# NaseForXP技术手册

目录

[NaseForXP技术手册 1](#_Toc430880808)

[第一章、 软件简介 3](#_Toc430880809)

[1.1、介绍 3](#_Toc430880810)

[1.2、运行环境 3](#_Toc430880811)

[1.3、部署方式 3](#_Toc430880812)

[第二章、 软件功能 3](#_Toc430880813)

[2.1、客户端 - 安全管理员账户功能 3](#_Toc430880814)

[2.2、客户端 - 审计员账户功能 10](#_Toc430880815)

[2.3、管理中心 - 安全管理员账户功能 14](#_Toc430880816)

[2.4、管理中心 - 审计管理员账户功能 19](#_Toc430880817)

[第三章、 软件特色 24](#_Toc430880818)

[3.1、管理账户与审计账户分离 24](#_Toc430880819)

[3.2、软硬件双因子认证 24](#_Toc430880820)

[3.3、集中管理 24](#_Toc430880821)

[3.4、数据分析 24](#_Toc430880822)

[3.5、图形化报表 24](#_Toc430880823)

[3.6、保护项全面 24](#_Toc430880824)

[3.7、操作简单方便 24](#_Toc430880825)

1. 软件简介

1.1、介绍

NaseForXP是为企业级用户提供的，全方位的XP操作系统保护软件，能有效防止病毒威胁，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、运行环境

运行环境为XP操作系统。

1.3、部署方式

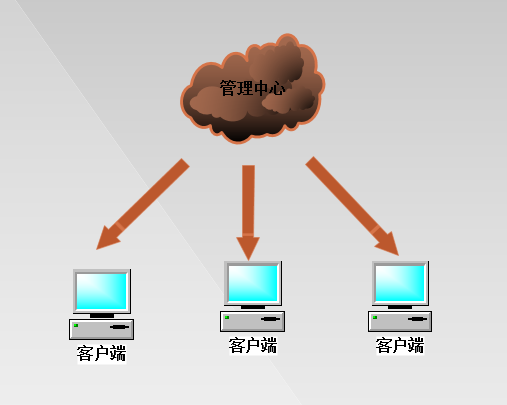
部署方式有两种：单机版，集中管理版本。

1.3.1、单机版部署

主要针对个人用户，可以只安装单机版客户端，用来保护单台主机。

1.3.2、企业版部署

主要针对企业用户，进行二级部署，可以在终端安装单机版，然后在管理端安装管理中心，对子节点进行集中管理。



1. 软件功能

2.1、客户端 - 安全管理员账户功能

2.1.1、登录安全验证

登录采用软硬件双因子认证体系，极大的增强了安全性。

a）、软件认证

管理员需要输入密码。

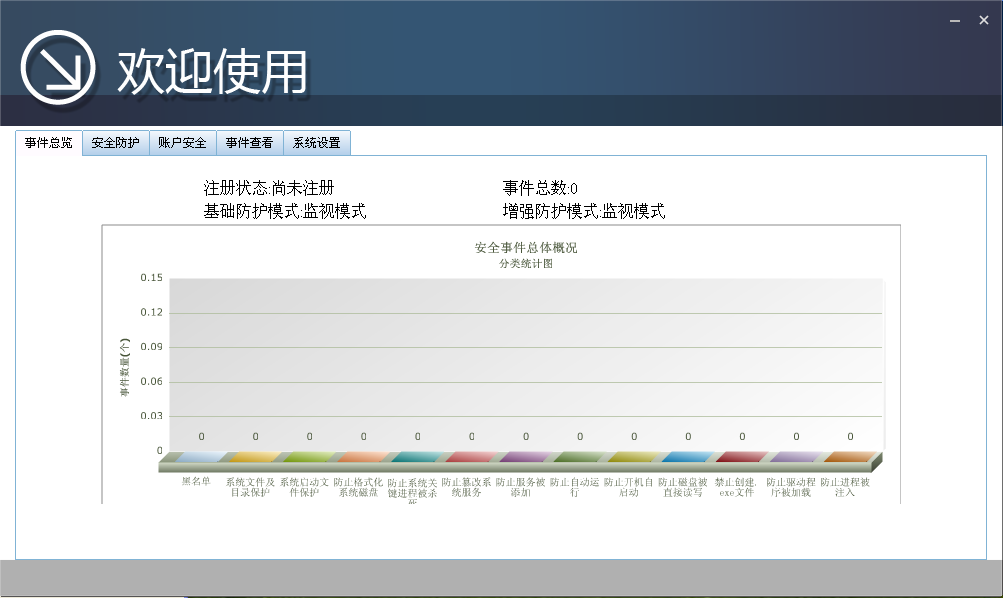
b）、硬件认证

管理员需要插入USBKEY，且该USBKEY是特定的，只能在当前机器上使用。

必须软硬件认证都通过，才可以正常登录软件。点击“登录”的同时，会将客户端注册到管理中心，这样管理中心就可以远程操作客户端了。

2.1.2、事件总揽

主界面展示了系统的基本状态和信息。采用图像化展示，美观，且直观。可以方便的看到系统的安全事件概况。



2.1.3、安全防护 - 基本防护

用来配置系统的安全项，采用开关方式来配置，不需要用户懂技术就可以很方便的进行配置，这里包括了对系统目录及文件保护、系统启动文件保护、防止格式化系统磁盘、防止系统关键进程被杀死、防止篡改系统服务等。

同时还支持“监视模式”和“防护模式”，方便您随时切换，以适应不同的环境。



2.1.3.1、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。

2.1.3.2、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。很多病毒都会修改系统目录下的文件，也会在system32目录释放病毒文件，而此项开启后，则可以拦截病毒对系统目录的操作。

2.1.3.3、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。有部分敲诈者病毒会对系统启动文件进行修改，阻止系统启动，从而敲诈用户，而开启此项，则可以避免此类病毒的危害。

2.1.3.4、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。

2.1.3.5、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。

2.1.3.6、防止篡改系统服务

开启后，会防止恶意程序修改系统服务。很多恶意程序或者病毒都会在运行时，先关闭安全软件的服务，从而达到对自身的保护，开启此项后，恶意程序将无法随意关闭或者启动服务。

2.1.4、安全防护 - 增强防护

来配置系统的高级安全项，采用开关方式来配置，不需要用户懂技术就可以很方便的进行配置，这里包括了：防止服务被添加、防止自动运行恶意程序、防止添加开机自启动项、防止磁盘被直接读写、禁止创建.exe文件、防止驱动被加载、防止进程被注入等。



2.1.4.1、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。

2.1.4.2、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。

2.1.4.3、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。很多病毒，例如rose病毒等，会来盘符根目录下创建autorun文件，从而达到用户双击打开磁盘时，就会预先运行autorun指定的病毒，而这个开关开启之后，则会禁用所有的autorun，让此类病毒无法运行。

2.1.4.4、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。恶意程序或者病毒，将自身添加到开机自启动项里面，随机启动，是一种很常见的手法，而此项开启后，则恶意程序或者病毒无法将自身添加到开机自启动项里，无法随开机启动。

2.1.4.5、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。

2.1.4.6、禁止创建.exe文件

开启后，会拦截恶意程序生成.exe的文件。很多类病毒都是会先释放出一个exe可执行文件，然后使用该exe可执行文件，进行病毒操作，而开启此项后，会拦截病毒释放exe可执行文件，致使病毒的主要运行体无法正常释放，从而达到对此类病毒的防御。

2.1.4.7、防止驱动被加载

开启后，会拦截恶意程序加载驱动。部分高级别的恶意程序或者病毒会挂载驱动，去监控一些敏感信息，进行敏感信息窃取，而开启此项，对导致恶意程序或者病毒无法加载驱动，从来达到保护系统的目的。

2.1.4.8、防止进程被注入

开启后，会拦截恶意程序注入其他进程。很多病毒都会注入explorer或者svchost进程，进行一些恶意操作，而开启此项，则可以拦截跨进程的注入行为，有效杜绝病毒注入危害。

2.1.5、账户安全

用来配置系统账户的密码安全性策略，因为很多管理员的系统密码设置比较简单，很容易被破解，所以密码的安全性也值得关注，这里就是为用户提供密码的复杂性策略配置。



2.1.5.1、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。

2.1.5.2、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。

2.1.5.3、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。

2.1.5.4、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。

2.1.5.5、最短使用期限

开启后，设定密码最短使用期限为当前值。

2.1.5.6、最长使用期限

开启后，设定密码最长使用期限为当前值。

2.1.5.7、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。

2.1.6、事件查看

用来查看发生的安全事件，很详细的记录了每个安全事件的信息，包括：用户名称，哪个进程对哪个对象进行了何种操作，被软件的哪个模块所拦截，当前的保护模式是什么，最终的操作结果是放行还是拦截，以及操作发生的精确时间。同时事件查看还支持按时间段的模糊查询，可以通过选择时间段，输入关键字，筛选符合条件的事件。



2.1.7、系统设置 – 系统防护

2.1.7.1、设置白名单

在白名单列表里的程序，不会被软件拦截操作。



2.1.7.2、设置黑名单

在黑名单里的程序，会拦截其所有操作。



2.1.8、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。

2.2、客户端 - 审计员账户功能

2.2.1、登录安全验证

登录采用软硬件双因子认证体系，极大的增强了安全性。

a）、软件认证

管理员需要输入密码。

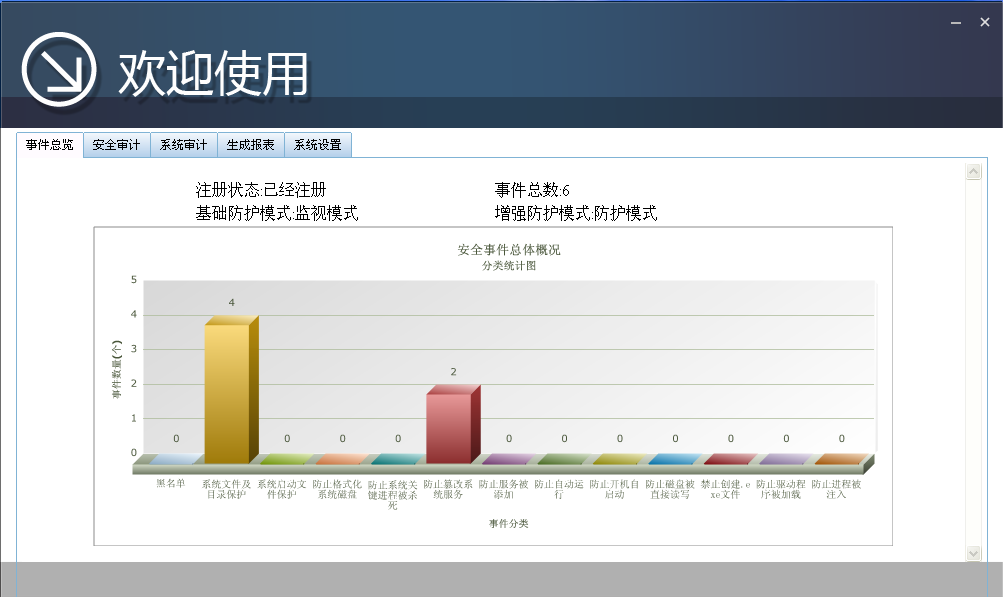
b）、硬件认证

管理员需要插入USBKEY，且该USBKEY是特定的，只能在当前机器上使用。

必须软硬件认证都通过，才可以正常登录软件。

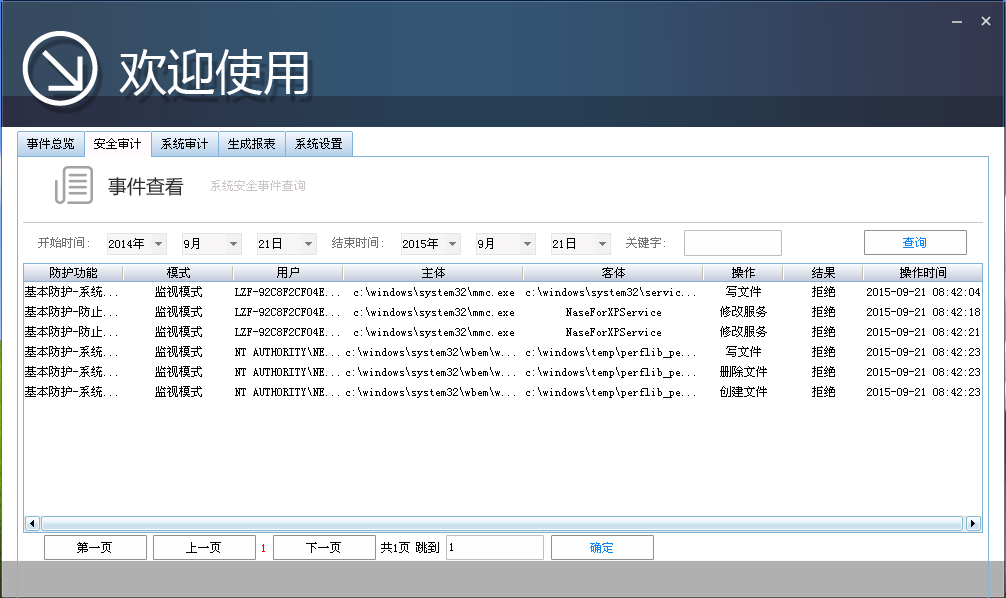
2.2.2、事件总揽

主界面展示了系统的基本状态和信息。采用图像化展示，美观，且直观。可以方便的看到系统的安全事件概况。



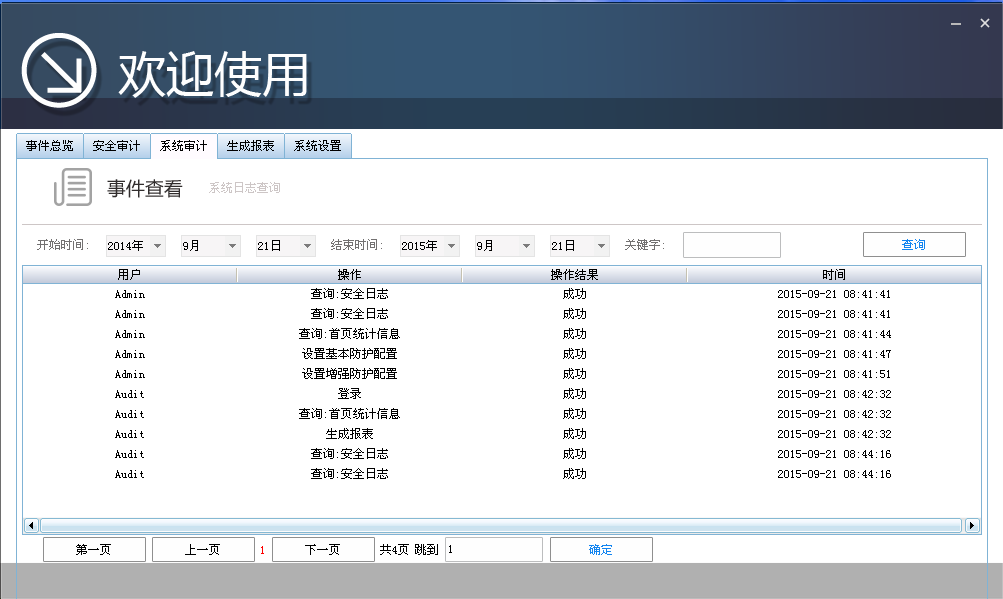
2.2.3、安全审计

与3.6章节的“事件查看”一致，用来查看发生的安全事件，很详细的记录了每个安全事件的信息，包括：用户名称，哪个进程对哪个对象进行了何种操作，被软件的哪个模块所拦截，当前的保护模式是什么，最终的操作结果是放行还是拦截，以及操作发生的精确时间。同时事件查看还支持按时间段的模糊查询，可以通过选择时间段，输入关键字，筛选符合条件的事件。



2.2.4、系统审计

记录和查询软件的操作和运行记录。例如哪个用户登录了管理界面，并且进行了哪些操作。同时事件查看还支持按时间段的模糊查询，可以通过选择时间段，输入关键字，筛选符合条件的事件



2.2.5、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。以图形化方式展示系统当前的安全状况。







4.6、系统设置

设置当前审计管理员的登录密码。



2.3、管理中心 - 安全管理员账户功能

2.3.1、登录安全验证

登录采用软硬件双因子认证体系，极大的增强了安全性。

a）、软件认证

管理员需要输入密码。

b）、硬件认证

管理员需要插入USBKEY，且该USBKEY是特定的，只能在当前机器上使用。

必须软硬件认证都通过，才可以正常登录软件。

2.3.2、事件概览

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。

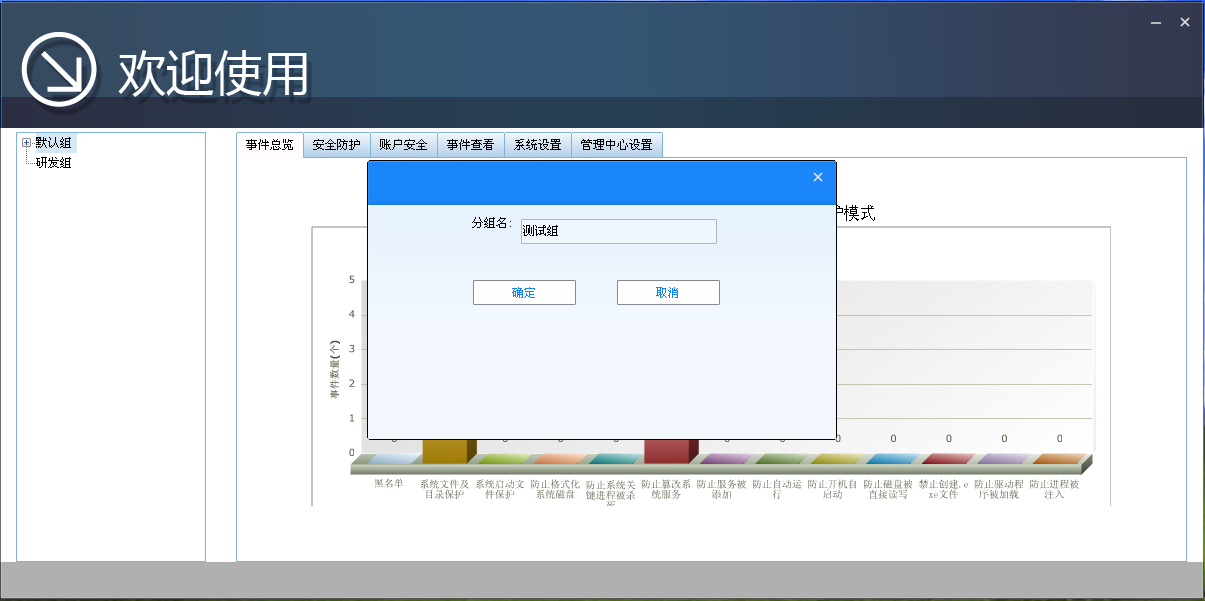


2.3.3、IP分组管理

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”。



2.3.3.1、添加分组

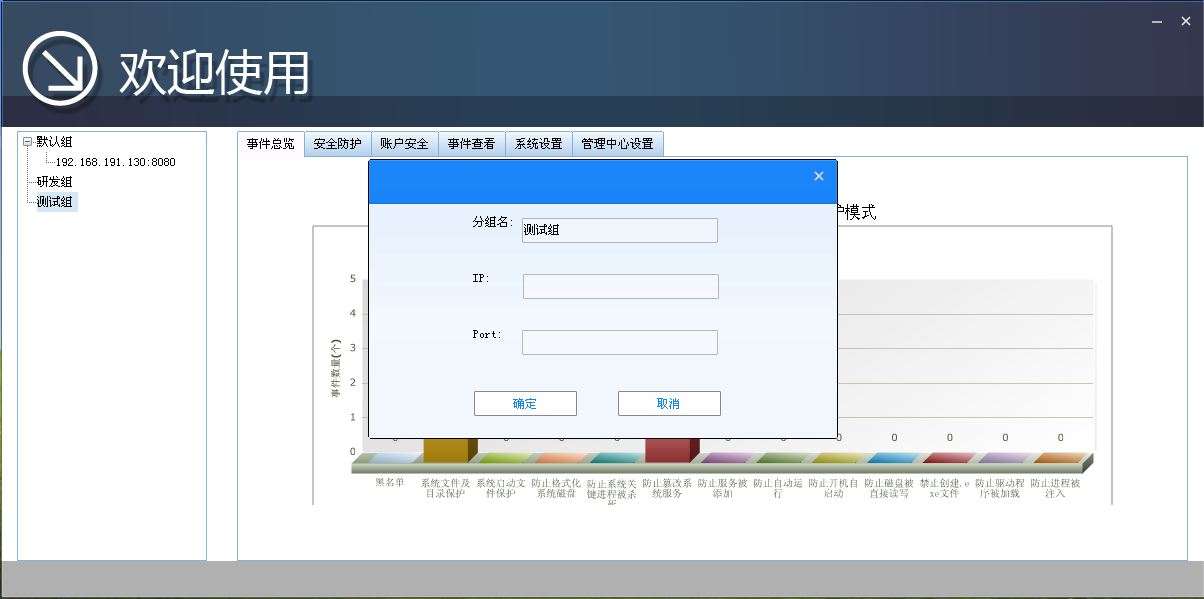


2.3.3.2、删除分组

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”。



2.3.3.3、添加分组IP



2.3.3.4、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。



2.3.3.5、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2.1.3，2.1.4。





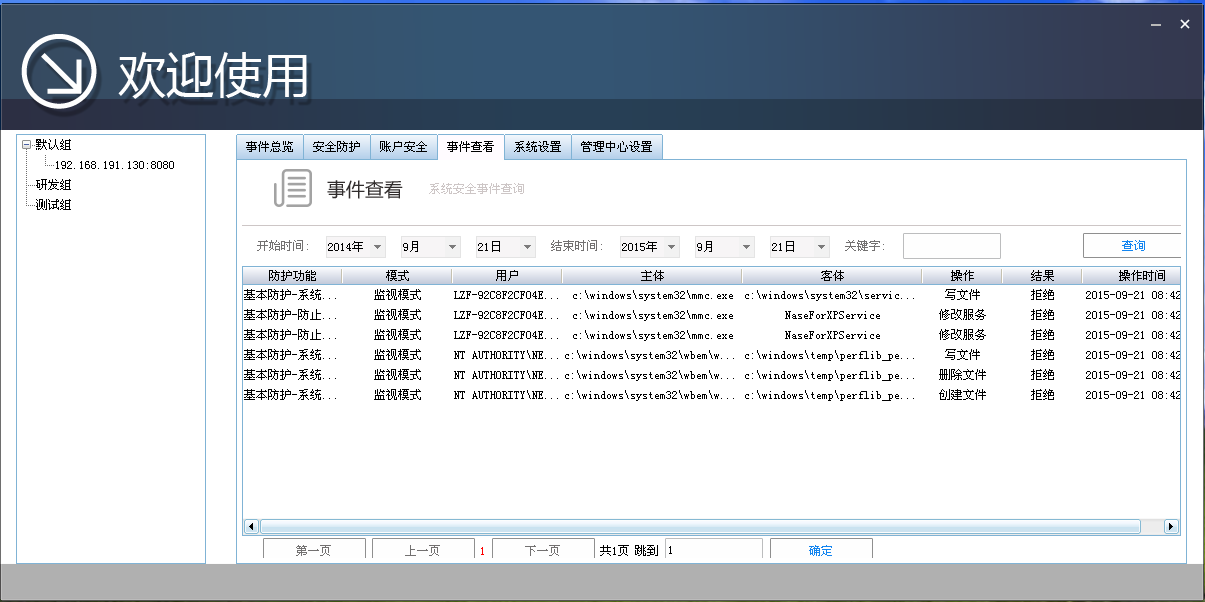
5.6、账户安全

与客户端一致，参照2.1.5。



5.7、事件查看

与客户端一致，参照2.1.6。



5.8、系统设置

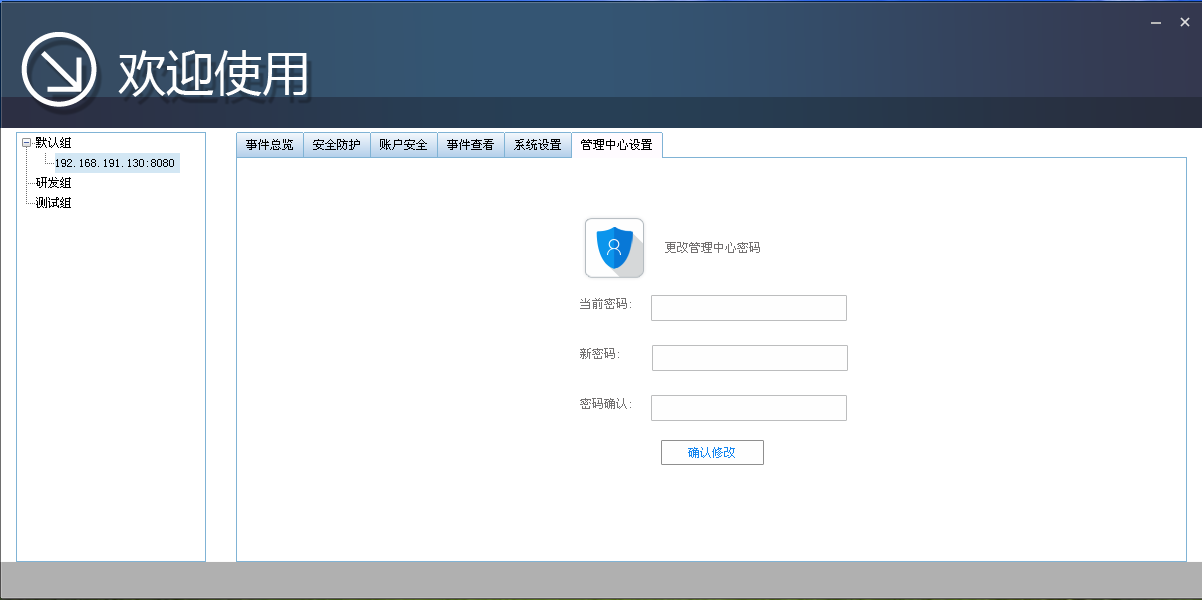
与客户端一致，参照2.1.8。这里没有客户端账户密码修改，以及策略导入导出等。





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。



2.4、管理中心 - 审计管理员账户功能

2.4.1、登录安全验证

登录采用软硬件双因子认证体系，极大的增强了安全性。

a）、软件认证

管理员需要输入密码。

b）、硬件认证

管理员需要插入USBKEY，且该USBKEY是特定的，只能在当前机器上使用。

必须软硬件认证都通过，才可以正常登录软件。

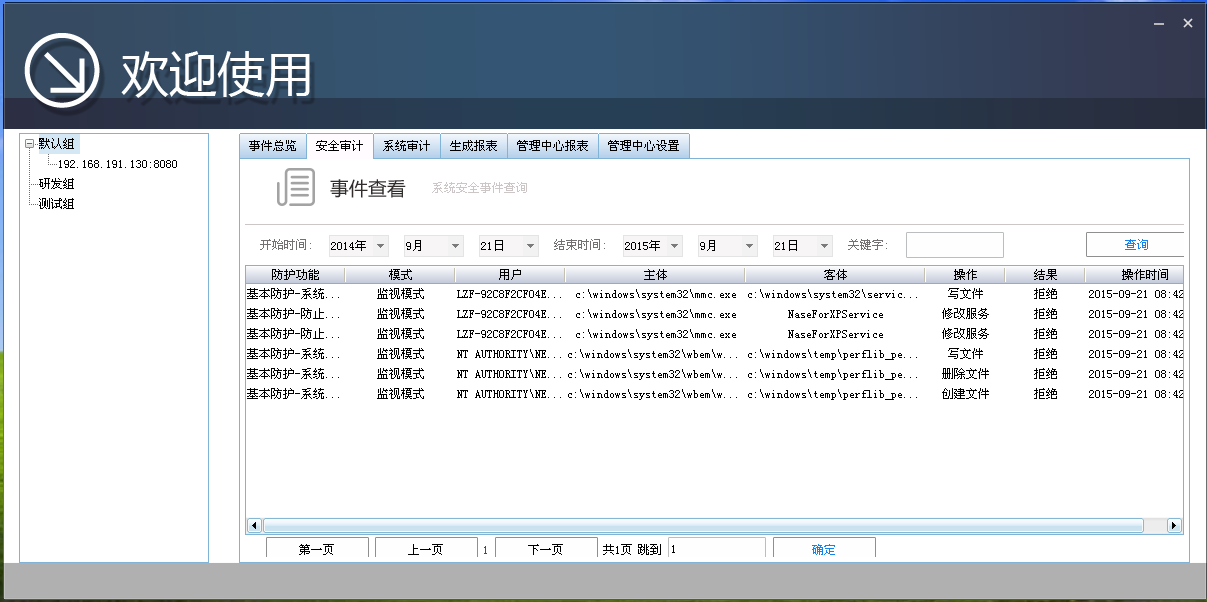
2.4.2、事件概览

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。



2.4.3、安全审计

与客户端一致，参照2.2.3。



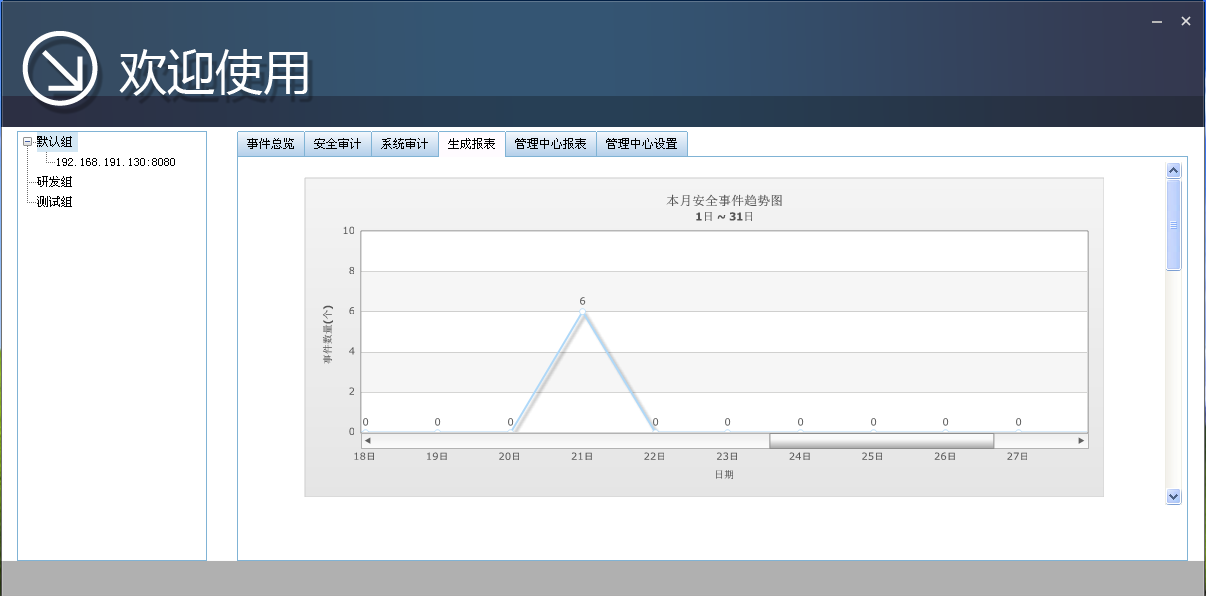
2.4.4、系统审计

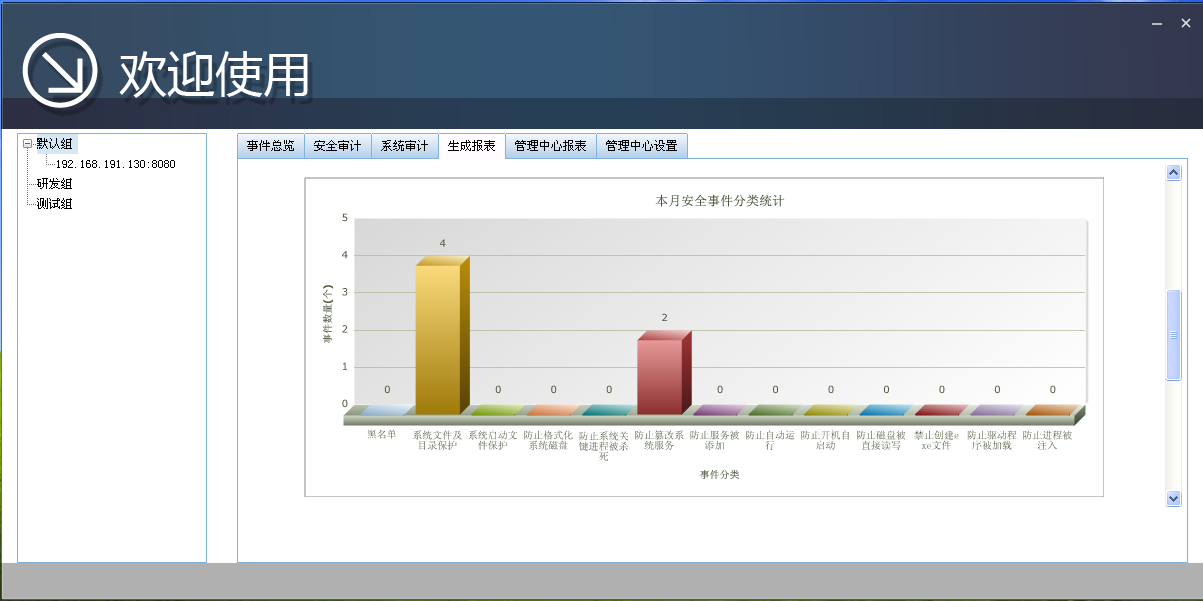
与客户端一致，参照2.2.4。



2.4.5、生成报表

与客户端一致，参照2.2.5。

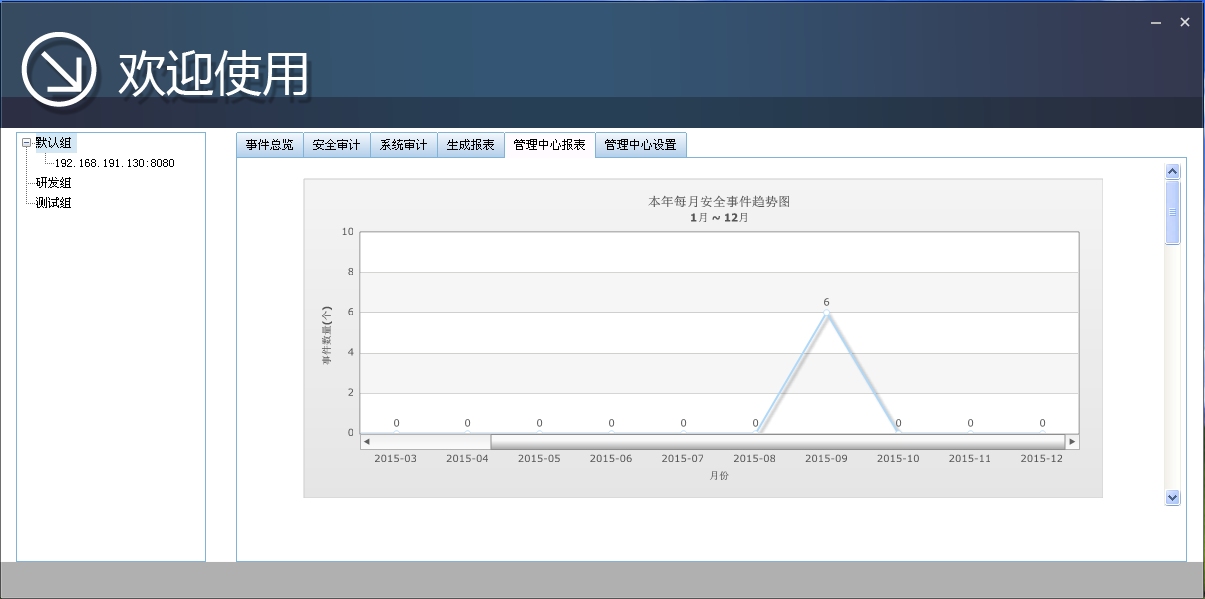






2.4.6、管理中心报表

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。









2.4.7、管理中心设置

修改当前管理中心 - 审计账户的登录密码。



1. 软件特色

3.1、管理账户与审计账户分离

符合等级保护的设计，让管理账户和审计账户分离。

3.2、软硬件双因子认证

采用双因子登录认证，极大程度上增强了安全性，防止了非法人员操作软件。其中软认证采用密码方式验证，硬认证，采用USBKEY绑定主机的方式，一个USBKEY只能用于同一个客户端或者管理中心，从而达到高级别的安全性。

3.3、集中管理

集中管理是针对企业用户的特定版本，支持两级分布式部署，管理中心可以对其下属的各个客户端进行统一管理，统一审计。

3.4、数据分析

在报表部分，会有一些数据分析结果展示，例如发生安全事件最多的IP有哪些？哪些安全事件发送的频率比较高等。

3.5、图形化报表

采用曲线图，直方图等美观的展示方式来展现报表，除了精美，同时也更加直观。

3.6、保护项全面

保护项划分细致、全面，覆盖了XP系统安全的各个方面，极大限度的保护了系统的安全，有效抵御病毒感染。

3.7、操作简单方便

配置非常方便，几乎都是以开关方式进行设置，不需要培训成本，就可以学会如何使用。