# NaseForXP安装使用手册

目录

[NaseForXP安装使用手册 1](#_Toc430694217)

[第一章、简介 4](#_Toc430694218)

[1.1、功能 4](#_Toc430694219)

[1.2、软件模块 4](#_Toc430694220)

[第二章、软件安装 4](#_Toc430694221)

[2.1、使用获取硬件信息工具 4](#_Toc430694222)

[2.2、使用USBKEY初始化工具 5](#_Toc430694223)

[2.3、安装管理中心 6](#_Toc430694224)

[2.4、安装客户端 6](#_Toc430694225)

[第三章、管理中心统一初始化USBKEY及注册软件 7](#_Toc430694226)

[第三章、客户端 - 安全管理员账户功能 8](#_Toc430694227)

[3.1、登录 8](#_Toc430694228)

[3.2、事件总揽 9](#_Toc430694229)

[3.3、安全防护 - 基本防护 9](#_Toc430694230)

[3.4、安全防护 - 增强防护 10](#_Toc430694231)

[3.5、账户安全 11](#_Toc430694232)

[3.6、事件查看 12](#_Toc430694233)

[3.7、系统设置 – 系统防护 13](#_Toc430694234)

[3.8、系统设置 - 账户设置 14](#_Toc430694235)

[第四章、客户端 - 审计员账户功能 15](#_Toc430694236)

[4.1、登录 15](#_Toc430694237)

[4.2、事件总揽 16](#_Toc430694238)

[4.3、安全审计 16](#_Toc430694239)

[4.4、系统审计 16](#_Toc430694240)

[4.5、生成报表 17](#_Toc430694241)

[4.6、系统设置 18](#_Toc430694242)

[第五章、管理中心 - 安全管理员账户功能 19](#_Toc430694243)

[5.1、登录 19](#_Toc430694244)

[5.2、主界面 19](#_Toc430694245)

[5.3、IP分组管理 19](#_Toc430694246)

[5.4、策略导入、导出 21](#_Toc430694247)

[5.5、安全防护 22](#_Toc430694248)

[5.6、账户安全 23](#_Toc430694249)

[5.7、事件查看 23](#_Toc430694250)

[5.8、系统设置 23](#_Toc430694251)

[5.9、管理中心设置 24](#_Toc430694252)

[第六章、管理中心 - 审计管理员账户功能 24](#_Toc430694253)

[6.1、登录 24](#_Toc430694254)

[6.2、主界面 25](#_Toc430694255)

[6.3、安全审计 25](#_Toc430694256)

[6.4、系统审计 26](#_Toc430694257)

[6.5、生成报表 26](#_Toc430694258)

[6.6、管理中心报表 27](#_Toc430694259)

[6.7、管理中心设置 28](#_Toc430694260)

[第七章、卸载客户端 29](#_Toc430694261)

[7.1、停止保护 29](#_Toc430694262)

[7.2、运行卸载脚本 29](#_Toc430694263)

[第八章、卸载管理中心 29](#_Toc430694264)

[8.1、运行卸载脚本 29](#_Toc430694265)

第一章、简介

1.1、功能

NaseForXP是全方位保护XP操作系统，防止病毒威胁的安全软件，支持二级部署和集中管理，同时符合等级保护要求，采用三权分立的设计，让管理账户和审计账户分离，支持软硬件双因子登录认证。

1.2、软件模块

软件包含四个模块：

核心模块（2个）：Nase管理中心安装程序、Nase客户端安装程序。



辅助工具（2个）：USBKEY初始化工具、获取硬件信息工具。



第二章、软件安装

2.1、使用获取硬件信息工具

管理中心和客户端的登录，都需要进行密码和USBKEY的双认证，USBKEY会将机器硬件信息和KEY做绑定，从而限制一把KEY只能在一台机器上使用。而初始化KEY需要下面的“获取硬件信息”工具。

USBKEY的类型有两种，一种是提供给管理中心登录使用，另外一种是提供给客户端登录使用。

运行程序后会得到两个信息：“管理中心序号”，“客户端序号”，这两个序号分别用来初始化管理中心登录KEY和客户端登录KEY。

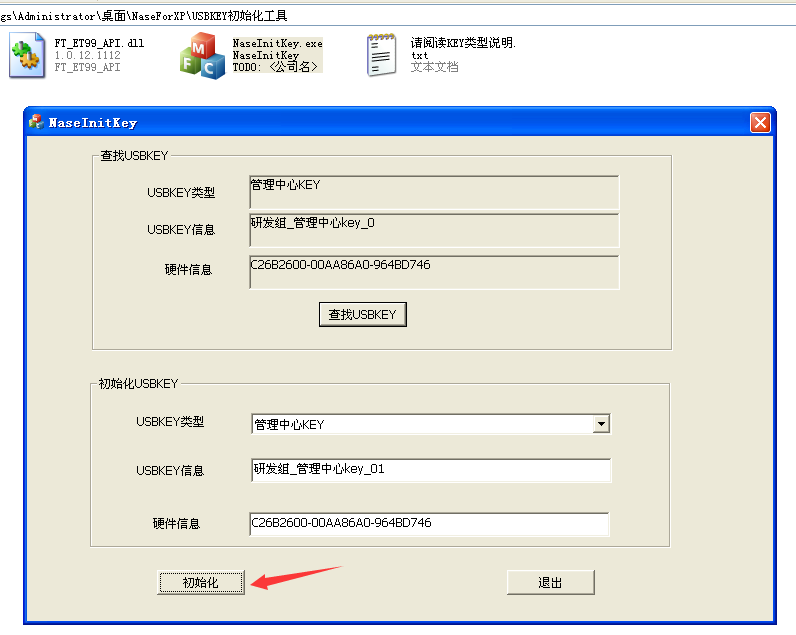


2.2、使用USBKEY初始化工具

插入本公司的USBKey，并运行“USBKEY初始化工具”，该工具可以将USBKEY初始化成管理中心KEY或者客户端KEY。

1. USBKEY类型，选择“管理中心KEY”或“客户端KEY”
2. USBKEY信息，写入KEY描述信息
3. 硬件信息，写入2.1中获取到的“管理中心序号”或“客户端序号”。
4. 点击“初始化”，完成对KEY的初始化，绑定KEY和硬件信息。
5. 点击“查找USBKEY”，可以查看已经初始化的KEY信息。

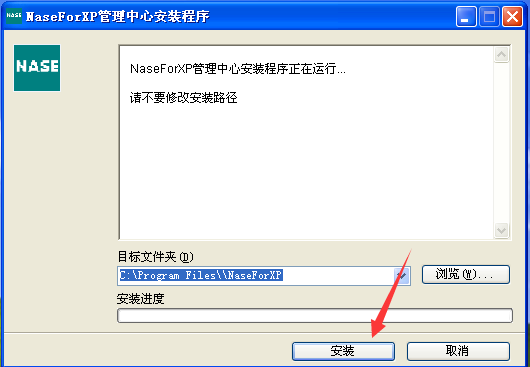
这样就完成了一个USBKEY的初始化，然后就可以使用这把KEY登录对应的管理中心或者客户端了



2.3、安装管理中心

第一步、运行Nase管理中心安装程序：

注意：请直接点击安装，不要修改安装路径。



安装完成后，会在桌面生成一个快捷方式：

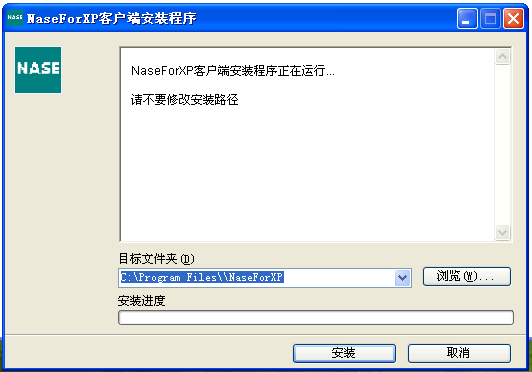


管理中心已经安装成功，并且后台已经启动。

2.4、安装客户端

第一步、运行Nase客户端安装程序：

注意：请直接点击安装，不要修改安装路径。



安装完成后，会在桌面生成一个快捷方式：



第三章、管理中心统一初始化USBKEY及注册软件

由于采用了双因子严格认证，客户端的安装也会带来很多不方便，例如：安装完客户端，需要在每台客户机上初始化USBKEY才可以登录。同时软件注册也需要去单独的客户端上注册，非常不方便。

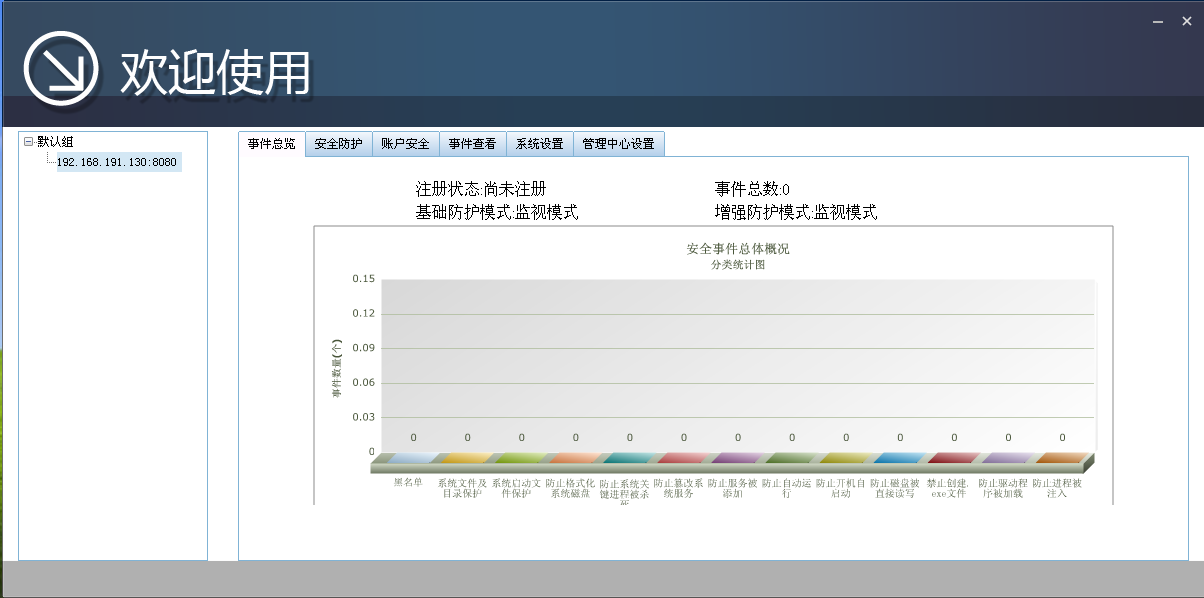
为了简化安装流程，我们提供了一套方案，可以在管理中心完成所有USBKEY的初始化，以及软件注册。

其步骤原理如下：

1. 先安装管理中心
2. 安装客户端，在“管理员账户”登录界面，填写管理中心的“IP：端口”，点击“登录”。此时客户端虽然无法登录，但是会将客户端信息发送到管理中心。



1. 初始化一把管理中心的KEY，以“管理员账户”登录管理中心，就可以看见连接进来的客户端了。



1. 选中左列一个IP --》系统设置 --》帐号设置，可以看见里面有一个“注册信息”，这就是当前客户端的硬件信息，“注册信息”与使用2.1中工具在客户端获取到的“客户端序号”一致。



1. 拔掉“管理中心USBKEY”（因为一台机器上只能使用一个USBKEY），管理中心登录完成后，在下次登录前，不需要使用USBKEY。
2. 插入一把新KEY，打开“USBKEY初始化工具”，使用第四步的“注册信息”,初始化一把“客户端KEY”。并对KEY贴加标签。
3. 输入注册码，对客户端软件进行软件注册。

通过上面这种方式，就可以在管理中心，对USBKEY和注册码进行统一生成了。之后只需要将USBKEY下发下去即可。

第三章、客户端 - 安全管理员账户功能

3.1、登录

a）插入客户端USBKEY

b）切换登录账户为：安全管理员

c）输入默认密码:123456

d）输入管理中心IP端口:

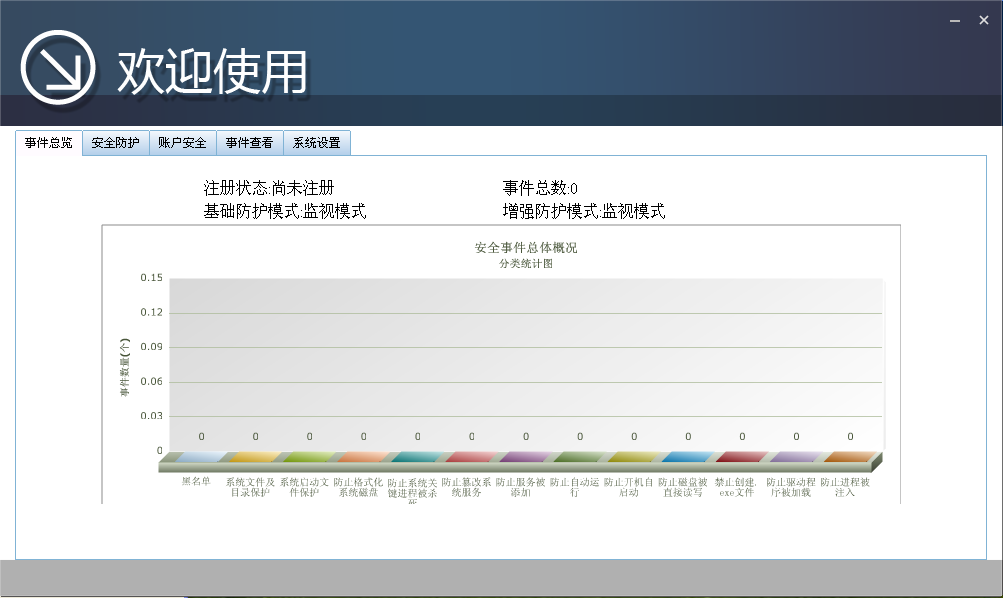
e）点击登录，进入“事件总揽”主界面。

注：安全管理点击“登录”时候，会将自身信息发送到管理中心，这样管理中心就可以控制此客户端。



3.2、事件总揽

主界面展示了系统的基本状态和信息。



3.3、安全防护 - 基本防护

用来配置系统的安全项，需要软件注册后才可以使用，配置完，点击“应用”按钮生效。



3.3.1、防护模式

模式有两种：

a）、监听模式

对触犯安全防护规则的操作，只进行日志记录，不会做拦截操作。

b）、防护模式

对触犯安全防护规则的操作，进行日志记录，并且拦截操作。

3.3.2、系统目录及文件的保护

开启后，会对Windows系统目录进行保护，防止恶意程序修改、删除系统目录下的文件。

3.3.3、系统启动文件保护

开启后，会对boot.ini和ntldr进行保护，防止恶意程序破坏启动文件。

3.3.4、防止格式化系统磁盘

开启后，会对磁盘格式化进行拦截，防止磁盘被恶意程序格式化。

注：当开启“防止磁盘被直接读写”后，格式化操作会被“防止磁盘直接读写”优先拦截。

3.3.5、防止系统关键进程被杀死

开启后，会防止恶意程序kill系统关键进程：csrss，lsass，services，smss，svchost，winlogon。

3.3.6、防止篡改系统服务

开启后，会防止恶意程序修改系统服务。

3.4、安全防护 - 增强防护

用来配置系统的安全项，需要软件注册后才可以使用，配置完，点击“应用”按钮生效。



3.4.1、防护模式

模式有两种：

a）、监听模式

对触犯安全防护规则的操作，只进行日志记录，不会做拦截操作。

b）、防护模式

对触犯安全防护规则的操作，进行日志记录，并且拦截操作。

3.4.2、防止服务被添加

开启后，会防止恶意程序将自身添加到服务中。

3.4.3、防止自动运行恶意程序

开启后，会拦截autorun自动运行恶意程序。

3.4.4、防止添加开机自启动项

开启后，会拦截恶意程序将自己添加到开机启动注册表项里面。

3.4.5、防止磁盘被直接读写

开启后，会拦截恶意程序对磁盘的直接读写操作。

3.4.6、禁止创建.exe文件

开启后，会拦截恶意程序生成.exe的文件。

3.4.7、防止驱动被加载

开启后，会拦截恶意程序加载驱动。

3.4.8、防止进程被注入

开启后，会拦截恶意程序注入其他进程。

3.5、账户安全

用来配置系统账户的密码安全性策略，需要软件注册后才可以使用，配置完，点击“应用”按钮生效。



3.5.1、密码复杂度

开启后，设置系统密码，会检查密码复杂度，要求使用复杂密码。

3.5.2、最小密码长度

开启后，设置系统密码，会检查密码的最小长度。

3.5.3、锁定时长

开启后，如果密码验证错误，则会锁定账户相应时长。

3.5.4、锁定次数

开启后，如果密码输入错误次数超过设定值，则账户被锁定。

3.5.5、最短使用期限

开启后，设定密码最短使用期限为当前值。

3.5.6、最长使用期限

开启后，设定密码最长使用期限为当前值。

3.5.7、强制密码历史

开启后，最近使用的密码将不可以被再次使用。

3.6、事件查看

用来查看发生的安全事件。



3.7、系统设置 – 系统防护

3.7.1、设置白名单

在白名单列表里的程序，不会被软件拦截操作。



3.7.2、设置黑名单

在黑名单里的程序，会拦截其所有操作。



3.8、系统设置 - 账户设置



3.8.1、修改管理员密码

可以修改当前安全管理员的登录密码。

3.8.2、注册

可以使用注册码对软件客户端进行注册，软件只有注册之后，才可以开启防护功能。

3.8.3、日志导出

点击后会将日志导出到指定文件，用来防止日志文件不断变大。



3.8.4、策略导出

将当前客户端的安全配置策略，导出到文件。

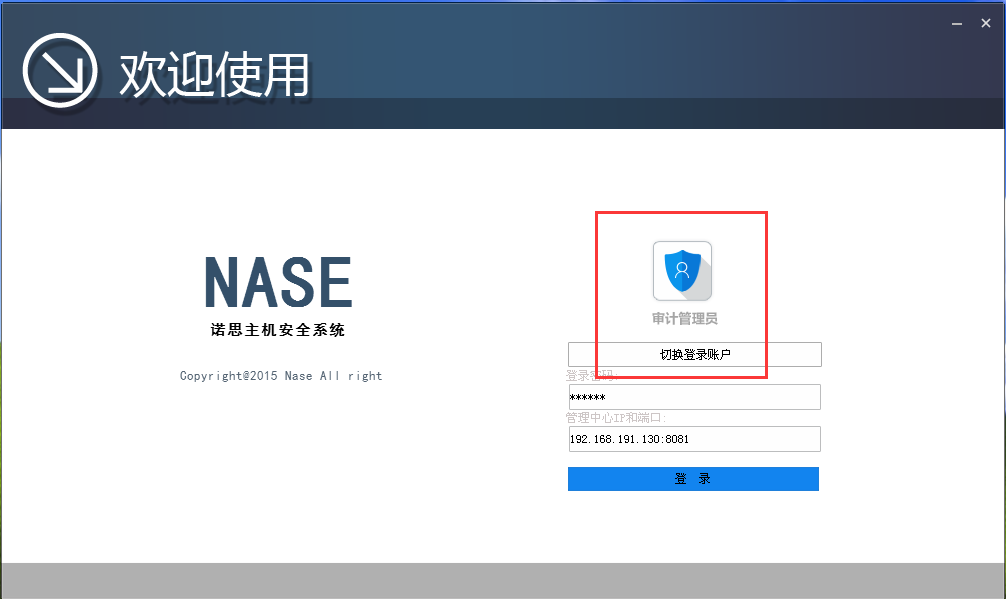
3.8.5、策略导入

使用指定策略文件导入和替换掉当前客户端的策略。

第四章、客户端 - 审计员账户功能

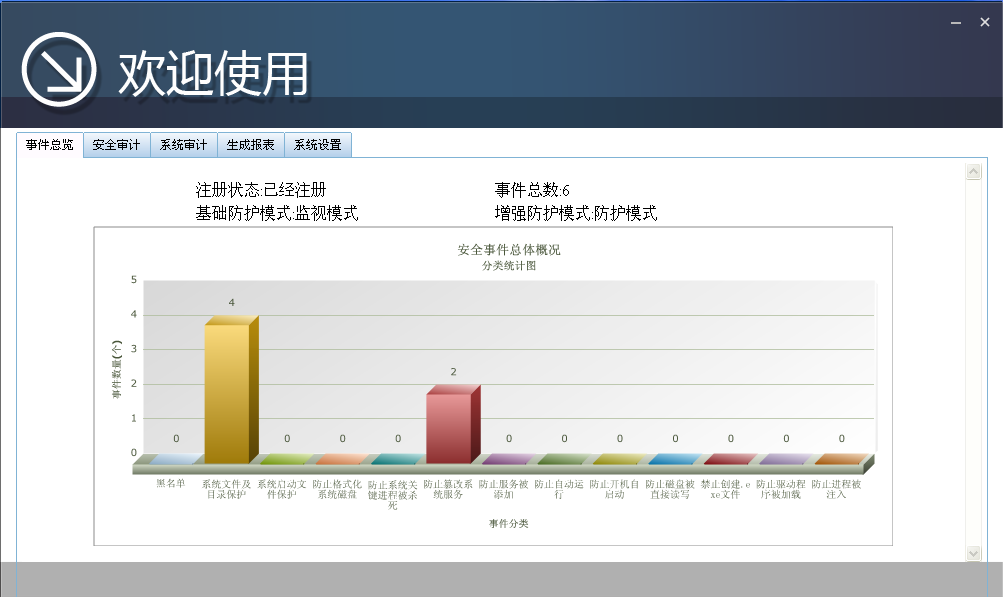
4.1、登录

双击“NASE客户端”，在登录界面，切换成“审计管理员”，输入默认密码：“123456”，点击“登录”，登录成功后，进入“事件总揽”主页面。



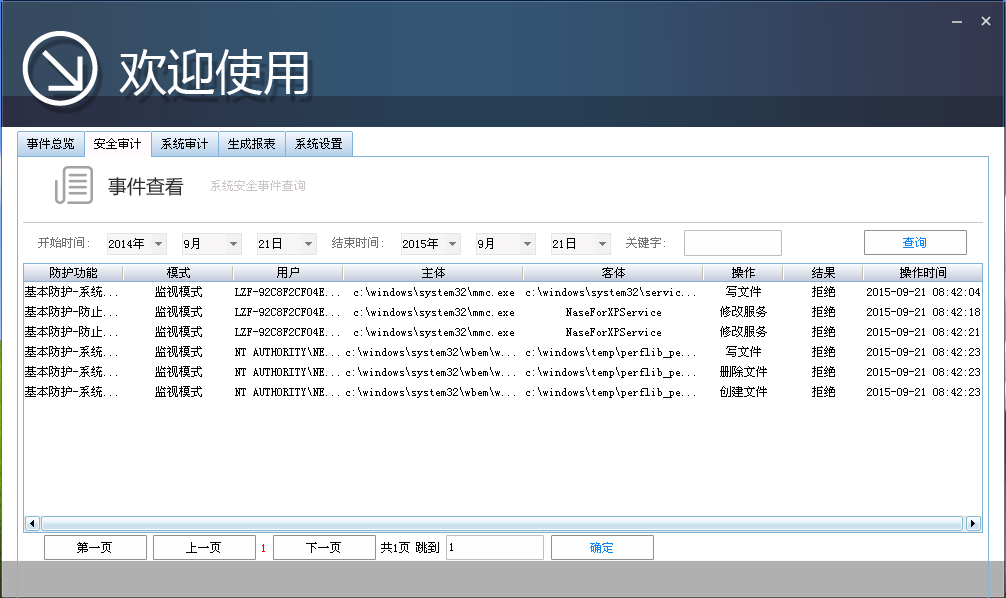
4.2、事件总揽

主界面展示了系统的基本状态和信息。



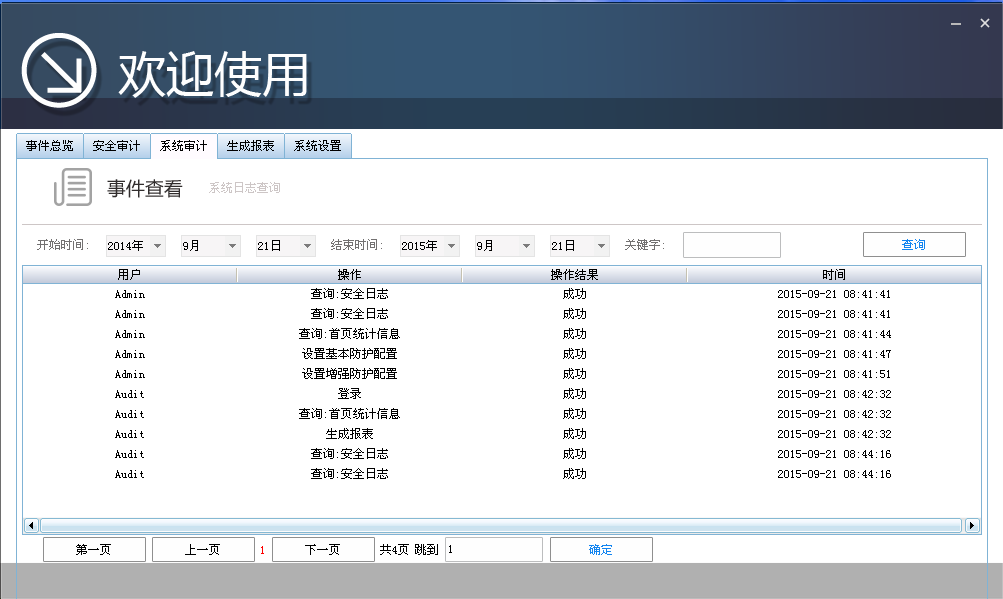
4.3、安全审计

与3.6章节的“事件查看”一致，用来查看安全事件。



4.4、系统审计

记录和查询软件的操作和运行记录。



4.5、生成报表

生成客户端的安全事件报表。报表有三部分：本月安全事件趋势图，本月安全事件分类图，本年安全事件分类图。







4.6、系统设置

设置当前审计管理员的登录密码。



第五章、管理中心 - 安全管理员账户功能

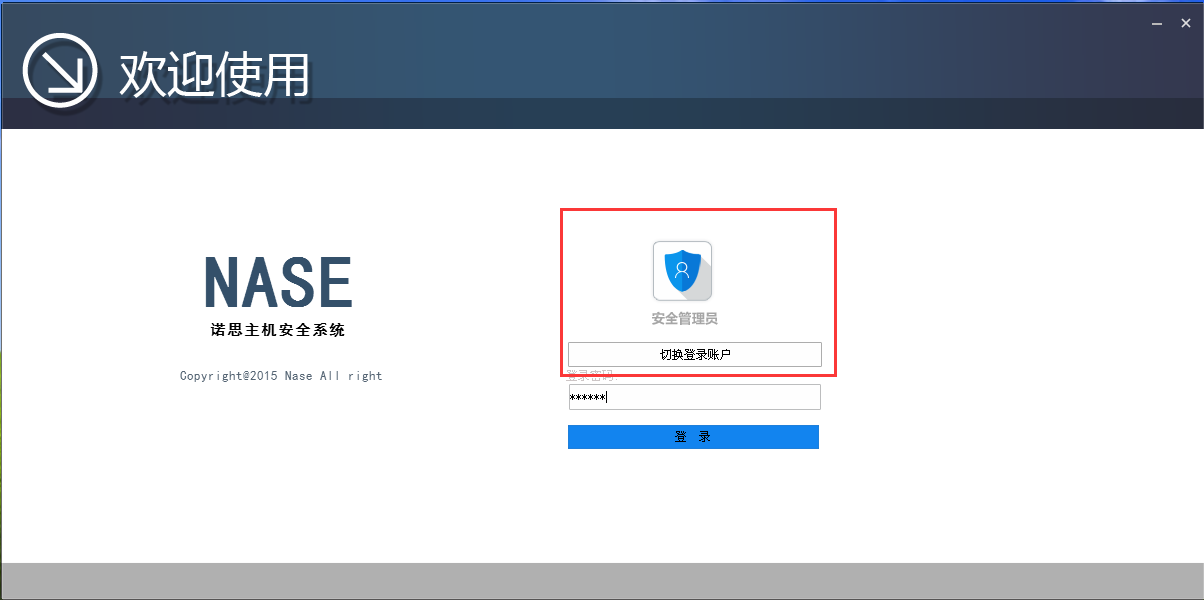
5.1、登录

a）插入管理中心USBKEY

b）切换登录账户为：安全管理员

c）输入默认密码:123456

d）点击登录，进入主界面



5.2、主界面

默认显示左侧IP列表中的第一个IP的首页。点击列表中的IP时候，则会切换到该IP的管理页面。

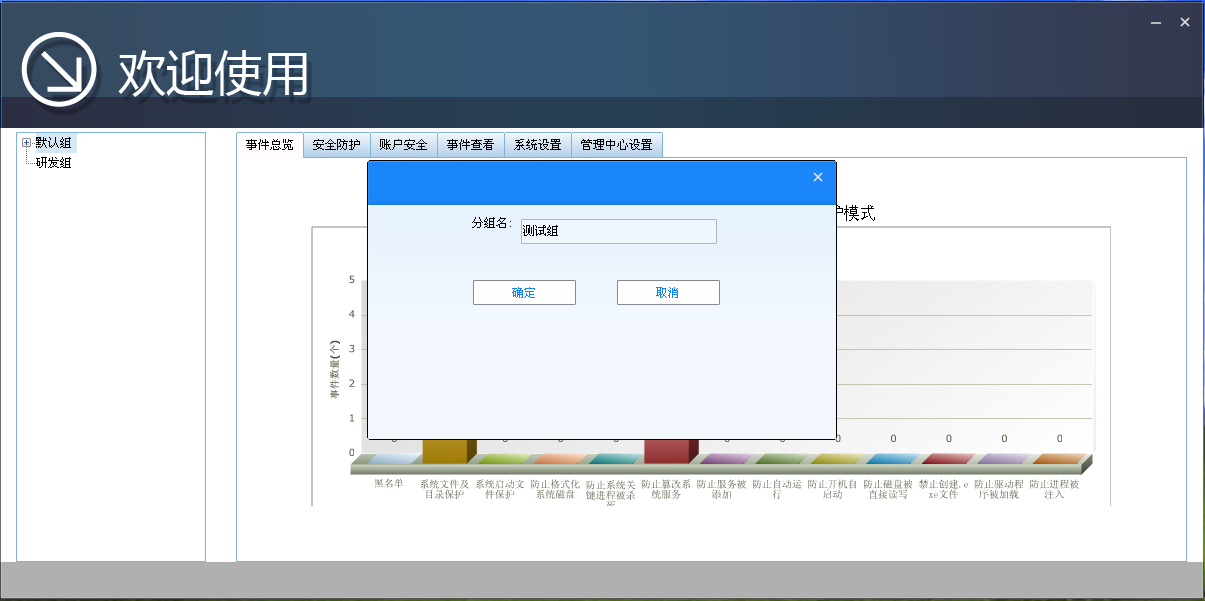


5.3、IP分组管理

鼠标右键“分组”名称，会弹分组管理菜单，包括“添加分组”、“删除分组”、“添加分组IP”、“IP移动到分组”。



5.3.1、添加分组

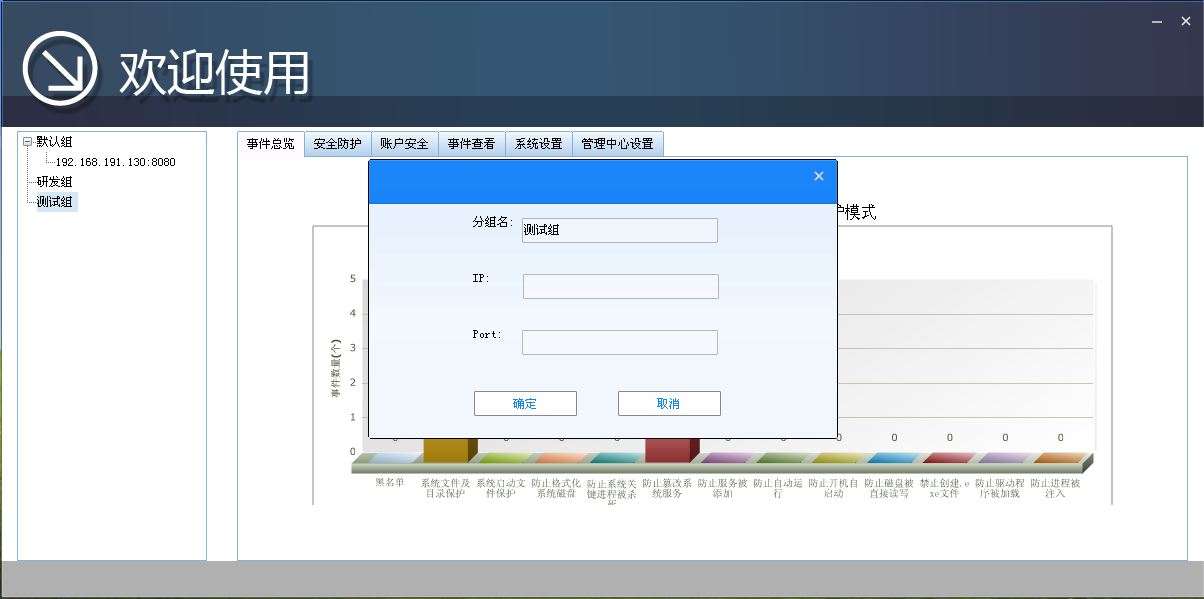


5.3.2、删除分组

鼠标右键分组名，可以删除分组，删除分组后，该组的IP自动移到“默认组”。



5.3.3、添加分组IP



5.3.4、IP移动到分组

鼠标右键指定IP，可以将该IP移动到指定分组。



5.3.5、刷新列表

新登录的客户端，可能还没有显示在管理中心，点击刷新，会获取最新的客户端列表。

5.4、策略导入、导出

鼠标右键指定IP，选择“策略导出”，可以导出当前IP的策略，点击“策略导入”，则可以将当前的策略导入到当前IP。

鼠标右键分组，选择“策略导入”，则可以将指定策略导入到当前分组。



5.5、安全防护

与客户端一致，参照3.3，3.4。





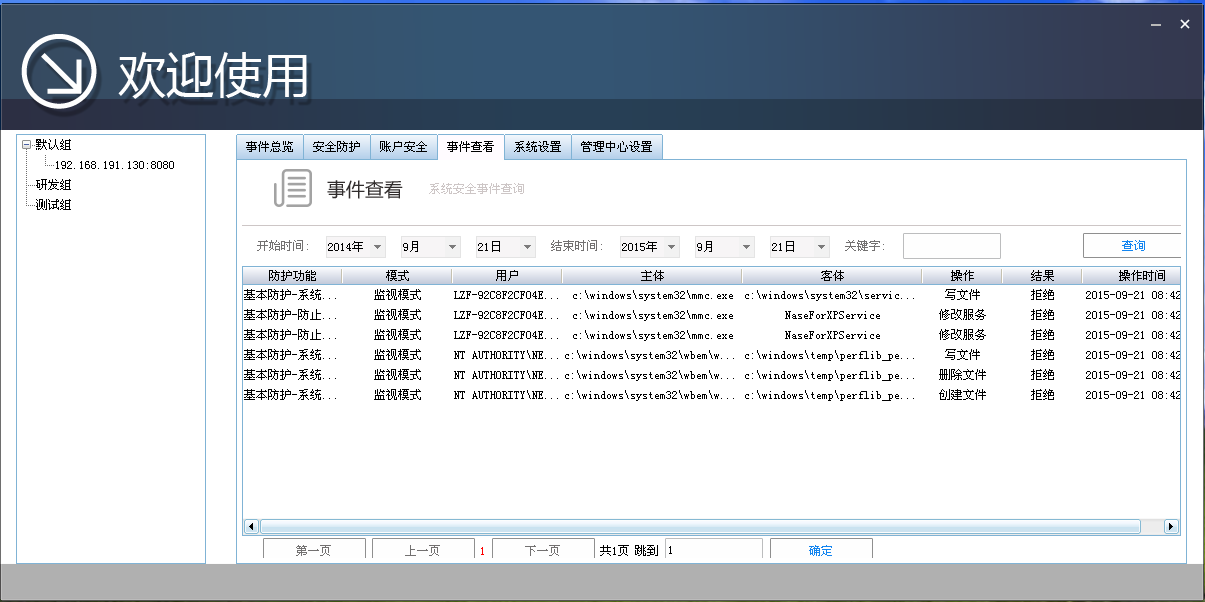
5.6、账户安全

与客户端一致，参照3.5。



5.7、事件查看

与客户端一致，参照3.6。



5.8、系统设置

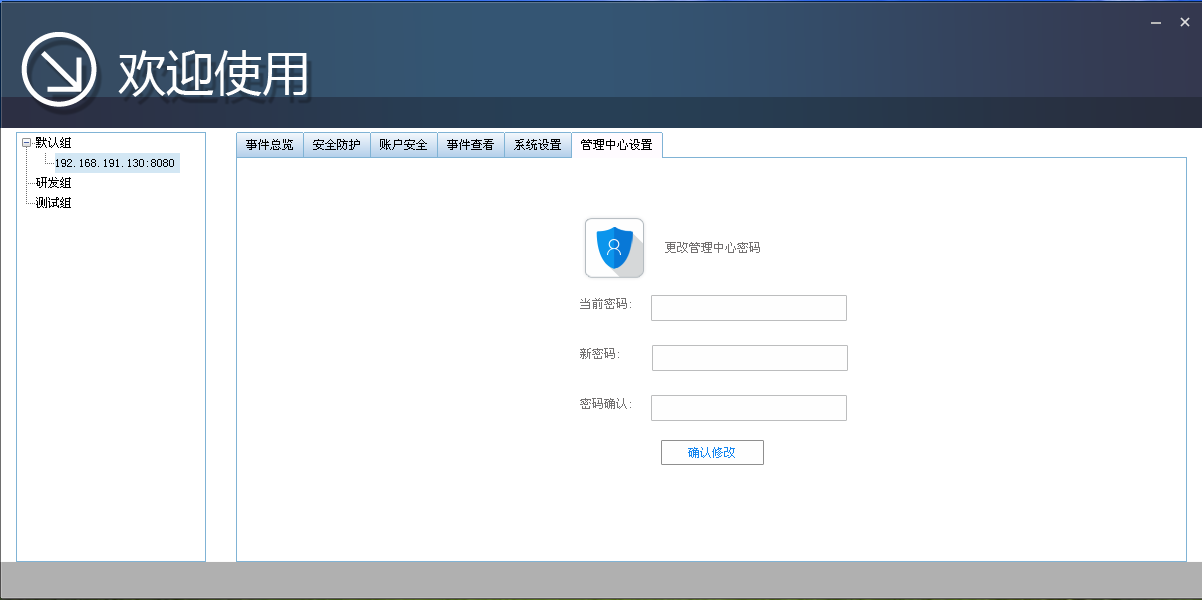
与客户端一致，参照3.8。这里没有客户端账户密码修改，以及策略导入导出等。





5.9、管理中心设置

修改管理中心，安全管理员账户的登录密码。



第六章、管理中心 - 审计管理员账户功能

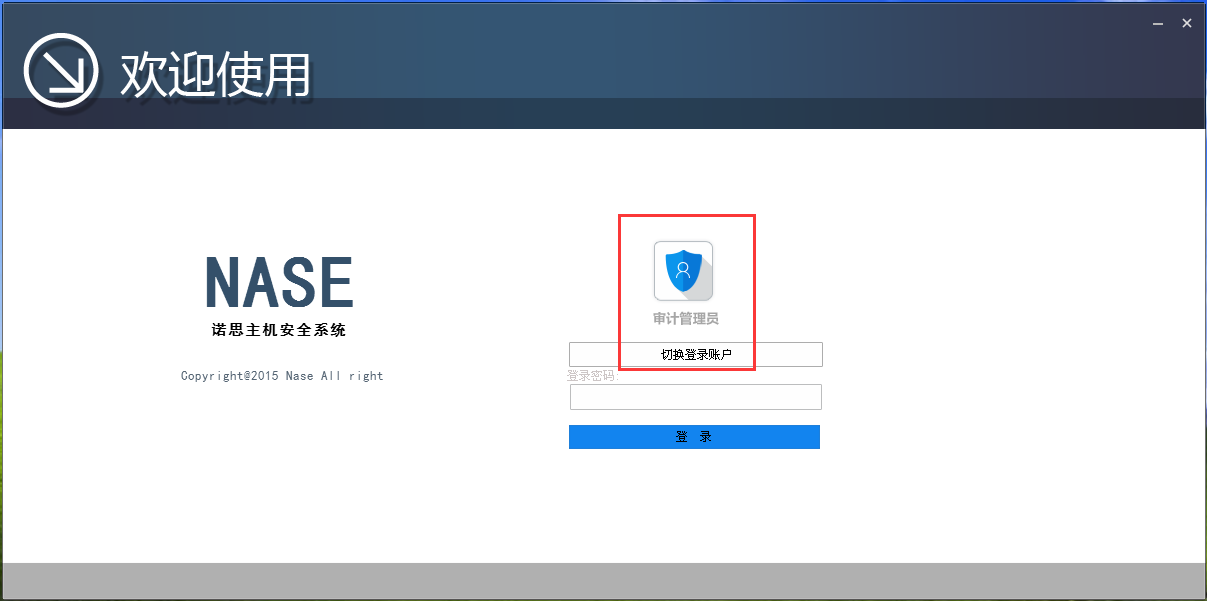
6.1、登录

a）插入管理中心USBKEY

b）切换登录账户为：审计管理员

c）输入默认密码:123456

d）点击登录，进入主界面



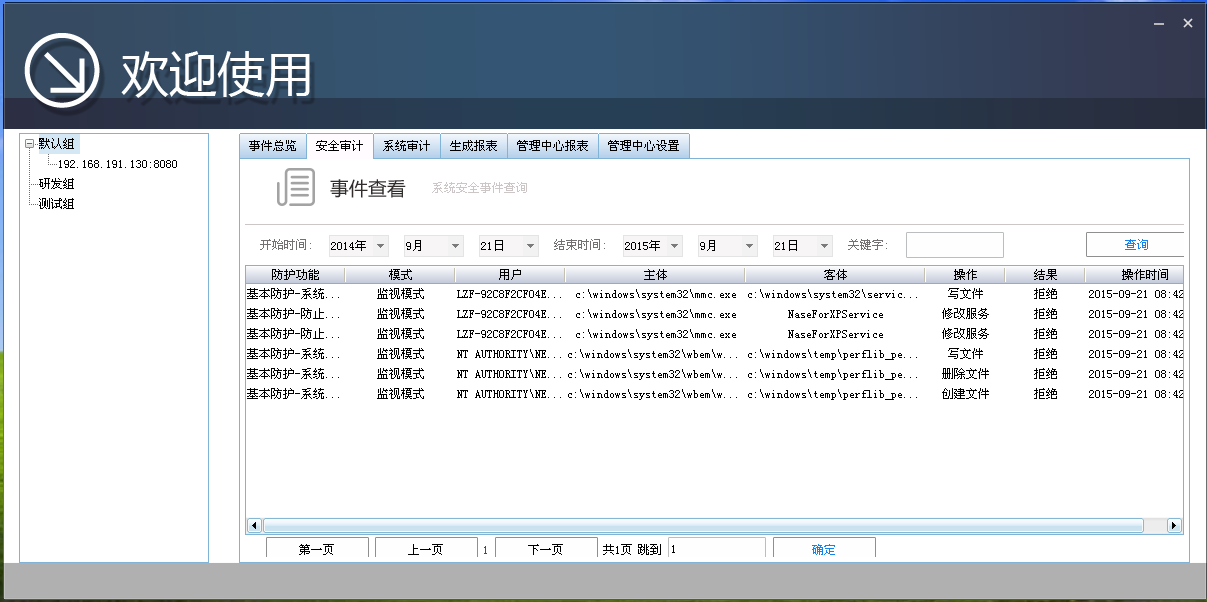
6.2、主界面

默认显示左侧IP列表中的第一个IP的首页。点击列表中的IP时候，则会切换到该IP的审计页面。



6.3、安全审计

与客户端一致，参照4.3。



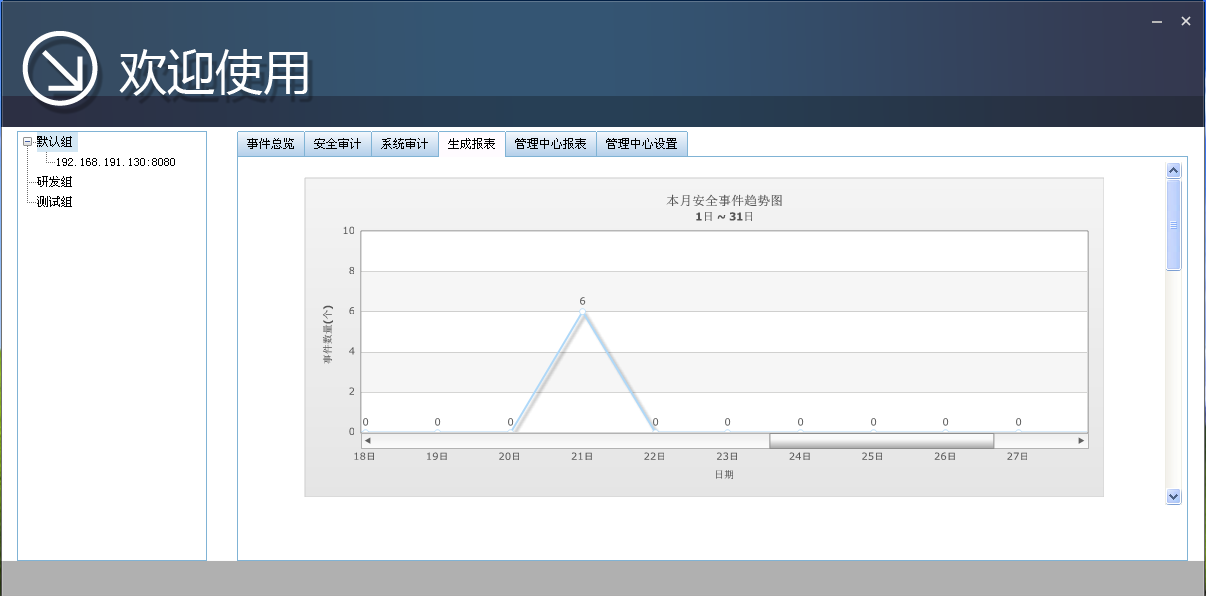
6.4、系统审计

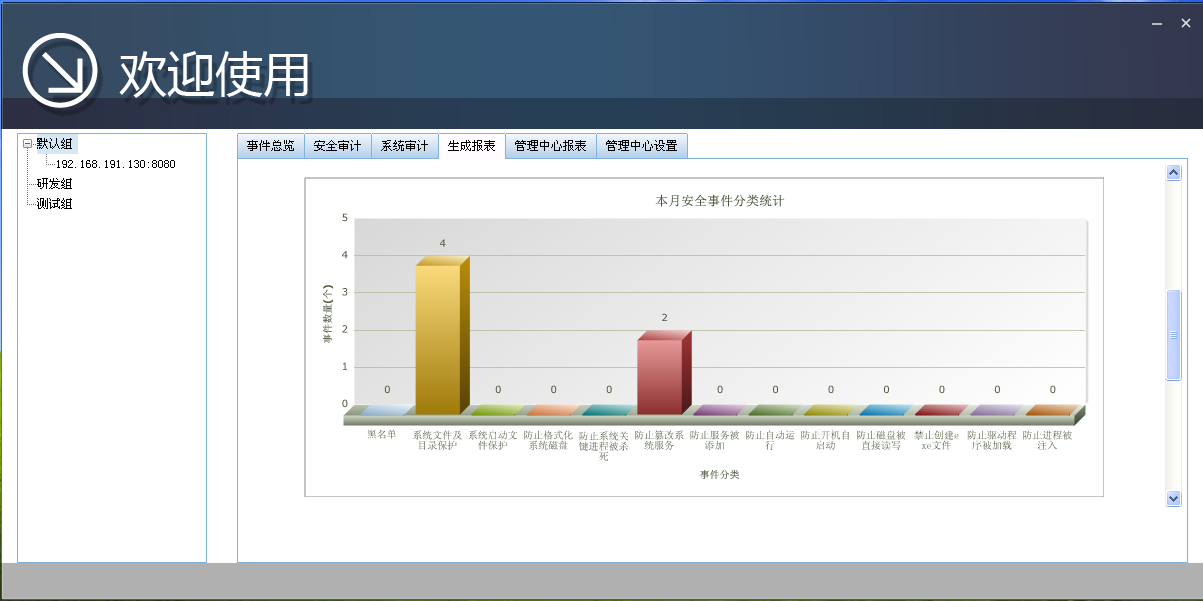
与客户端一致，参照4.4。



6.5、生成报表

与客户端一致，参照4.5。

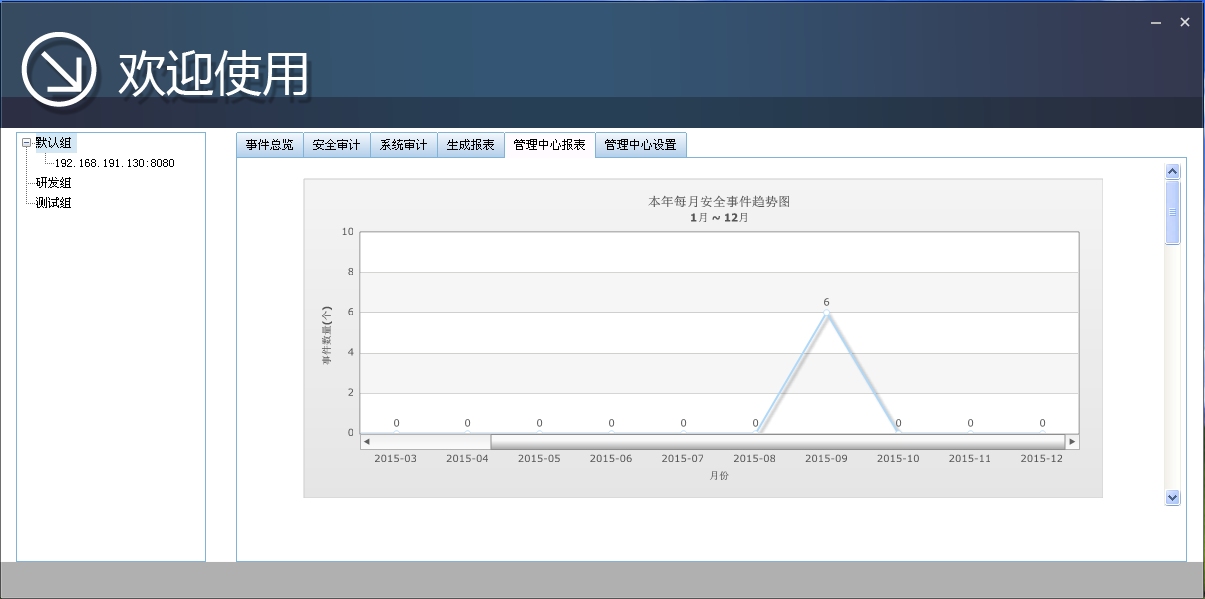






6.6、管理中心报表

管理中心报表，会对所有IP进行统计和生成报表。报表有四部分：本年每月安全事件趋势图，本月安全事件统计图，本月主机排名，本年主机排名。









6.7、管理中心设置

修改当前管理中心 - 审计账户的登录密码。



第七章、卸载客户端

为了加强软件的安全性，所以对卸载部分，增加了验证，并且提高了卸载难度。

7.1、停止保护

a)、登录客户端—安全管理员账户

b）、在“安全防护”--》“基本防护”里设置“当前模式”为“监听模式”。

c）、在“安全防护”--》“增强防护”里设置“当前模式”为“监听模式”。

7.2、添加一条白名单

“系统设置”-->“系统防护”-->“白名单”添加一条记录:

"C:\Windows\System32\taskkill.exe"



7.3、运行卸载脚本

进入C:\Program Files\NaseForXP\NaseClient目录，运行

Uninstall.bat

重启系统完成卸载。

第八章、卸载管理中心

8.1、运行卸载脚本

运行卸载脚本

Uninstall.bat