# XP安全防护功能列表

1、需求

1.1、管理中心：

1.1.1、安全管理员登陆

|  |  |  |  |
| --- | --- | --- | --- |
| 功能 |  |  |  |
| 客户端列表 |  |  | 列出所有登陆的客户端机器IP  点击后，进入每个单独客户端。默认显示第一个客户端信息。 |
| 客户端分组 |  | 组增加属性，鼠标悬停时候，会显示属性 | 曾管理中心可以把登陆的IP分成不同的组，要有添加删除组，添加IP到组的功能 |
| 策略下发 |  |  | 导出规则，下发到选定的IP |
| 事件总览 | 已保护主机多少天 |  |  |
| 拦截疑似攻击次数 |  |  |
| 处理账户变动次数 |  |  |
| 当前基本防护状态 |  | 防护|监控 |
| 当前增强防护状态 |  | 防护|监控 |
| 当前账户监视状态 |  | 开启|关闭 |
| 当前账户安全级别 |  | 高中低|自定义 |
| 状态图 |  | 简易的事件图形展示 |
| 安全防护 | 模式设置 |  | 防护|监控 |
| 系统目录及文件保护 |  | 开启|关闭 |
| 系统启动文件保护 |  | 开启|关闭 |
| 防止格式化 |  | 开启|关闭 |
| 防止关键进程被杀死 |  | 开启|关闭 |
| 防止篡改系统服务 |  | 开启|关闭 |
| 规则导出 |  |  |
| 增强防护 | 模式设置 |  | 防护|监控 |
| 防止服务被添加 |  | 开启|关闭 |
| 防止自动运行恶意程序 |  | 开启|关闭 |
| 防止添加开机自启动项 |  | 开启|关闭 |
| 防止磁盘被直接读写 |  | 开启|关闭 |
| 禁止创建.exe文件 |  | 开启|关闭 |
| 防止驱动被加载 |  | 开启|关闭 |
| 防止进程被注入 |  | 开启|关闭 |
| 规则导出 |  |  |
| 账户安全 | 状态 |  | 监控开启|关闭 |
| 账户策略设置 |  | 自定义|高中低 |
| 锁定时长 |  | 错误登陆间隔 |
| 锁定次数 |  | 错误登陆次数 |
| 最短使用期限 |  | 密码使用指定时长后可修改 |
| 最长使用期限 |  | 使用多久后必须修改 |
| 强制密码历史 |  | 旧密码不重复个数 |
| 事件查看 | 安全事件 |  |  |
| 账户事件 |  |  |
| 系统设置 | 账号设置 |  | 登陆密码修改 |
|  | 黑名单 |  | 添加|删除 |
|  | 白名单 |  | 添加|删除 |

1.1.2、审计管理员

|  |  |  |  |
| --- | --- | --- | --- |
| 系统设置 |  |  | 登陆密码 |
| 首页展示统计 |  |  | 单个IP |
| 操作日志 |  |  |  |
| 违规日志 |  |  | 安全事件|违规事件 |
| 生成报表 |  |  | 单独标签页，里面可选IP组或者多个IP生成报表 |

1.2、客户端（只有管理员账号）

1、管理中心界面没有客户端列表、客户端分组、策略下发。

2、客户端安装时候，要指定管理中心的IP，启动时候，连接到管理中心。

3、授权，提取客户机的硬件信息，生成一个码，然后我们单独有程序计算序列号，生成一个序列号，提供给安装机器。

2、软件设计

2.1、共用约定

2.1.1、编码

统一UTF8，给对方的数据必须是UTF8编码的。Http对外返回的数据为 UTF8编码后转成JSON。

* 1. 详细功能

2.2.1、卸载密码

与安全管理员登录密码一致。卸载时候，需要验证，错误情况下，不允许卸载。

2.2.2、授权

授权针对客户端，提取客户端机器码，用授权软件生成一个注册码，然后注册。

客户端未授权，也可以正常登录。但是登录后，首页会有未注册提示。点击可以进行注册。管理中心，打开单个的客户端，一样可以注册。

* 1. 接口

【注意】所有的URL的传入参数，和结果都是经过json编码的。

2.3.1、获取管理中心IP和端口

URL：center/getaddr

参数：无

返回值：

{

"CenterIP" : "192.168.1.100",

"CenterPort" : 8080

}

2.3.2、客户端登录

URL：login

参数：data = {

"User":"Admin",

"Password":"123456",

"CenterIP":"192.168.1.1",

"CenterPort":"8080"

}

返回值：

{

"Status":1,

"Errmsg":"登录成功",

"User":"admin",

"Usertype":2

}

用户名和默认密码：

|  |  |  |  |
| --- | --- | --- | --- |
| 用户名 | 密码 | 类型(int) | 备注 |
| CenterAdmin | lzf:24324962@qq.com | 1 | 管理中心用户 |
| Admin | 123456 | 2 | 操作管理员 |
| Audit | 123456 | 3 | 审计管理员 |

2.3.3、系统设置-修改密码

URL：/sys/changepassword

参数：data = {

"User":"Admin",

"OldPwd":"123456",

"NewPwd":"654321"

}

返回值：

{

"Status":1,

"Errmsg":"密码修改成功"

}

2.3.4、系统设置 - 白名单

**1、白名单添加**

URL：sys/addwhite

参数：data={

"File":"C://test"

}

返回值：

{

"Status":1,

"Errmsg":"添加白名单成功"

}

**2、白名单删除**

URL：sys/delwhite

参数：data={

"File":"C://test"

}

返回值：

{

"Status":1,

"Errmsg":"删除白名单成功"

}

**3、获取白名单数量**

URL：sys/totlewhite

参数：无

返回值：

{

"Status":1,

"Errmsg":"查询白名单总数成功",

"TotCnt":10

}

**4、查询白名单内容**

URL：sys/querywhite

参数：data={

"Start":0,

"Length":10

}

返回值：

{

"Status":1,

"Errmsg":"查询白名单成功",

"Files":["C:\\test","C:\\test\\dd"]

}

2.3.5、系统设置 – 黑名单

**1、黑名单添加**

URL：sys/addblack

参数：data={

"File":"C://test"

}

返回值：

{

"Status":1,

"Errmsg":"添加黑名单成功"

}

**2、黑名单删除**

URL：sys/delblack

参数：data={

"File":"C://test"

}

返回值：

{

"Status":1,

"Errmsg":"删除黑名单成功"

}

**3、获取黑名单数量**

URL：sys/totleblack

参数：无

返回值：

{

"Status":1,

"Errmsg":"查询黑名单总数成功",

"TotCnt":10

}

**4、查询黑名单内容**

URL：sys/queryblack

参数：data={

"Start":0,

"Length":10

}

返回值：

{

"Status":1,

"Errmsg":"查询黑名单成功",

"Files":["C:\\test","C:\\test\\dd"]

}