边界卫士

用户手册

V8.3

目录

产品功能列表

功能模块	功能概要	
系统管理	用户管理（支持本地用户增删改查、导入、导出、AD 域用户导入及认证）	
	组管理（支持用户组增删改查）	
	策略管理（用户或用户组两种方式下发策略）	
	用户绑定（支持用户名与机器绑定）	
	策略更新（自动更新、手动更新）	
	客户端更新（自动更新、手动更新）	
边界控制模块	网络应用控制	QQ、微信、钉钉等社交工具外发文件加密，接收有权限的密文自动解密
		IE、火狐、谷歌、360 等任意浏览器上传外发文件加密
		outlook、foxmail 等邮件系统外发文件加密及邮件地址白名单功能（outlook 可定制只能给指定邮件地址发送邮件）
	网络共享控制	拷贝到共享目录自动加密或禁止设置共享目录
		拷贝到网络磁盘文件自动加密
	硬件接口控制	拷贝到 U 盘、移动硬盘文件自动加密
	外设控制	文档打印自动添加背景水印（记录打印用户、时间、IP）
	审批控制	经审批后的外发文件不加密
	安全防护	磁盘加密（防止通过 PE 方式启动系统）
	DLP 扩展控制	敏感内容识别外发加密（office 系列）
	追溯备份	外发文件远端备份（用于后期追溯）
	防拍照	参考屏幕水印模块
流转水印功能（需要采购水印插件）	针对 office 文档，可以添加流转水印，以实现通过指定工具追溯文档都流经过哪些机器，以及最后是通过哪个机器流转到互联网的	
屏幕水印模块	浏览 office、wps 文档时自动添加文档水印（防止通过拍照泄密）	
	屏幕强制添加防拍照水印（添加屏幕隐形水印，出现通过手机、相机等对屏幕进行拍照的风险时，通过本功能可具体到某个终端。）	
	启动某些应用软件时，自动添加应用水印	
打印控制模块	不登录账号，无法打印控制，有效记录打印人员	
	打印文档时页眉、页脚、页中添加水印	
	打印流水号记录	
	打印日志可以导出 excel 报表	
文档加密模块	可以主动加密文件，并可以设置用户或用户组只读、打印、水印、再授权、解密、时间范围等权限控制	
	可以制作瘦客户加密文件	
	可以制作绑定某硬件设备的加密文件	
	可以制作离线加密文件、硬件 KEY 绑定加密文件	
	可以设置自动加密、解密文件夹	
文档二次编辑加密模块	任意文件编辑后，自动无感知加密	
	使用时自动无感知解密	
	支持申请审批解密文档	
网络控制模块	允许或禁止某些应用程序访问网络	

功能模块	功能概要
业务系统安全模块（含准入控制模块）	禁止非法计算机访问受保护的服务器，保障服务器的安全
	终端将加密文档上传到服务器自动解密，服务器文档下载到本地自动强制加密，防止服务器数据下载泄密
	支持企业常见的信息管理系统 OA、ERP、PLM、SVN、文件服务器等等，支持 B/S 和 C/S 两种架构模式
	计算机安装了客户端程序，通过指定的安全进程才可以访问服务器 对于特殊的计算机，比如公司领导的电脑或临时访客，可以通过设置 IP/MAC 地址白名单，允许其访问服务器
	加密的文件的权限可以设置为只读、修改、打印、打印水印、屏幕水印、脱密、再授权、时间等；
	可以控制业务系统（包括：U8、财务软件、ERP 以及所有 IE 浏览器）内加密文件自动解密。实现业务系统输出文档是密文，在业务系统内流转是明文。
运维安全模块	指定运维 IP 地址，通过任意工具从该 IP 地址下载的数据强制加密
	具备录屏功能
	下载的加密文件可以绑定硬件进行认证
审批模块	终端审批功能
	移动端审批功能
	支持有审批任务，自动提示功能。
	支持审批解密文件
	支持审批外发文件
U 盘管理模块	控制写入 U 盘的文件自动按权限加密（同时禁用文件另存到受控 U 盘）
	设置只读 U 盘
	设置仅能使用登记 U 盘
	对 U 盘进行注册管理，注册 U 盘可接入内网，未注册 U 盘将无法在客户端上使用，实现“外盘外用”
	对 U 盘进行加密管理，加密 U 盘只能在企业内部使用，脱离企业后，必须格式化删除里面所有数据后，才能再使用
私有云备份功能（需要购买私有云平台）	可自定义备份磁盘或文件夹
	终端文件有更新时，自动启动备份
客户端功能	手动解密
	手动加密
	截屏工具
	切换用户
	修改密码
	绑定硬件
	自动升级
客户端自身安全	卸载 DLP 客户端需要管理员密码
	禁止操作系统切换安全模式
	防止暴力破解、删除、卸载 DLP 客户端
日志模块	用户登录日志
	U 盘操作日志
	打印日志

功能模块	功能概要
	业务系统加密日志
	共享文件日志
	审批日志
	外发日志
统计模块	统计外发文件总数
	输出应用排名
	输出人员排名
	输出文件类型排名
部署方式	客户端安装（手动安装、如果客户有域环境可以使用域推送方式）
其它	操作系统支持 windows 全系

一、 服务器使用

1 服务器安装

1.1 安装服务器

环境说明

服务器环境

项目	配置	备注
系统版本	Windows Server 2012 R2	
CPU	8 核	
内存	8GB	
硬盘	系统盘 100G，数据盘 100G 以上	
网络要求	固定 IP 地址	
服务端口	TCP 8443（控制台登录管理） TCP 9999（终端与控制台通讯）	

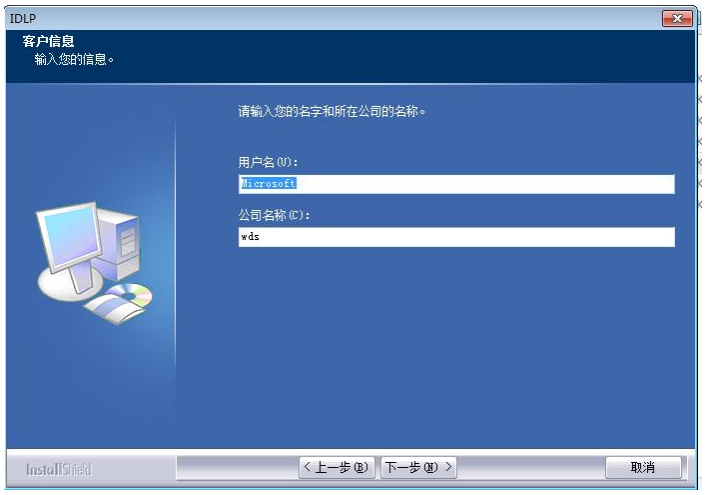
客户端环境

项目	配置	备注
操作系统	Windows XP/7/10	
处理器	双核以上	
内存	4GB 以上	
硬盘	60GB 以上	
网络要求	能访问服务器的 TCP 9999 端口	

温馨提示：安装数据防泄密系统之前建议先关闭杀毒软件、防火墙；

选择要安装的目录，默认即可（如自定义目录，目录必须使用英文目录）

下一步下一步即可



完成后服务器自动启动，无需再进行操作。

安装完成后，桌面上出现两个快捷方式，用于停止和启动服务的（重启服务也可以通过重启计算机来完成），如下图：

1.2 卸载服务器

点击计算机“开始-所有程序-数据防泄密系统-卸载”，按照提示卸载即可，如下图：

1.3 登录服务器

- 在浏览器中输入分配给数据防泄密系统对应的 IP 地址+端口号+/DLP，（注意 DLP 三个字母必须大写）即可在浏览中访问数据防泄密系统首页。例如：https://192.168.1.200:8443/DLP
- 打开登录页面并通过用户名和密码登录数据防泄密系统
- 输入用户名和密码：初始用户名：admin，密码：admin，登录后可自行

修改密码

1.4 服务器授权

- 登录服务器，点击左侧菜单中 “授权管理”-“授权信息”；
- 将页面中硬件信息中的 4 位数字反馈给厂商，厂商会根据这 4 位数字提供授权码；
- 在授权信息页面中授权码一栏输入授权码，完成服务器授权，无需重启服务。

1.5 服务器数据库备份方案

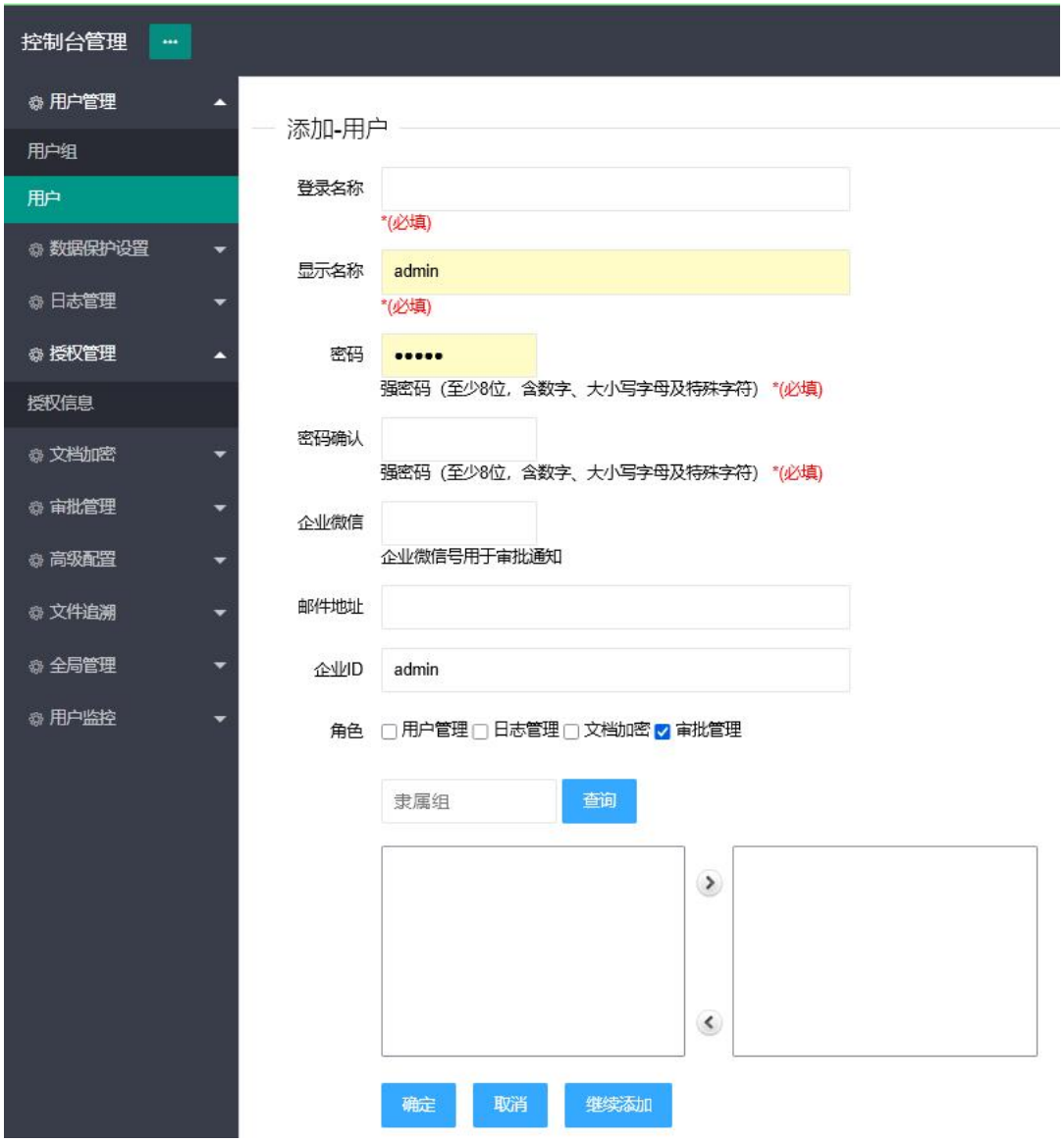
利用操作系统定时任务，执行安装目录 mysql 目录下面 autobackup.bat 文

件，在当前目录生成备份文件

2 用户管理

2.1 用户管理

点击“添加”按钮可以添加用户

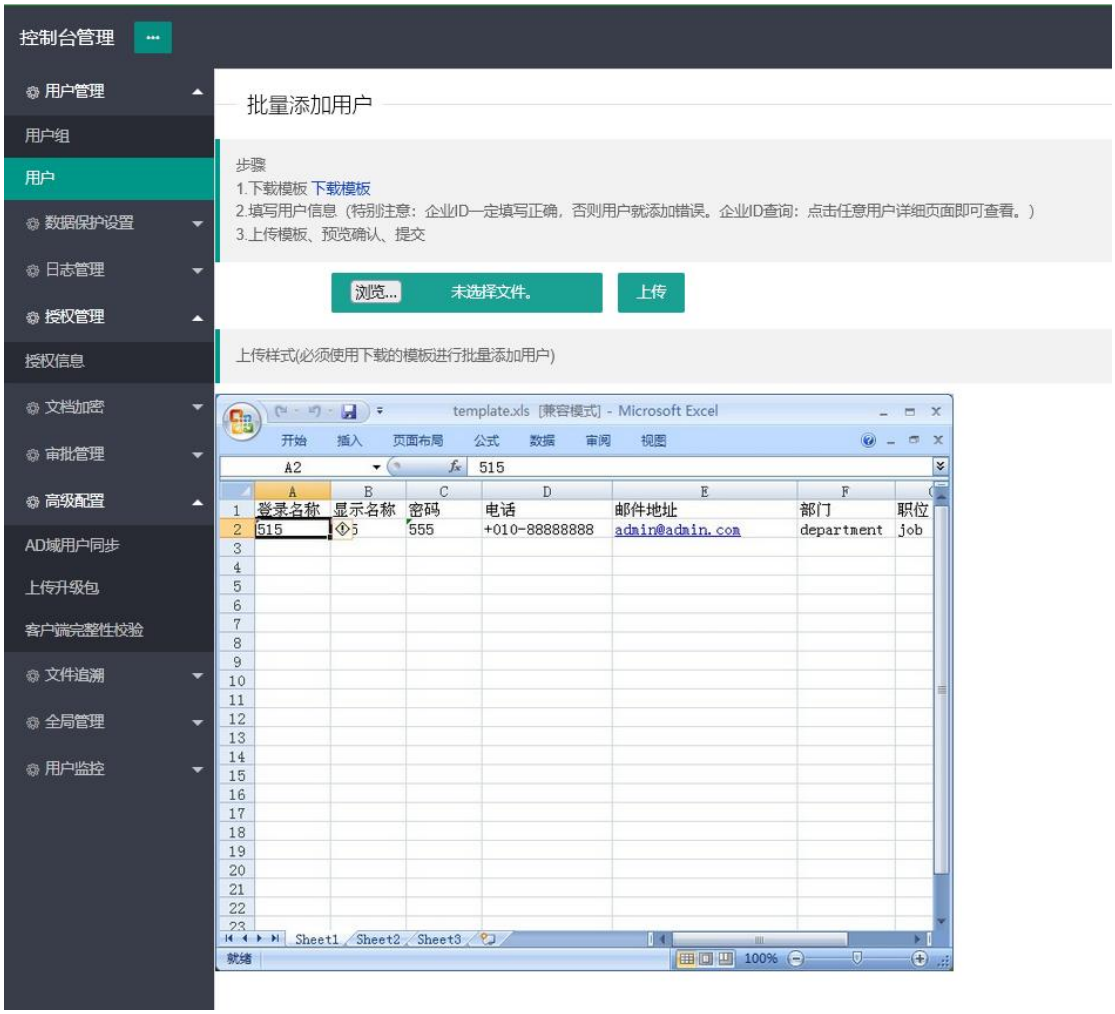


2.2 用户组管理

2.3 批量添加用户

- 下载模板，选择“用户”菜单，点击“批量上传”按钮，在弹出的页面中点击“下载模板”链接，下载批量上传用户模板文档。

- 上传模板数据，按照模板文档格式进行填写后，再回到下载页面，点击“浏览”按钮，将编辑好的用户模板文档上传，即可完成用户导入。



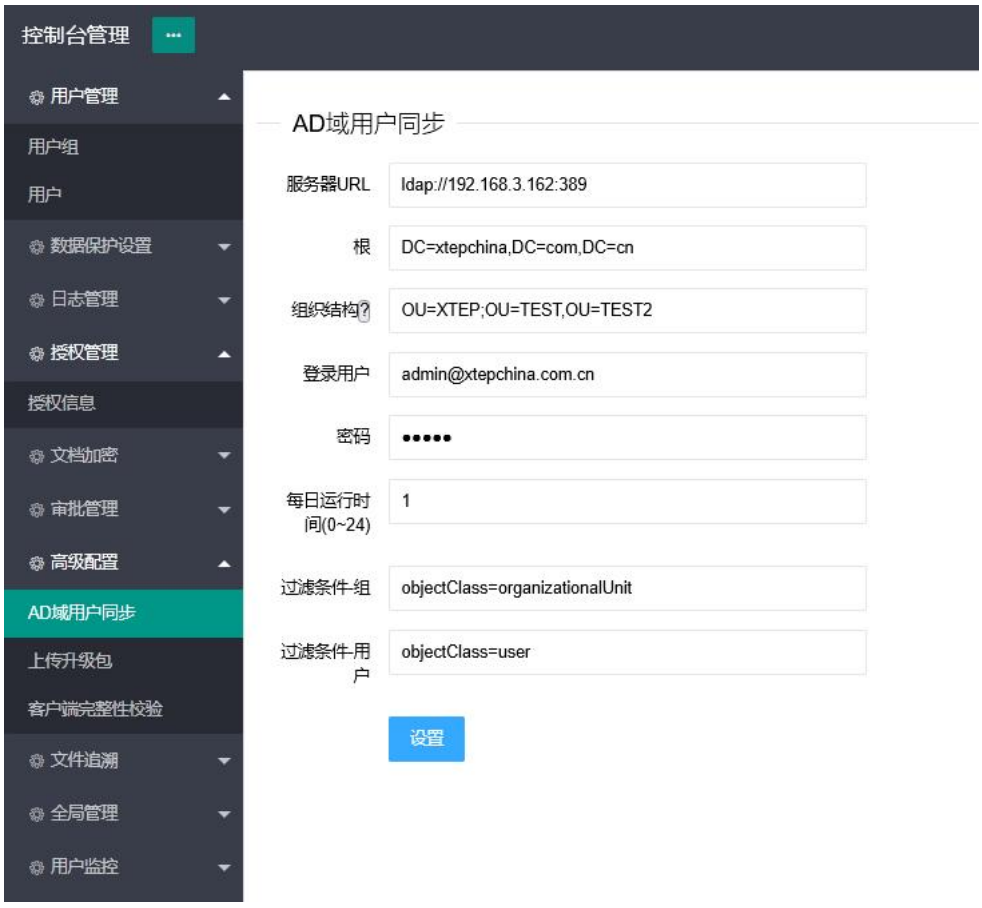
如遇到导入错误，请确认导入的用户，系统是否已经存在，存在的用户无法导入。

2.4 AD 域用户同步

- 点击“AD 域用户同步”菜单，按照如下图所示设置即可

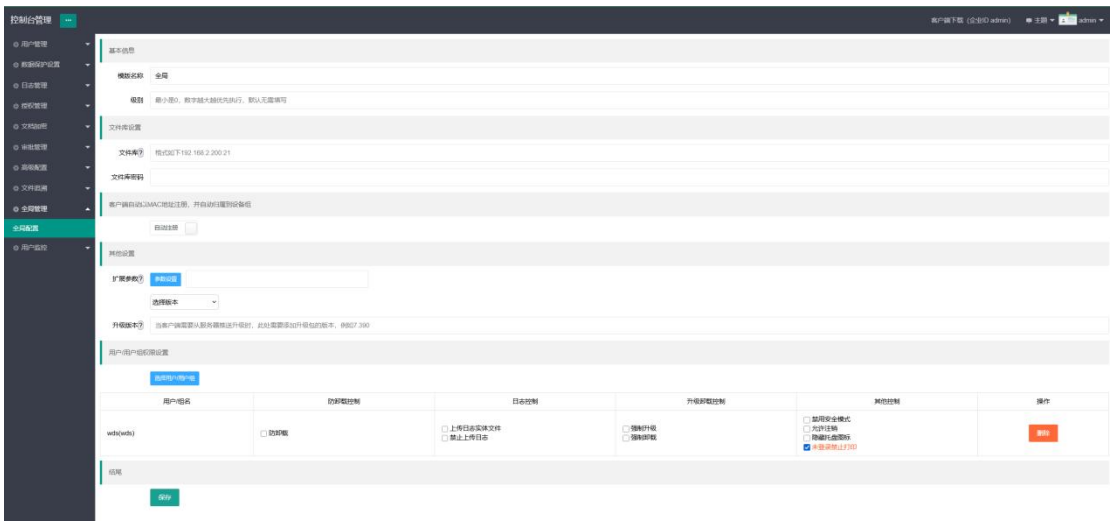
- 注意：登录用户名必须带后缀

- 每日运行时间是指每日到该时段，系统会自动同步一次 AD 域用户
- 过滤条件无需修改
- 多个 OU，使用;间隔，例如 OU=XTEP;OU=TEST;OU=TEST2



3 数据保护设置

3.1 全局配置



1）防破解防卸载：有该权限的用户客户端是有防暴力破解防卸载的，并且卸载时需要链接服务器并输入管理员密码。

2）上传日志实体文件：有文件外发操作时，记录日志的同时同步上传备份小于 50M 的实体文档。

3）禁止上传日志：禁止终端记录日志。

4）强制升级：静默升级指定版本的客户端。

5）强制卸载：卸载指定用户的客户端。

6）禁用安全模式：禁止使用系统安全模式。

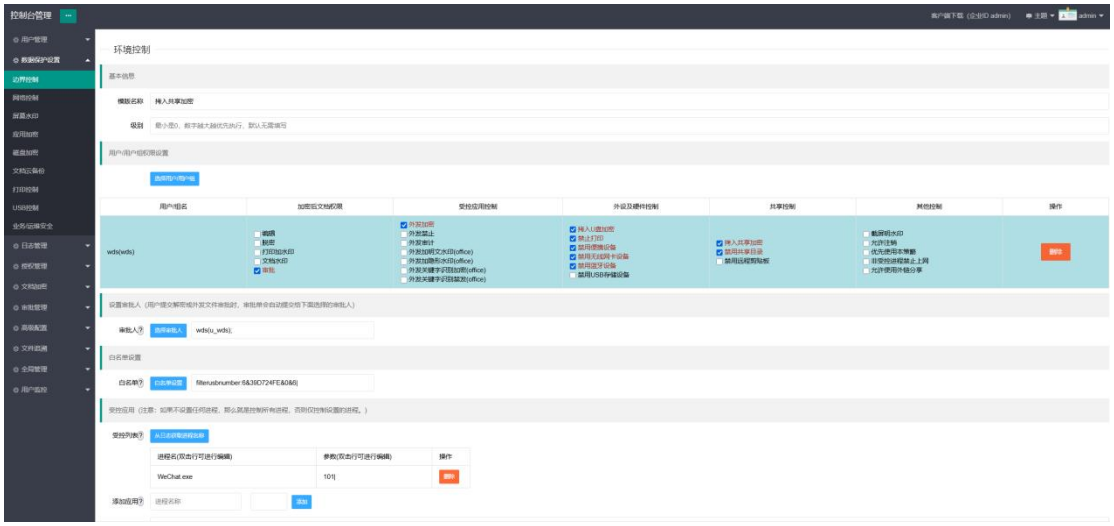
7）允许注销：客户端允许注销客户端登录账号，注销后没有任何权限控制。

8）隐藏托盘图标：隐藏托盘图标  ，可以通过 CTRL+ALT+M 唤醒。

9）未登录禁止打印：安装客户端后，不登录账号，禁止打印文档。

3.2 边界控制

基本信息：



权限信息：

3.2.1 加密后文档权限

如果产生加密文档（比如拷入 u 盘加密），那么加密文档可以通过这里设置相应权限

1）编辑：有该权限的文档可以进行编辑。

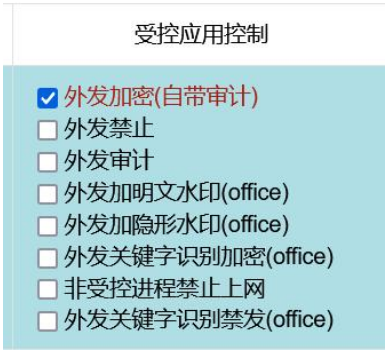
2）脱密：有该权限的文档可以脱密成明文。

3）打印加水印：有该权限的文档打印时会在文档上面强制添加水印，水印内容包括打印时间、IP 地址及打印者账号 ID。

4）文档水印：有该权限的文档打开时会在文档上方浮动一个水印，水印内容包括打开时间、IP 地址及打开者账号 ID。

5）审批：有该权限的用户可以审批外发、脱密等申请。

3.2.2 网络控制



1) 外发加密：终端计算机通过受控应用程序外发文档的时候会把文档强制加密并赋予相应权限。

2) 外发禁止：禁止终端计算机通过受控应用程序外发明文文档离开终端。

3) 外发审计：记录终端计算机通过受控应用程序外发的文档全路径。

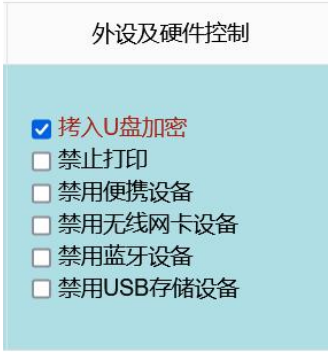
4) 外发加明文水印(office)：针对 office 文件，通过受控应用外发文件时，强制添加明文水印。

5) 外发加隐形水印(office)：针对 office 文件，通过受控应用外发文件时，强制添加隐形水印（隐形水印通过专用工具可以提取外发人、时间、终端 ip 地址）。

6) 外发关键字识别加密(office)：通过受控应用外发 word、excel、ppt 文档时，会自动检测 word、excel、ppt 文档中是否含有非法关键字，如果含有，外发的文件会强制加密。

7) 非受控进程禁止上网：非受控的进程禁止上网

3.2.3 外设及硬件控制



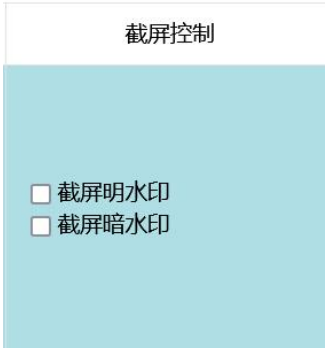
1）拷入 U 盘加密：拷贝到 U 盘的文档强制加密并赋予相应权限。

2）禁止打印：禁止终端电脑打印文档。

3）禁用无线网卡设备：禁止终端计算机使用无线网卡。

4）禁用蓝牙设备：禁止终端计算机开启蓝牙。

3.2.4 截屏控制



1）截屏明水印 ：终端计算机通过受控应用程序截图时会强制添加明水印，包括截图时间 IP 截图者账号 ID。[定制功能]

2）截屏暗水印：终端计算机通过受控应用程序截图时会强制添加用户无感知的隐形水印，包括截图时间 IP 截图者账号 ID。[定制功能]

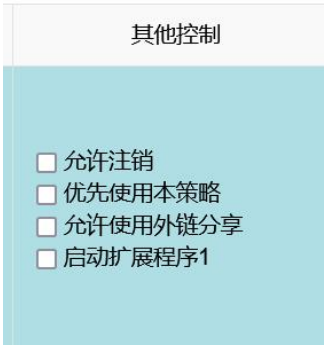
3.2.5 共享控制

1）拷入共享加密：拷贝到任意共享目录的文档强制加密并赋予相应权限（包括本地计算机共享以及远端计算机共享）。

2）禁用共享目录：禁止本地计算机设置共享。

3）禁用远程剪贴板：禁止终端计算机通过远程协助方式拷贝文件离开受控终端。

3.2.6 其他控制



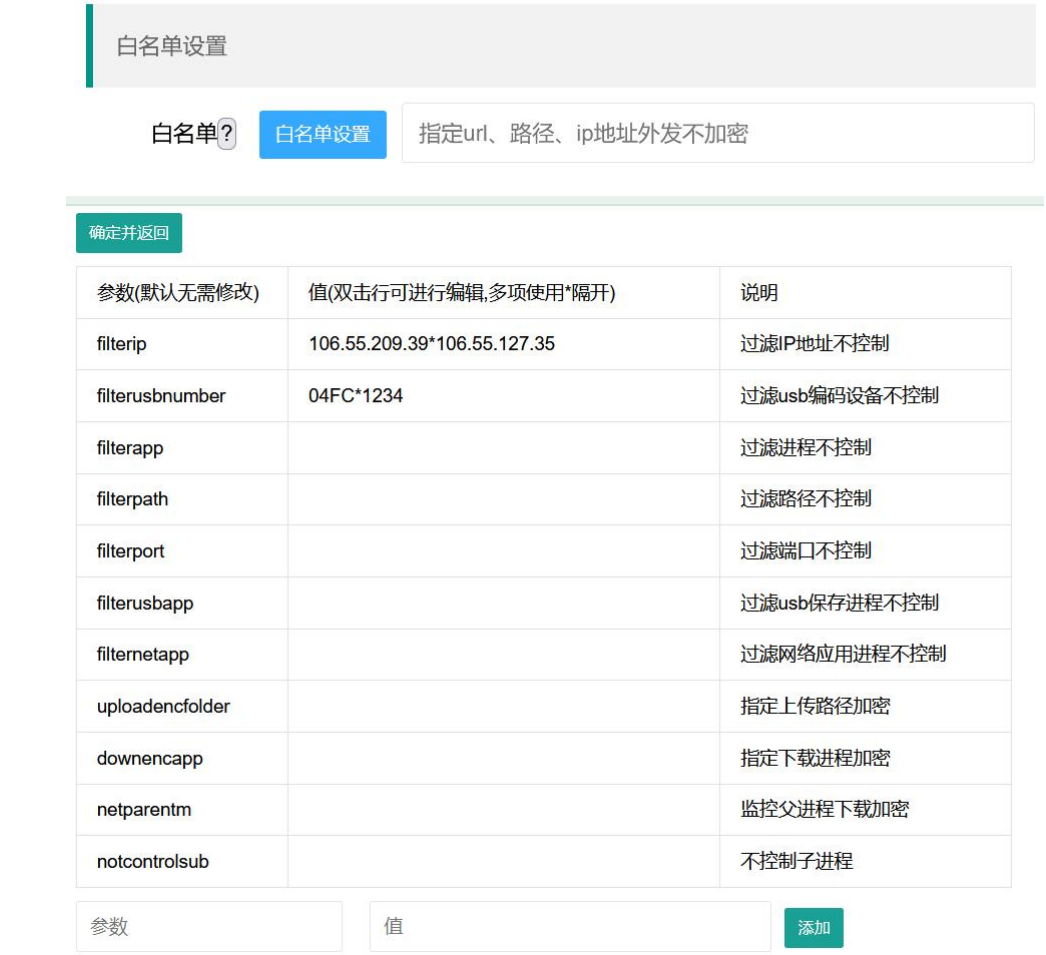
1）允许注销：允许注销客户端登录账号。

2）优先使用本策略：当对一个用户多次下策略后，默认情况都是进行策略累加合并，但是如果指定了优先使用本策略，那么只会执行本策略。

3）允许使用外链分享：允许使用外链分享功能。

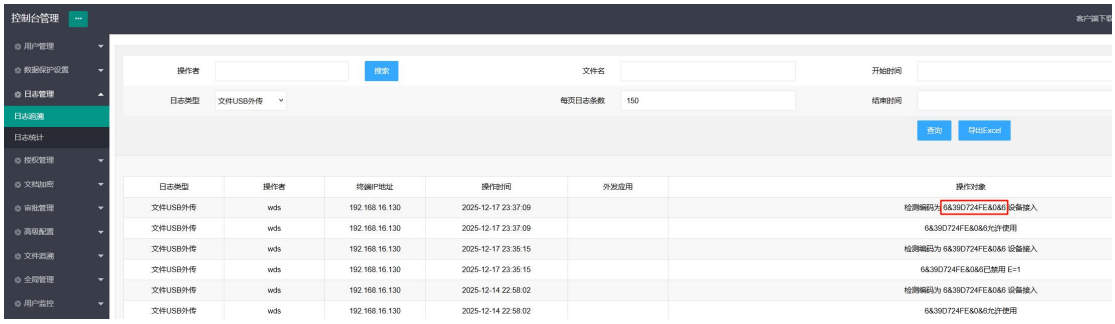
3.2.7 白名单设置

主要是进行一些白名单设置



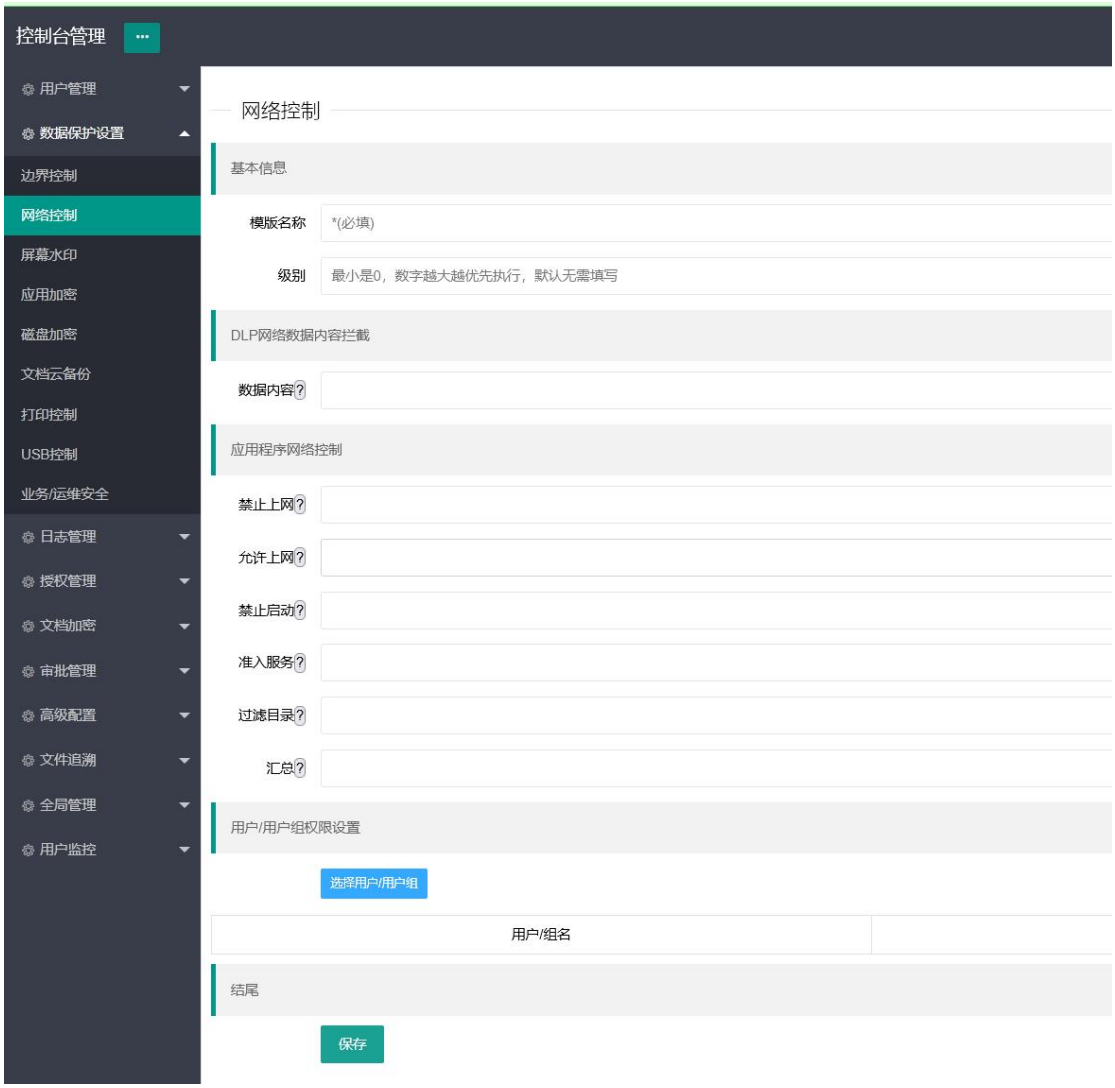
注：usb 设备的编码获取方法如下：

打开日志追溯页面，选择文件 usb 外传的日志类型，然后进行查询，参考如下图：



如上图 6&39D724FE&0&6 就是 u 盘的编码，多个编码使用*间隔

3.3 网络控制



DLP 网络数据内容拦截

录入待拦截的数据，多个数据使用;分开间隔

应用程序网络控制

1）禁止上网：指定进程禁止上网，其他进程允许上网，多个进程使用分号;间隔。

2）允许上网：指定进程允许上网（如果允许上网的进程是系统进程，比如 ie 等，需要设置过滤目录），其他进程禁止上网，多个进程使用分号;间隔 。与环境控制策略结合使用时，外发加密进程默认允许上网。

3) 禁止启动：指定进程禁止运行，多个进程使用分号;间隔。

4) 过滤目录：参数 netfilterpath?windows;system32|*

5) 准入服务：格式说明

netdenyport?9999;9998|*netallowport?9991|*netcleartime?5|*

nedenyport 阻断端口，多个端口用;间隔

netcleartime 定时清除已连接客户端，单位 5 秒

netallowport 客户端心跳包端口

6) linux 服务器准入控制：

✓ wdsgate.ini 放入 bin 目录

✓ 安装 wdsgate.ko，命令如下

insmod wdsgate.ko

✓ 卸载命令如下

rmmod wdsgate

wdsgate.ini 配置文件说明

DenyPort1 = 9999

DenyPort2 = 0

DenyPort3 = 0

DenyPort4 = 0

DenyPort5 = 0

AllowClientPort = 9991

DelAllowClientPort = 9992

AllowClientIp1 = 0

AllowClientIp2 = 0

AllowClientIp3 = 0

AllowClientIp4 = 0

AllowClientIp5 = 0

log = 1

✓ DenyPort1-5 可以设置 5 个准入端口；

✓ AllowClientPort 心跳端口，默认 9991 无需修改

✓ DelAllowClientPort 心跳端口，默认 9992 无需修改

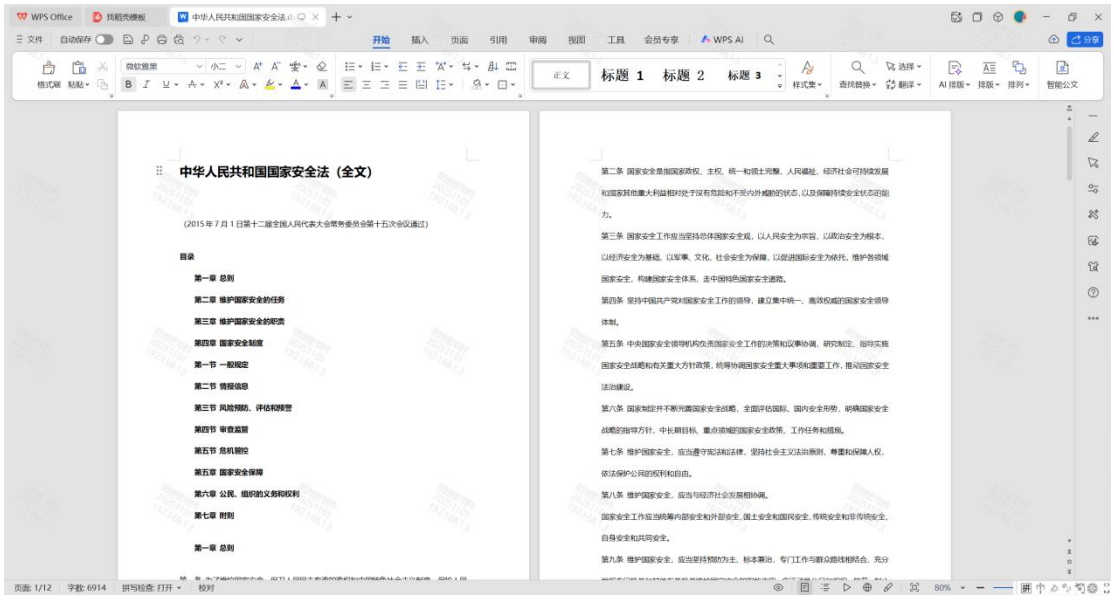
✓ AllowClientIp1-5 可以设置 5 个绿色 ip 地址，不进行拦截，但是设置值必须是数字，可以去百度搜“ip 转数字”，如何在网上进行转换后，再填入。

3.4 屏幕水印

设置终端计算机显示隐性水印或明文水印。


控制台管理
用户管理
数据保护设置
边界控制
网络控制
屏幕水印
应用加密
磁盘加密
文档云备份
打印控制
USB控制
业务/运维安全
日志管理
授权管理
文档加密
审批管理
高级配置
文件追溯
全局管理
用户监控
屏幕水印
基本信息
模版名称
文字水印
级别
最小是0，数字越大越优先执行，默认无需填写
水印设置
样式
条纹水印
文字水印
窗口水印
内容
用户名
IP
时间
内容汇总
*文字水印*用户名*IP*时间
水印加深
水印参数
设置默认值
参数(默认无需修改)
值(双击行可进行编辑)
线条宽度
9
文字/线条间隔宽度(0-1000数字越大间隔越大)
200
文字或线条颜色
188,188,188
水印背景颜色
0,220,255
主色
188,188,188
非主色降低透明度值
10
字体
微软雅黑
字号
18
角度
3300
显示几行
4
显示几列
8
监控进程(针对文字水印和窗口水印)

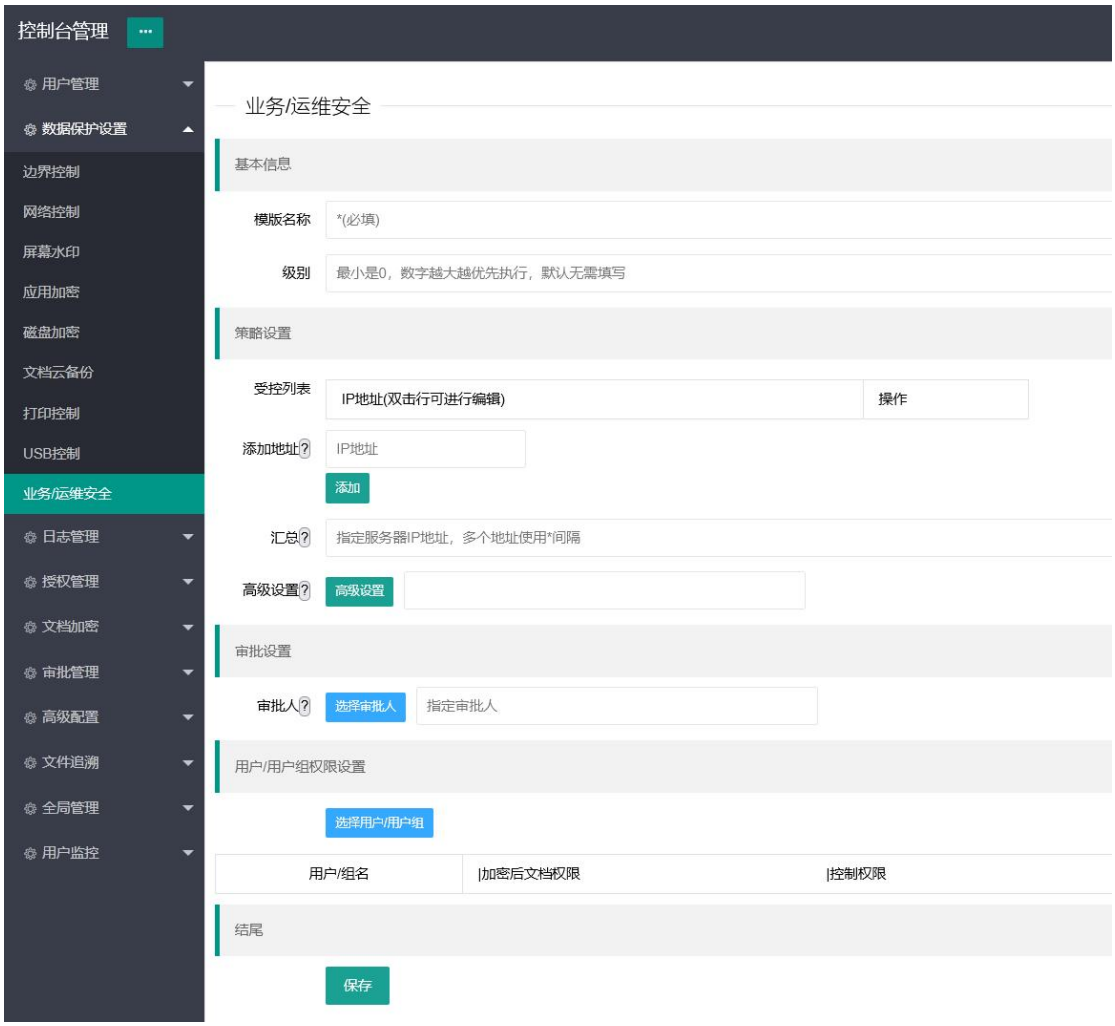
水印效果如下图：



3.5 业务系统安全

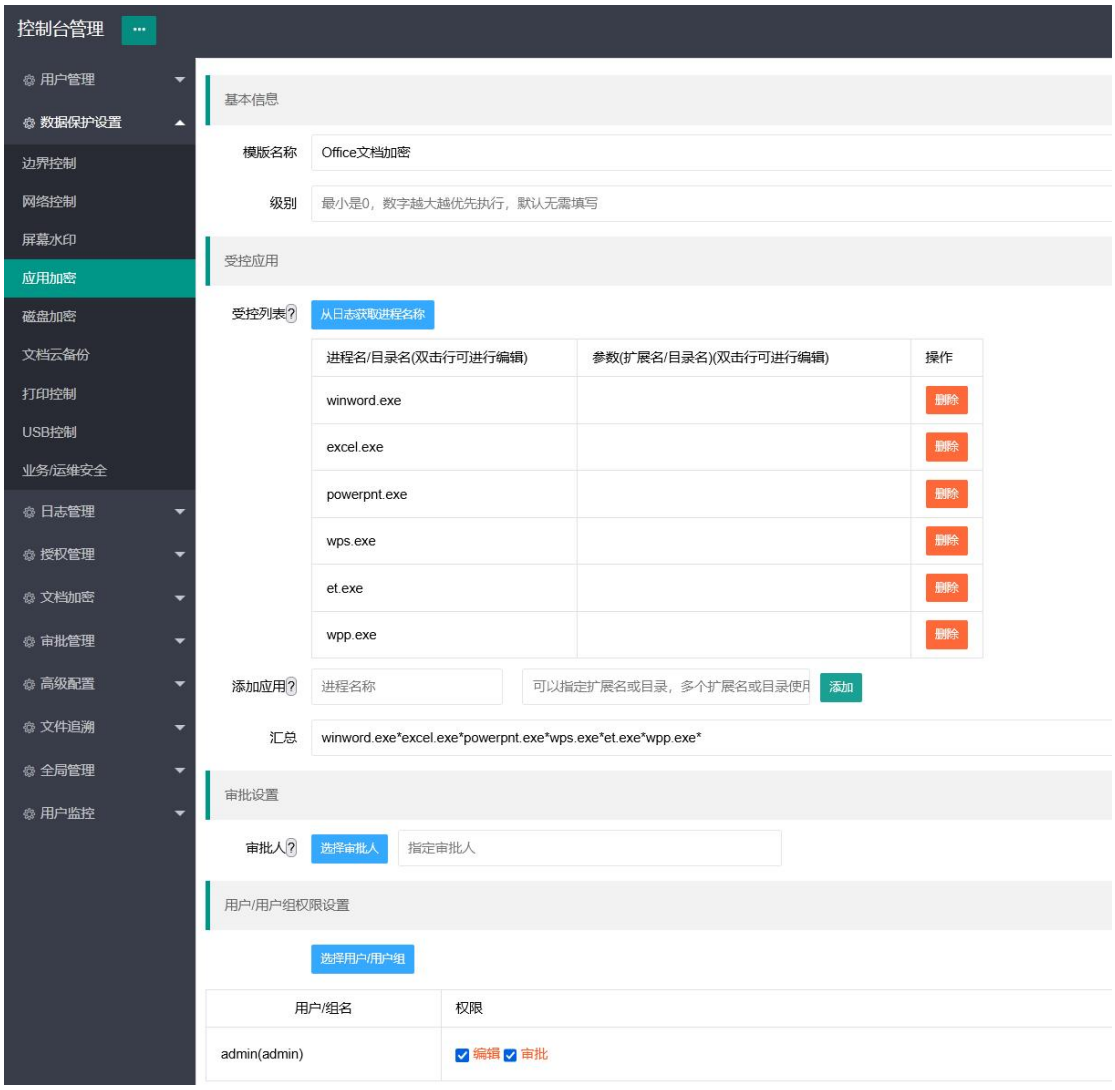
该模块合并到运维安全里面了，下策略去运维安全里面下策略

当浏览器访问受控地址时，该浏览器下载的所有文档会强制加密并赋予相应权限。



3.6 应用加密

1）是应用程序指落地保存加密，office 等应用程序二次编辑保存文档后，强制加密保存。策略设置参考如下：



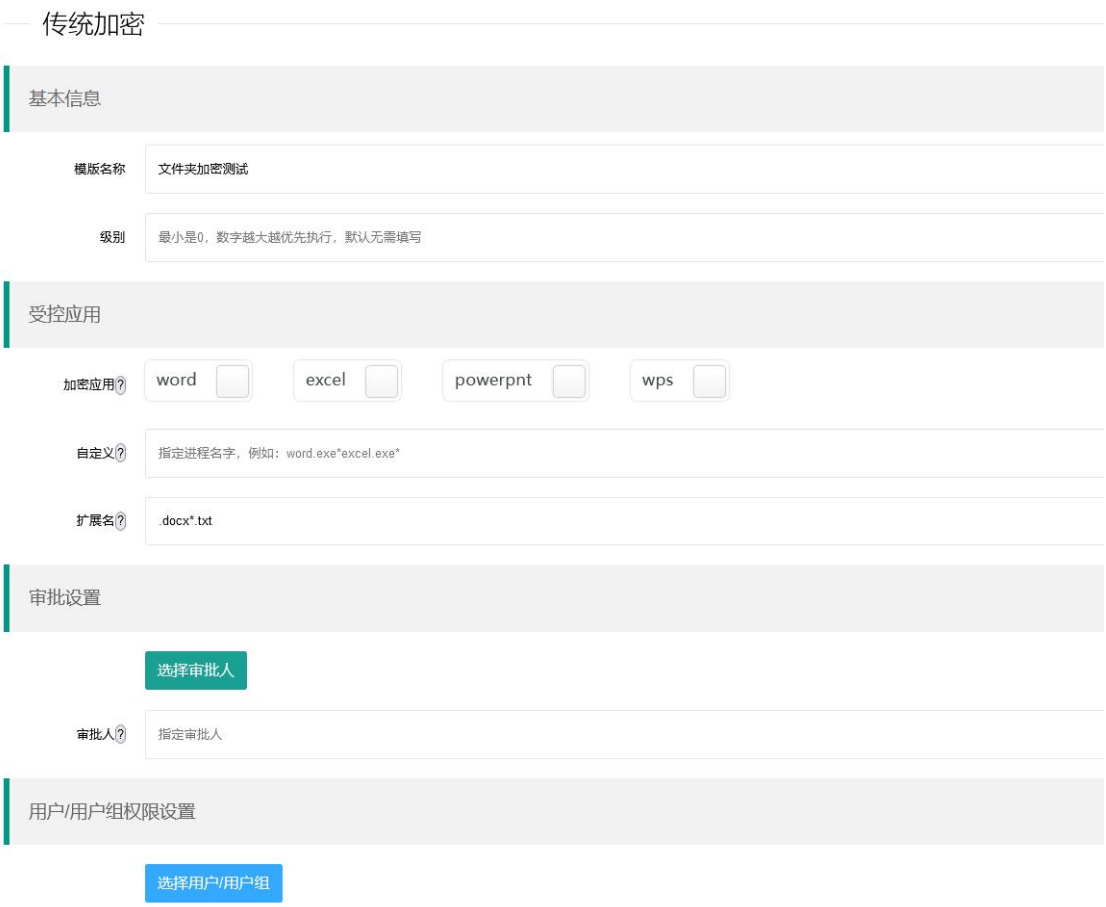
加密的文档如果要脱密成明文，需要进行审批，具体操作参考客户端部分-申请外发（申请脱密）

2）高级设置：

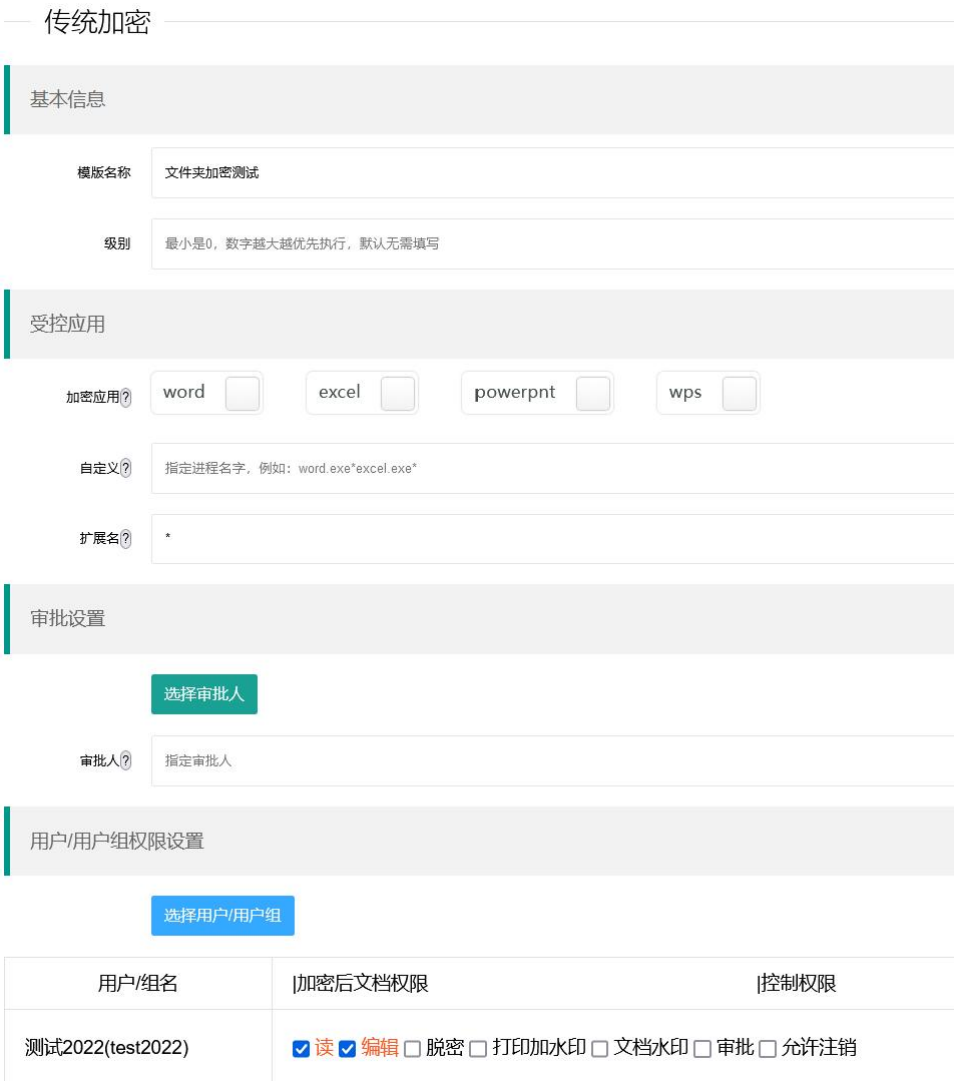
✓ 可以指定应用程序保存指定目录时自动加密并赋予相应权限。（举例：node.exe?\views\|*）node.exe 是应用程序名称，\views\是路径；可以实现前端开发的文件加密，防泄密，防篡改。

✓ 可以无需指定应用程序，仅指定扩展名的文档保存时自动加密并赋予相应权限。（举例：*.cad*.jpg，那么.cad 和.jpg 扩展名文件保存时就会自动加密）

3）传统加密也包括文件夹加密策略设置，参考如下：



如果扩展名设置为一个星号，即“*”，那么就是全部扩展名，参考如下：



常见复杂应用默认策略：

Solidworks：

受控列表

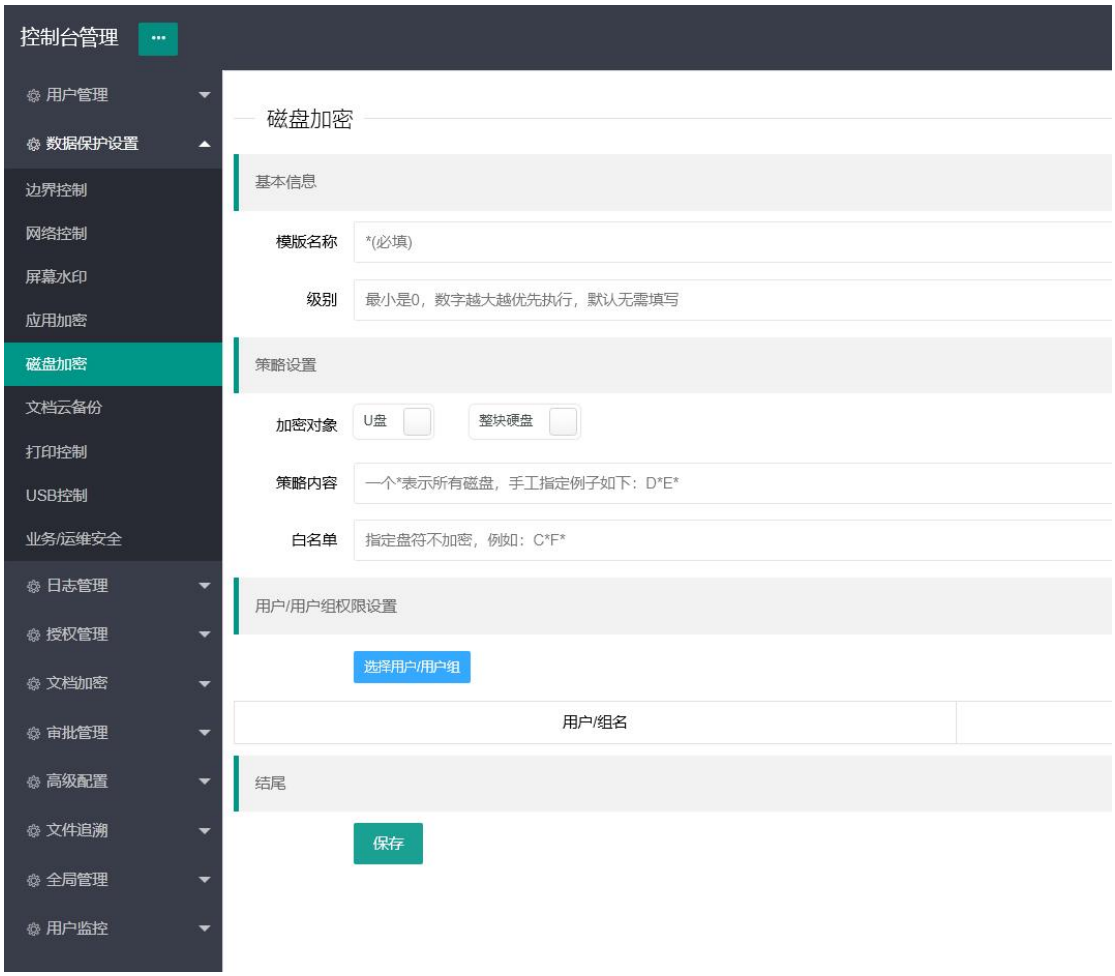
进程名/目录名(双击行可进行编辑)	参数(扩展名/目录名)(双击行可进行编辑)	操作
SLDWORKS.exe	.sldprt|.sldasm|.slddrw|	删除
sldProcMon.exe	.sldprt|.sldasm|.slddrw|	删除
sldworks_fs.exe	.sldprt|.sldasm|.slddrw|	删除
Launcher.exe	.sldprt|.sldasm|.slddrw|	删除

3.7 磁盘加密

1）对终端计算机进行磁盘加密，防止磁盘丢失或被盗取。

2）对终端计算机进行磁盘加密，防止通过 PE 方式启动绕过计算机密码保护。

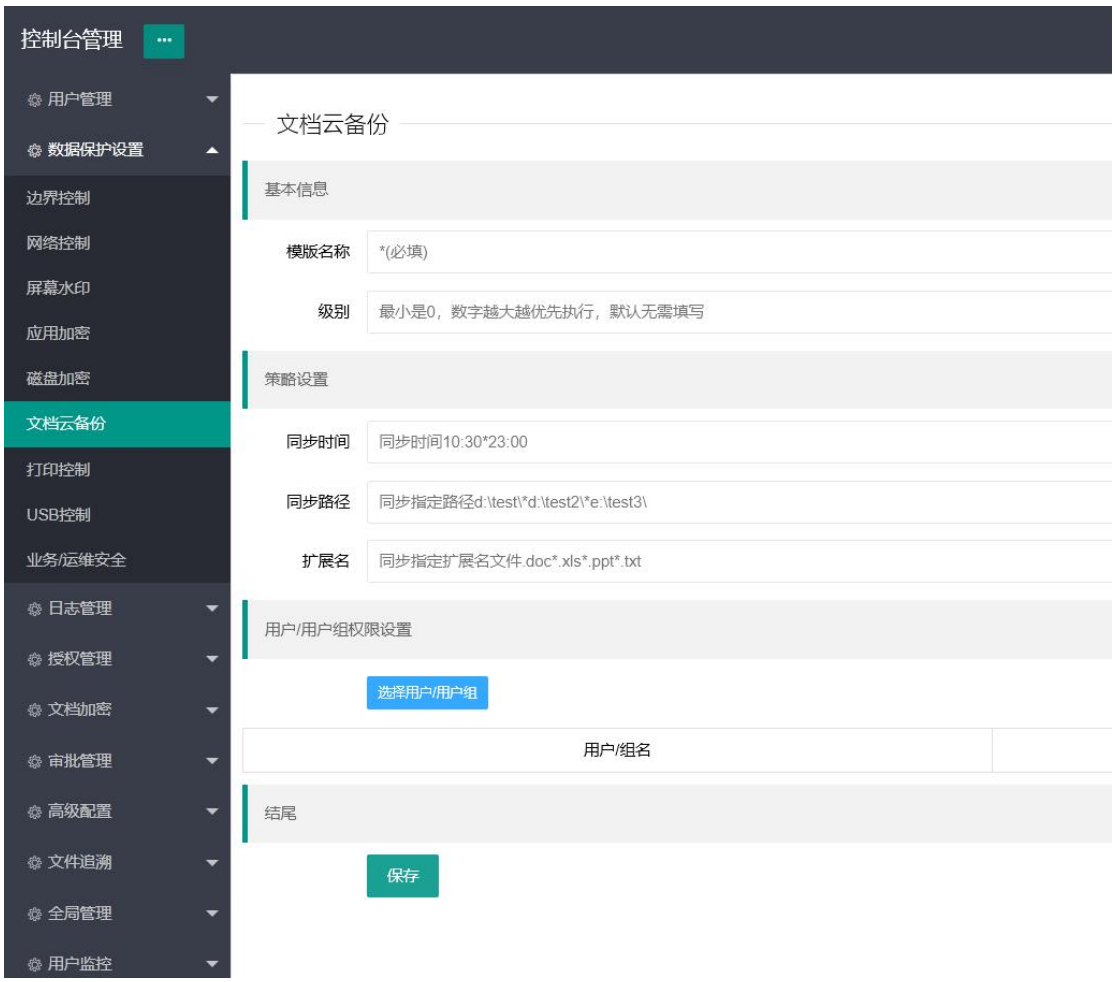
3）对 U 盘、移动硬盘进行加密，防止磁盘丢失或被盗取。



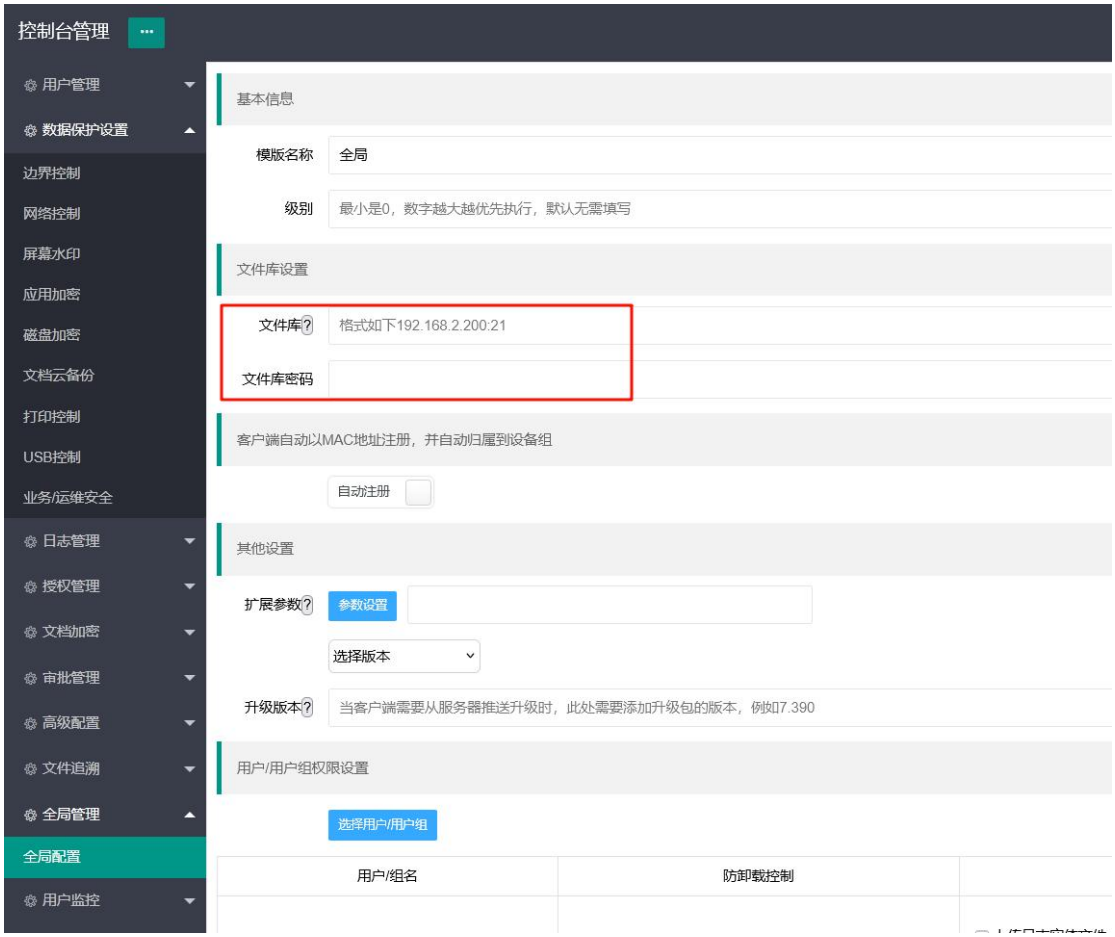
3.8 文档云备份

对终端计算机指定扩展名文件进行备份及增量备份。

1）策略设置如下图所示：.doc*.xls*.ppt 该策略会对终端电脑（账号 syybf）上磁盘中所有扩展名是 doc、xls、ppt 等文件进行备份，并每隔 1 小时进行一次增量备份。备份的文件默认会存储到边界卫士所在服务中。



2）如果要备份到指定文件服务器上，请参考如下图所示：



当需要使用 FTP 协议进行备份时，必须指定文件库管理员密码。

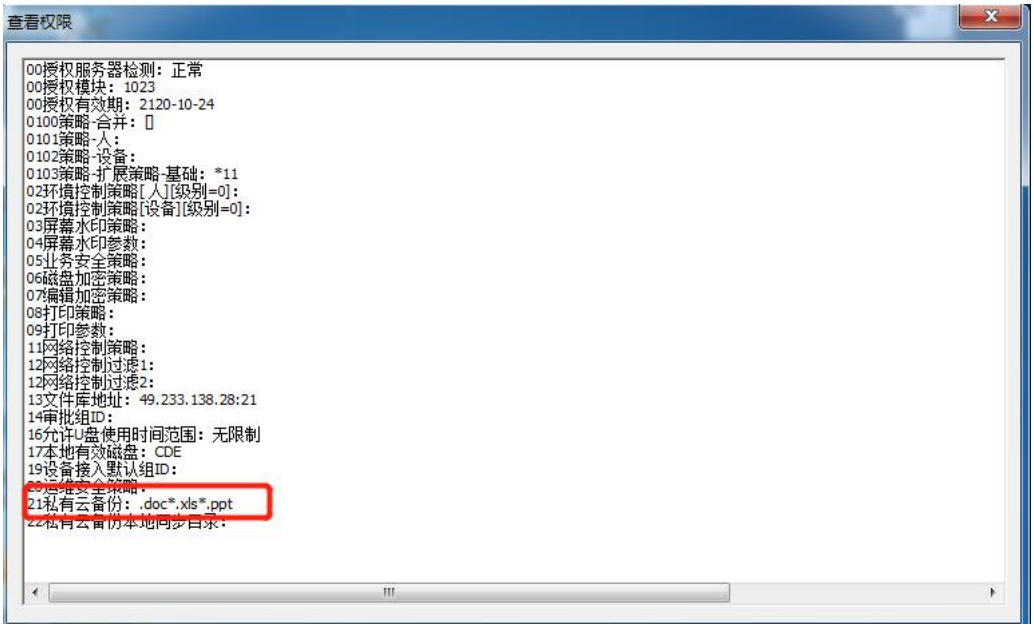
3）备份后文件存储效果图如下图：

略

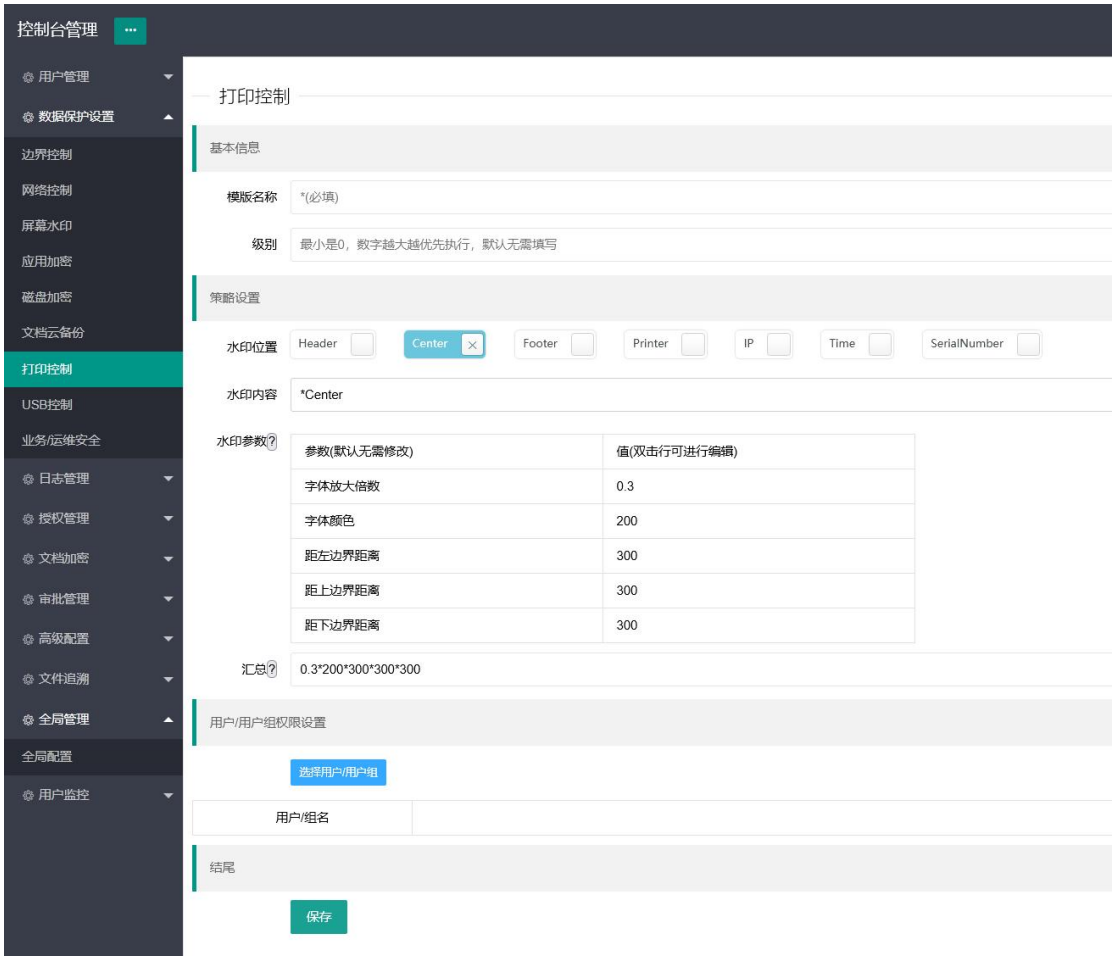
用户主页下面必须有该用户的文件夹

4）默认只同步小于 200M 的文件，可调整。

5）客户端策略如下图所示：



3.9 打印控制



1）禁止打印：禁止终端计算机打印文档。

2）打印加水印：文档打印时会在文档上面强制添加水印，水印内容包括打

印时间、IP 地址及打印者账号 ID。

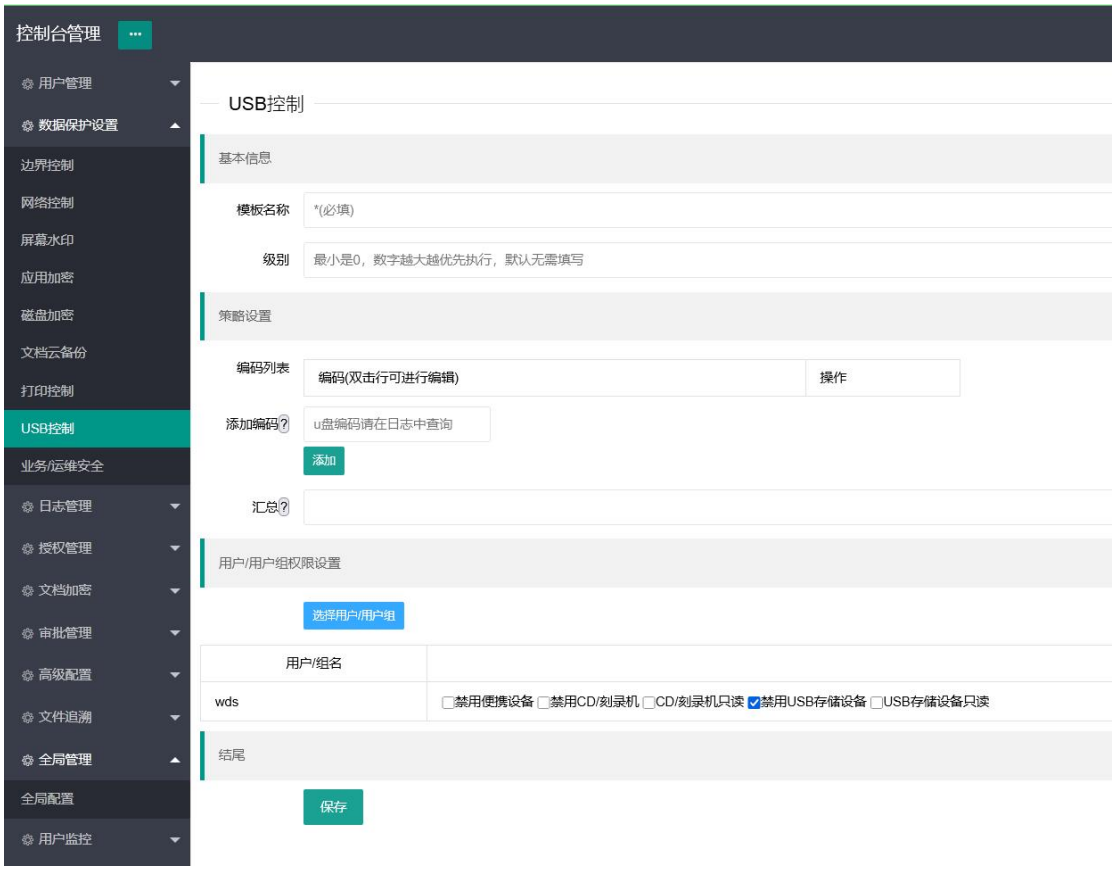
3）打印日志：记录终端计算机打印的文件名、打印终端 IP 地址、打印时间、打印用户 ID。

3.10 USB 控制

● Usb 控制模块可以针对通过终端电脑 Usb 口接入的移动存储设备进行审计、禁用、只读控制等策略。

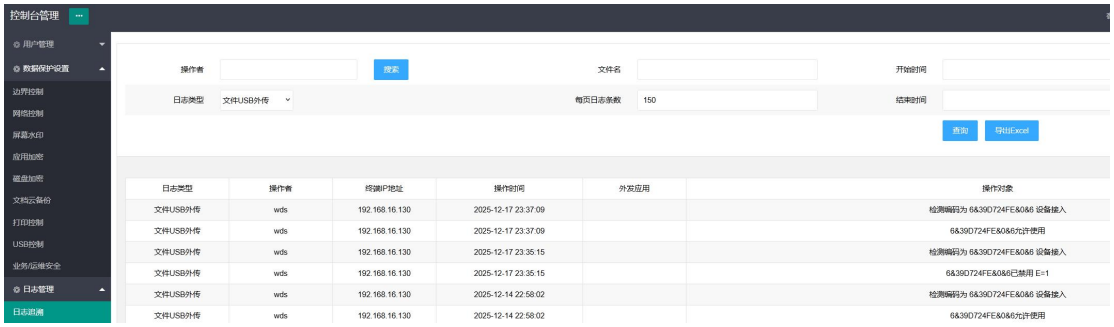
● 加密 u 盘无法禁用，但是当加密 u 盘和非加密 u 盘共同使用时，两者都禁用。

● 设置如图：

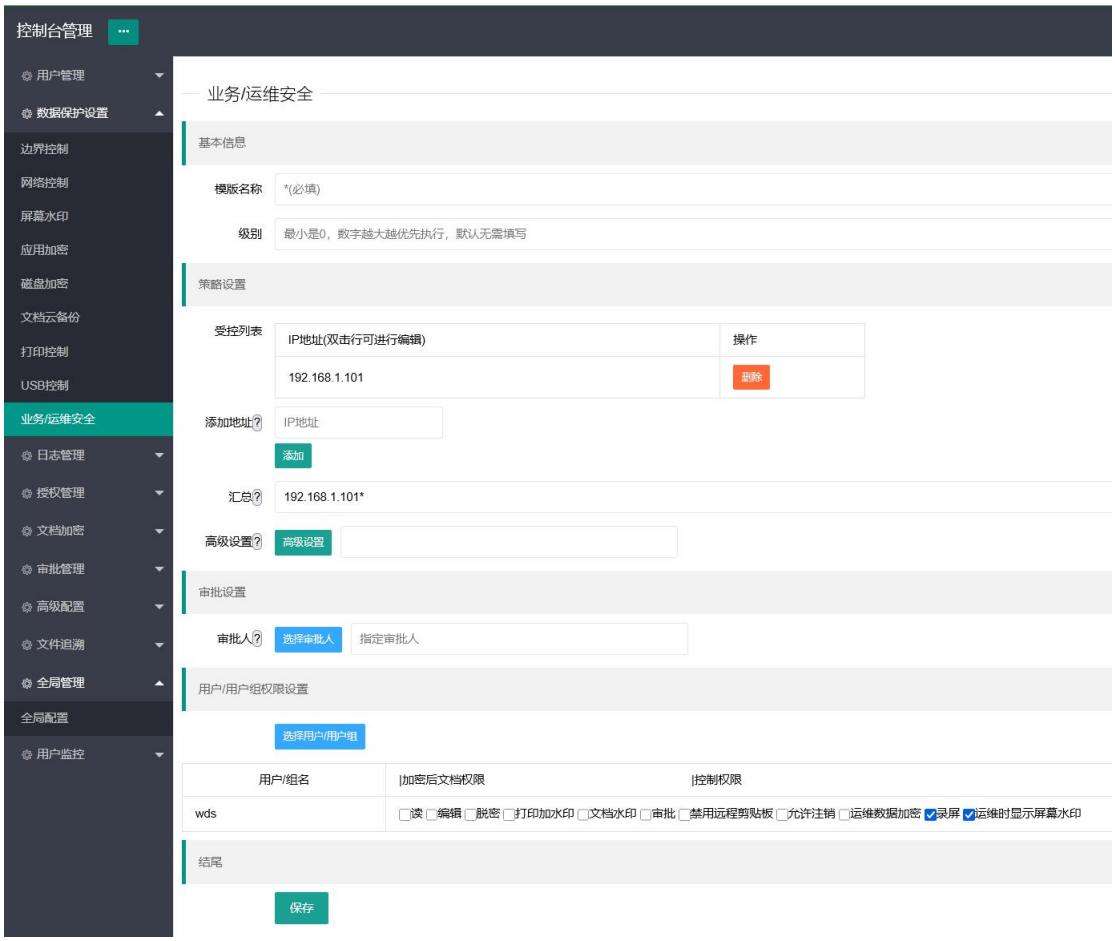


● Usb 禁用后，会出现如下提示：

- 审计日志：



3.11 运维安全



1）当终端电脑通过远程桌面或其他运维工具进行远程运维时（即访问上图策略中受控 IP 地址），拷贝出来的数据会自动强制加密并赋予相应权限；

2）录屏：通过远程桌面或其他运维工具运维过程中录屏备份（需要单独安装录屏模块）。

3.12 云加密

用户直接使用浏览器就可以进行文件的加密和分享。控制文档的二次传播，防止文档被滥用和泄密。

主要功能：

1. 设置打开文档的账号和密码；
2. 设置文档查阅时间，可以精确到小时。.
3. 制作瘦客户端加密方式，对方无需安装边界卫士即可打开，但是打开后文档受管理限制。

移动端如下图：

电脑端如下图：

4 客户端升级

4.1 客户端升级（自动）

- 第一步 选择高级配置，进入如上图页面后，上传升级包（升级包文件名命名方式：8.8444.exe），点击“上传“按钮，完成第一步，即已支持手动升级；
- 第二步 选择全局配置，从其他设置中，版本升级处，选择一个待升级的版本，然后从用户/用户组权限设置处，选择待升级用户或组，勾选“强制升级”，点“保存”按钮，即完成客户端自动推送升级的配置。客户端收到策略后（默认间隔 1 小时），会自动静默升级，重启计算机后生效。

4.2 客户端升级（手动）

右键电脑边界卫士托盘图标，选择更新客户端。

点击开始升级，等待完成升级提示成功后，重启计算机后生效。

二、 客户端使用

1 安装客户端

- 手动安装，默认下一步下一步即可（安装时需要输入服务器 IP 地址），安装后 win7 需要重启计算机，win10 和 win11 无需重启；
- 绑定 IP 地址安装：在安装包同级目录下创建一个 ip.txt 文件，里面输入 IP 地址或域名即可，如下图。

- 有新版本的时候把文件名改成 update.exe 可直接覆盖安装；
- 安装完成后，会在屏幕右下角出现托盘图标；
- 点击托盘图标会出现操作菜单；

2 桌管系统静默安装客户端

安装包后面需要带 /SILENT /VERYSILENT 参数

参考如下：

setup.exe /SILENT /VERYSILENT

3 域推送安装客户端

- 域推送自动静默安装；
- 将下述内容保存到“域推送关机或开机脚本.bat”文件中，然后通过域推送下去即可

::123456 是机器密码 test 是用户名 \\192.168.1.113\Users 是共享目录 setup.exe 是安装文件名

```
@echo off
ping -n 50 127.1>c:\bsssetup_temp\null
tasklist /nh|find/i"agent.exe"
```

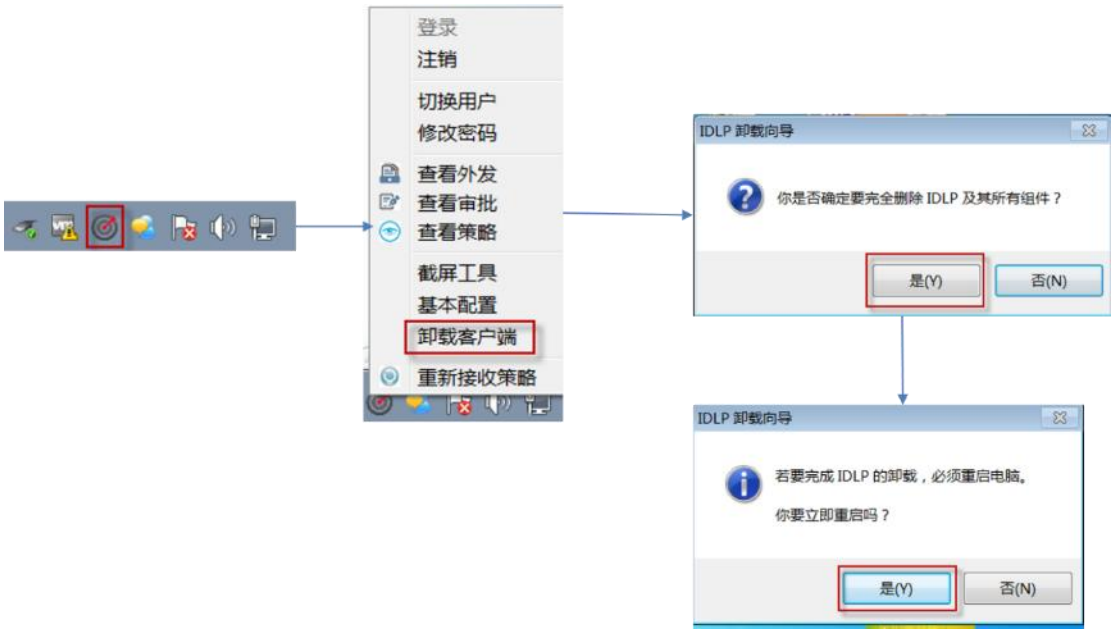
```
    if %errorlevel%==0 ( exit ) else (
    md c:\bsssetup_temp
    ping -n 2 127.1>c:\bsssetup_temp\null
    echo 内网安全软件更新维护中 请勿关闭此对话框
    ping -n 2 127.1>c:\bsssetup_temp\null
    net use \\192.168.1.113\Users 123456 /user:192.168.1.113\test
    ping -n 4 127.1>c:\bsssetup_temp\null
    copy \\192.168.1.113\Users\test\setup.exe
c:\bsssetup_temp >c:\bsssetup_temp\null
    ping -n 4 127.1>c:\bsssetup_temp\null
    start c:\bsssetup_temp\setup.exe /SILENT /VERYSILENT
    ping -n 2 127.1>c:\bsssetup_temp\null
    net use \\192.168.1.113 /delete
    net use * /del /y
    ping -n 50 127.1>c:\bsssetup_temp\null
    exit
    )
```

4 客户端连接服务器

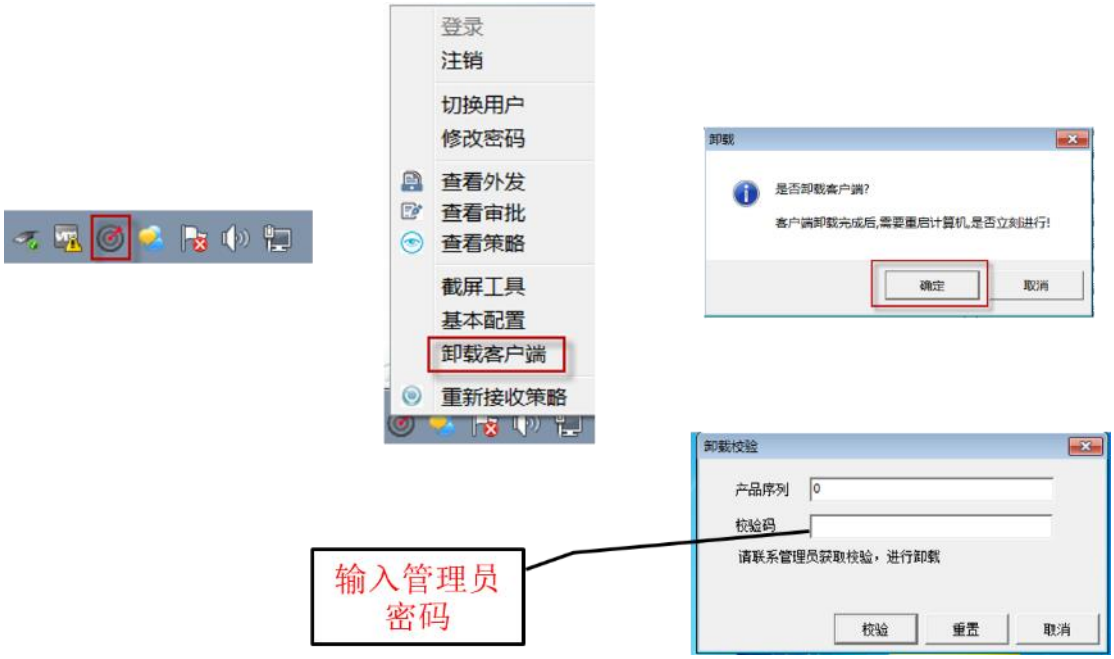
- 托盘图标-设置-设置服务器地址 点击应用按钮即可

5 卸载客户端

- 点击托盘托盘图标会出现操作菜单，选择菜单中的卸载客户端；



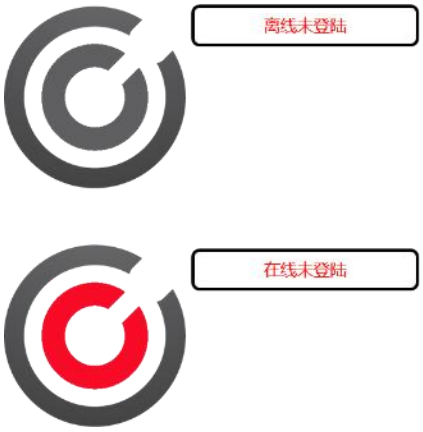
- 防卸载版本需要密码认证，密码就是管理员 admin 的密码；
- 防卸载版本的离线演示版本密码为固定 009；



6 客户端状态说明

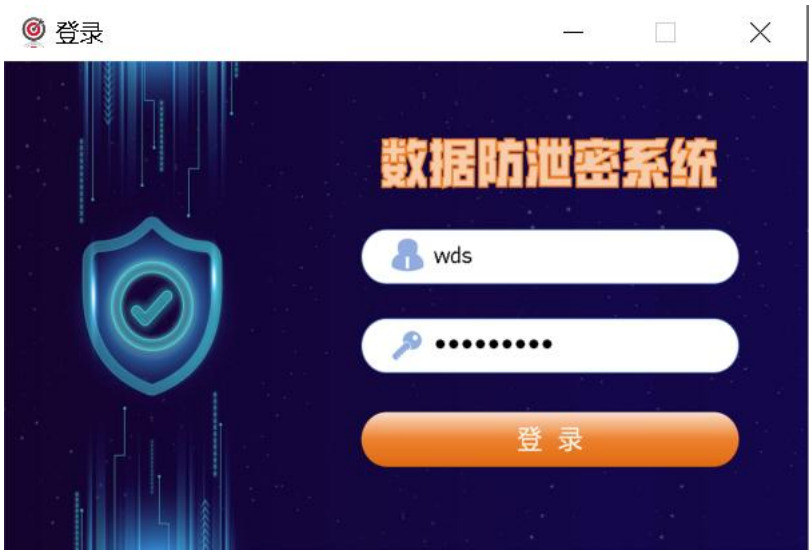
- 离线未登录；
- 在线未登录；
- 在线登录；

- 离线登录；
- 有待审批文件；
- 云备份进程中；



7 客户端登录

- 手工登录指定用户；
- 开机自动登录上次登录账号；
- 域账号单点登录；
- 其他系统单点登录；



8 设备登录

- 设备登录后，禁止使用其他账号进程二次登录
- 登录菜单是灰色，禁止使用
- 设备绑定会叠加设备策略

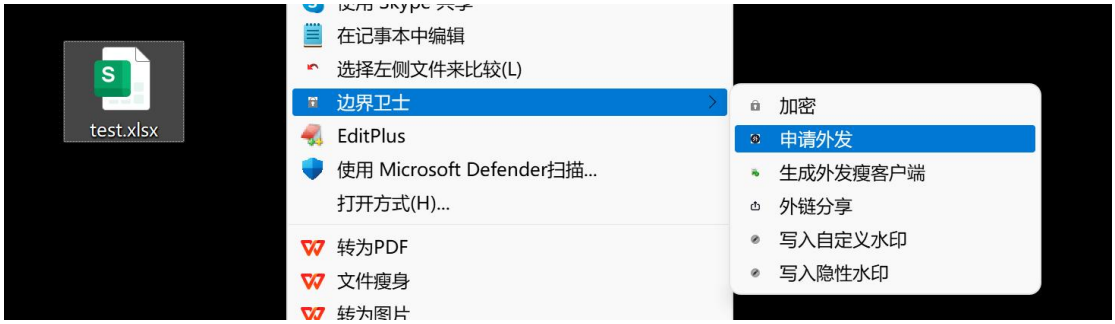
9 接收策略时机

- 客户端接收策略有如下 4 种场景；
- 1. 开机；
- 2. 登录用户（个别策略需要重新 agent 后生效）；
- 3. 切换用户（个别策略需要重新 agent 后生效）；
- 4. 通过重新接收策略功能；
- 为了减少服务器压力，其他情况不会主动去服务器查询最新策略。所以服务器变更策略后，终端用户除了上述 4 种场景外，不会收到最新策略。

10 申请外发

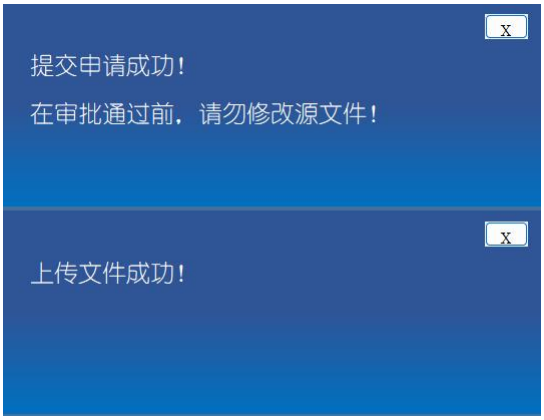
- 用户可以申请文档外发明文，或将加密文档解密成明文。

- 右键选择待外发文档，选择边界卫士-申请外发

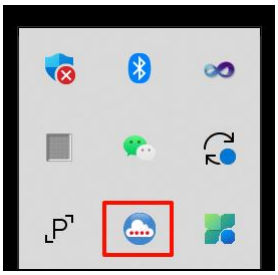


- 在弹出的窗口中添加申请说明，点击确认，完成外发申请。

提交成功后提示如下：



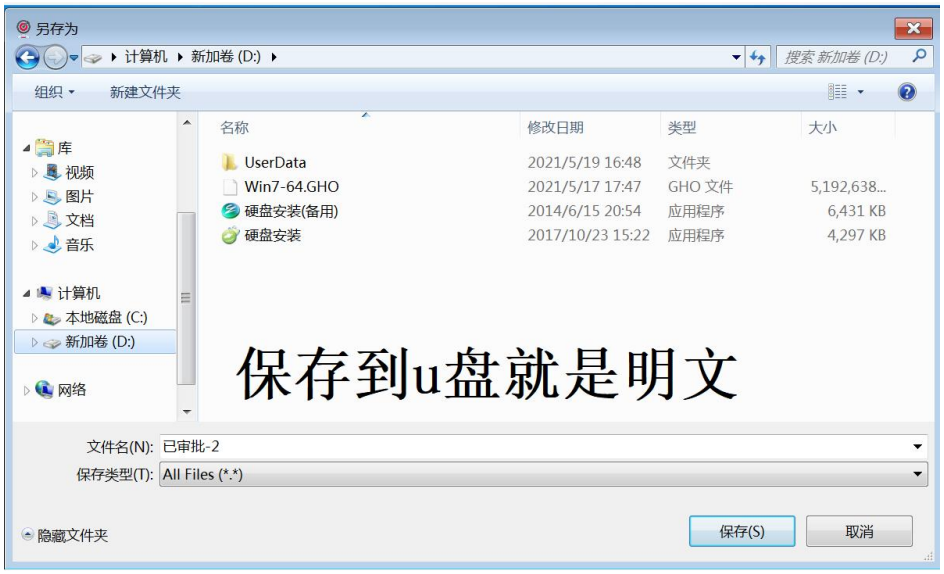
- 文档经过审批人审批后，右下角托盘图标会有提示，点击右下角托盘图标菜单中的查看外发



在弹出的页面中双击您要外发的文件，下载到本地即可

id	申请说明	文件名	申请时间	审批状态
1	411	1.docx	2025-2-9 22:15:00	通过
2	111	1.docx	2025-2-9 22:36:37	完成
3	11144	1.docx	2025-2-9 22:39:11	完成
4	111	1.docx	2025-2-9 22:40:53	完成
5	11	1.docx	2025-2-9 22:49:03	完成
6	111	1.docx	2025-2-9 22:11:30	通过
7	1111	1.docx	2025-2-8 12:34:11	通过
8	111	1.docx	2025-2-8 12:27:50	通过

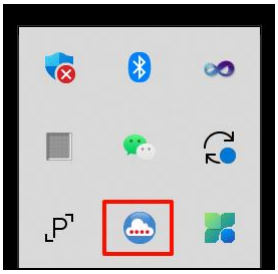
- 下载到本地会生成一个特殊文件，使用这个特殊文件再执行外发，就不会被加密了。如果外发途径是 u 盘，那么需要直接保存到 u 盘中。



- 申请外发也可以将加密文件变成明文。

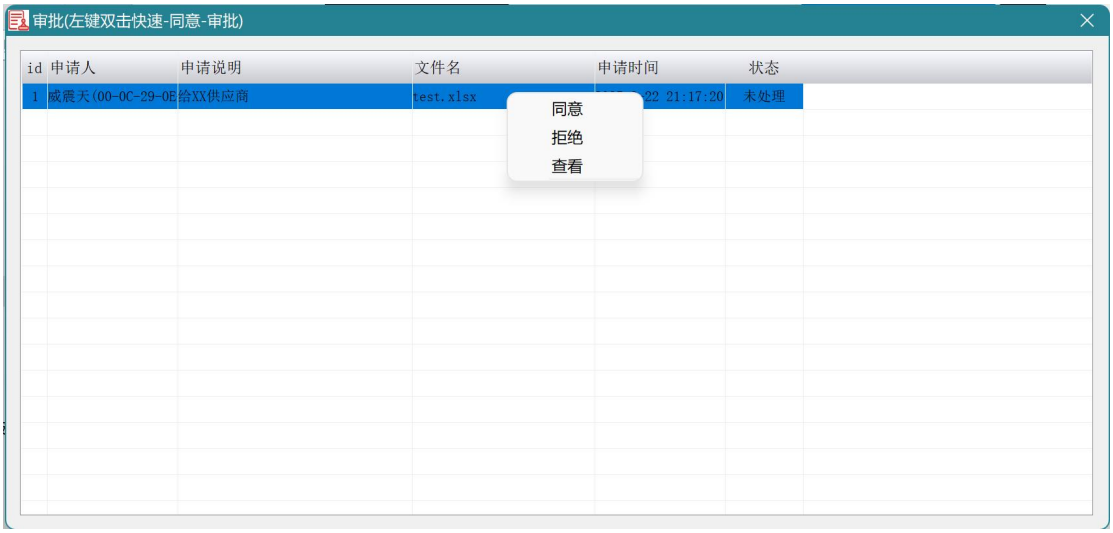
11 审批

- 支持 web 端和手机移动端审批
- 支持在线查看审批内容
- 有待审批信息提醒



点击右下角托盘图标菜单中的查看审批

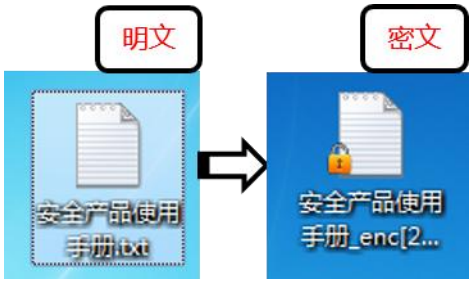
电脑端审批（双击待审批条目，快速审批（默认同意））



WEB 端或移动端

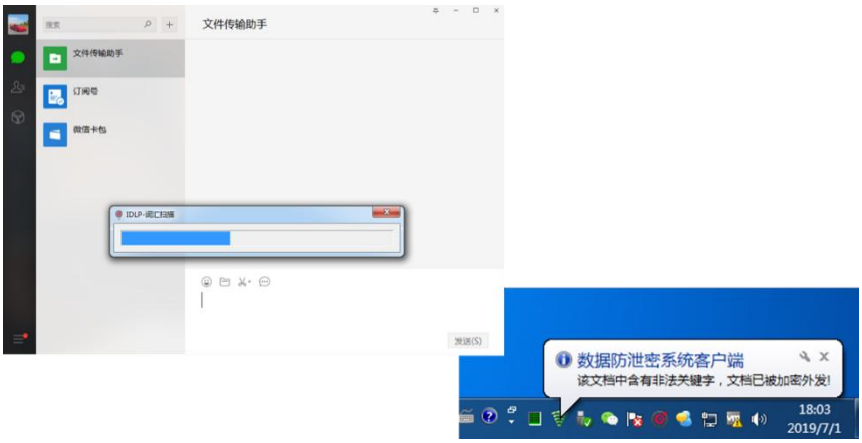
12 主动加密-文档加密

- 加密：主动加密，对文件进行加密并指定用户或组设置权限。



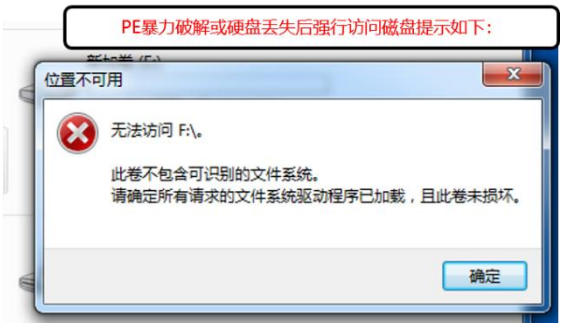
13 终端控制-外发文件关键字识别加密

- 微信、QQ、浏览器等外发文件时根据服务器策略强制对外发的 office 系列文档进行扫描，发现匹配关键字，自动将文档加密后外发；



14 终端控制-磁盘透明加解密（防暴力破解）

- 安装客户端并接收策略后磁盘自动、强制加密，防止磁盘数据泄密
- 用户正常使用磁盘时不会感觉到磁盘加解密过程的存在
- 非法用户暴力破解或磁盘丢失后访问磁盘时，无法还原磁盘数据

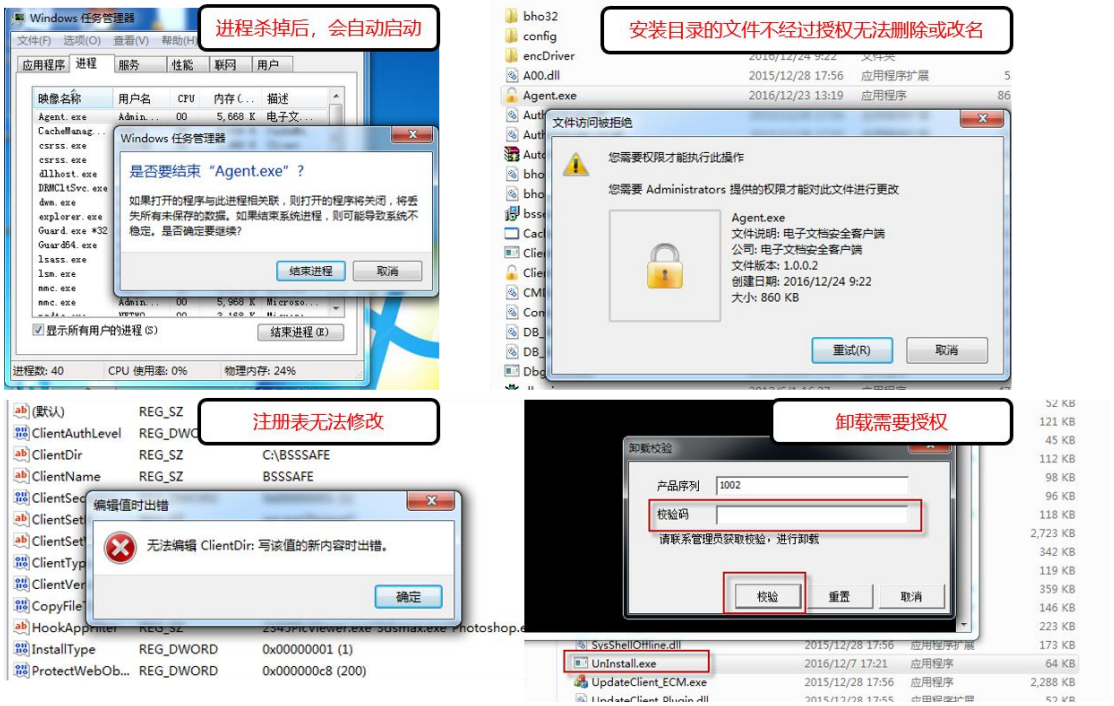


15 加密文档权限控制

- 加密文档通过账号密码认证打开后会受相应权限控制
- 控制的权限有只读、打印、打印水印、防截屏录屏屏幕水印、打开次数、打开时间脱密、再授权等控制

16 客户端程序自保护（防暴力破解）

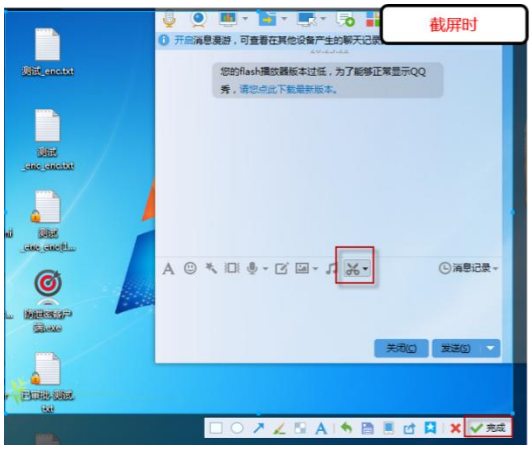
- 客户端安装启动后会自动执行自保护，防止用户强行破坏；
- 客户端卸载时需要经过管理员授权。

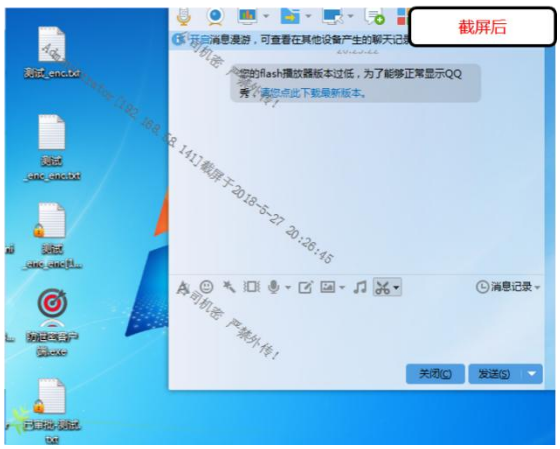


17 终端控制-打印控制

- 可以强制添加打印水印；

18 终端控制-截屏控制



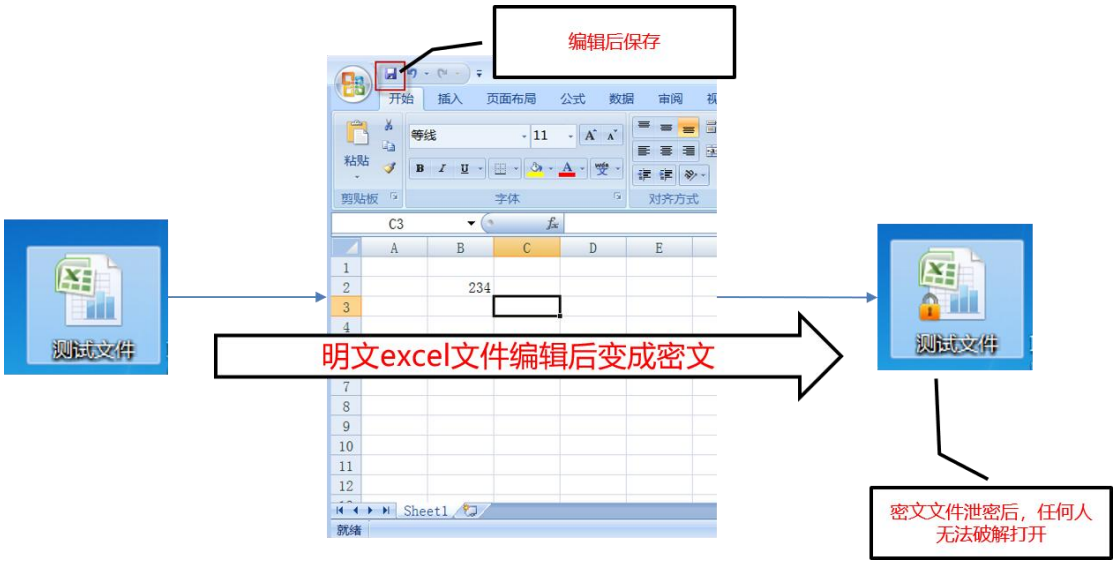


19 终端控制-文档外发加密

- 文件外发自动、强制加密，防止终端泄密；
- 加密过程合理使用无明显感知，打开、保存及使用方式无改变；

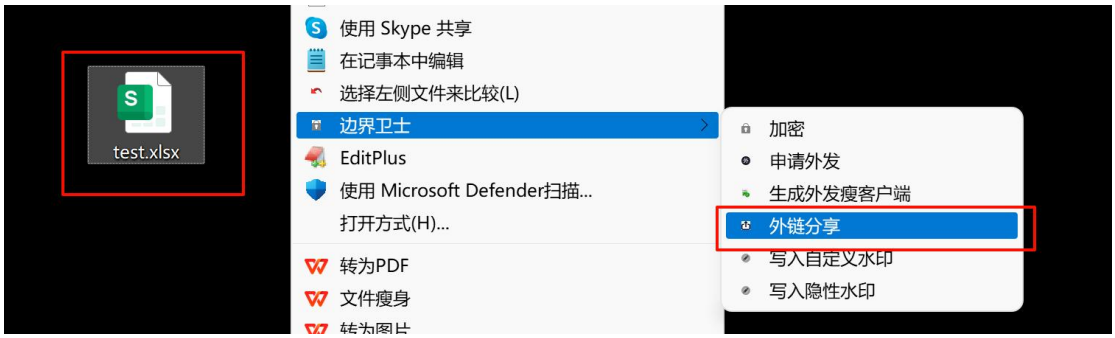
20 终端控制-文档二次编辑加密

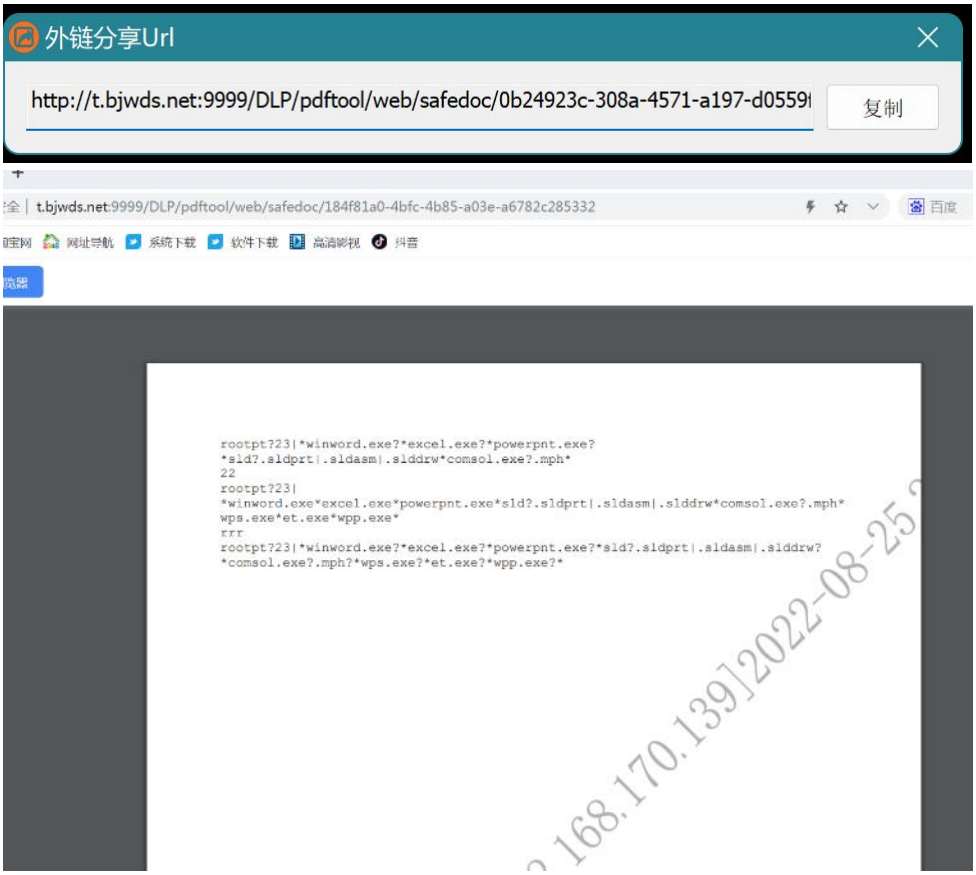
- 文件打开后，如果编辑后进行保存，会强制加密；



21 外链分享

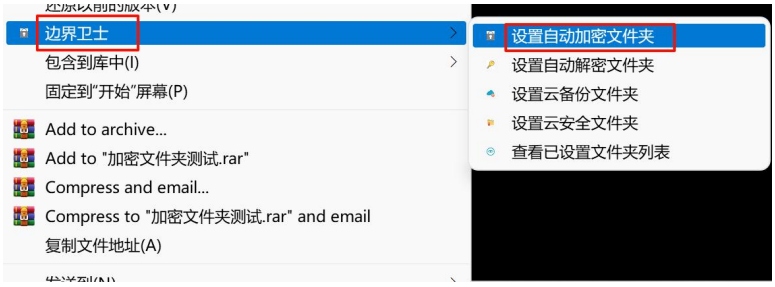
- 用户可以创建明文或密文的外链，通过外链可以在手机、苹果等非 windows 系统上查看文件。但仅限查看、并且查看文档有水印。





22 主动加密-自动加密文件夹

- 终端计算机用户选择任意一个待加密的文件夹，右键，在弹出的菜单中选择“边界卫士”->“设置自动加密文件夹”选项。如下图：



- 权限信息里面的脱密账号和密码是指设置后可以使用该账号和密码进行文件打开以及脱密操作。

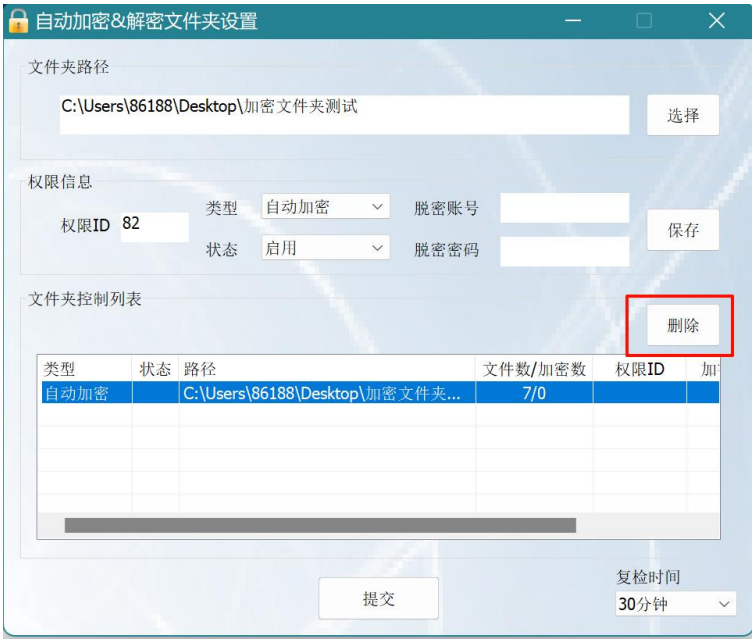
- 复检时间是指当出现某些特殊场景导致文件漏加密的情况，程序会通过间隔每 30 分钟进行检查，完成剩余文件加密。

- 设置完成后文件夹左下角会有一个小锁图标，如下图：

文件夹及子文件夹内的文件会被自动加密，并且新增的文件也会被实时加密。

- 加密文件打开或脱密都需要认证。

23 取消文件夹加密



24 自动解密文件夹

- 终端计算机用户选择任意一个待加密的文件夹，右键，在弹出的菜单中选择“边界卫士”->“设置自动解密文件夹”选项。

- 程序会对该文件夹及子文件夹内的有权限的加密文件进行自动解密。
- 自动解密文件夹图片如下：

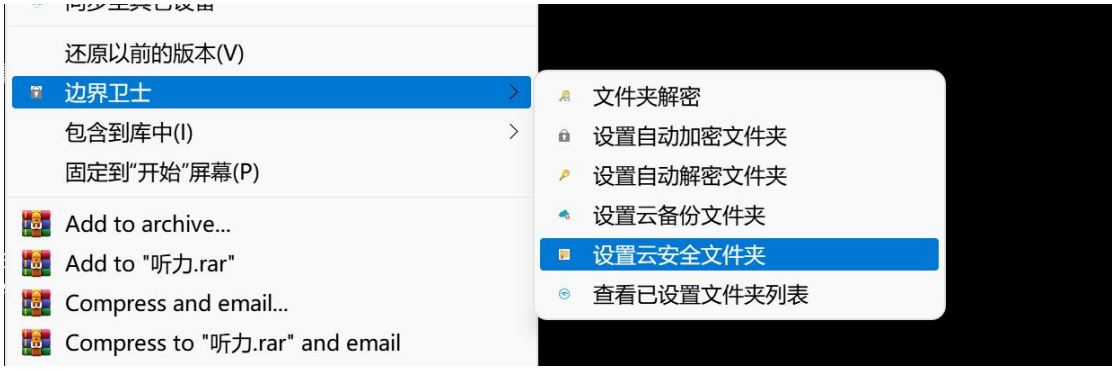
- 目前解密文件夹无复检功能。

25 云备份文件夹

- 终端计算机用户选择任意一个待加密的文件夹，右键，在弹出的菜单中选择“边界卫士”->“云备份文件夹”选项。
- 程序会对该文件夹及子文件夹内的文件自动备份到私有云平台。

26 云安全文件夹

- 终端计算机用户选择任意一个待加密的文件夹，右键，在弹出的菜单中选择“边界卫士”->“云安全文件夹”选项。
- 程序会对该文件夹及子文件夹内的文件自动解密。



27 绑定硬件打开

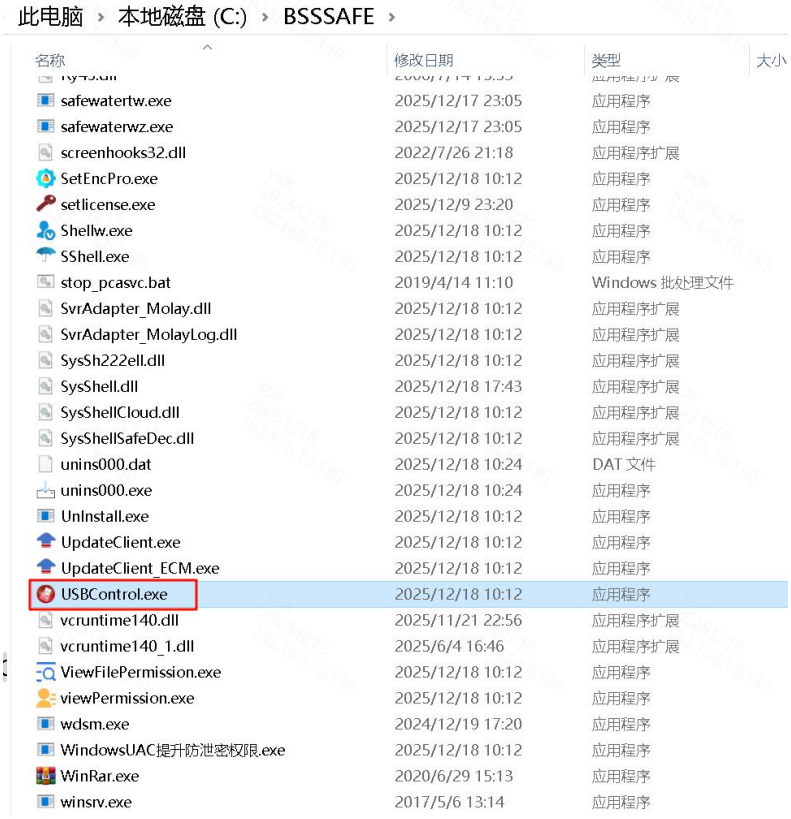
- 主动加密时可以绑定硬件码，打开时无需进行认证操作，直接双击打开即可。

- 绑定硬件码的加密文件只能在非 C 盘操作。

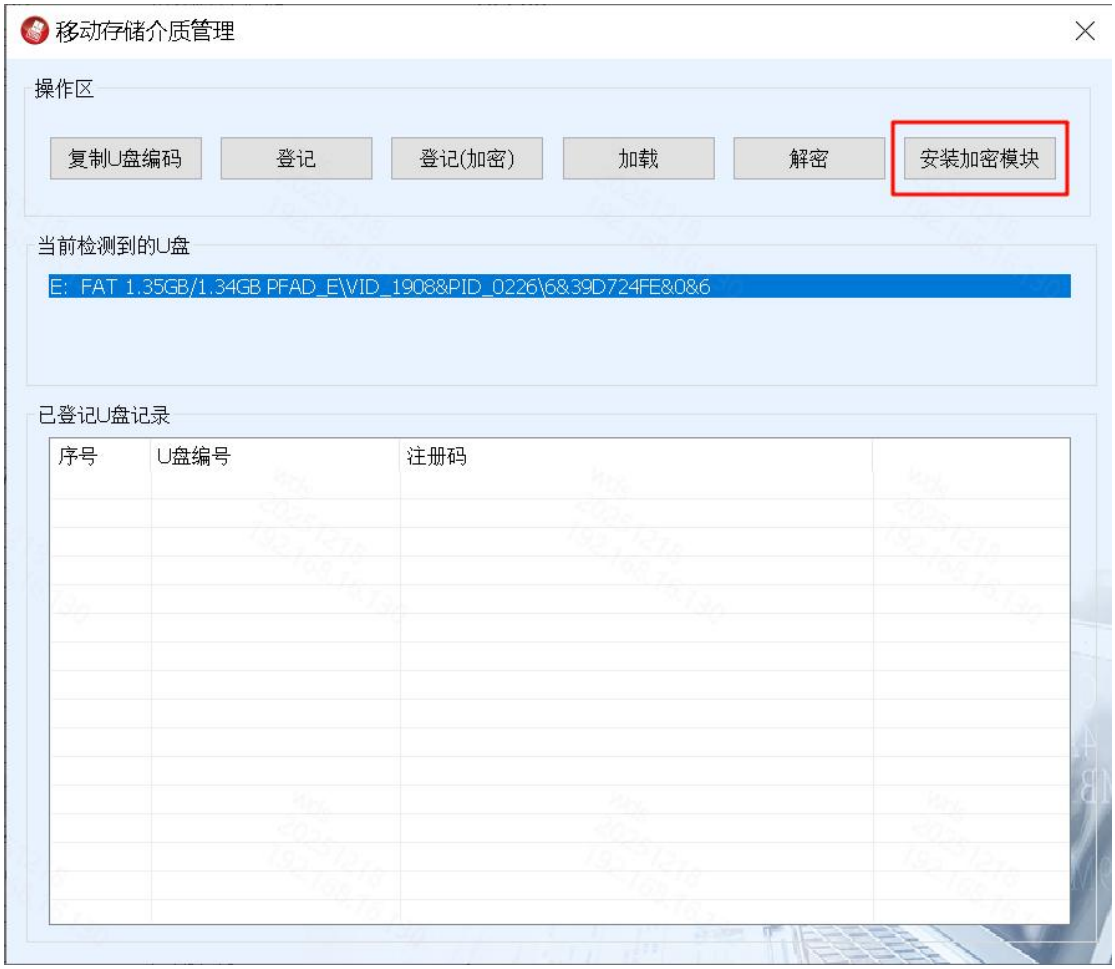
28 企业加密 U 盘

28.1 手工加密方式

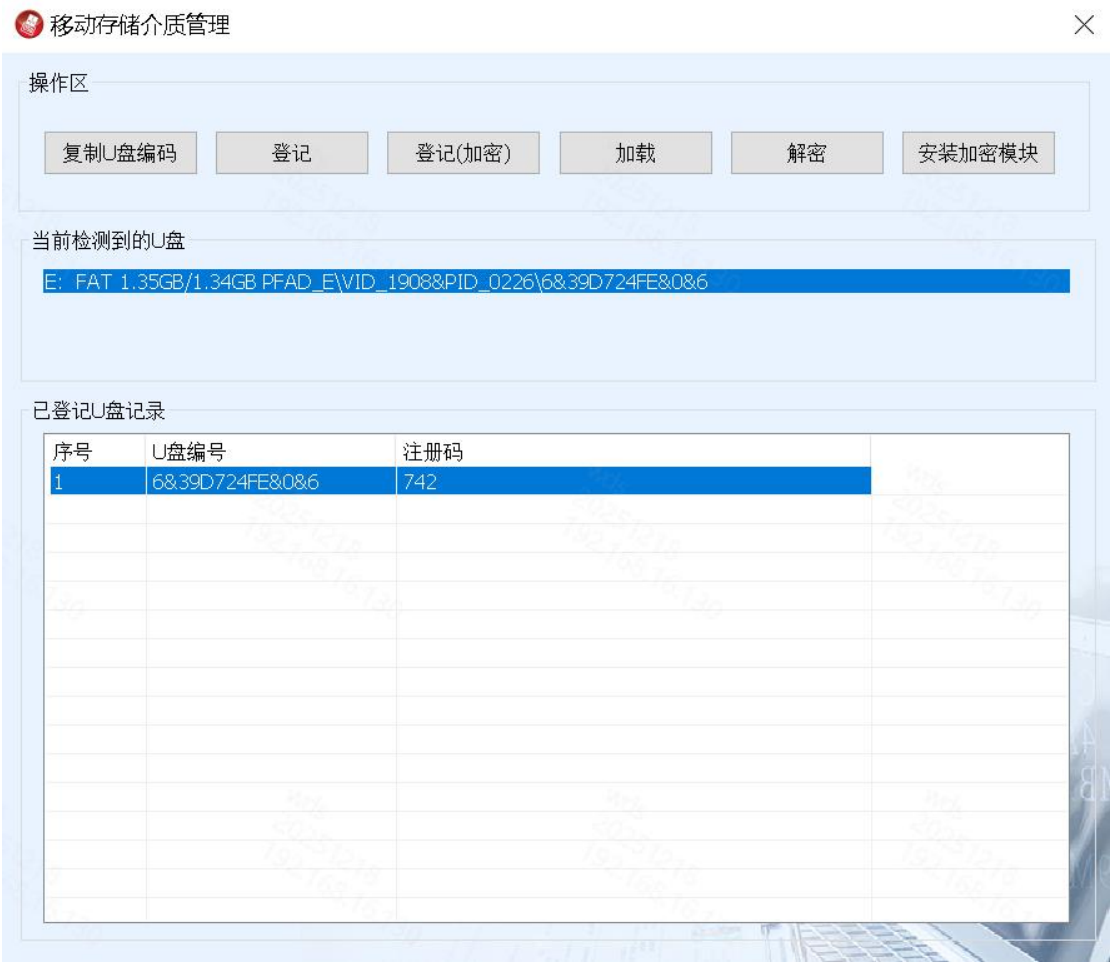
- 运行安装目录 C：\BSSSAFE 目录下 USBControl.exe 文件：



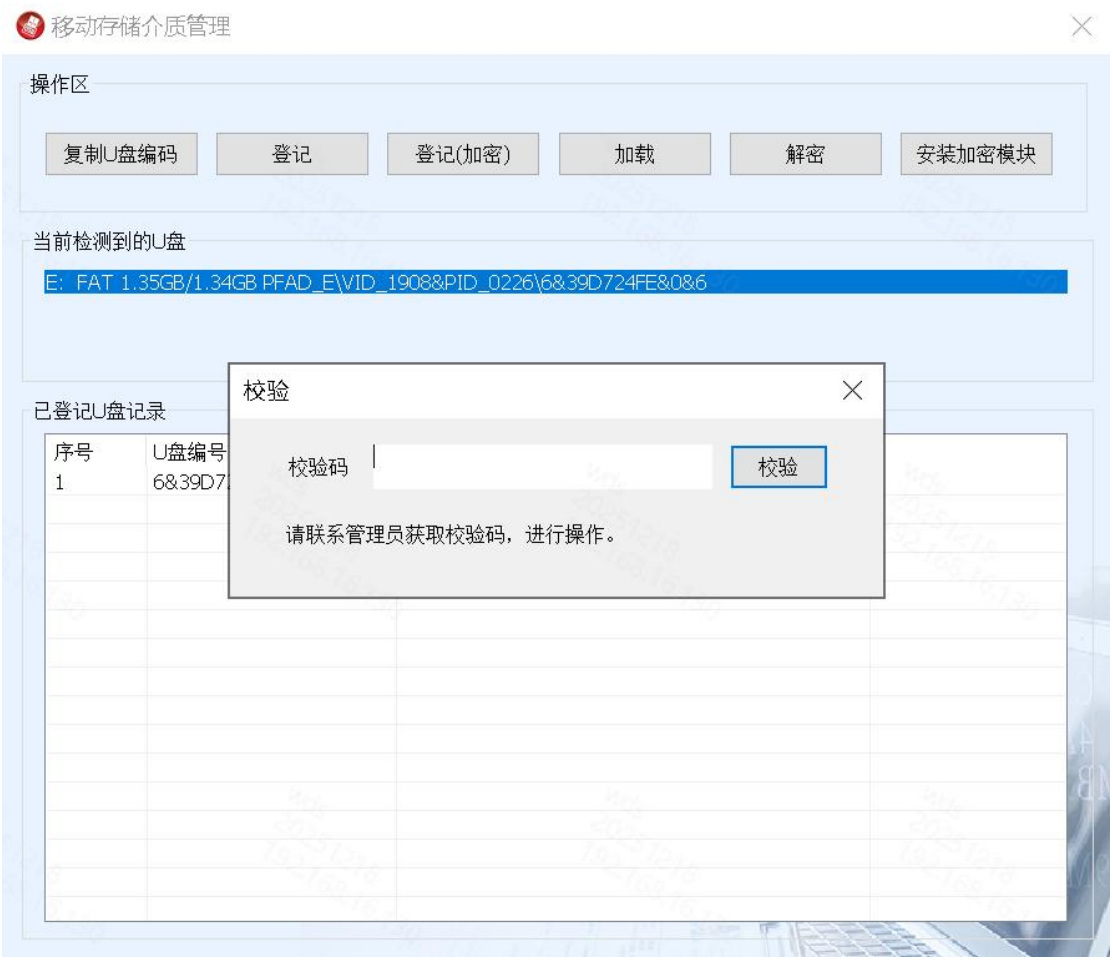
- 点击程序“安装加密模块”按钮，按照提示完成后（如已自动安装会提示已经安装，直接重启计算机即可），重启计算机。



- 插入待加密 u 盘，从“当前检测到的 u 盘”列表中选择该 u 盘，如下图所示：



- 点击“登记(加密)”按钮后，会提示密码校验，输入管理员密码（默认 admin）即可，完成后点“OK”按钮，完成 u 盘加密。



- 完成 u 盘加密的 u 盘，在非内部受控计算机上无法使用，会有如下提示：

- 如果强行格式化，里面所有数据都将消除，可以有效防止 u 盘丢失泄密，并且原加密 u 盘数据通过任何 u 盘恢复工具也无法恢复。

- 完成 u 盘加密的 u 盘，在内部受控计算机上登录账号后可以正常使用，如果出现上述格式化提示，点取消即可，不会影响正常使用。

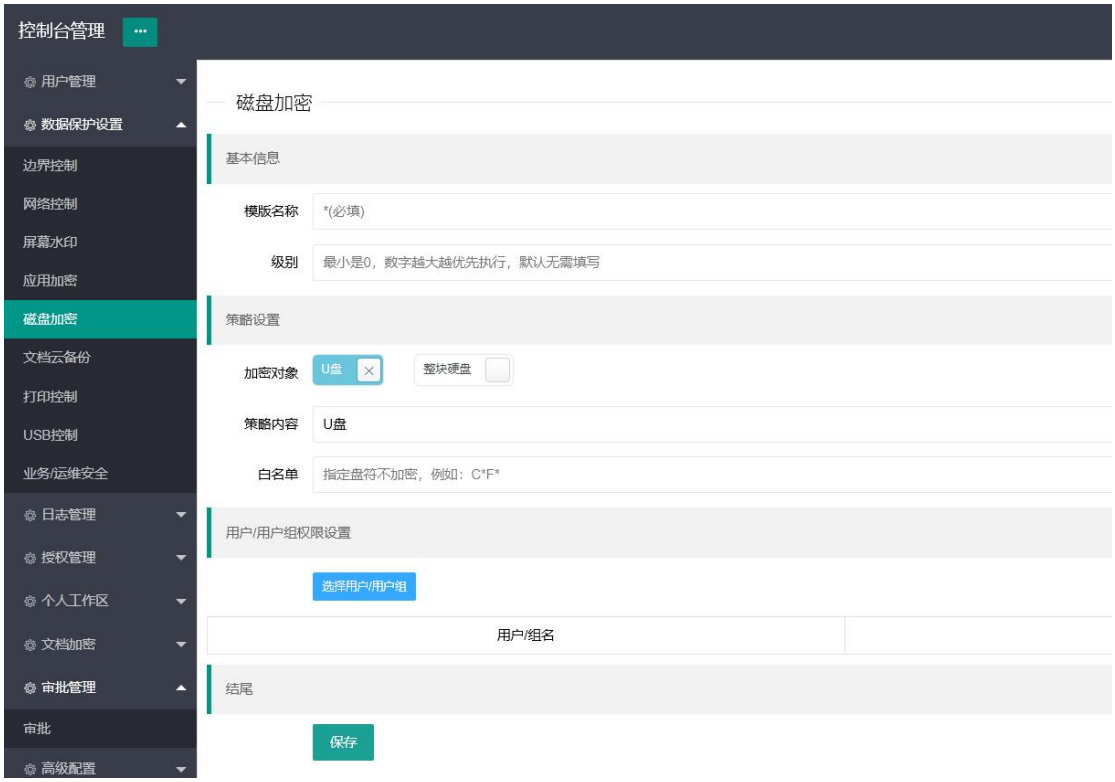
- 如要解密 u 盘，点击“解密”按钮，即完成加密 u 盘的解密动作，解密后该 u 盘恢复正常普通 u 盘，里面的内容不受任何影响。

28.2 自动加密方式

- 参考下图下发策略，终端电脑检测到 u 盘插入后会自动强制无感知加密

该 u 盘，完成 u 盘的自动加密。

- 加密 u 盘在其他非受控终端上无法使用。



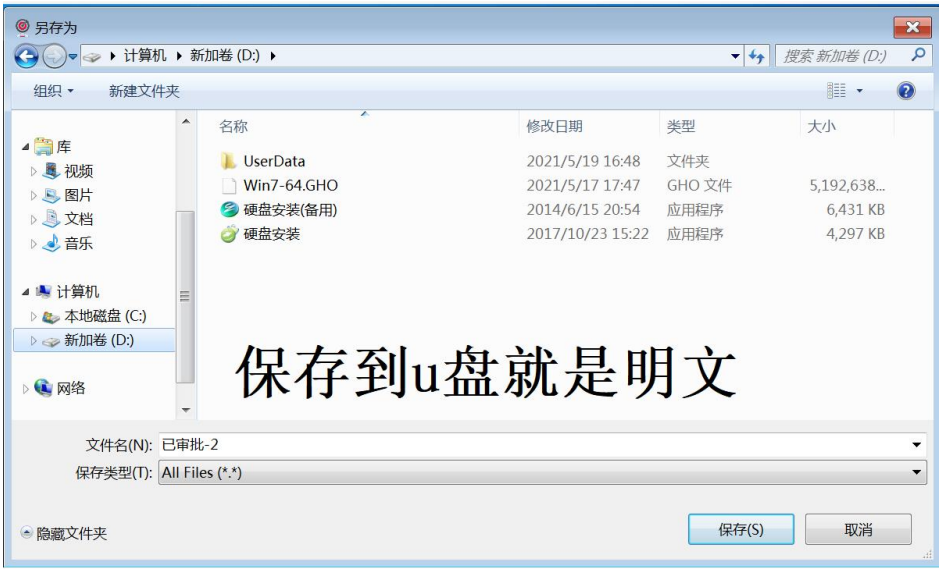
29 拷入 u 盘文档自动加密控制

- 选“环境控制”-勾选“拷入 U 盘加密”策略即可；
- 如何拷入明文？

审批后通过文件外发下载另存到 u 盘才可以完成审批解密，直接拷贝审批后的文件无法自动解密的。操作如下图所示：

外发文件列表(左键双击下载审批文件)

id	申请说明	文件名	申请时间	审批状态
1	给刘总	111.txt	2025-12-18 11:28:4	wds 完成
2	13	111.txt	2025-12-18 11:19:0	wds 完成
3	test士大夫	111.enc.txt	2025-12-18 11:16:0	wds 完成

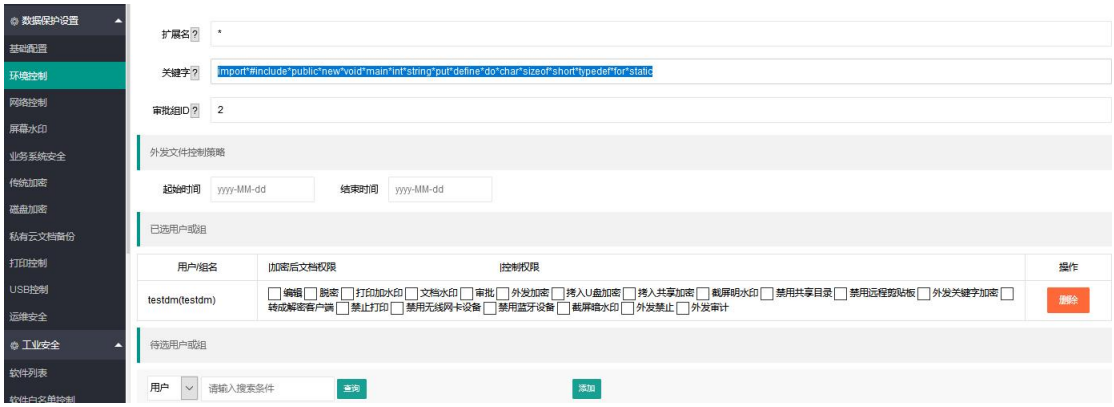


30 源码检测

- 在“环境控制”中“关键字”区域添加

import*#include*public*new*void*main*int*string*put*define*do*char*sizeof*short*typedef*for*static

- 添加受控账号



- 终端电脑右键选择一个待检测的文件夹，选择“设置自动检测源码文件夹”菜单即可

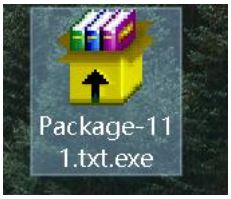
- 如果发现源代码文件，会将疑似源码文件移动到C盘CodeBack目录下面。目前支持文本类、doc、xls、ppt、docx、xlsx、pptx 、rar、zip等格式。

31 瘦客户端

瘦客户端是使用客户端将待加密的文档和客户端打包成一个 exe 应用程序，用户在浏览加密文件时无需再安装客户端。

制作瘦客户端 3 种方式：

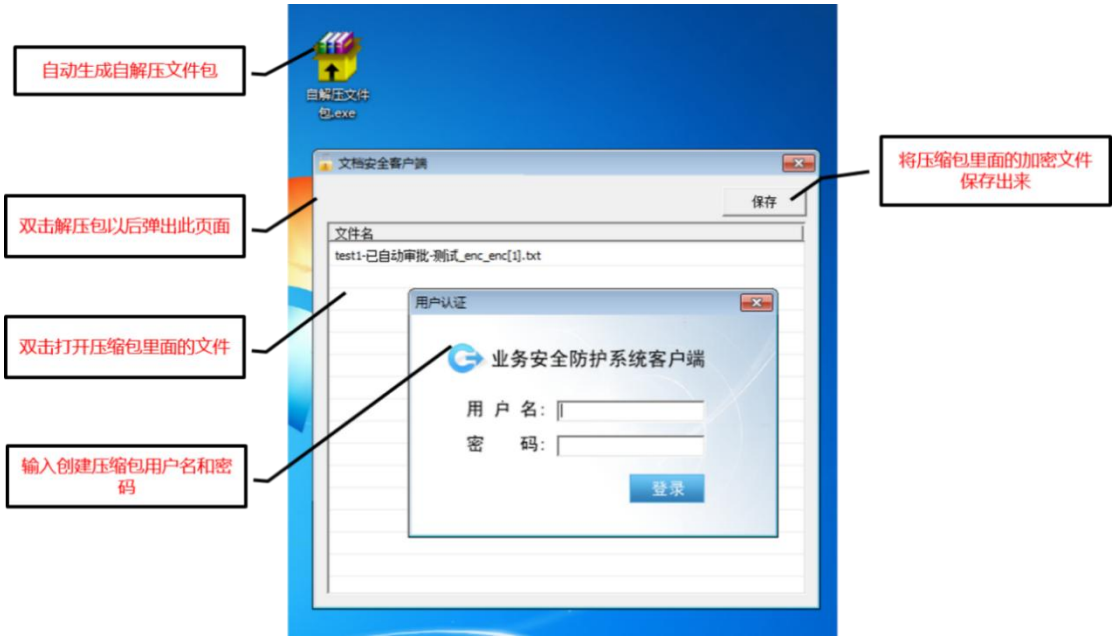
1）通过右键菜单直接生成外发瘦客户端。



2）通过云加密方式

使用瘦客户端：

双击打开瘦客户端，进行用户认证



三、 其他设置

1 服务器邮箱及企业微信配置

安装目录下 tomcat\webapps\DLP\WEB-INF\classes\wds_idlp.properties 文件

蓝色字体时企业需要后期自行设置的，请参考

邮件通知设置，用于审批时邮件通知以及邮件中审批

mail_protocol=smtp

mail_host=smtp.163.com

mail_port=25

mail_username=idlp2019@163.com

mail_key=BUYFRPRQKYVZEQZU

mail_sys_login_url=https://xxx.xxx.xxx/DLP/

效果如下图：

企业微信设置，用于审批时企业微信通知以及企业微信中审批

weixin_corpId=ww9ee4293d142079e8

weixin_corpSecret=X3cQWtlV1FtKKkevj7pnAm2JLdfQcTwNCPH9SNRI90Y

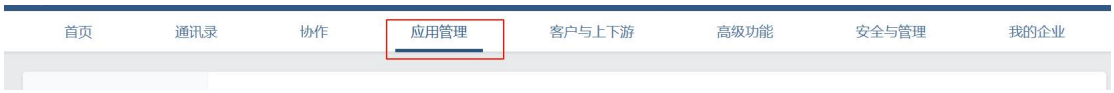
weixin_agentid=1000002

效果如下图：

✓ **获取 weixin_corpId 方法：**

最下面有个企业 id 就是 weixin_corpId

✓ **获取 weixin_corpSecret 方法：**



创建一个新的应用后，会有如下图所示

点击查看获取

✓ **获取 weixin_agentid 方法：**

创建一个新的应用后，会有如下图所示

✓ 可信 IP 设置

(3) 在对话框中输入您的公网IP地址（就是配置消息通道时显示的错误信息中的那个IP地址），然后点击"确定"保存。