ☒ 最近 7 天 ☐ 从 到

TopN: 10

图表类型: ☒ 无图 ☐ 饼状图 ☐ 横向柱状图

创建状态: 全局

创建者: administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
TOPN	输入要统计的终端最大数
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



告警次数历史统计

告警次数历史统计

报表名称: 告警次数历史统计

所属部门: 所有部门 [选择部门]

时间范围: ☒ 最近 7 天 ☐ 从 [] 到 []

图表类型: ☒ 无图 ☐ 饼图折线图

创建状态: 全局

创建者: administrator

[保存并执行] [保存] [执行] [删除] [取消]

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”



15.9. 移动存储

15.9.1. 配置介绍

客户端使用移动存储设备时记录的审计信息

请选择查询统计图表类型：

☐ 移动存储文件审计

☐ 移动存储设备审计

☐ 解扰审计

移动存储管理审计

客户端使用移动存储设备时记录的审计信息

报表类型	移动存储设备审计
报表名称	移动存储设备审计
所属部门	所有部门 选择部门
时间范围	☒ 最近 7 天 ☐ 从 到
IP地址范围	
操作类型	不指定
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项：	说明
查询类型	此报表的类型
查询名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的终端 IP 地址范围
移动存储管理审计筛选	选择记录的审计内容，如删除、改名、创建等

点击执行

移动存储设备审计					
设备名称	设备类型	设备名称	设备	操作	时间
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 15:20:30
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 14:30:30
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 14:39:30
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 12:28:01
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 12:28:01
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 12:13:32
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 12:13:32
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 12:11:51
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 12:11:51
移动存储设备	移动存储设备	移动存储设备	移动存储设备	移动存储设备	2012/10/31 11:35:29

解扰审计

客户端移动存储设备进行分区表解扰时记录的审计信息

报表类型

解扰审计

报表名称

解扰审计

所属部门

所有部门

选择部门

时间范围

最近 7 天

从 到

IP地址范围

解扰审计筛选

不指定

创建状态

全部

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
查询类型	此报表的类型
查询名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的终端 IP 地址范围
解扰审计筛选	选择记录的审计内容，如解扰、启动工具等

点击执行



移动存储文件审计

报告类型	移动存储文件审计
报告名称	移动存储文件审计
所属部门	所有部门 选择部门
时间范围	☒ 最近 ☐ 天 ☐ 从 到
IP地址范围	
源文件名称	
目标文件名称	
操作类型	不指定
创建状态	全部
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的终端 IP 地址范围
操作类型	选择记录的审计内容，如插入、移除设备等

点击执行

移动存储文件审计

记录ID	主机名称	源主机	目标主机	移动文件名称	操作	路径	时间
10.2011.90.2.1.1	kyuan-PC	H:\8980890808.txt	H:\8980890808.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/31 9:53:58
10.2011.90.2.1.2	kyuan-PC	H:\0.txt	H:\0.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/31 9:53:59
10.2011.90.2.1.3	kyuan-PC	H:\8980890808.txt	H:\8980890808.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 14:59:27
10.2011.90.2.1.4	kyuan-PC	H:\0.txt	H:\0.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 14:59:27
10.2011.90.2.1.5	kyuan-PC	H:\8980890808.txt	H:\8980890808.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 12:19:32
10.2011.90.2.1.6	kyuan-PC	H:\0.txt	H:\0.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 12:19:32
10.2011.90.2.1.7	kyuan-PC	H:\8980890808.txt	H:\8980890808.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 12:18:32
10.2011.90.2.1.8	kyuan-PC	H:\0.txt	H:\0.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 12:18:32
10.2011.90.2.1.9	kyuan-PC	H:\8980890808.txt	H:\8980890808.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 12:18:32
10.2011.90.2.1.10	kyuan-PC	H:\0.txt	H:\0.txt	C:\Windows\system32\WUDFHost.exe	读取		2012/10/30 12:18:32

第1页/共44页数据

15.10. 桌面运维

15.10.1. 配置介绍

请选择查询统计图表类型：

- ☐ 终端资源使用状况告警查询
- ☐ 短消息阅读统计
- ☐ 指定终端短消息阅读查询
- ☐ 指定终端资源使用状况查询
- ☐ 终端网络累计使用状况TopN
- ☐ 计算机名规范查询
- ☐ 单点登录客户端查询

终端资源使用状况查询需在“桌面运维”中配置“终端资源使用状况监控与告警策略”

终端资源使用状况告警查询

报表类型

终端资源使用状况告警查询

报表名称

终端资源使用状况告警查询

所属部门

所有部门

选择部门

主机名

时间范围

☒ 最近 7 天

☐ 从 到

IP地址范围

告警事件

所有类型

创建状态

全部

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
主机名	输入要查询的终端主机名
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址	输入要查询的终端 IP 地址
告警事件	选择告警事件，如 CPU 使用率、内存使用率等

点击执行

终端资源使用状况告警查询

数据报表

历史报表

导出报表

IP地址	主机名称	端口名称	事件内容	告警类型	更新时间
10.201.140.22	WIN-yangwei	二部A	28%	CPU使用率高告	2012/10/25 15:33:04
10.201.140.22	WIN-yangwei	二部A	30.37%	内存使用率高告	2012/10/25 15:33:04
10.201.140.22	WIN-yangwei	二部A	50%	硬盘剩余空间告	2012/10/25 15:33:04
10.201.140.22	WIN-yangwei	二部A	684	网络异常告警	2012/10/25 15:33:04
10.201.140.22	WIN-yangwei	二部A	75.85K	网络断连告警	2012/10/25 15:33:04

第1页/共有4页5条数据

计算机名规范查询

报表类型
计算机名规范查询

报表名称
计算机名规范查询

所属部门
所有部门

计算机名长度
1 至 1

域/工作组名称

是否加入域
未指定

创建状态
全局

创建者
administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
报表类型	此查询的类型
报表名称	此查询的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
计算机名长度	输入计算机名的长度
域/工作组名称	输入计算机的工作组或域名称
是否加入域	选择是否加入域

计算机名规范查询

修改报表 导出报表 报表预览

IP地址	主机名	安全系统	IP地址	域/工作组名称	在域中
1					

第1页/共有1页0条数据

指定终端资源使用状况查询

指定终端在一段时间内 cpu , 内存，硬盘，网络数据包，字节数曲线图

报表类型
指定终端资源使用状况查询

报表名称
指定终端资源使用状况查询

时间范围
最近7天

IP地址
0.0.0.0

创建状态
全局

创建者
administrator

保存并执行 保存 执行 删除 取消

配置项:	说明
------	----

报表类型	此报表的类型
报表名称	此报表的名称
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址	输入要查询的终端 IP 地址

点击执行



终端网络累计使用状况 TopN

报表类型

终端网络累计使用状况TopN

报表名称

终端网络累计使用状况Top10

所属部门

所有部门

选择部门

时间范围

☒ 最近 7 天

☐ 从 到

IP地址范围

-

资源类型

收发数据包

TopN

10

图表类型

☐ 无图

☒ 饼状图

☐ 横向柱状图

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
时间范围	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址范围	输入要查询的终端 IP 地址范围
资源类型	选择记录的审计内容，如收发数据包、收发字节数等
TOPN	输入要展现的终端数量
图表类型	选择图表类型，可选择“饼状图”和“横向柱状图”

短消息阅读统计

报表类型	短消息阅读统计
报表名称	短消息阅读统计
所属部门	所有部门 选择部门
创建日期	☒ 最近 7 天 ☐ 从 到
短消息标题	(可模糊查询)
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“选择部门”来进行选择
创建日期	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
短消息标题	输入要查询的已发布的短消息的标题，可模糊查询

指定终端短消息阅读查询

桌面运维查询与统计	
报表类型	指定终端短消息阅读查询
报表名称	指定终端短消息阅读查询
所属部门	所有部门 选择部门
创建日期	☒ 最近 7 天 ☐ 从 到
IP地址	172.25.90.18
创建状态	全局
创建者	administrator
保存并执行 保存 执行 删除 取消	

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称

所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
创建日期	可选择最近更新的天数也可通过点击日期图表选择具体时间范围
IP 地址	输入要查询的终端 IP 地址

单点登录客户端查询



报表类型: 单点登录客户端查询

报表名称: 单点登录客户端查询

所属部门: 所有部门 [选择部门]

是否启用单点登录: 不指定

创建状态: 全部

创建者: administrator

[保存并执行] [保存] [执行] [删除] [取消]

配置项:	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属部门	选择需要查询的终端所属的部门，也可点击“ 选择部门 ”来进行选择
是否启用单点登录	可选择“不指定”“不启用”“启用”

15.11. 级联报表

15.11.1. 配置介绍

查询在系统级联中，下级单位向上级单位上报的报表，以便上级单位系统管理员能够了解其下级单位的情况，包括终端发现、操作系统统计、主机类型统计、补丁安装信息。安全基线违规终端统计

级联报表

级联报表

请选择查询统计图表类型：

☐ 终端发现_级联报表

☐ 资产信息_操作系统统计_级联报表

☐ 资产信息_主机类型统计_级联报表

☐ 补丁安装信息_级联报表

☐ 安全基线违规终端统计_级联报表

☐ 策略分发统计_级联报表

下一步

取消

比如点击“终端发现_级联报表”，进入查询页面

报表类型

终端发现_级联报表

报表名称

终端发现_级联报表

所属单位

天珣测试增强身份高级版

选择单位

创建状态

全局

创建者

administrator

保存并执行

保存

执行

删除

取消

配置项：	说明
报表类型	此报表的类型
报表名称	此报表的名称
所属单位	选择需要查询的单位，也可点击“选择单位”来进行选择，以来查询该单位的报表

点击“执行”后

终端发现_级联报表

单位名称	终端数量	主机数量	操作系统数量	非操作系统数量	其他数量	平均数量
直属单位	126	35	33	93	19	14
10.201.112.24	0	0	0	0	0	0
10.201.112.211	20	18	1	19	0	1
合计	146	53	34	112	19	15

其他查询报表的配置也类似这样

注意：直属单位的终端数量就是本级单位的终端数量，下级单位（如“天河办事处”）的终端数量就是下级与其所有间接下级（下级的下级到最下一级）终端数量和，其他数字和报表的数字也是这样理

解

16. 系统维护

16.1. 关于系统维护

- “系统维护”确保了系统能够正常、高效运行。
- “系统日志”为管理员提供了管理的可追溯性。更重要的是，系统日志反馈“系统维护”的配置是否合理。
- “license 管理”通过 web 页面显示出用户授权信息，包括此 license 到期时间、相应功能模块和目前已使用的 license 授权数量等信息。

16.2. 系统维护

16.2.1. 客户端升级配置页面

配置介绍

客户端升级

策略名称 *

策略描述

客户端版本在: (含)至 *间, 执行升级

☒ 禁止弹出重启提示框

☐ 禁止安装检测提示

☐ 使用延迟升级方式 (重启后替换)

☐ 使用客户端升级包升级 (updaterun)

生效时间

☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 0:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

策略应用对象 [查看及编辑](#)

创建类型 全局

创建者 jing

注: 右边有*号的项目必须输入。

配置项:	说明
策略名称	输入合适的策略名称, 以方便管理。
说明	用以说明升级历史记录信息, 以方便管理。
客户端版本版本	升级策略有效的客户端版本范围
禁止弹出重启提示框	如果选择, 升级后不会提示用户重启。该参数不支持 66930000 版本以下的客户端。
禁止安装检测提示	勾选后即使客户端有启动 360 安全卫士时也不会再弹出提示框。该参数不支持 66930000 版本以下的客户端。
使用延迟升级方式	强制使客户端在重启后才进行升级。该参数不支持 66930000 版本以下的客户端。
使用客户端升级包升级	选择此项后, 前面三项配置会均会失效, 采用客户端 updaterun.exe 的方式升级
应用到 IP 组	点击“ 查看及编辑 ”超链接, 选择指定的 IP 组、

	工作组、主机名。
--	----------

配置要点

6693 升级可以采用 2 种方式：

方法一：保留原有的升级方式，即将客户端升级包改名成为 updaterun.exe 放在服务器安装目录下的 updateNT 目录中，配置升级策略。

客户端升级配置

自动卸载客户端

数据库自动维护

软件分发IP组同步

客户端升级

策略名称

策略描述

客户端版本在: 1 (含)至 66940001 *间, 执行升级:
☐ 禁止弹出提示框
☐ 禁止安装检测提示
☐ 使用强制升级方式(重启后生效)
☒ 使用客户端升级包升级(updaterun)

生效时间
☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间限

开始时间	结束时间	编辑	删除
2012-03-10 09:00	2012-03-10 18:30		添加

在线模式
☒ 在线生效 ☒ 离线生效

策略应用对象
<还没有应用到任何对象> [查看及编辑](#)

创建类型
全局

创建者
jing

注: 右边有*号的项目必须输入。

保存 删除 取消

方法二： 不需要使用客户端 patch 包。配置升级策略后，客户端自动在后台通过和服务器的通信进行升级，配置如下：

客户端升级配置 自动卸载客户端 数据库自动维护 软件分发IP组同步

客户端升级

策略名称: *

策略描述:

客户端版本在: (含)至 *间, 执行升级

☐ 禁止弹出重启提示框

☐ 禁止安装检测提示

☐ 使用延迟升级方式(重启后替换)

☐ 使用客户端升级包升级(spdatarun)

生效时间: ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式: ☒ 在线时生效 ☒ 离线时生效

策略应用对象: (还没有应用到任何对象) [查看及编辑](#)

创建类型: 全局

创建者: jing

注: 右边有*号的项目必须输入。

[保存](#) [删除](#) [取消](#)

说明: 大多数客户端升级涉及到客户端驱动升级, 可能需要重启操作系统。

16.2.2. 自动卸载客户端页面

配置介绍

自动卸载客户端

策略名称: *

策略描述:

生效时间: ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式: ☒ 在线时生效 ☒ 离线时生效

策略应用对象: (还没有应用到任何对象) [查看及编辑](#)

创建类型: 全局

创建者: jing

注: 右边有*号的项目必须输入。

[保存](#) [取消](#)

配置项:	说明
策略名称	输入合适的策略名称，以方便管理。
策略描述	用以说明升级历史记录信息，以方便管理。
生效时间	可以选择“所有时间”“工作时间”“非工作时间”“以下时间段”生效，“开始时间”以及“结束时间”仅对“以下时间段”有效。
策略应用对象	点击“查看及编辑”超链接，选择指定的 IP 组、工作组、主机名，立即触发客户端自动卸载。

说明： 客户端卸载功能无需任何版本信息，V6691 以上版本均支持该功能。

配置要点

1、 点击“添加”自动卸载客户端策略，如下图：

自动卸载客户端

策略名称 *

策略描述

生效时间 ☒ 所有时间 ☐ 工作时间 ☐ 非工作时间 ☐ 以下时间段

开始时间	结束时间	编辑	删除
2012-03-10 9:00	2012-03-10 13:30	添加	

在线模式 ☒ 在线时生效 ☒ 离线时生效

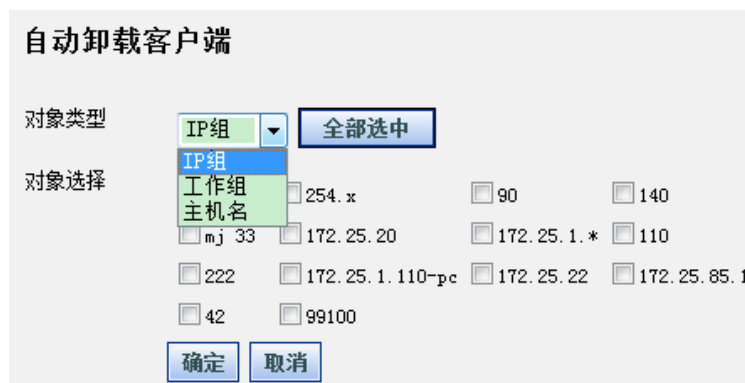
策略应用对象 (还没有应用到任何对象) [查看及编辑](#)

创建类型 全局

创建者 jing

注：右边有*号的项目必须输入。

2、 点击策略应用对象“查看及编辑”超链接，选择指定的 IP 组、工作组、主机名。客户端获得改规则后，立即触发客户端自动卸载。



16.2.3. 数据库自动维护

“数据库自动维护”的三种策略均含其他策略，只需配置任一策略即可。

- “数据库自动维护”通过“压缩数据库”提高系统运行效率。
- “数据库自动维护”通过“备份数据库”以备份系统审计数据。
- “数据库自动维护”通过“清除数据库”清除过期审计数据释放磁盘空间。
- “备份数据库”策略首先对过期数据清除，然后备份原有数据库，最后压缩数据库以节省空间，故配置备份数据库后不需要配置“清除数据库”。
- “清除数据库”不需备份原有数据，适合对审计数据不敏感的环境中使用。
- “压缩数据库”前系统将自动清除超出保留数据月的数据。

压缩数据库页面

配置介绍



配置项:	说明
任务名称	压缩数据库，建议不要更改。
保留数据月数	压缩数据库同时会删除保留数据月以前的数据。
是否启用	如果选择为“是”，则数据库压缩策略生效。

配置要点

- 1、点击“压缩数据库”策略超链接，进入配置页面，如下图：



客户端升级配置 | 自动卸载客户端 | **数据库自动维护** | 软件分发IP组同步

数据库自动维护

任务名称: 压缩数据库

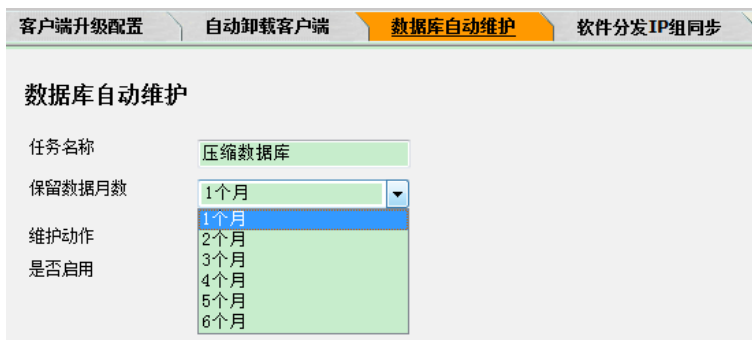
保留数据月数: 1个月

维护动作: 压缩

是否启用: ☒ 是 ☐ 否

保存 取消

- 2、选择“保留数据月数”的下拉列表框，如下：



客户端升级配置 | 自动卸载客户端 | **数据库自动维护** | 软件分发IP组同步

数据库自动维护

任务名称: 压缩数据库

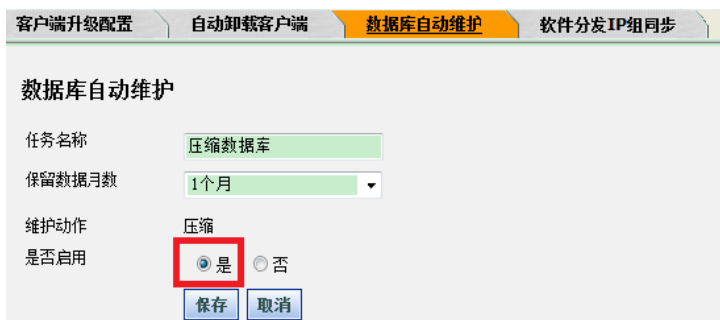
保留数据月数: 1个月

维护动作: 1个月, 2个月, 3个月, 4个月, 5个月, 6个月

是否启用: ☐ 是 ☐ 否

保存 取消

- 3、点击“是否启用”该策略为“是”，保存：



客户端升级配置 | 自动卸载客户端 | **数据库自动维护** | 软件分发IP组同步

数据库自动维护

任务名称: 压缩数据库

保留数据月数: 1个月

维护动作: 压缩

是否启用: ☒ 是 ☐ 否

保存 取消

清除数据库页面

配置介绍



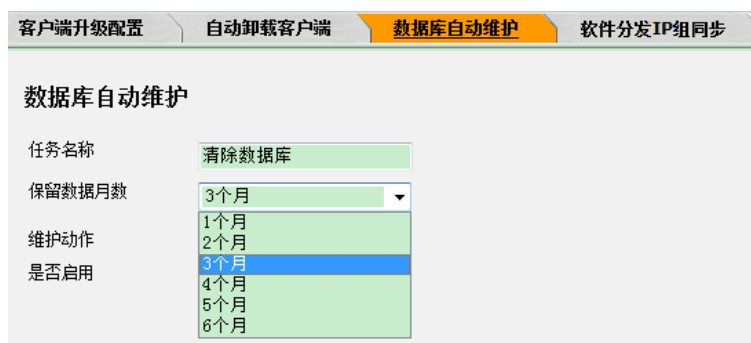
配置项:	说明
保留数据月数	直接删除“保留数据月”以前的数据但不压缩，不备份。

配置要点

1、 点击“清除数据库”策略超链接，进入配置页面，如下图：



2、 选择“保留数据月数”的下拉列表框，如下：



3、 点击“是否启用”该策略为“是”，保存：

客户端升级配置 自动卸载客户端 **数据库自动维护** 软件分发IP组同步

数据库自动维护

任务名称: 清除数据库

保留数据月数: 3个月

维护动作: 清除

是否启用: ☒ 是 ☐ 否

备份数据库页面

配置介绍

客户端升级配置 自动卸载客户端 **数据库自动维护** 软件分发IP组同步

数据库自动维护

任务名称: 备份数据库

保留数据月数: 1个月

维护动作: 备份

备份路径: \\10.201.1.204\share 格式: \\192.168.0.2\share
*请输入,用户名(包括域),格式:192.168.0.2\administrator (确认拥有该以上路径的写权限)

用户名: 10.201.1.204\administ

密码:

是否启用: ☐ 是 ☒ 否

配置项:	说明
保留数据月数	数据备份后系统会自动清除“保留数据月数”前的数据。
备份路径	数据以示例格式备份。备份文件夹不支持中文。
用户名	具有写入共享文件夹权限的系统用户

配置要点

- 1、 点击“备份数据库”策略超链接，进入配置页面，如下图：

客户端升级配置 自动卸载客户端 **数据库自动维护** 软件分发IP组同步

数据库自动维护

任务名称: 备份数据库

保留数据月数: 1个月

维护动作: 备份

备份路径: \\10.201.1.204\share 格式: \\192.168.0.2\share
*请输入, 用户名(包括域), 格式: 192.168.0.2\administrator (确认拥有该以上路径的写权限)

用户名: 10.201.1.204\administ

密码:

是否启用: ☐ 是 ☒ 否

2、选择“保留数据月数”的下拉列表框，如下：

客户端升级配置 自动卸载客户端 **数据库自动维护** 软件分发IP组同步

数据库自动维护

任务名称: 备份数据库

保留数据月数: 1个月

维护动作: 备份

备份路径: \\10.201.1.204\share 格式: \\192.168.0.2\share
*请输入, 用户名(包括域), 格式: 192.168.0.2\administrator (确认拥有该以上路径的写权限)

用户名: 10.201.1.204\administ

密码:

是否启用: ☐ 是 ☒ 否

3、填写备份路径和用户信息。

4、点击“是否启用”该策略为“是”，保存：

客户端升级配置 自动卸载客户端 **数据库自动维护** 软件分发IP组同步

数据库自动维护

任务名称: 备份数据库

保留数据月数: 2个月

维护动作: 备份

备份路径: \\10.201.1.204\share 格式: \\192.168.0.2\share
*请输入, 用户名(包括域), 格式: 192.168.0.2\administrator (确认拥有该以上路径的写权限)

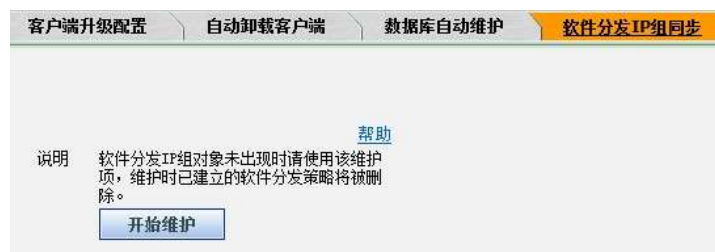
用户名: 10.201.1.204\administ

密码:

是否启用: ☒ 是 ☐ 否

16.2.4. 软件分发 IP 组同步

- 软件分发 IP 组对象未出现时请使用该维护项，维护时已建立的软件分发策略将被删除。



16.3. 系统日志

16.3.1. 管理员操作日志页面

- “管理员操作日志”：记录了日志时间、管理员、操作、对象、详细信息，并提供了删除功能。



说明：三权分立版本中，审计员的操作只能由帐号管理员查看和删除。
帐号管理员操作由审计员查看和删除。

- “详细信息”：对系统操作的行为记录，以 SQL 语句的形式记录，如下：



16.3.2. 按需支援日志页面

■ “按需支援日志”：记录了管理员 IP 地址、管理员登录名、客户端 IP 地址等。



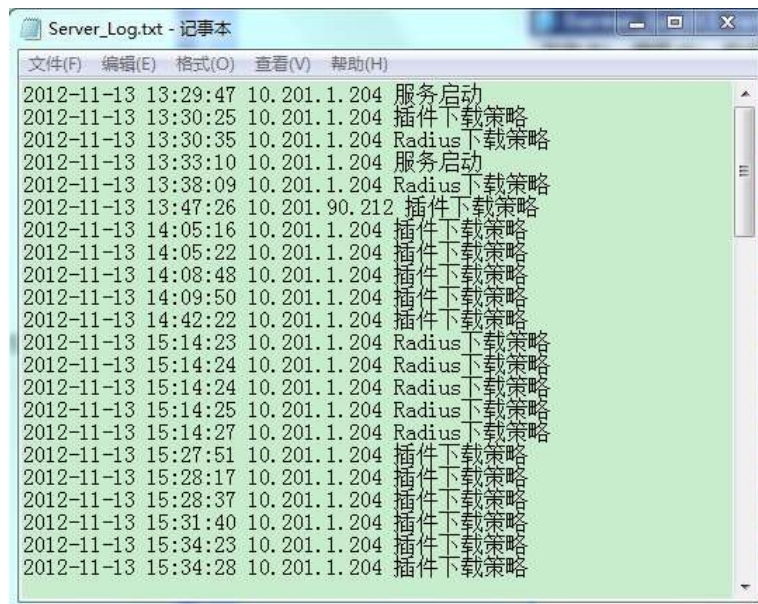
说明：三权分立版本中，按需支援管理员由系统操作员创建和维护。按需支援管理员无删除操作日志的权利，操作日志有系统操作员删除。

15.2.3策略服务器日志页面

■ “策略服务器日志”：记录了策略网关代理、RADIUS 服务器、ES 软件分发服务等启动、取策略的行为，以及客户端取策略和发送报表的行为。



- “策略服务器日志”以TXT文档格式提供查看，如下图：



15.2.4告警服务器同步日志页面

- “查看策略服务器同步日志”：记录了本地告警服务器和中心告警服务器的同步信息。

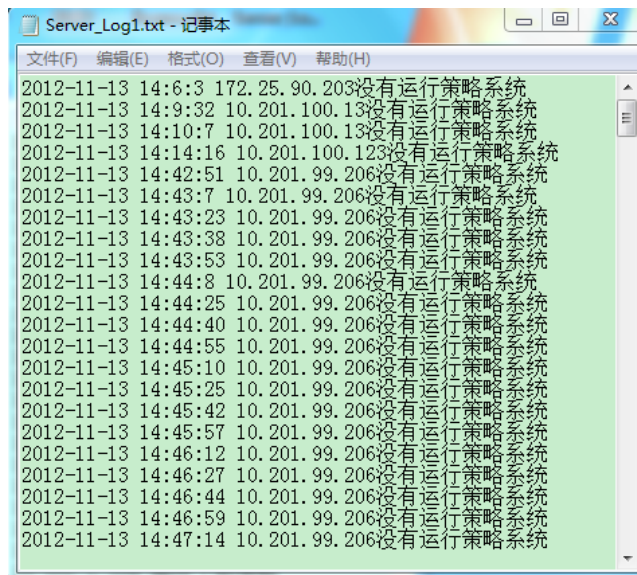


15.2.5策略网关日志页面

- “策略网关日志”：记录了未安装天珣客户端终端信息。



- “策略网关日志”：以 TXT 文档格式提供查看，如下图：



15.2.6 RADIUS 日志页面

- “RADIUS 日志”：记录了网络准入下客户端认证信息。



15.2.7 补丁同步日志页面

- “补丁同步日志”：记录了补丁同步服务器与外网服务器同步的

[管理服务器日志](#)
[保留文件日志](#)
[网络事件日志](#)
[查看各系统日志内容日志](#)
[网络地址日志](#)
[RADIUS日志](#)
[热了再学日志](#)

[同步日志](#)
[清空日志](#)

时间	内容
10/31/2012 11:42:53 AM	本市的设备补丁管理完成
10/31/2012 11:42:53 AM	设备更新完成的热修复
10/31/2012 11:42:53 AM	设备更新完成的热修复
10/31/2012 11:42:53 AM	开始设备热修复补丁管理
10/31/2012 11:42:53 AM	设备同步完成成功完成
10/31/2012 11:42:53 AM	设备热修复同步完成 找到热修复, 0个文件需要下载
10/31/2012 11:42:53 AM	找到14个设备需要热修复
10/31/2012 11:42:49 AM	设备同步完成
10/31/2012 11:42:49 AM	设备补丁已安装成功
10/31/2012 11:42:49 AM	设备补丁已安装成功, 正在处理数据
10/31/2012 11:42:49 AM	设备补丁已安装成功
10/31/2012 11:42:49 AM	设备同步开始
10/31/2012 11:42:49 AM	设备同步完成(成功完成)
10/31/2012 11:42:49 AM	设备同步完成(成功完成), 正在处理数据
10/31/2012 11:42:49 AM	设备同步完成(成功完成)
10/31/2012 11:42:49 AM	设备同步完成(成功完成)
10/31/2012 11:42:49 AM	正在处理设备数据(成功完成)
10/31/2012 11:42:49 AM	设备同步完成(成功完成), 正在处理数据
10/31/2012 11:42:49 AM	设备同步完成(成功完成)
10/31/2012 11:42:49 AM	设备同步完成(成功完成)
10/31/2012 11:42:49 AM	设备同步完成(成功完成)
10/31/2012 11:42:49 AM	设备同步完成(成功完成)

[1. 2. 3. 4. 5. 6. 7. 8. 9. 10.](#)

配置介绍

License管理

授权客户端管理

产品授权信息

导入license

导出license

帮助

产品名称	天珣内网安全风险管理与审计系统
授权单位	天珣测试高级版授权
授权类型	正式授权, 升级维护服务有效期截止到2013年9月30日!
授权IP	10.201.1.204
授权数量	1000
授权模块	基本模块 网络准入 终端审计 移动存储管理 桌面管理
当前授权客户端	35

配置项：	说明
导入 License	从服务器管理界面导入天珣授权文件
导出 License	从服务器管理界面导出天珣授权文件

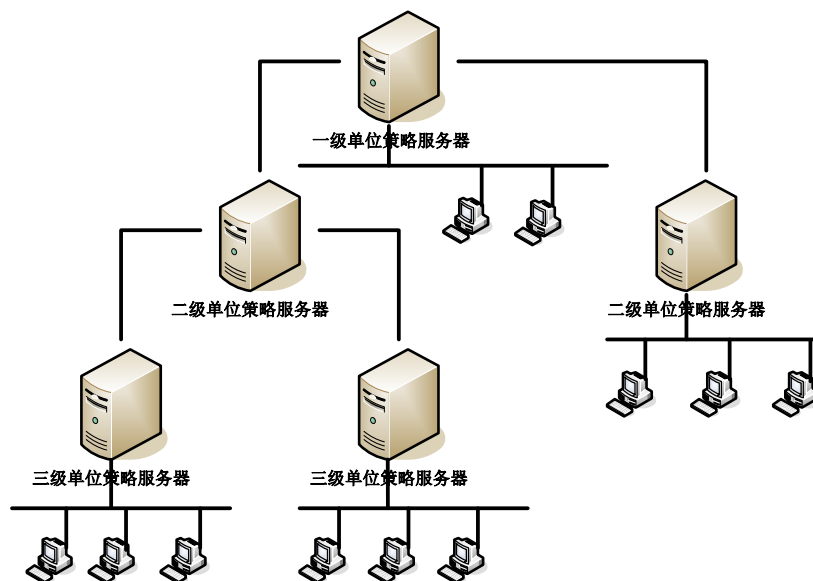
产品名称	天珣内网安全风险管理与审计系统
授权单位	使用单位
授权类型	正式授权或试用授权
授权 IP	授权的单位服务器 ip
授权数量	客户端授权的数量
授权模块	天珣内网安全风险管理与审计系统当前授权的模块
当前授权客户端	授权的客户端数量



注意:删除选中的授权客户端只能删除当前不在线的客户端.

16 系统级联

16.1 关于系统级联

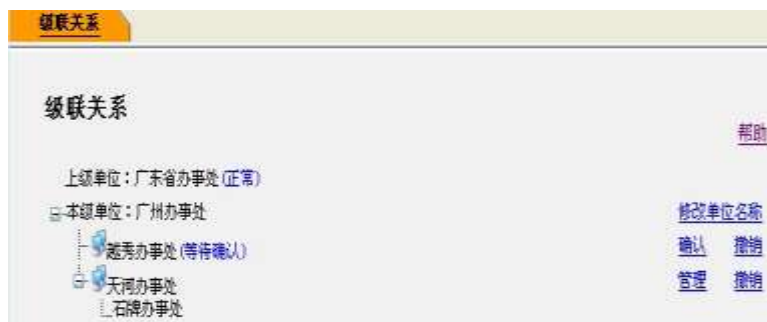


- 各个单位都部署有自己的策略服务器(一个中心服务器和 0 到多个本地服务器), 并且都有直属自己策略服务器管理的终端, 不同单位的中心服务器根据单位的从属关系进行互联, 形成物理上分层的多级架构。
- 上级能够选择性下发策略策略到所有下级服务器。下级接受到上级下发的策略后, 仅仅只能关联下级所属的 IP 组下发到客户端, 不能对上级下发的策略进行其他修改、删除等操作。
- 级联架构下支持仅使用唯一一个 license.dat 授权文件, 并支持上级为下级服务器分配终端授权数量。

16.2 级联关系

16.2.1 配置介绍

拥有系统级联操作权限的系统管理员能在本级单位向上级单位发起申请和确认下级单位的请求, 从而建立上下级关系; 没有权限的管理员对级联关系页面只读。



一个单位有零到一个上级单位，若还未添加上级，则可以点击“**添加上级**”，填入上级单位服务器的 IP 地址，保存后等待上级确认即可。



注意：在上级单位未对下级单位的请求确认之前，下级单位处于“提交请求”或“等待确认”的状态时，下级单位可以将上级单位删除，一旦上级单位确认请求，下级单位就不能将上级单位删除，只能由上级单位撤销下级单位。

点击“**修改单位名称**”，可以修改本级单位名称并同步到上下级



一个单位可以有零到多个下级单位，对于下级单位向本级单位提出的请求，可以点击“**确认**”来建立关系，或者点击“**撤销**”来拒绝请求

对于已确认的下级单位，可以点击“**管理**”查看下级单位的策略和报表，或者点击“**撤销**”来删除下级单位。（对于已分配授权的下级服务器，上级是无法撤销该下级服务器的）

若下级单位被上级撤销了，下级单位（处于已被上级删除，如下图）需要管理员在页面人工点击“**删除上级**”（已确保管理员能被通知到上级已将本单位删除）



注意：要保持上下级单位服务器网络是可达的，并且只能由下级向上级申请，上级对下级进行确认关系。下级单位名称的图标亮着表示服务器在线。

16.3 级联策略管理

16.3.1 配置介绍

级联策略管理”页面，用于管理员选择和下发策略到下级。

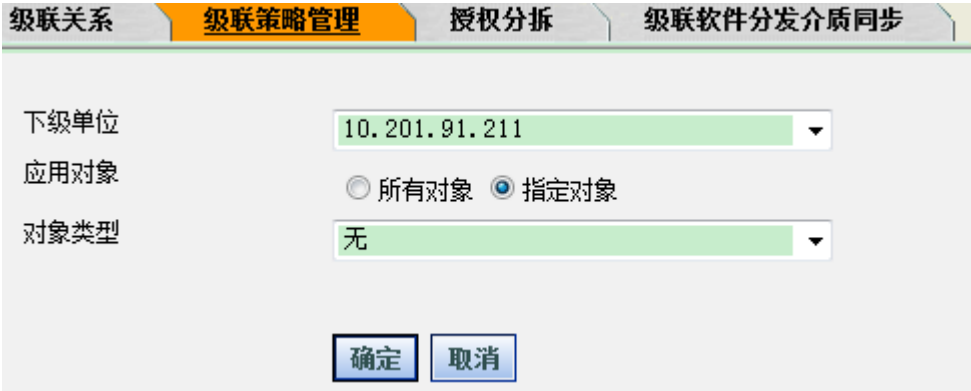


点“**编辑**”



“确认”，该策略会下发至所有下级服务器。下级服务器只能应用该策略，不能编辑，修改和删除该策略。

点击策略应用对象的“查看及编辑”



应用对象可以选择“无”“ip 组”“工作组”“主机名”,选择“无”表示取消全部下发策略，取消后，下级服务器可以进行编辑，修改和删除。

如果在上级服务器删除某条已下发的策略，则下级服务器可以进行编辑，修改和删除。

16.4 授权分拆

16.4.1 配置介绍

级联架构能够支持按照实际需求，将上级授权逐级向下分发授权数量，并可以查看各级授权情况。



授权分拆可以本级授权使用情况，及下级服务器的授权状态。

本级已注册终端数量：显示本级服务器已注册的终端数

已分配的授权数量：显示本级已分配给下级服务器的全部授权数量

可分配的授权数量：产品授权数量-（本级已注册终端数量+已分配的授权数量）

点击“修改授权”笔形按钮可以对下级已分配的授权数量进行修改。

注意：修改授权数不允许小于已使用授权数。

16.5 级联软件分发介质同步

16.5.1 配置介绍

级联软件分发介质同步主要用来同步上级服务器 SDDownload 目录下文件夹 cascadeSD 的文件到下级服务器同样的目录下，在这个过程中，需要手动才能同步。



注意:级联软件分发策略下发前需要先同步介质,否则,下级策略在做 MD5 摘要校验时,如果找不到对应文件,会出现校验失败,导致下级策略分发失败。

17 更新策略

17.1 关于更新策略

- “更新策略”是管理员操作最为频繁的页面,每次策略更新、服务器同步、在线认证与授权时都必须通过“更新策略”,使天珣策略系统各组件取得最新策略。

名词解释

- “更新策略”:是在不影响网络带宽的前提下,根据策略配置的需求,即时通知天珣策略系统各组件获得最新规则以满足企业策略变更的需求。

说明:“更新策略”不仅包括 WEB 管理控制台(<http://localhost:8833>)上由天珣中心服务器主动发送更新策略的指令。“更新策略”也包括客户端上点击右键“更新策略”。“更新策略”还包括客户端每隔一个指定的周期重新获取一次策略的系统架构。

17.2 更新策略的流程

- 1、客户端向服务器发送客户端报表,服务器确认客户端存在;
- 2、管理员在 web 管理控制台(<http://localhost:8833>)发送更新策略指令;
- 3、天珣中心服务器根据已有客户端报表信息提取 IP 地址列表并以此表为准向客户端发送更新策略的指令;
- 4、客户端得到“更新策略”的指令后更新策略。

注意：若客户端仍未向服务器发送客户端报表，将无法获知更新策略的指令。

5、客户端若未收到服务器更新策略的指令，用户可以右键点击客户端 **“更新策略”**；

6、“客户端全局参数” - “重新从 Server 上下载策略的时间间隔”默认值为 24 小时，客户端每 24 小时重新从服务器更新一次规则。

说明：策略服务器发送客户端更新策略使用的是 udp 7891 端口，这样比使用 tcp 端口发送更新策略占用网络带宽低。

17.3 Server 策略版本页面

17.3.1 配置介绍



配置项：	说明
策略版本	配置完策略后，可以手工增加策略版本，用以标记该配置。若客户端“关于”项中策略版本和服务器端不同，则客户端未取得新的策略，需手工更新策略。
增加策略版本	每配置新规则时，可点击“增加策略版本”用以标识。
备份当前策略	可以对当前配置的策略进行备份，如果新的策略存在问题，可以用备份的策略快速恢复。
策略历史记录	即备份的历史策略，点击该按钮可以选择历史策略版本并快速恢复。
本地服务器	本地策略服务器受中心策略服务器管理，此处显示了所有本地服务器的相关信息。可以针对单台本地服务器，

	确认策略版本。可以针对单台本地服务器同步策略。
全部刷新	即刷新所有本地服务器的策略版本。
同步全部 Server 策略	即同步所有本地服务器的策略版本。

说明：本地服务器大多网络独立导致网络时延较大，如果刷新或同步失败可能由于网络超时导致，建议多此尝试。

17.3.2 本地服务器操作简介

- 1、所有策略均由中心服务器配置和管理，所有报表日志均由中心服务器 web 管理控制台查看。本地服务器只需要获取策略并为客户端提供服务即可。
- 2、安装完本地服务器后，点击“**基本配置-策略服务器**”添加本地服务器

策略服务器

服务器名称	本地服务器 *
服务器描述	
IP地址	10.201.12.34 *格式如: 10.156.100.18
中心服务器IP地址	10.201.1.204 *
使用中心服务器的数据库连接参数	☒ 是 ☐ 否
SQL Server数据库连接参数	
数据库服务器IP地址	
端口	
用户名	
密码	
检查数据库连接	

注：右边有*号的项目必须输入。

- 3、添加管理网段，该管理网段的第一服务器为本地服务器，第二服

务器为中心服务器。

管理网段

管理网段

管理网段名称

192.168.12

*

管理网段描述

管理网段开始IP地址

192.168.12.1

*

管理网段结束IP地址

192.168.12.254

*

Primary Server

本地服务器

*

Secondary Server

CenterServer

*

是否使用默认的下栽服务器

☐ 否

☒ 是

下载服务器地址

停止客户端服务程序时是否需要验证密码

☒ 否

☐ 是

卸载客户端时是否需要验证密码

☒ 否

☐ 是

客户端卸载及停止服务密码

显示明文

注：右边有*号的项目必须输入。

保存

取消

- 4、配置该管理网段的 IP 组信息（略）；
- 5、返回 Server 策略版本页面，将看到本地服务器信息。



- 6、点击本地服务器的“刷新”或“同步”按钮将或得本地服务器的程序版本和策略版本。

重要：每配置完策略后，必须将策略同步至本地服务器。若忘记同步规则至本地服务器未取得新策略，导致测试中遇到非预期结果。

17.3.3 配置要点

- 1、配置策略前，选择“**Server 策略版本**”页面，点击“**备份当前策略**”。
- 2、配置完策略后，选择“**Server 策略版本**”页面，点击“**增加策略**

版本”，如下图：

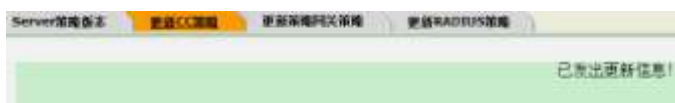


3、点击“同步”本地服务器，确保服务器获得最新规则。

17.4更新 CC 策略版本页面

17.4.1 配置介绍

- 何时需要更新 CC 策略？管理员配置了新的安全策略，并要求所有客户端均需及时同步，则可以及时更新 CC 策略。
- 点击更新 CC 规则后，为什么提示更新完成？提示的是已发出更新信息，但这并不表示所有客户端已经更新策略。



名词解释

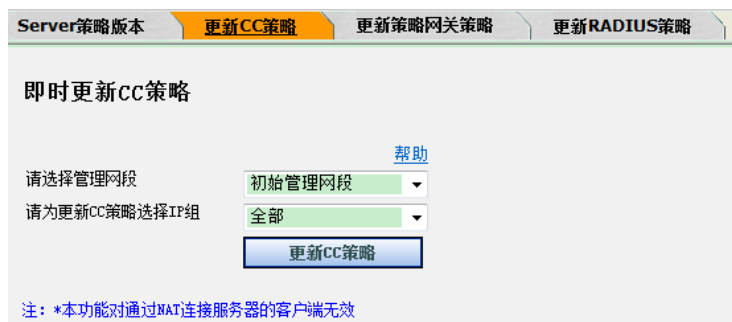
“CC”：即天珣客户端（Client Control）。

17.4.2 配置要点

1、选择更新 CC 策略页面，选择管理网段名称，如下图：



2、点击“更新 CC 策略”



17.5 更新策略网关策略页面

17.5.1 配置介绍

- 更新“策略网关策略”实际上是通知策略网关代理获取配置的新策略。
- 策略网关代理策略变更必须手工更新才能生效，即每次更改策略网关策略后必须手动更新策略。
- 需要确保策略网关代理 IP 地址属于已配置的 IP 组，否则无法正常工作。

名词解释

“更新策略网关策略”：即通知策略网关获取最新的应用准入策略，因策略网关策略由策略网关代理统一“代理”，所以更新的策略实际是选择策略网关代理的服务器做更新。请参考《[用户手册-准入控制-应用准入](#)》。

17.5.2 配置要点

1. 选择更新策略网关策略页面，选择策略网关所属的策略服务器，如下图：



2. 点击“更新策略网关策略”



注意:请确保策略网关代理所属策略服务器，如果策略网关代理所在的管理网段第一服务器不是中心服务器，而是本地服务器。在确保已经同步本地服务器规则后，更新策略务必选择本地服务器，否则功能将不正常。



17.6 更新 RADIUS 策略页面

17.6.1 配置介绍

- 更新“RADIUS 策略”实际上是通知 radius server 获取配置的新策略。
- RADIUS 策略变更必须手工更新才能生效，即每次更改准入控制策略后必须手动更新策略。
- 需要确保 Radius server IP 地址属于已配置的管理网段，否则无法正常工作。

17.6.2 配置要点

1. 选择“请选择 RADIUS Server”下拉列表框，如下图：



18. 附录：单点登录配置手册

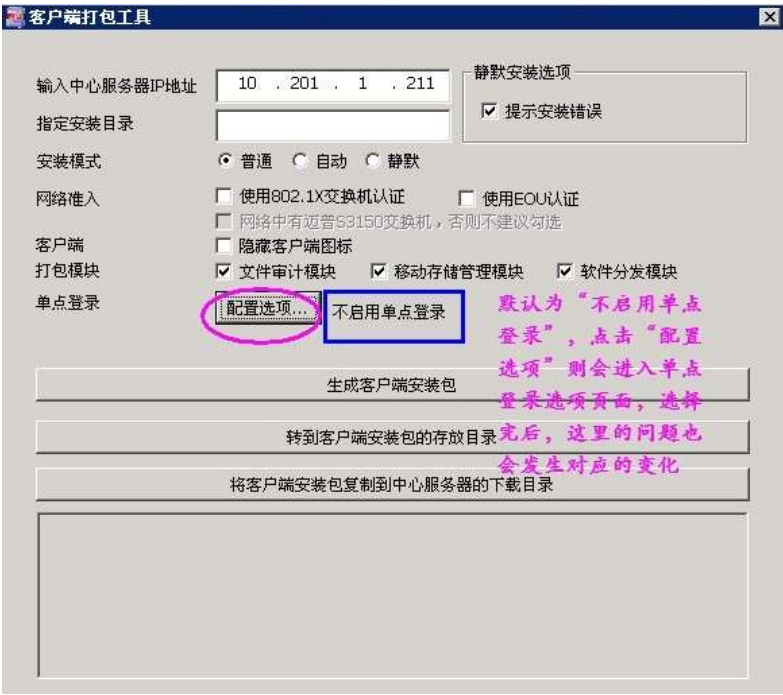
18.1 天珣单点登录简介

单点登录是指在进行身份认证时，只需输入一次用户身份信息，即可以进行多次用户身份认证，实现一次登录全网漫游，一次登录全系统漫游。作为新兴的终端准入控制认证系统，天珣的用户认证是基本要求，安装单点登录功能的天珣客户端，用户就可只输入一次登录凭证就能实现操作系统及天珣系统的双重身份认证，也提升了数据的准确性。

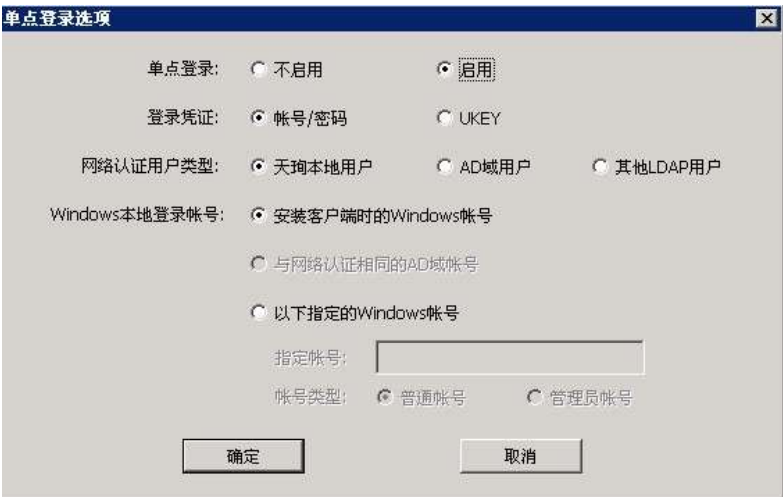
天珣单点登录是指安装完特殊的天珣安装包后，在登录操作系统时，只需要在登录 Windows 系统的时候输入一次登录凭证，天珣客户端就将获取对应的用户认证信息，后台进行和完成相应的用户认证或者准入控制认证。

18.2 单点登录客户端打包

天珣客户端安装包分为普通安装包和单点登录安装包，如果想要具有单点登录功能的话，就必须安装单点登录的安装包，下面就是就其打包的相关选项解释。启动客户端打包工具，点击“单点登录选项”中的“配置选项”，如下图：



点击“配置选项”进入如下页面



配置项:	说明
单点登录:	可选择是否启用单点登录。勾选“不启用”，则安装包为普通安装包；勾选“启用”，安装包则带有单点登录功能
登录凭证:	选择一种身份认证的方式。 帐号/密码 是指在 windows 登录界面上输入帐号密码进行身份认证； UKey 是指在 windows 登录界面上输入智能卡 PIN 码进行身份认证
网络认证用户类型:	规定天珣客户端以哪一类的用户来进行天珣用户认证。

	天珣本地用户 即天珣自己维护的轻量级的目录服务 AD 域用户 即 Active Directory 用户 LDAP 用户 即非 AD 域用户的第三方 LDAP 用户
Windows 本地登录帐号:	此帐号是用于规定登录 Windows 系统的帐号。 安装客户端时的 Windows 帐号 即安装天珣客户端时的当前 Windows 帐号; 与网络认证相同的 AD 域帐号 即以天珣用户认证用户名相同的用户进行 windows 登录, 此选项只有当“网络认证用户类型”选择“AD 域用户”时才可选; 以下指定的 Windows 帐号 指定一个登录 windows 系统的帐号
指定帐号	当“Windows 本地帐号”选择为“以下指定的 Windows 帐号时”, 此项才变为可编辑, 可指定登录的帐号名同帐号类型

选择完相关选项后, 点击“确定”就跳转到打包工具的初始界面, 生成客户端安装包, 此安装包就是具有天珣单点登录功能的安装包了。

18.3 天珣单点登录的两种登录方式

天珣单点登录按照登录凭证可分为帐号/密码单点登录和 UKEY 单点登录, 其主要区别在于登录方式的不同, 下面就这两种登录方式做详细介绍。

18.3.1 帐号/密码单点登录

帐号/密码单点登录是指在 windows 登录界面上, 输入用户名及密码并选择所需登录的域从而实现两次用户身份认证的登录方式(两次用户身份认证是指 Windows 身份认证及天珣用户认证)。帐号/密码登录支持的用户类型包括天珣本地用户、AD 域用户、LDAP 用户。详细配置示例如下, 具体注意事项如下:

注意:

- ◆ “基本配置” — “用户组” — “目录服务”, 这里可以新增一个目录服务, 新增加的目录服务名称必须与目录服务路径的第一个 dc 值一致; 如目录服务的路径为 dc=sunshine, dc=com, 则目录服务名称就为 sunshine;
- ◆ 如果客户端没有启用用户认证时, 选择“用户名/密码登录”登录方式登录时, 无法成功登录
- ◆ 如果终端的用户认证是网络准入下的用户认证, 则只有当网络准入通过后, 才能成功登录系统

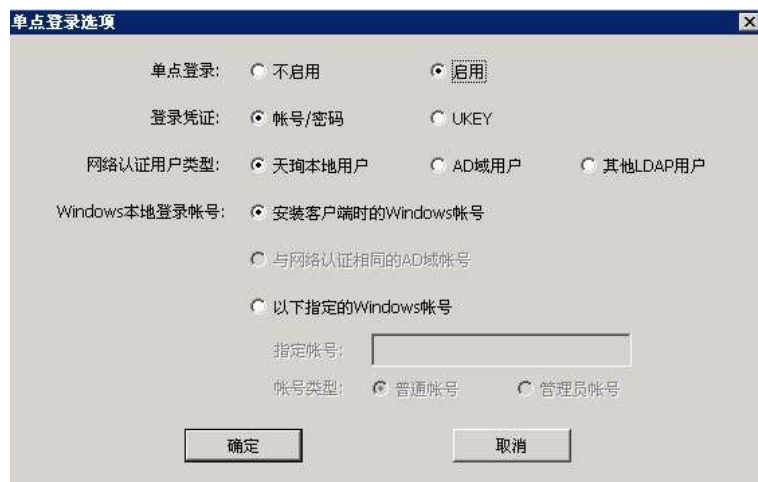
以如下打包选项为例：

登录凭证：帐号/密码

网络认证用户类型：天珣本地用户

Windows 本地登录帐号：安装客户端时的 Windows 帐号

(1) 打包账户/密码登录方式的客户端，见下图，具体解释详见 [18.2](#)



(2) 终端安装步骤(1)打包出来的客户端，重启终端，windows 登录界面变为如下页面



按 ctrl+Alt+delete 跳转到登录界面，vista 以下版本同 vista 以上版本登录界面分别如下：



Vista 及以上版本可能初始登录框不是上图，这是点击“切换用户”就 ok 了。见到上图后，就说明你客户端的配置已成功完成了，先恭喜你了；下面再跟着我转到服务器端进行相关信息配置了。

(3) 首先，进入天珣 Web 控制台（Web 页面），在 Web 控制台上为客户端启用用户认证，非网络准入下的用户认证或者是网络准入下的用户认证；
非网络准入下的用户认证

“基本配置” — “IP 组” “是否启用用户认证” 勾选为启用，并选择你所有启用的目录服务



网络准入下的用户认证

“准入控制” — “网络准入” — “radius server”，点开一个 radius server 配置项，勾选用户认证，并且选择要启用的目录服务



页面配置完成后，在 web 控制台上更新 CC 策略（非网络准入）或者更新 radius 策略（网络准入）。

至此页面上的配置也就基本完成了，现在我们再回到客户端的 windows 登录界面，之前已经有 windows 登录界面的截图了，在用户名、密码输入框输入正确的用户名同密码，并且选择该用户名所对应的域名称，点击“确定”。

成功登录系统后，右键天珣客户端点击“用户登录控制”发现天珣自带的用户认证也已成功完成了。

18.3.2 UKey 单点登录

Ukey 单点登录是指在 windows 登录界面上, 输入 Ukey 的 PIN 码从而实现两次用户身份认证的登录方式(两次用户身份认证是指 Windows 身份认证及天珣用户认证)。UKey 单点登录支持天珣自带的轻量级 CA 和第三方 CA 机构。详细配置示例如下，先查看如下注意事项

注意：

- ◆ 用于 UKey 单点登录的 UKey 必须具有支持智能卡登录操作系统的功能,如:epass 3000、epass 2000FT (epass 2000 FT 不支持 Windows7 系统)
- ◆ 目前天珣系统自带的 CA 只支持将证书颁发到飞天诚信的 UKey, 请确认你 UKey 的牌子及型号
- ◆ 如果天珣客户端跟天珣服务器未连通时,则会采用之前的缓存登录,但必须有一次成功登录缓存登录功能才会生效
- ◆ **“基本配置” — “用户组” — “目录服务”**, 这里可以新增一个目录服务,新增加的目录服务名称必须与目录服务路径的第一个 dc 值一致;如目录服务的路径为 dc=sunshine, dc=com, 则目录服务名称就为 sunshine;
- ◆ 如果客户端没有启用用户认证时, 选择“用户名/密码登录”登录方式登录时, 无法成功登录
- ◆ 如果终端的用户认证是网络准入下的用户认证, 则只有当网络准入通过后, 才能成功登录系统

以如下打包选项为例：

登录凭证：UKey

网络认证用户类型：AD 域用户

Windows 本地登录帐号：与网络认证相同的 AD 域帐号

(1) 打包 Ukey 登录方式的客户端，见下图，具体解释详见 [18.2](#)



(2) 终端安装 UKey 驱动，并且终端加入域，务必记住要安装 UKey 驱动，未安装该驱动就无法采用 UKey 登录系统了

(3) 终端安装步骤 (1) 打包出来的客户端，重启终端，windows 登录界面变为如下页面



按 ctrl+Alt+delete 跳转到登录界面，vista 以下版本同 vista 以上版本登录界面分别如下：



Vista 及以上版本可能初始登录框不是上图，这是点击“切换用户”就 ok 了。见到上图后，就说明你客户端的配置已成功完成了，先恭喜你了；下面再跟着我转到服务器端进行相关信息配置了。

以 windowsCA 为例，windowsCA 安装及证书生成详见 [18.4](#)

- (3) 首先，进入天珣 Web 控制台（即 Web 页面），进入 [“认证管理→第三方 CA 机构”](#) 添加一个第三方 CA 根证书；
- (4) 根证书添加完成后，再去到“认证管理→身份认证”，在“用户及证书信息管理”页面上导入 AD 域用户，详见 [14.3.2](#)；
- (5) 将导入的第三方用户同 UKey 里面的证书相关联。只需要在“用户及证书信息管理”页面上，点击你需要关联的那个用户后，在“证书用户名”里填写 UKey 里面的证书用户名；详见 [14.3.2](#)；
- (6) 配置完上面这些之后，进入最后一个配置环节：为客户端启用用户认证。启用方法同帐号/密码单点登录的第（3）步配置；

配置完成后，在 web 控制台上更新 CC 策略（非网络准入）或者更新 radius 策略（网络准入）。

至此页面上的配置也就基本完成了，现在再回到客户端的 windows 登录界面，之前已经有 windows 登录界面的截图了，将 UKey 接入安装了单点登录客户端的终端后，在 PIN 码对应的输入框输入正确 PIN 码，点击“确定”即可登录了。至此，UKey 单点登录功能也算大功告成了。

成功登录系统后，右键天珣客户端点击“用户登录控制”发现天珣自带的用户认证也已成功完成了。

18.4 配置利用智能卡进行 windows 身份验证

准备工作：

- 1、搭建域环境
- 2、安装 IIS，并将“Active Server Pages”服务设置为“允许”



- 3、客户端加入域以及相关 USBKey 驱动安装



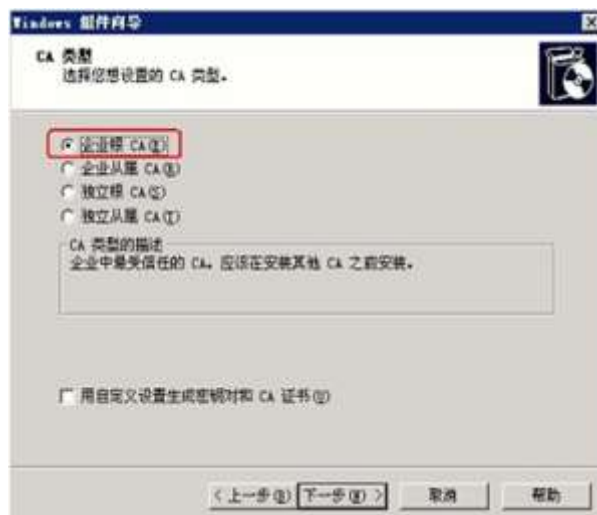
一、安装证书服务器

打开“windows组件安装”，选择“证书服务”



选择“企业根 CA”

注明：要颁发智能卡登录证书，必须选择“企业根 CA”才可以使用，企业根 CA 和独立根 CA 都是证书颁发体系中最受信任的证书颁发机构，可以独立的颁发证书。企业根 CA 需要 Active Directory 支持，而独立根 CA 不需要，从属级的 CA 由于只能从另一证书颁发机构获取证书，所以一般不被选择。而创立根主要用于外部网的 CA，在安装后不能增加证书模板，不能颁发智能卡证书，所以我们这里不选择独立 CA



输入证书的识别名称，这里我们输入“hetech”



选择证书数据库和日志的安装路径，我们设置为默认



安装证书服务需要重启 IIS 服务，我们这里选择“是”



安装证书服务



安装证书完毕后，进入第二个阶段，

下载证书

打开 IE，访问证书服务器的地址 <http://证书服务器的 IP 地址/certsrv>，
下载一个证书：



选择“下载 CA 证书”



选择保存路径:



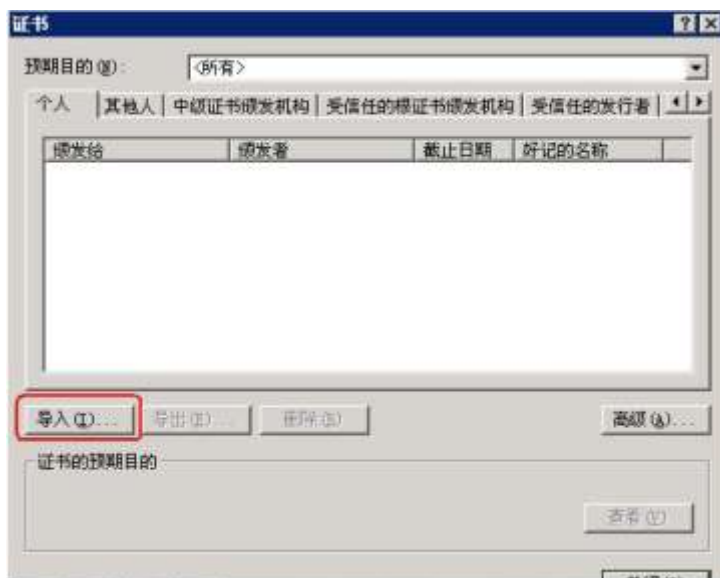
下载完毕后，接下来需要导入到机器中

导入根证书

打开 IE 属性，选择“内容—》证书”



选择“导入”



进入证书导入向导，进入“下一步”



选择证书存放的路径，点击“下一步”



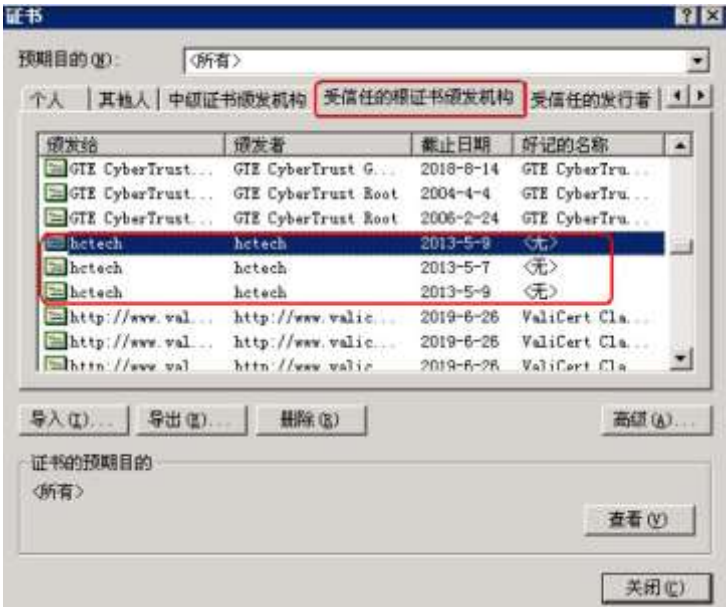
选择证书存放的方式，这里我们选择默认



确认导入信息



导入完成后，我们可以在“中级证书颁发机构”和“受信任的根证书颁发机构”中看到刚导入的证书信息



添加证书模板

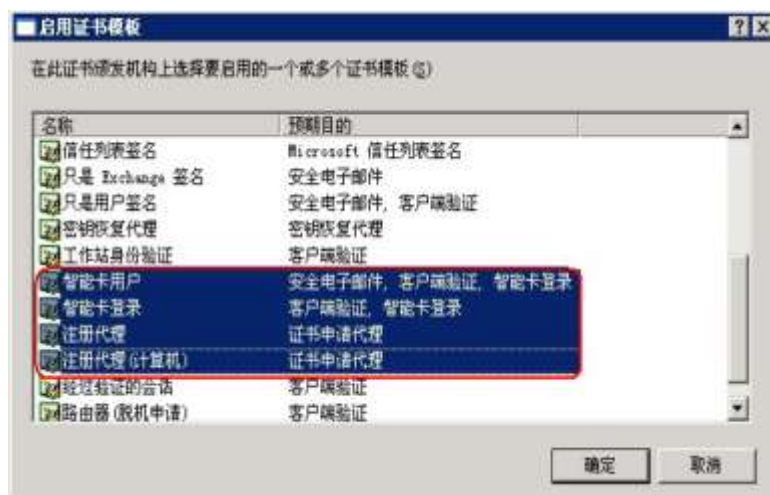
打开管理工具，选择“证书颁发机构”



右键“证书模板”-“新建”-“要颁发的证书模板”



选择要启用的证书模板：智能卡用户、智能卡登录、注册代理、注册代理（计算机），然后“确定”



申请注册代理

打开 mmc，然后添加“证书”管理单元





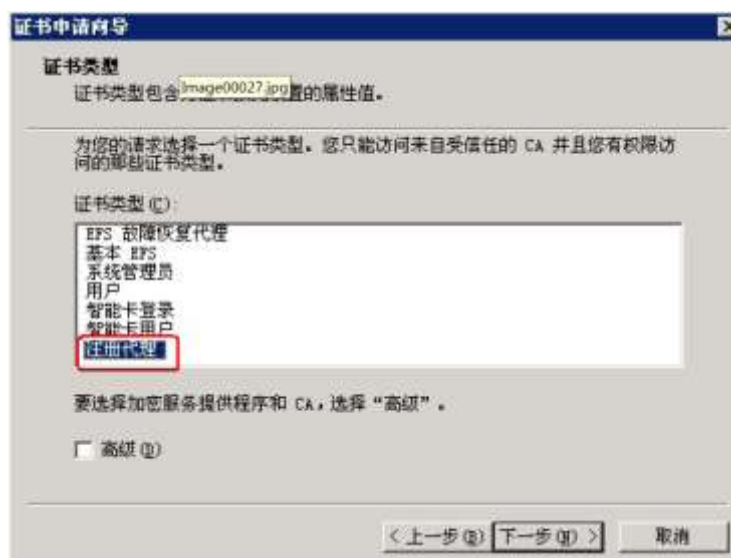


选择“证书”，选择“添加（A）”按钮后，根据系统提示完成证书管理单元选择。在控制台管理界面，选择“证书-当前用户”，选择“个人”，点击鼠标右键，选择“所有任务”，选择“申请新证书...”，进行证书类别选择





选择“注册代理”，选择“下一步 (N) >”按钮，根据系统提示填写出现证书的名称和描述等信息完成注册代理证书的申请





完成注册代理申请后，可以在看到已经颁发给个人的证书的信息





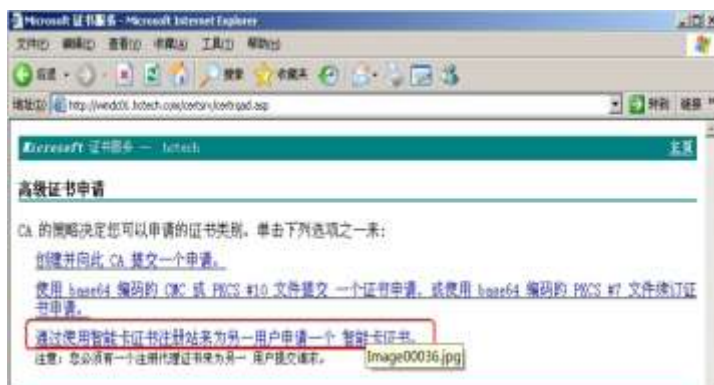
申请证书



选择“高级证书”进行高级证书申请



选择“通过使用智能卡证书注册站来为另一个用户申请一个智能卡证书”，出现智能卡证书注册站



在弹出的“ActiveX”警告框中，选择“是”



进入智能卡证书注册站界面后，可以看到相关的一些基础信息



选择证书模板为“智能卡登录”，选择加密服务提供程序为：“FEITIAN ePassNG RSACryptographic Service Provider”，选择用户后，选择“注册”按钮，出现输入用户 PIN 码的对话框



完成证书的导入，然后利用智能卡进行身份验证登录AD域