

“数字替身” 数据资源防护系统  
( Digital Scapegoat Data Resource  
Protect System )  
用户使用手册 ( windows ) -v2.1.11

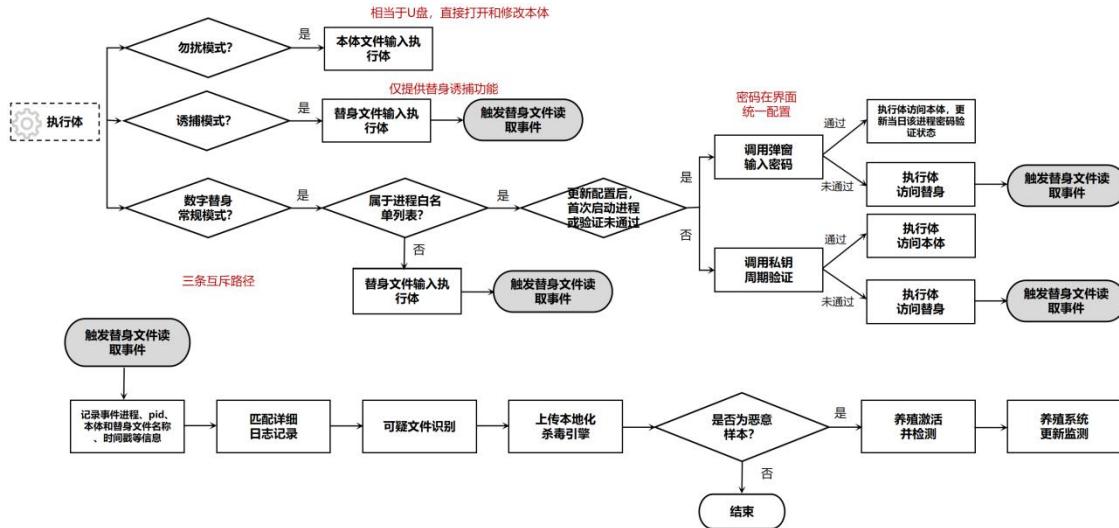
2025.1.17

# 目 录

一、软件整体工作流程 .....	2
二、软件安装与卸载 .....	3
2.1 安装“数字替身”资源防护程序 .....	3
2.2 卸载“数字替身”资源防护程序 .....	4
2.3 “数字替身”资源防护程序升级 .....	5
三、快速开始 .....	5
3.1 新用户挂载并测试文件系统 .....	5
3.2 用户日常办公持续使用系统 .....	9
(1) 用户可以新增需要防护的本体文件 .....	9
(2) 用户持续使用和修改本体文件 .....	14
(3) 用户导出本体文件 .....	14
(4) 用户开启和关闭“勿扰模式” .....	15
(5) 用户开启和关闭“诱捕模式” .....	18
3.3 用户查看系统状态 .....	21
四、详细使用手册 .....	21
4.1 防护文件列表配置 .....	21
(1) 新增待防护的本体文件 .....	21
(2) 设置替身文件模版路径和列表 .....	25
4.2 系统配置 .....	35
(1) 设置系统挂载信息 .....	35
(2) 设置身份验证信息 .....	40
(3) 设置日志采集信息 .....	46
(4) 恢复默认系统配置 .....	47
4.3 系统虚拟加密盘挂载与文件查看 .....	48
(1) 挂载文件系统 .....	48
(2) 查看文件 .....	49
(3) 修改文件 .....	54
(4) 删除文件 .....	55
(5) 重命名文件 .....	56
(6) 导出文件 .....	57
(7) 卸载文件系统 .....	60
4.4 日志采集与展示 .....	61
(1) 日志采集与停止 .....	61
(2) 日志信息表展示 .....	62

## 一、软件整体工作流程

下图详细展示了“数字替身”数据资源防护程序的整体工作流程：



当用户通过应用程序（如 Office Word、WPS、记事本等）发起文件访问行为时，首先对系统配置状态进行判断：

- (1) 如果用户已将系统设置为“勿扰模式”，则关闭用户身份验证机制，任意进程对任意被防护文件都可直接访问到本体。
- (2) 如果用户已将系统设置为“替身模式”，任意进程对任意被防护文件都将直接重定向到替身模版文件。
- (3) 如用户未设置以上两种模式，则为软件常规使用状态。每个应用程序进程当日新挂载文件系统后首次访问被防护文件时，会弹出密码验证框，需要用户手动输入验证密码。

如果密码输入正确，身份验证通过，用户能够通过该应用程序进程访问到本体文件，同时，该进程后续的身份验证将通过私钥签名验证的方式在后台完成。

如果用户输入错误密码或超时未输入密码，则该应用程序进程对本体文件的访问将被重定向到替身模版文件，同时，该进程后续的身份验证仍将弹出密码验证框，直至用户输入正确密码。

对于每个进程，身份验证状态（通过/未通过）默认有效期为 1 分钟，即每次验证 1 分钟后，进程再次对被防护文件执行打开、保存等操作时，仍将再次发起验证。

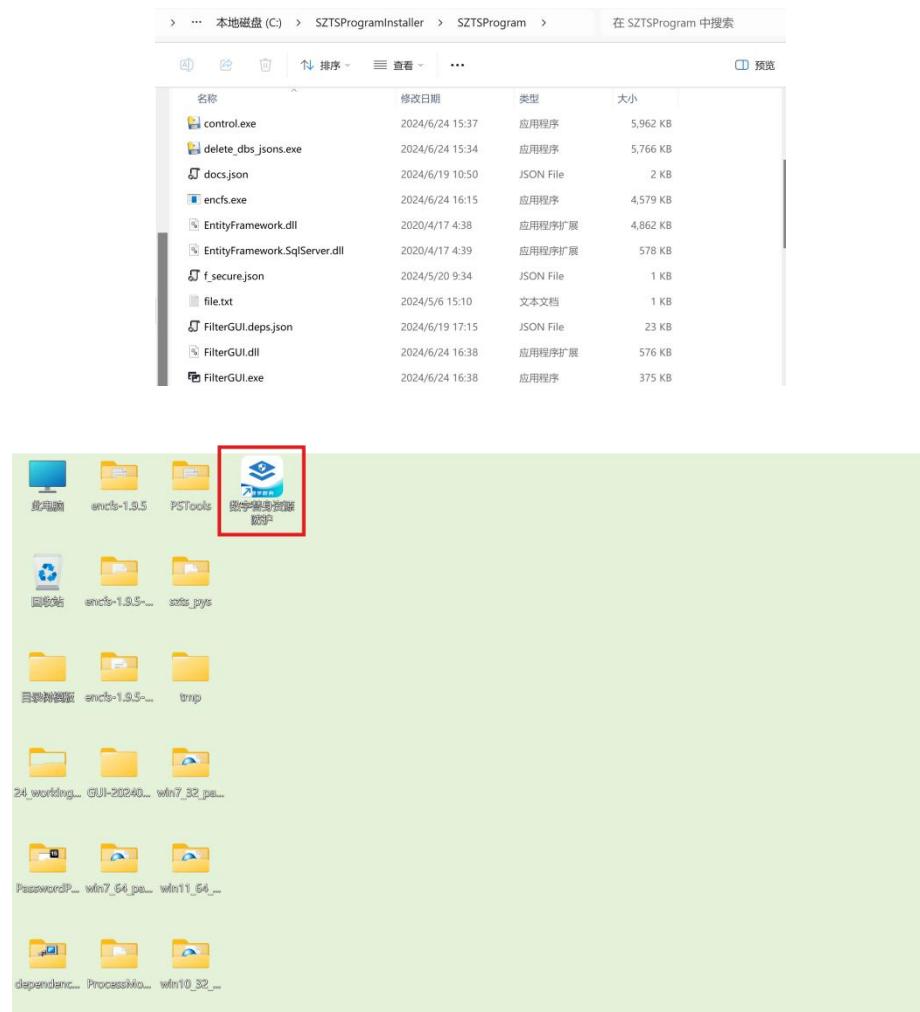
另外，系统设置了可配置的进程白名单列表，包含对查看和编辑 txt、doc、docx、pdf、ppt、pptx、xls、xlsx、csv 等文件类型的常规软件进程及依赖的系统进程。白名单列表之外的进程对于被防护文件的访问将直接被重定向到替身模版文件。

当用户打开日志采集功能时，系统将持续采集设备全量运行状态日志，并根据用户设置的文件路径关键字进行日志筛选和入库存储。对于触发了替身模版文件操作行为的潜在攻击事件，系统将在日志数据库历史数据中进行匹配和关联分析，筛选并统一存储潜在可疑文件，用于后续分析研判。

## 二、软件安装与卸载

### 2.1 安装“数字替身”资源防护程序

运行 `DAIDeveloperProgramInstaller.exe` 安装程序，默认安装路径为 `C:\SZTSProgramInstaller\SZTSProgram`，目前暂不支持安装路径的修改)，安装期间弹出的提示信息请均选择“允许”。安装完成后，桌面出现“数字替身”资源防护程序快捷方式，相应程序和数据文件存储在 `C:\SZTSProgramInstaller\SZTSProgram` 中。

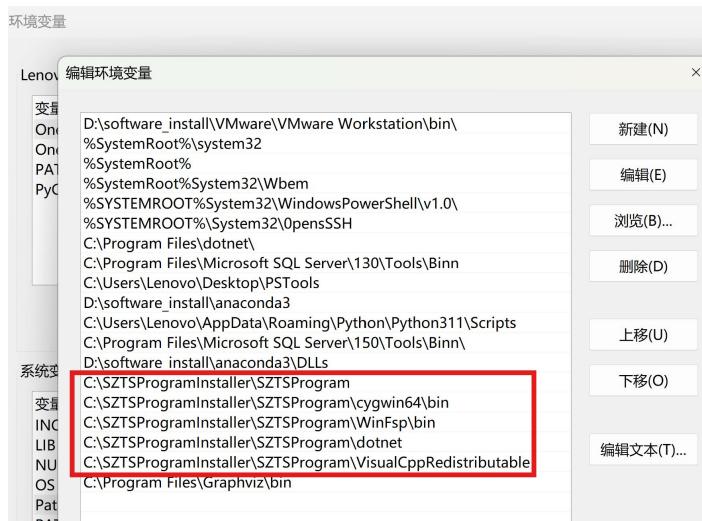
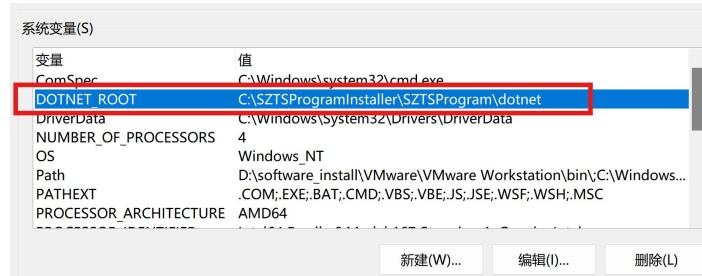


安装程序会自动创建 `C:\SZTSProgramInstaller\SZTSConfig` 目录，用于存放系统配置文件和日志文件。

名称	修改日期	类型	大小
szts_encdir	2024/7/17 20:18	文件夹	
目录树模版	2024/7/17 20:18	文件夹	
docs.json	2024/6/25 18:43	JSON File	2 KB
f_secure.json	2024/6/19 11:38	JSON File	1 KB
forms.json	2024/7/5 16:03	JSON File	1 KB
graph.png	2024/7/2 15:56	PNG 文件	380 KB
szts_log.db	2024/7/2 12:40	Data Base File	1,776 KB

其中：

- “szts\_encdir” 文件夹为示例加密文件目录，对应的解密挂载密码为 12345678，目录中的文件名和文件内容均为密文形态。程序启动后，系统默认解密挂载此目录，提供本体文件和替身文件模版供用户初步使用，用户可在此基础上添加自己想要防护的本体文件和配置替身文件模版；
- “目录树模版” 文件夹提供示例本体文件、不同类型替身文件模版目录树；安装程序会自动创建 cygwin64、dotnet、winfsp 等相关环境变量以确保程序和依赖库正常运行。



## 2.2 卸载“数字替身”资源防护程序

运行 C:\SZTSPProgramInstaller\Uninstall\unins000.exe 即可卸载“数字

替身”资源防护程序。或可通过 Windows 设置——应用进行卸载：



## 2.3 “数字替身”资源防护程序升级

暂定升级方案：程序支持差量自动升级，每次软件 GUI 界面启动时将调用升级程序。升级程序将检查服务端是否有新上传的离线升级包，如有则下发更新后的程序文件至客户端。

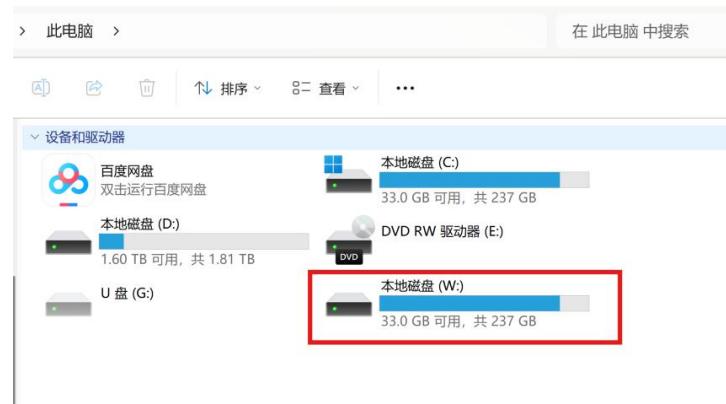
完成升级后，弹窗提示用户“已成功更新软件至某版本，请重新启动程序！”。用户需自行启动“数字替身”资源防护 GUI 界面程序，界面顶端版本号将更新为最新版本号，虚拟盘挂载程序将在后台自动重启。

## 三、快速开始

### 3.1 新用户挂载并测试文件系统

(1) 用户安装软件并启动“数字替身”资源防护快捷方式后，可以直接使用 GUI 界面中显示的系统全部默认配置信息。点击“挂载文件系统”，此时将使用示例加密文件目录 C:/SZTSPProgramInstaller/SZTSConfig/szts\_enkdir，自动解密挂载目录 (szts\_dir 目录对应密码为默认密码 12345678)。同时，系统文件资源管理器中将出现新盘符 W: 盘（如果未出现刷新一下文件目录列表即可）。点击“卸载文件系统”，系统文件资源管理器中 W: 盘将消失。

在 Windows 文件资源管理器中，W: 盘的总大小、已使用空间、剩余可用空间与挂载的加密文件目录位置所在磁盘相应信息一致（默认为 C: 盘，如将加密盘挂载路径设置为 D 盘下某一路经，则 W: 盘显示的总大小与可用空间等信息与 D: 盘一致。），W: 盘中存储的文件也使用该磁盘存储空间。





(2) 用户点击进入 W 盘“敏感文件资料”目录，显示默认的 7 个不同类型的本体文件；替身文件模版默认存储在 W 盘/敏感文件资料/temp/替身文件模版/文件夹下，包括 11 种格式文件的替身模版（txt、doc、docx、pdf、ppt、pptx、xls、xlsx、csv、json、md）。

此电脑 > 本地磁盘 (W:) > 敏感文件资料 >					在 敏感文件资料 中搜索
	名称	修改日期	类型	大小	操作
📁	raw-本体测试目录	2024/9/11 15:55	文件夹		...
📁	temp	2024/9/11 15:55	文件夹		...
📄	raw-docx版本-本体测试文件.docx	2024/7/30 11:25	DOCX 文档	11 KB	...
📄	raw-json版本-本体测试文件.json	2024/9/5 9:40	JSON 源文件	1 KB	...
📄	raw-md版本-本体测试文件.md	2024/9/5 9:37	Markdown 源文件	1 KB	...
📄	raw-pdf版本-本体测试文件.pdf	2024/6/24 10:58	WPS PDF 文档	51 KB	...
📄	raw-pptx版本-本体测试文件.pptx	2024/6/24 10:59	PPTX 演示文稿	56 KB	...
📄	raw-txt版本-本体测试文件.txt	2024/6/24 10:59	文本文档	1 KB	...
📄	raw-xlsx版本-本体测试文件.xlsx	2024/6/24 10:59	XLSX 工作表	10 KB	...

接下来，用户可以对被防护的本体文件和文件夹进行逐一测试。当用户通过某应用程序查看文件时，如果该应用程序是当日新挂载文件系统后首次访问被防护文件，将弹出密码验证框，需要用户输入身份认证密码（**默认为 123456**，可以在“数字替身系统配置——设定身份验证信息”界面中修改）。如果密码正确则打开正确的文件内容，同时该应用进程后续的身份验证将通过私钥签名验证的方式在后台完成；密码错误/超时未输入（默认 20 秒）/取消输入则打开替身文件内容，该进程后续的身份验证仍将弹出密码验证框。

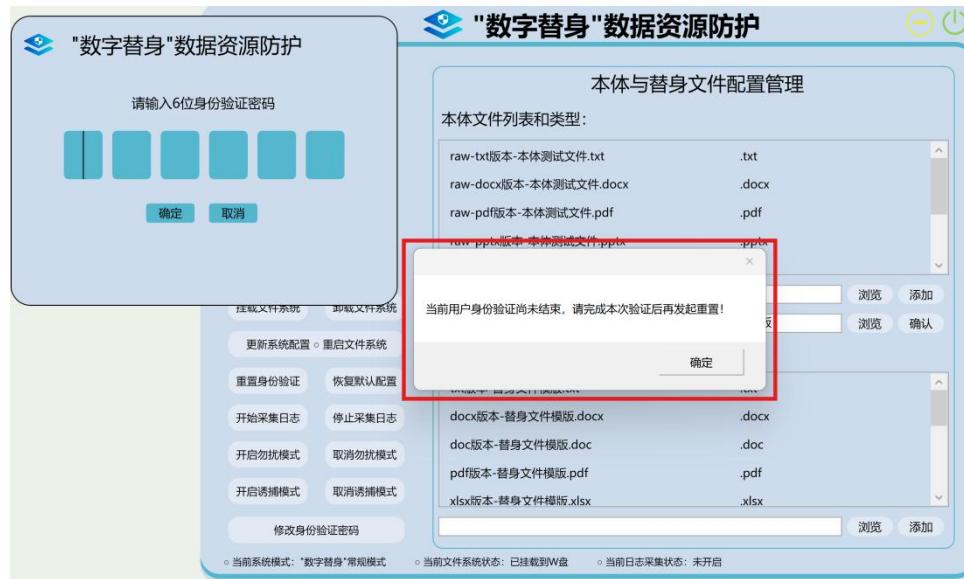
用户可以使用记事本、Notepad++、Sublime Text 等应用对 txt 格式文件进行测试，使用 WPS、Office-Word/PowerPoint/Excel、Adobe Acrobat 等应用对 docx/pptx/xlsx/pdf 格式文件进行测试。

经过身份验证后，在未超过身份验证有效时间时（默认 1 分钟）再次访问其他本体文件，将直接根据上一次身份验证结果打开本体或替身文件，否则会重新发起身份验证。验证通过时打开本体文件，验证未通过打开替身文件。

- ❖ **注意：**如果合法用户首次通过某应用程序访问本体文件时输入错误密码导致身份验证失败，在身份验证有效期内（默认 1 分钟）均只能获取到替身模版文件。此时如用户不想等待下一轮密码验证，可点击“**重置身份验证按钮**”，该按钮将重新挂载文件系统，用户再次访问本体文件时可重新输入密码。



另外，当用户点击“**重置身份验证按钮**”时，如果存在已启动且未完成的身份验证密码弹窗进程，将拒绝重置并提示“当前用户身份验证尚未结束，请完成本次验证后再发起重置”：



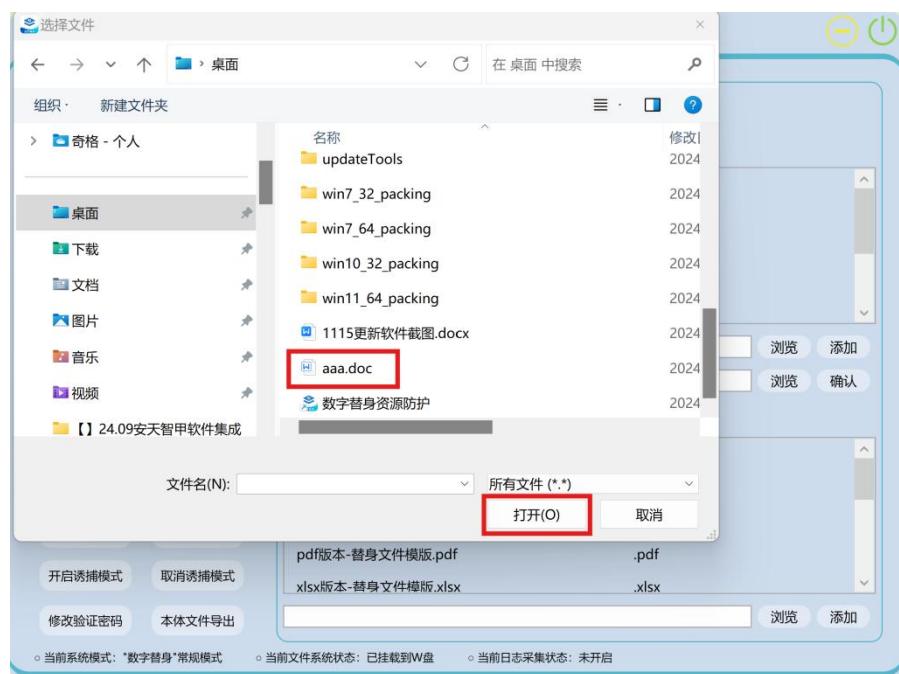
### 3.2 用户日常办公持续使用系统

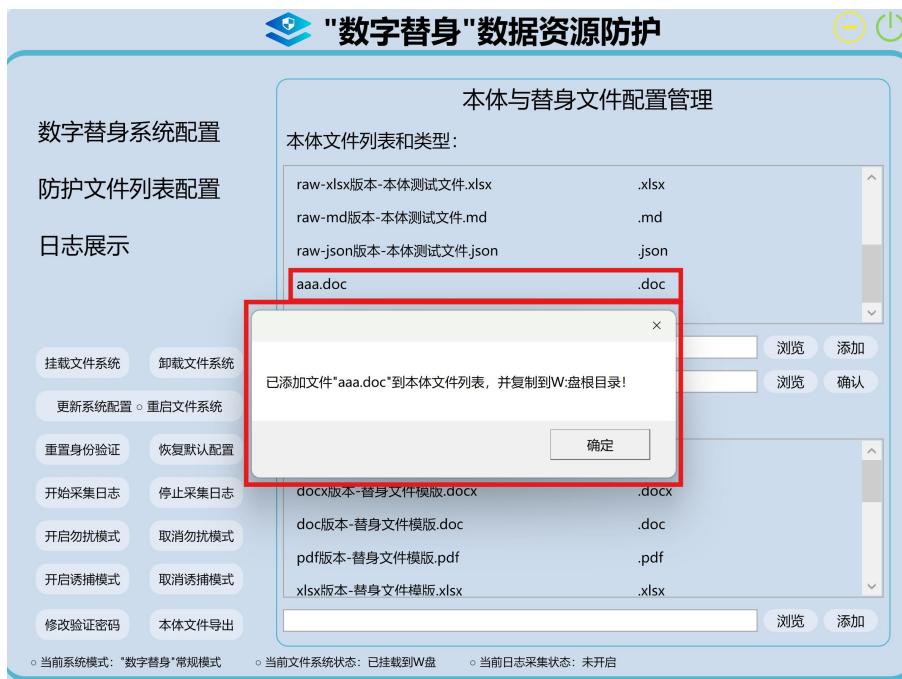
用户日常办公中持续使用“数字替身”资源防护系统，主要涉及两个操作：1) 新增需要防护的本体文件；2) 持续使用和修改本体文件。具体测试过程如下：

#### (1) 用户可以新增需要防护的本体文件

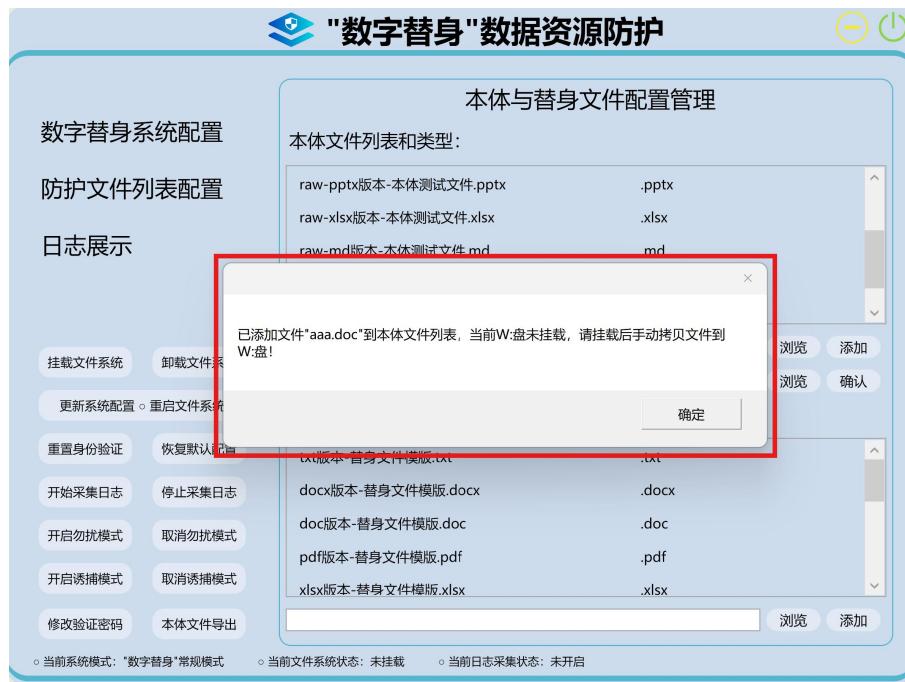
例如用户希望防护桌面上的个人文件 aaa.doc，则点击“防护文件列表配置——本体文件列表和类型”下方文本框右侧“浏览”按钮，在弹出的文件目录浏览器界面中导航到桌面并选中 aaa.doc 文件，点击“打开”。被选中的文件名将显示在文本框中，然后点击“添加”，本体文件列表和类型出现对应的新增项：





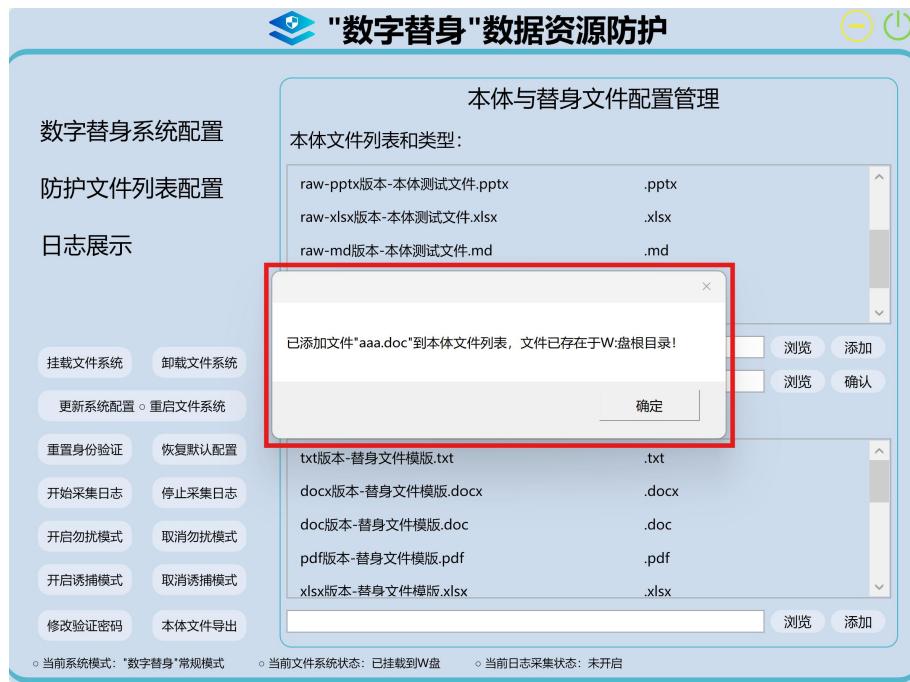


如果此时 W 盘处于挂载状态，系统会自动将该 aaa.doc 文件拷贝到 W 盘根目录下。如果当前尚未挂载文件系统，将提示用户挂载文件系统后手动拷贝该文件到 W: 盘中。注意，虚拟盘符中任意文件夹路径下命中防护文件列表中文件名的文件都将被系统作为本体文件。

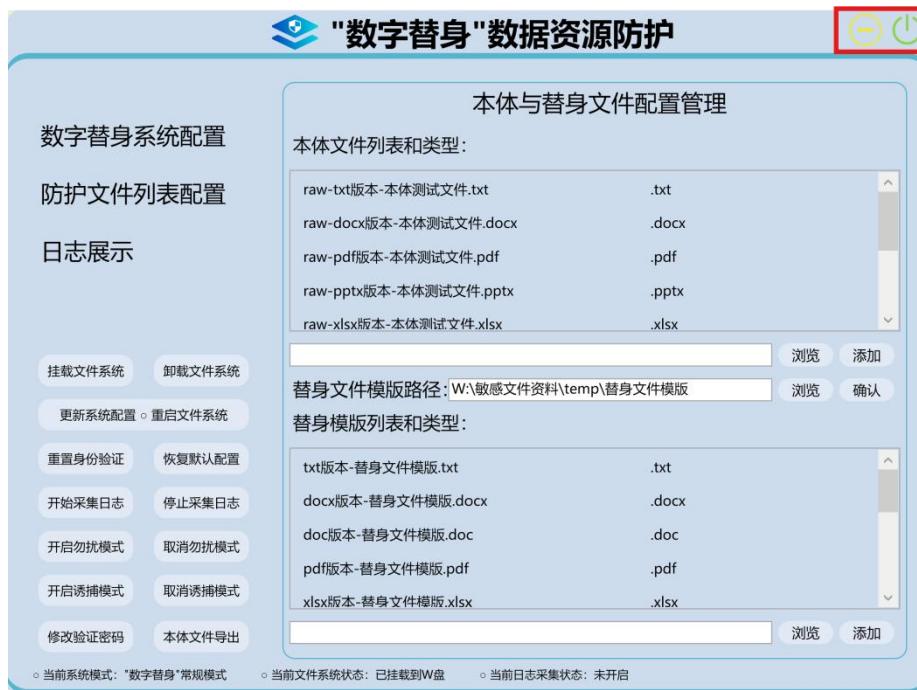


用户也可以直接在 W: 盘中任意目录位置新建想要增加的防护文件 aaa.doc，然后通过“浏览”按钮选中新建的 aaa.doc 并点击“添加”。此时对 aaa.doc 文件的防护生效，同时文件不会被移动或复制到其他路径：

此电脑 > 本地磁盘 (W:) > 敏感文件资料 >		在 敏感文件资料
		修改日期
名称		修改日期
raw-本体测试目录		2024/8/28 9:27
temp		2024/8/28 9:27
aaa.doc		2024/8/28 9:35
raw-docx版本-本体测试文件.docx		2024/7/30 11:25
raw-pdf版本-本体测试文件.pdf		2024/6/24 10:58
raw-pptx版本-本体测试文件.pptx		2024/6/24 10:59
raw-txt版本-本体测试文件.txt		2024/6/24 10:59
raw-xlsx版本-本体测试文件.xlsx		2024/6/24 10:59



完成系统挂载后，可点击 GUI 界面右上角左侧最小化按钮，将程序最小化到托盘，日常使用中无需开启 GUI。需要修改配置信息或卸载文件系统时，单击托盘中图标即可恢复原始 GUI 界面。点击界面右上角右侧关闭按钮即可退出 GUI 界面程序。



用户安装“数字替身”资源防护程序后，仅支持启动并运行一个 GUI 程序进程（包括托盘中程序）。当设备关闭后再开启时，GUI 界面程序会自启动并最

小化至托盘。同时，文件系统将自动挂载并显示虚拟盘符。

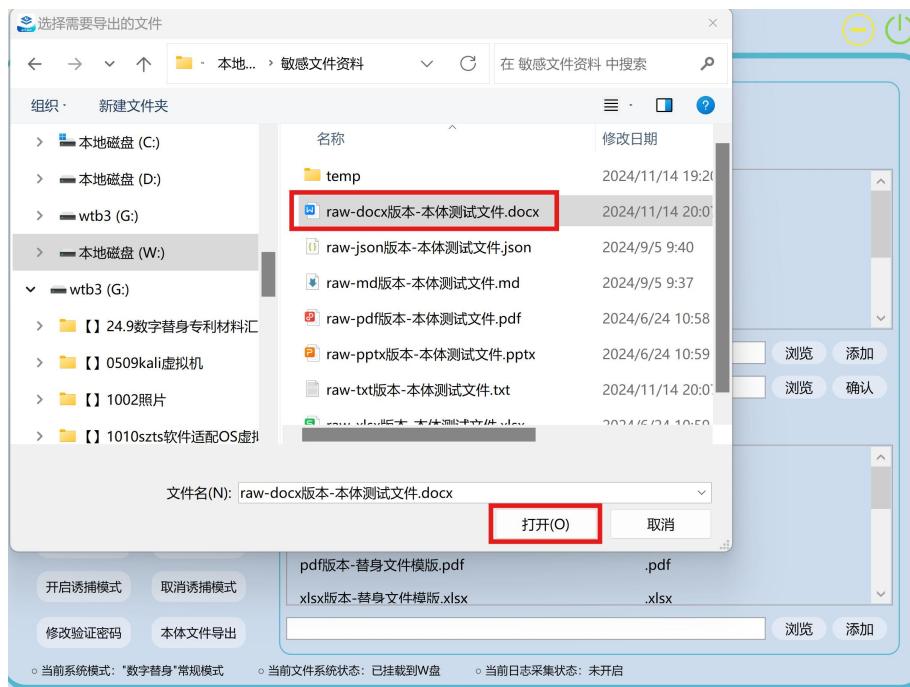
## (2) 用户持续使用和修改本体文件

用户打开本体文件，输入正确密码，然后对文件进行更新，保存时，如果超过身份验证有效期（默认1分钟），将通过私钥签名验证的方式在后台重新进行身份验证，无需用户重新输入密码。

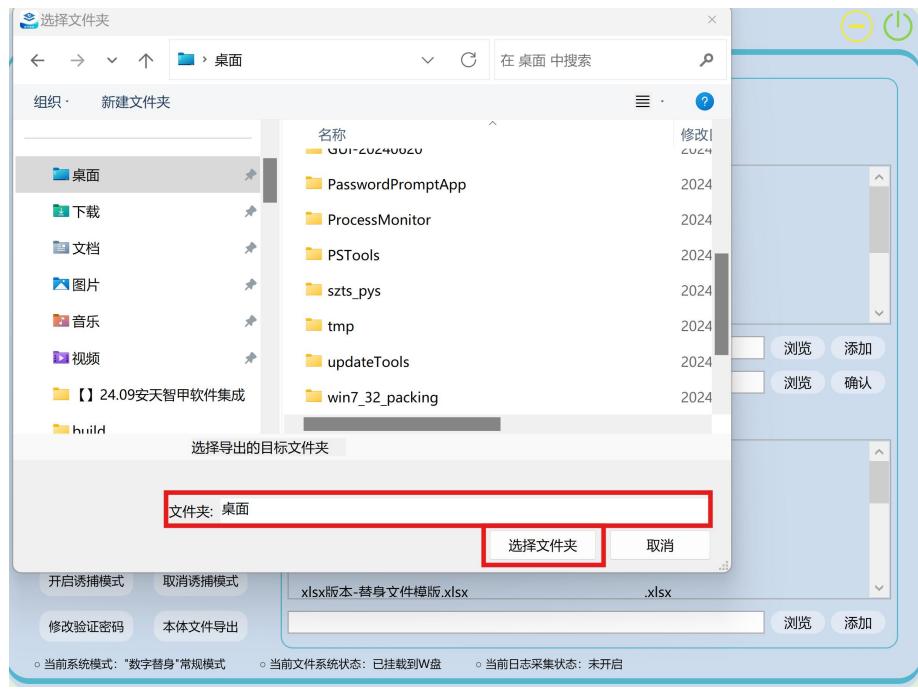
实际使用中，建议用户将进程身份验证有效时间改长（如设置为60分钟），避免打开和保存文件时频繁身份验证。

## (3) 用户导出本体文件

如果用户将W盘中的文件导出到设备其他磁盘路径，需通过软件GUI界面操作。点击“本体文件导出”按钮，将弹出第一个文件目录浏览框，用户选择W盘中需要导出的文件（如raw-docx版本-本体测试文件.docx）。



选中文件并点击“打开”后，将弹出第二个文件目录浏览框，用户选择要导出的目标文件夹（如桌面），点击“选择文件夹”后，弹出密码验证框。输入正确密码后，弹窗提示“文件已成功导出到目标文件夹”，W盘中 raw-docx 版本-本体测试文件.docx 文件被正确导出到桌面，可以直接打开查看。如果输入错误密码，将弹窗提示“身份认证失败，无法导出文件”。



- ❖ **注意：**如果用户直接将 W 盘中文件复制到设备其他磁盘路径，被复制出来的文件将无法正确打开。使用记事本、WPS、Office 等应用打开 txt/docx/pptx/pdf/xlsx 等格式文件将显示空文件或文件格式无效等相关提示。

#### (4) 用户开启和关闭“勿扰模式”

当用户对当前设备操作环境安全性充分信任时，可点击“开启勿扰模式”按钮，将以勿扰模式重新挂载磁盘，此后任意进程对本体文件的打开和修改等操作均不再需要密码弹窗身份验证和私钥签名验证。点击“开启勿扰模式”后将弹出密码验证框，输入正确身份验证密码后才能够成功切换模式，否则将提示“身份验证失败，无法开启勿扰模式”。





点击“取消勿扰模式”，将恢复对本体文件访问的正常身份验证机制。



用户无法同时处于“勿扰模式”和“诱捕模式”，当在“诱捕模式”状态下点击“开启勿扰模式”，无法成功设置。



## (5) 用户开启和关闭“诱捕模式”

当用户暂时离开当前设备或暂不操作防护文件时，可点击“开启诱捕模式”按钮，将以替身诱捕模式重新挂载磁盘，此后任意进程对本体文件的打开和修改等都将直接重定向到替身模版文件。点击“取消诱捕模式”，将恢复对本体文件访问的正常身份验证机制。

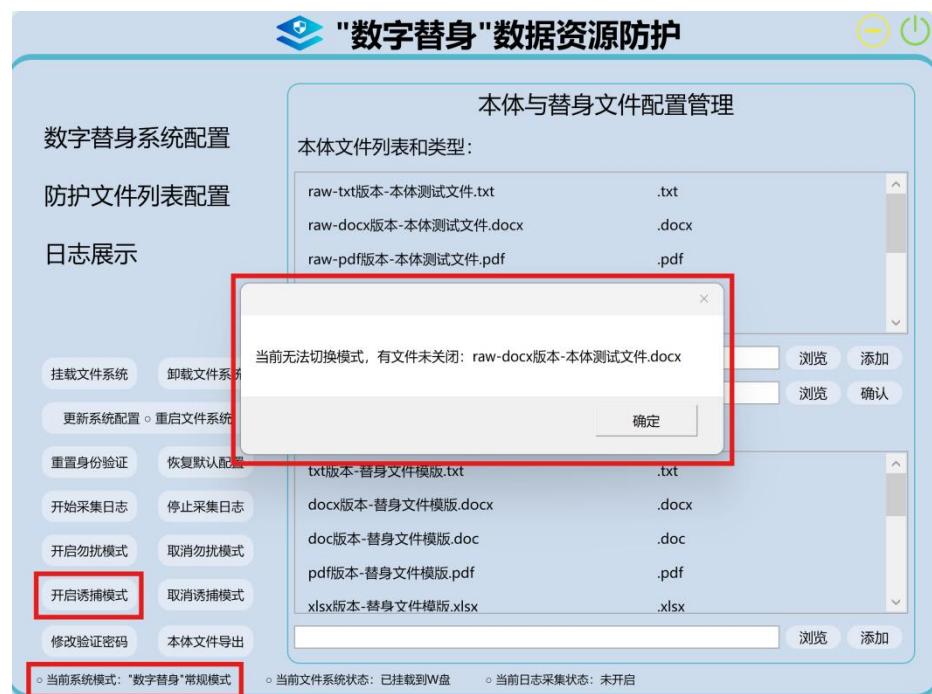




用户无法同时处于“勿扰模式”和“诱捕模式”，当在“勿扰模式”状态下点击“开启诱捕模式”，无法成功设置。



当用户通过按钮操作在“数字替身”常规模式、“勿扰模式”、“诱捕模式”之间切换时，如有文件通过WPS或Office Word/Powerpoint/Excel程序打开，会提示“当前无法切换模式，有文件未关闭”，需用户关闭相应文件才能完成切换，避免切换模式导致的文件查看、写入、保存错误或与模式状态存在不一致。（此功能目前仅适用于WPS和Office Word/Powerpoint/Excel应用打开本体情况。）



### 3.3 用户查看系统状态

“数字替身”数据资源防护软件 GUI 界面底部实时显示三组系统当前状态信息，包括“当前系统模式”（“数字替身”常规模式/勿扰模式/诱捕模式）、“当前文件系统状态”（已挂载到某盘/未挂载），“当前日志采集状态”（已开启/未开启）。



## 四、详细使用手册

### 4.1 防护文件列表配置

启动“数字替身”资源防护快捷方式，GUI 默认显示“防护文件列表配置”子界面。

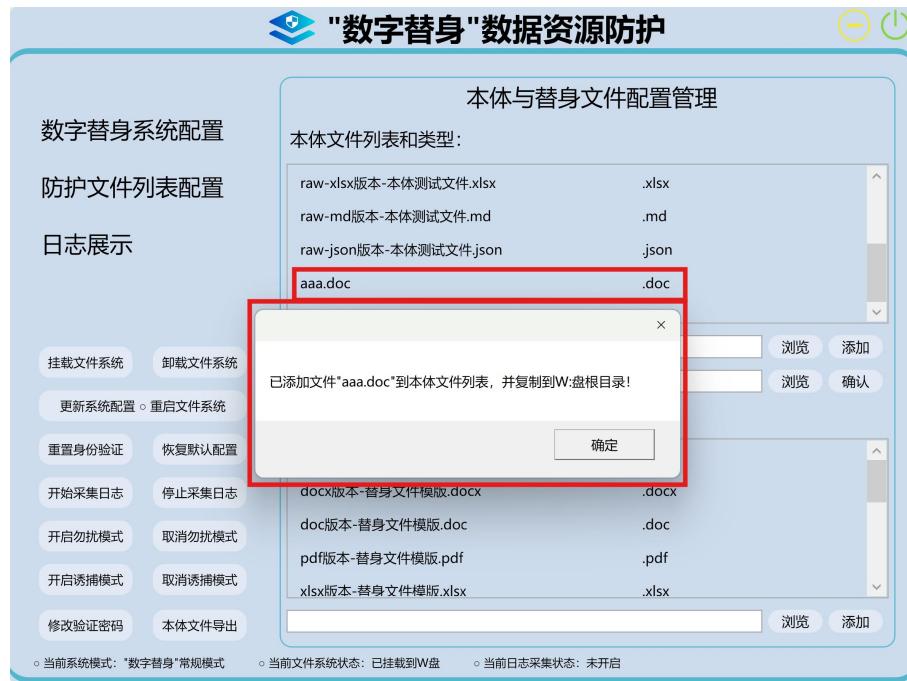
#### (1) 新增待防护的本体文件

“本体文件列表和类型”窗口预先显示 7 个默认被防护的本体文件。

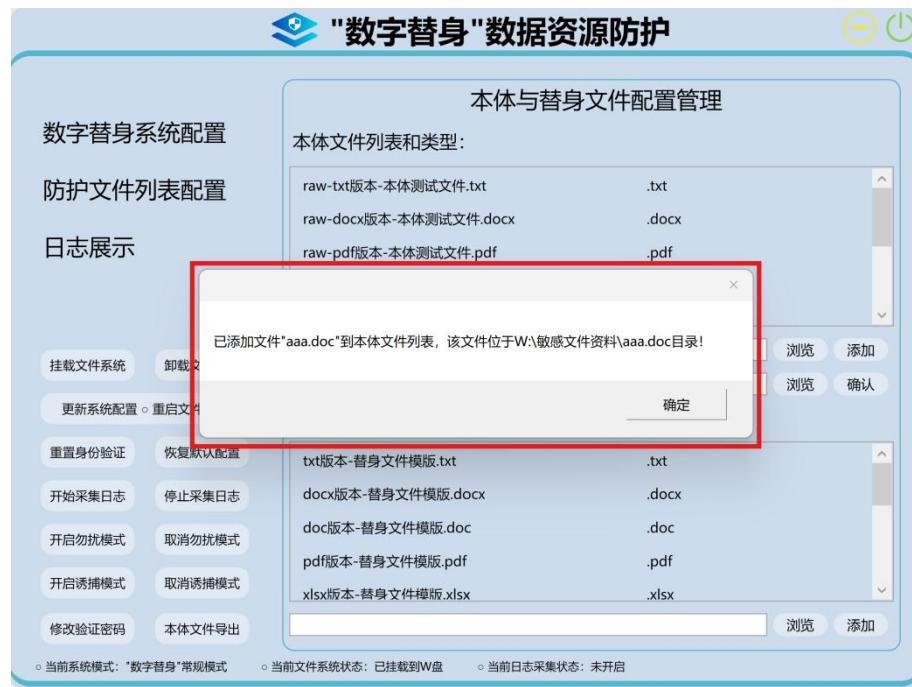


用户希望增加防护文件时，点击在白色文本框右侧“浏览”按钮，选中目标文件，点击“添加”按钮，系统将自动识别文件扩展名类型并添加到配置文件中。

如果用户选中的目标文件位于设备其他磁盘上，当添加防护文件到本体文件列表后，如果当前已挂载文件系统，新增的防护文件将自动被拷贝到挂载的虚拟盘符根目录中（如 W: 盘根目录）：



如果用户选中的目标文件本身即为用户在虚拟盘（如 W: 盘）中新建的文件或已经被预先拷贝到 W: 盘某目录下的文件，文件不会被移动或复制：

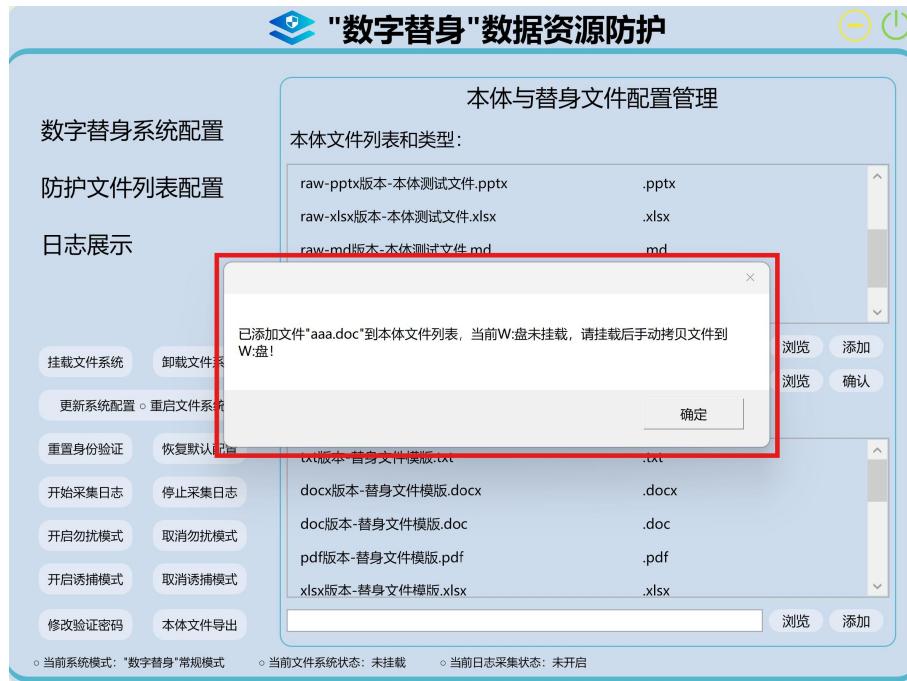


如果用户选中的目标文件位于设备其他磁盘上，但 W: 盘根目录中已存在该名称的文件，则不会重复复制并覆盖文件。



如果当前尚未挂载文件系统，将提示用户挂载文件系统后手动拷贝该文件到新增的虚拟盘符（如 W: 盘）中。注意，虚拟盘符中任意文件夹路径下命中防

护文件列表中文件名的文件都将被系统作为本体文件。

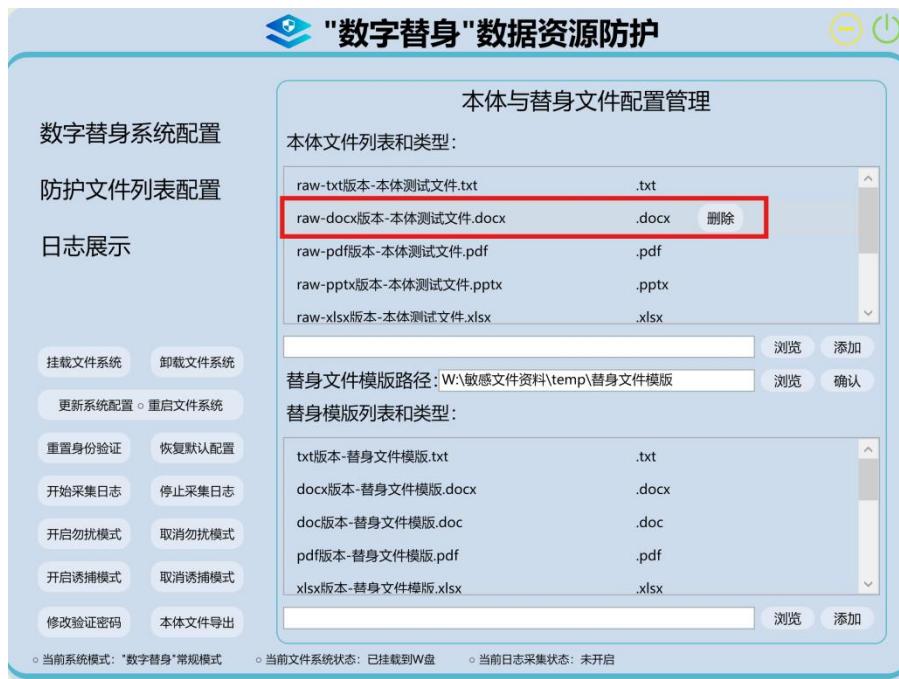


仅支持通过浏览选中方式添加本体文件，如用户手动在白色文本框中输入文件名称或文件路径，会弹出相应错误提示：



需要删除某个本体文件时，点击列表中的文件名，出现“删除”按钮，点击即可。注意，删除本体文件列表中的文件名只会更新软件对于被防护的文件

名的配置，不会同步删除虚拟盘符（如 W: 盘）中的真实文件。



- ❖ **注意：**如果某文件被设置为替身模版文件，则无法被添加到本体文件列表中，添加时将显示提示“本体文件不可以与替身模版文件重名！”



## (2) 设置替身文件模版路径和列表

点击“替身文件模版路径”右侧“浏览”按钮，可以选择替身文件模版存储位置，点击“确认”后保存。目前仅支持设置虚拟盘（如 W: 盘）内目录作为

替身文件模板路径，否则将弹出错误提示。默认替身模版均存放在“W:/敏感文件资料/temp/替身文件模版/”目录中。同时，如果虚拟盘为挂载导致无法设置正确的替身文件模版路径，也将弹出错误提示“请先挂载文件系统到W盘后再设置替身文件模版路径”。





系统默认设置 11 个模版替身文件，分别对应 txt、docx、doc、pdf、xlsx、xls、csv、pptx、ppt、json、md 11 种文件类型，即本体文件会根据其文件类型多对一对应到相应的替身模版文件上。当用户设置新的“替身文件模版路径”并点击“确认”时，会自动拷贝 11 个模版替身文件到新的“替身文件模版路径”目录中。

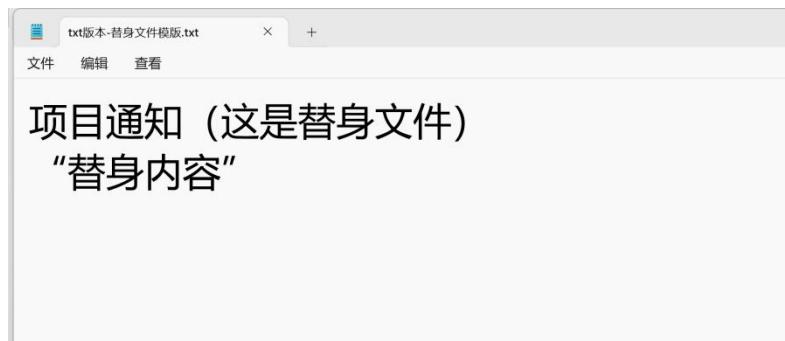


替身模版文件列表：

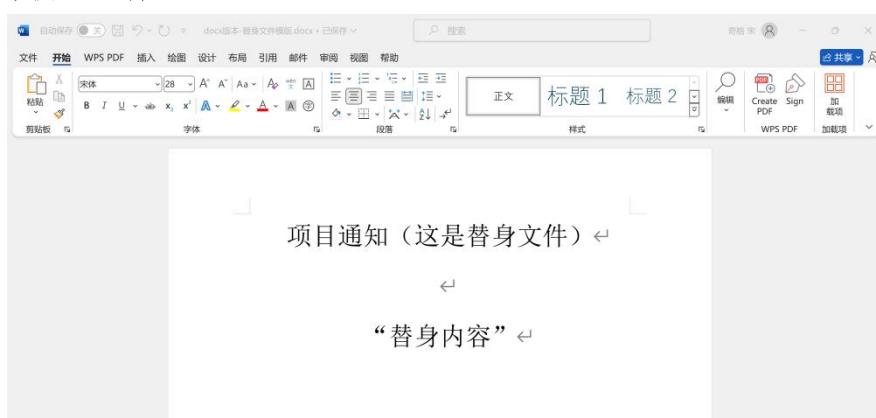
... 敏感文件资料 > temp > 替身文件模版 > 在 替身文件模版

名称	修改日期	类型	大小
szts_temp	2024/9/11 15:55	文件夹	
项目通知文件目录	2024/9/11 15:55	文件夹	
csv版本-替身文件模版.csv	2024/6/12 16:42	XLS 工作表	1 KB
docx版本-替身文件模版.docx	2024/6/12 16:31	DOCX 文档	13 KB
doc版本-替身文件模版.doc	2024/6/12 16:32	DOC 文档	13 KB
json版本-替身文件模版.json	2024/9/5 9:41	JSON 源文件	1 KB
md版本-替身文件模版.md	2024/9/5 9:38	Markdown 源文件	1 KB
pdf版本-替身文件模版.pdf	2024/5/10 18:47	WPS PDF 文档	29 KB
pptx版本-替身文件模版.pptx	2024/6/12 16:44	PPTX 演示文稿	36 KB
ppt版本-替身文件模版.ppt	2024/6/12 16:45	PPT 演示文稿	88 KB
txt版本-替身文件模版.txt	2024/5/11 15:23	文本文档	1 KB
xlsx版本-替身文件模版.xlsx	2024/6/12 16:34	XLSX 工作表	11 KB
xls版本-替身文件模版.xls	2024/6/12 16:35	XLS 工作表	26 KB

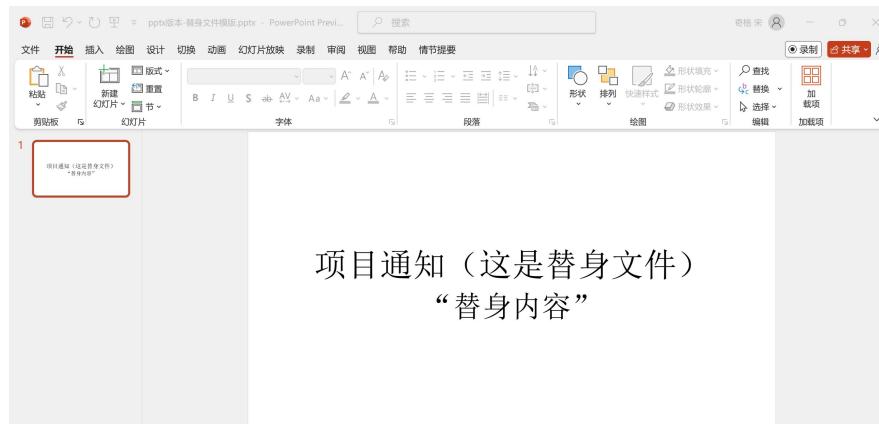
txt 替身模版文件:



docx 替身模版文件:



pptx 替身模版文件:

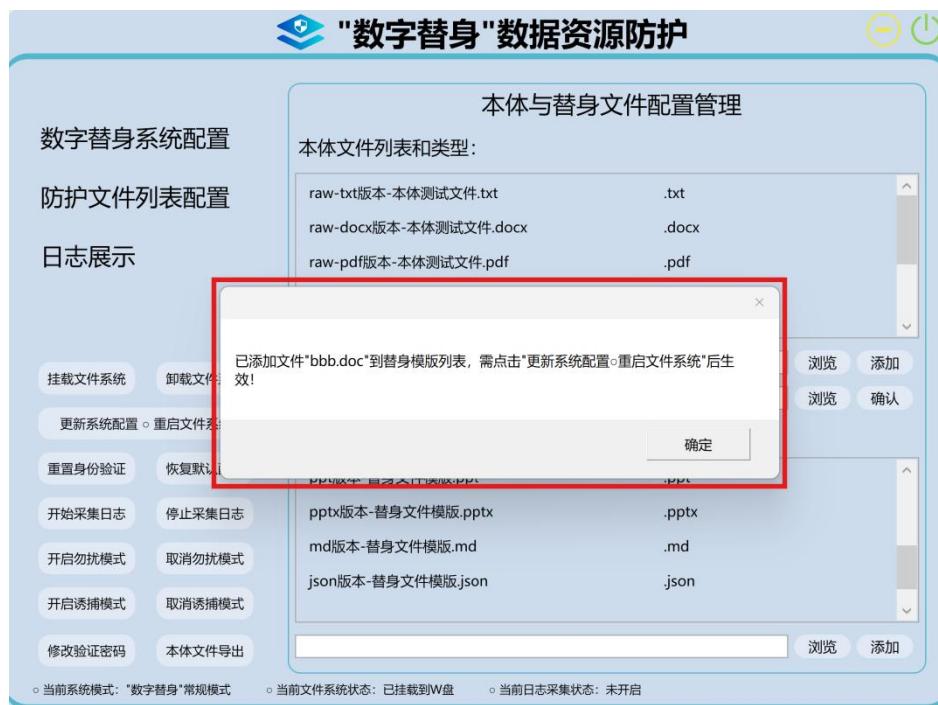
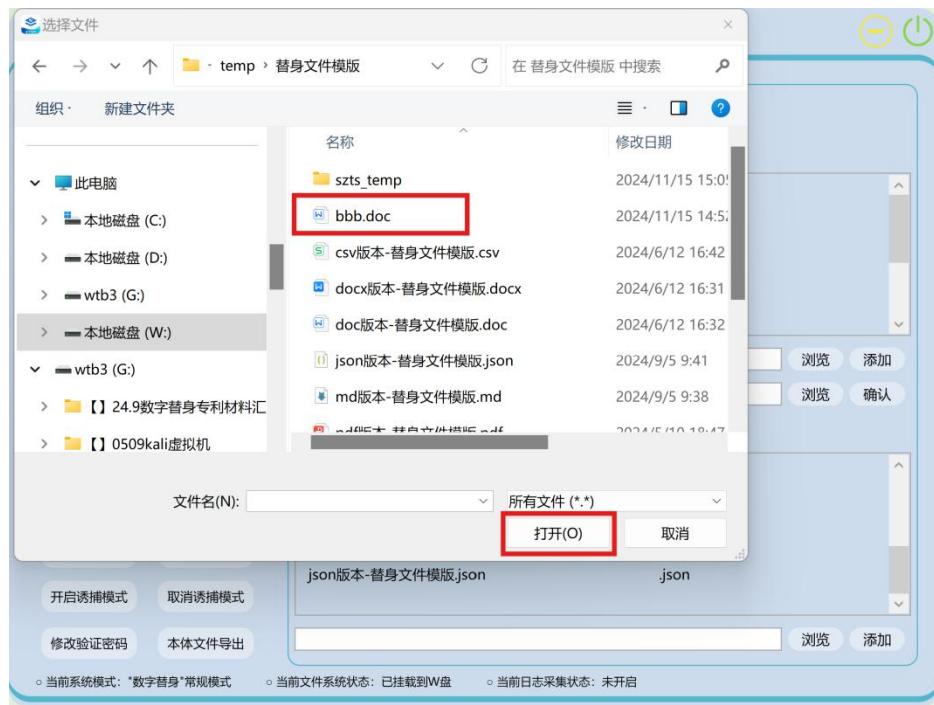


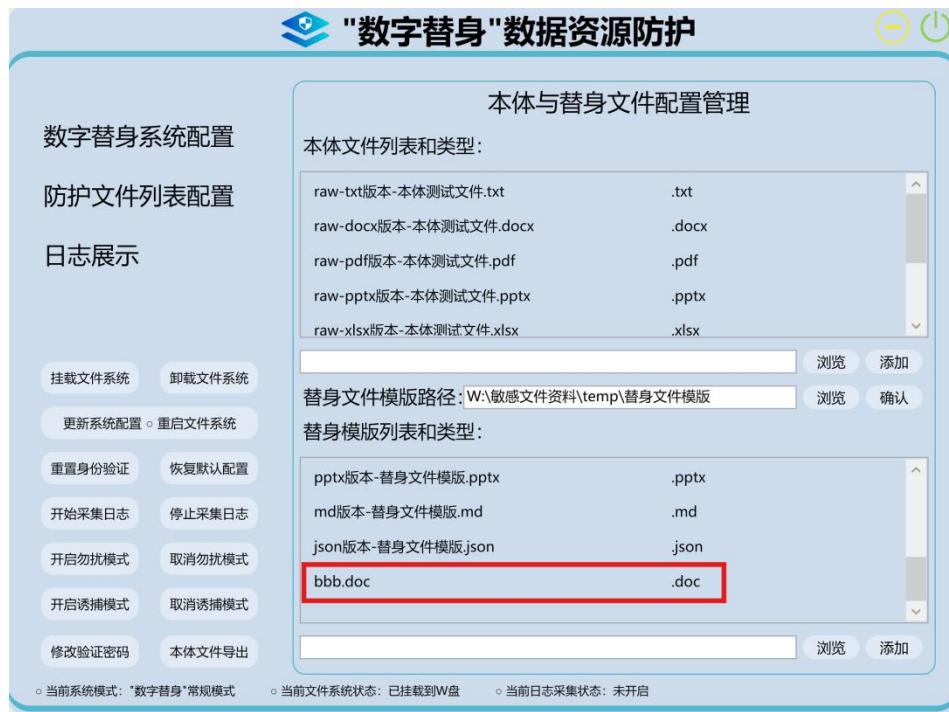
### xlsx 替身模版文件:

	A	B	C	D	E	F	G	H	I	J
1	这是替身文件									
2	姓名	年龄	性别	手机号	学历					
3	张**	3*	男	1380013****	本科					
4	李**	2*	女	1390013****	硕士					
5	王**	4*	男	1370013****	博士					
6	赵**	3*	女	1360013****	本科					
7	周**	5*	男	1350013****	硕士					
8										

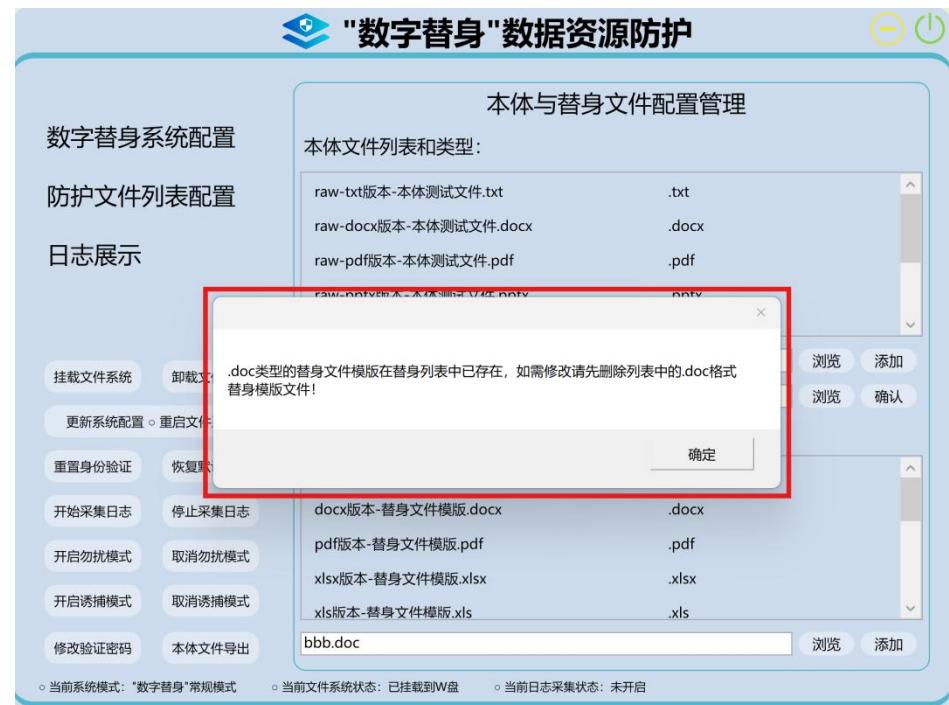
用户如果想更新某类型文件的替身模版，可以在列表中删除该类型的替身文件，然后点击下方文本框右侧“浏览”按钮，选中目标替身模版文件，然后点击“添加”，替身模版列表和类型目录中将显示新设置的替身文件信息。配置完成后，需要点击“更新系统配置·重启文件系统”方可生效。







如果列表中该类型替身文件模版已存在，添加新的同类型替身文件模版文件时将提示用户删除已有模版文件：



用户如果想对 txt、docx、doc、pdf、xlsx、xls、csv、pptx、ppt、json、md 11 种文件类型之外的其他类型文件进行防护，需要自行构建该文件类型对应的替身文件模版，放置到“替身文件模版路径”下，然后点击“替身模版列表和类型”下方文本框右侧“浏览”按钮，选中目标替身模版文件，然后点击

“添加”，替身模版列表和类型目录中将显示新设置的替身文件信息。(下图仅以.md 类型文件为例说明操作过程。)

> ... 敏感文件资料 > temp > 替身文件模版 > 在 替身文件模版

名称	修改日期	类型	大小
szts_temp	2024/8/2 14:53	文件夹	
项目通知文件目录	2024/8/2 14:53	文件夹	
csv版本-替身文件模版.csv	2024/6/12 16:42	XLS Worksheet	1 KB
docx版本-替身文件模版.docx	2024/6/12 16:31	DOCX Document	13 KB
doc版本-替身文件模版.doc	2024/6/12 16:32	DOC Document	13 KB
md版本-替身文件模版.md	2024/5/11 15:23	Markdown 源文件	1 KB
pdf版本-替身文件模版.pdf	2024/5/10 18:47	WPS PDF Docu...	29 KB
pptx版本-替身文件模版.pptx	2024/6/12 16:44	PPTX Presentation	36 KB
ppt版本-替身文件模版.ppt	2024/6/12 16:45	PPT Presentation	88 KB
txt版本-替身文件模版.txt	2024/5/11 15:23	文本文档	1 KB
xlsx版本-替身文件模版.xlsx	2024/6/12 16:34	XLSX Worksheet	11 KB
xls版本-替身文件模版.xls	2024/6/12 16:35	XLS Worksheet	26 KB

**"数字替身"数据资源防护**

本体与替身文件配置管理

本体文件列表和类型:

raw-txt版本-本体测试文件.txt	.txt
raw-docx版本-本体测试文件.docx	.docx
raw-pdf版本-本体测试文件.pdf	.pdf
raw-pptx版本-本体测试文件.pptx	.pptx
raw-xlsx版本-本体测试文件.xlsx	.xlsx

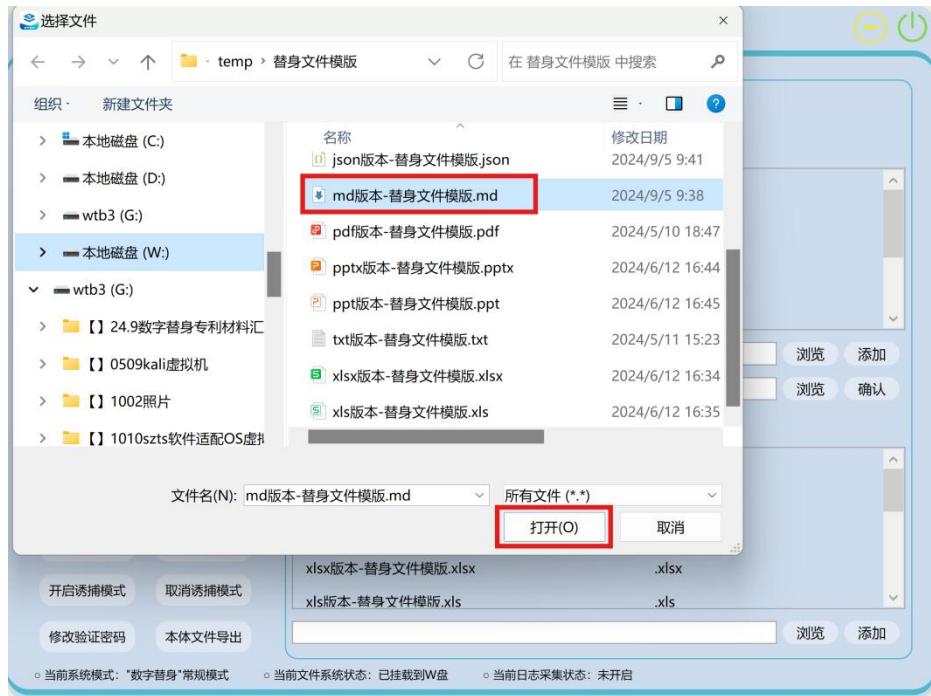
替身文件模版路径: W:\敏感文件资料\temp\替身文件模版 浏览 确认

替身模版列表和类型:

txt版本-替身文件模版.txt	.txt
docx版本-替身文件模版.docx	.docx
doc版本-替身文件模版.doc	.doc
pdf版本-替身文件模版.pdf	.pdf
xlsx版本-替身文件模版.xlsx	.xlsx

浏览 添加

当前系统模式：“数字替身”常规模式    当前文件系统状态：未挂载    当前日志采集状态：未开启



目前，在每次新挂载虚拟盘符后，会将“C:\SZTSPProgramInstaller\SZTSCConfig\目录树模版”文件夹下默认的替身模版目录自动拷贝到虚拟盘符中，保持替身模版文件的可用性。如果用户因误操作破坏虚拟盘符下的替身文件，可点击“更新系统配置·重启文件系统”按钮重新挂载虚拟盘符并回复替身文件。



## 4.2 系统配置

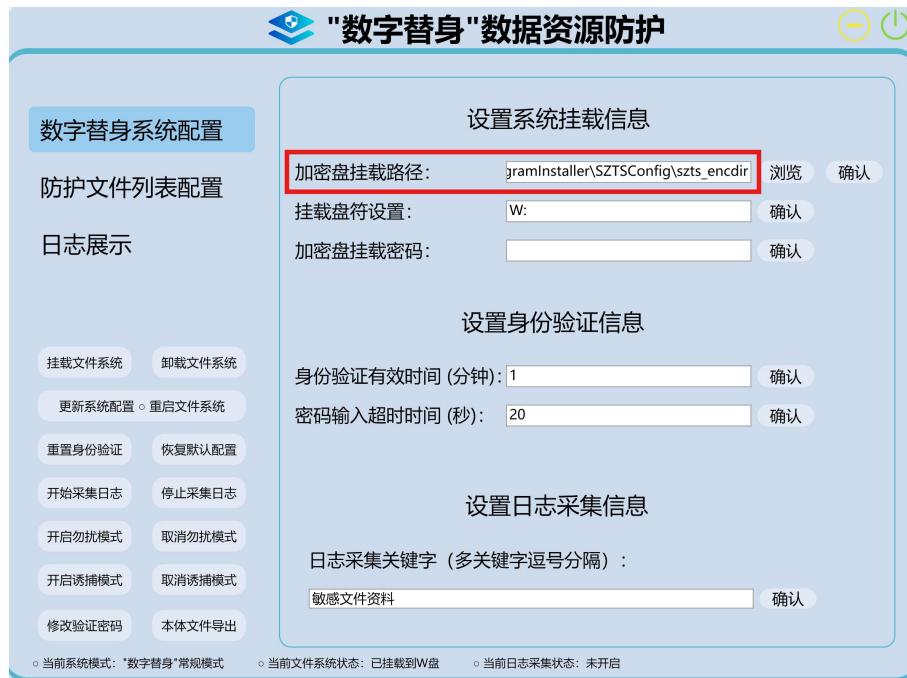
点击进入“数字替身系统配置”子界面。

### (1) 设置系统挂载信息

在“加密盘挂载路径”后白色文本框中输入路径并点击“确认”，表示系统解密挂载的虚拟盘符所对应的加密文件目录树和配置文件对应的路径。用户可以使用默认配置的 C:/SZTSPackageInstaller/SZTSConfig/szts\_enkdir 作为

加密盘挂载路径，该目录中已经放置了一组防护文件和 11 种替身模版文件目录树。每个加密盘目录有一个对应的解密挂载密码，存储在目录中的 sztsfs.xml 配置文件中。

szts\_encdir 目录对应的解密挂载密码为“12345678”。



如果用户选中其他已有路径作为加密盘挂载路径，点击“确认”时，系统将检查路径下是否存在合法的 xml 加密目录配置文件，如不存在将弹出相应错误提示：



如果用户将加密盘挂载路径设置为一个新目录，点击“挂载文件系统”时，会弹出黑色 cmd 窗口提示目录不存在，是否创建新目录。例如将加密盘挂载路径设置为不存在的目录“C:/SZTSConfig/szts\_encdir2”：



用户需要输入“y”确认创建新目录，然后选择“p”进入默认配置模式（“x”专家配置模式可以自行设置文件加解密算法、密钥大小、文件加密 block 大小等参数）：

```
C:\Windows\system32\cmd.exe > + <
目录 "/cygdrive/c/SZTSConfig/szts_encdir2/" 不存在, 是否创建新目录? (y,N) y
请选择以下Please choose from one of the following options:
输入 "x" 进入专家配置模式,
输入 "p" 进入默认配置模式,
输入其他信息将进入标准模式.
?> p
已选择默认配置模式.

配置已完成. 文件系统将被创建为以下属性:

文件系统加密算法: "ssl/aes", 版本 3:0:2
文件系统编码算法: "nameio/block32", 版本 4:0:2
密钥长度: 256 bits
Block Size: 1024 bytes, including 8 byte MAC header
每个文件包含8字节初始化向量 (IV) 数据头.
文件名采用IV链式模式编码.

请输入新目录挂载密码:
```

用户需要为新的加密盘挂载路径设置解密密码，并再次输入以确认密码：

```
C:\Windows\system32\cmd.exe > + <
目录 "/cygdrive/c/SZTSConfig/szts_encdir2/" 不存在, 是否创建新目录? (y,N) y
请选择以下Please choose from one of the following options:
输入 "x" 进入专家配置模式,
输入 "p" 进入默认配置模式,
输入其他信息将进入标准模式.
?> p
已选择默认配置模式.

配置已完成. 文件系统将被创建为以下属性:

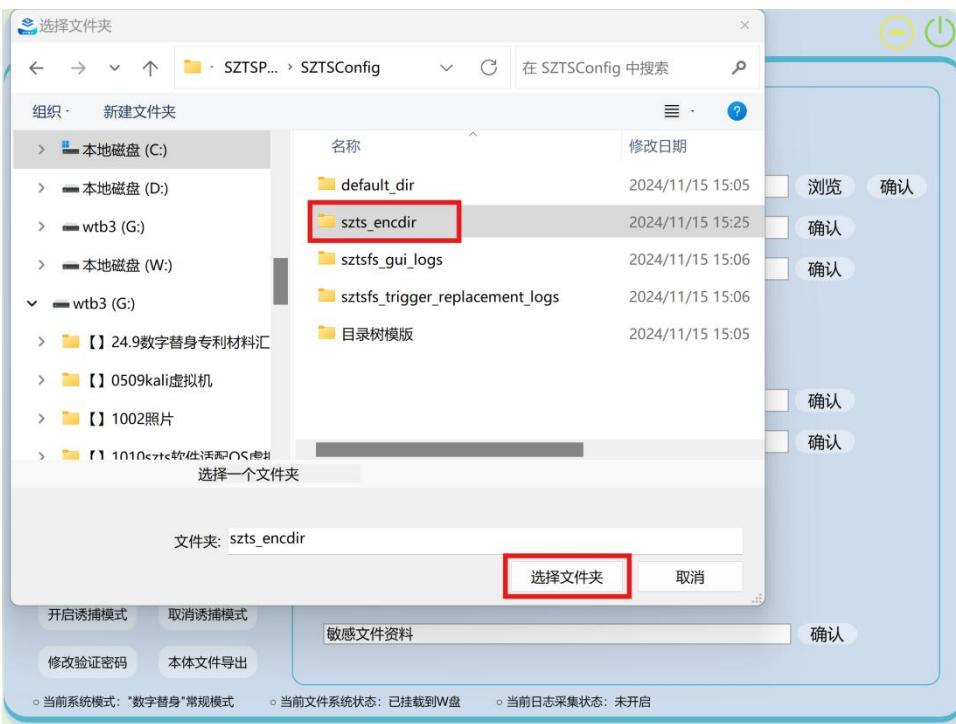
文件系统加密算法: "ssl/aes", 版本 3:0:2
文件系统编码算法: "nameio/block32", 版本 4:0:2
密钥长度: 256 bits
Block Size: 1024 bytes, including 8 byte MAC header
每个文件包含8字节初始化向量 (IV) 数据头.
文件名采用IV链式模式编码.

请输入新目录挂载密码:
请输入再次输入新目录挂载密码:
```

两次输入的密码验证一致后等待数秒，黑框消失，新设置的加密盘挂载路径将挂载为虚拟磁盘。此时新目录中数据文件为空，仅包含一个自动生成的配置文件，存储用户设置的目录解密挂载密码。用户可以向盘中拷贝本体、替身文件目录树，设置替身文件模版路径。



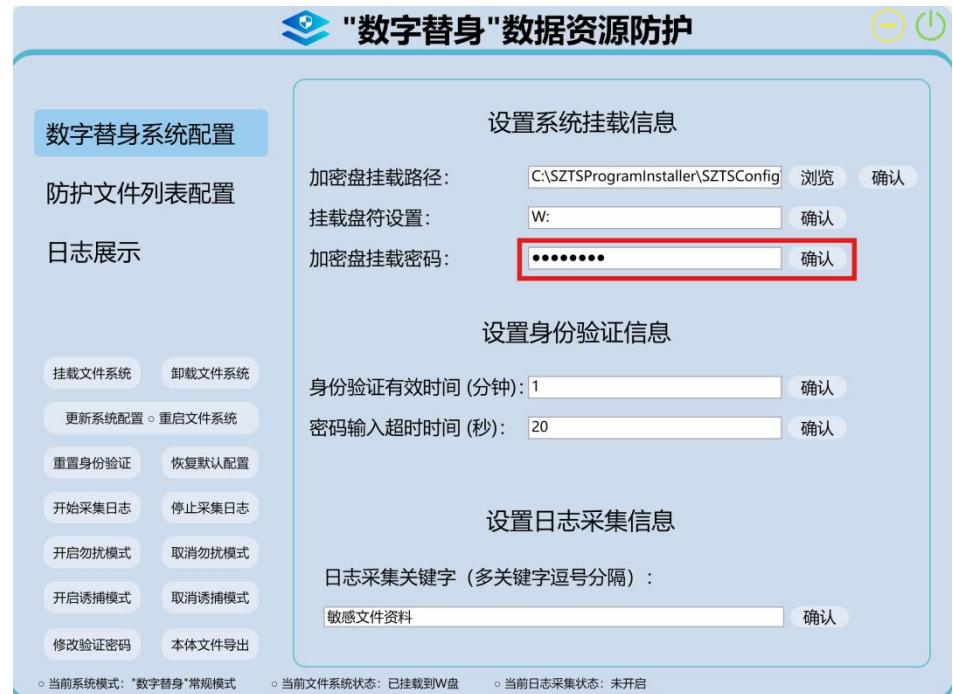
当用户想切换其他加密盘挂载路径时，可点击“浏览”按钮，选择目标文件夹，然后点击“确认”完成设置。



接下来，可以设置加密盘目录解密挂载后的虚拟盘符。虚拟盘符必须为 H 到 Z 之间的字母。默认为 W 盘：



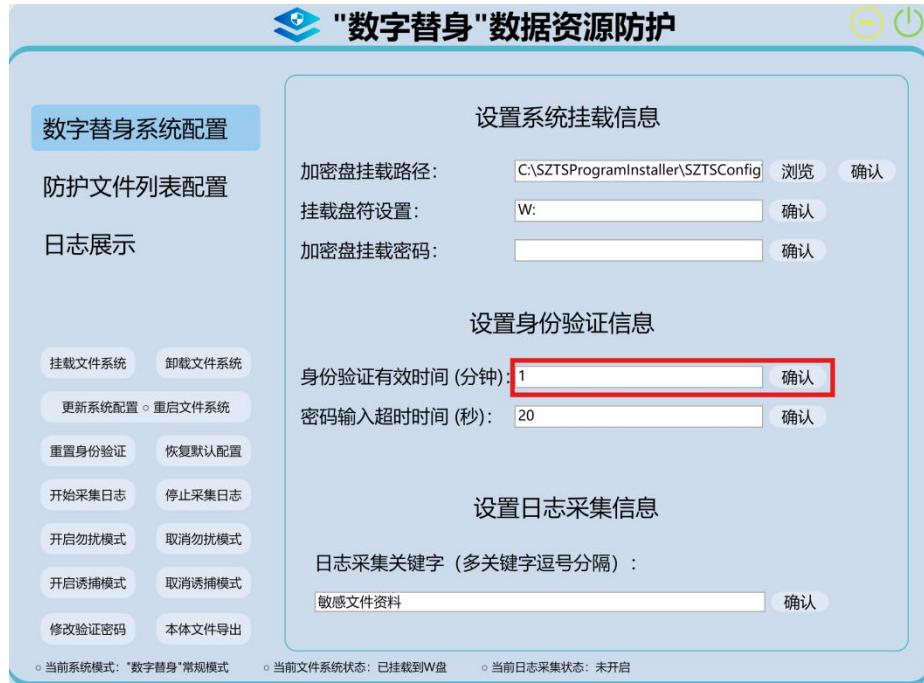
输入当前加密盘挂载目录对应的解密密码，点击“确认”，信息将以 base64 编码后的字符串存储到相应配置文件中。目前限制密码为 8 位字母或数字组合，默认密码为“12345678”：



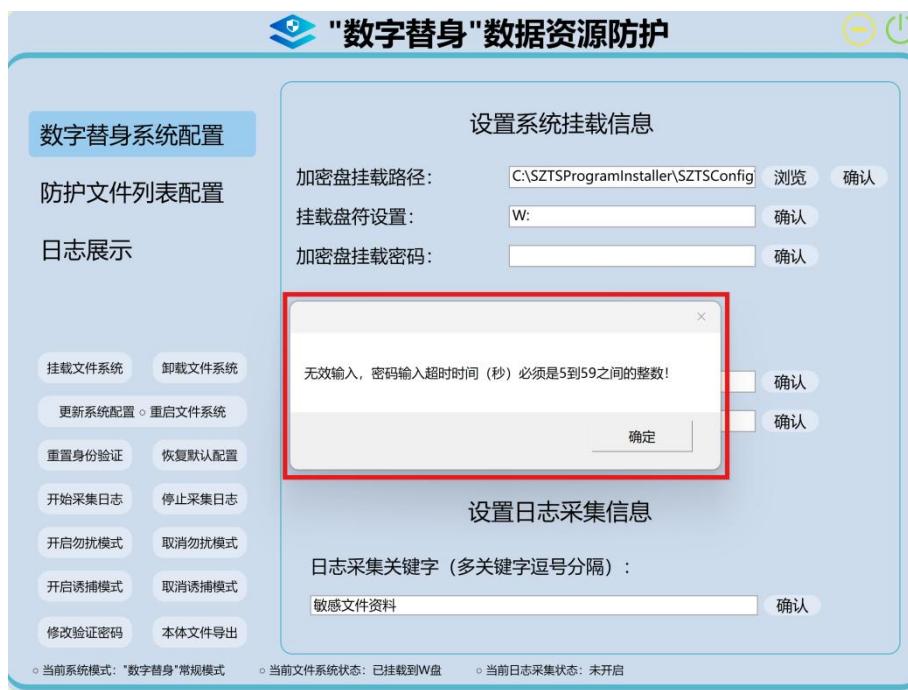
## (2) 设置身份验证信息

用户可以设置每次进行身份验证的有效时间（分钟），有效时间内多次点击本体文件，不需要再次验证。**身份验证有效时间（分钟）必须为 1 到 1440（24**

小时)之间的整数，默认为1分钟。如果输入的数值不在合法范围内将弹出相应错误提示：



用户可以设置密码弹窗框输入的超时时间(秒)，超过这个时间没有输入密码，按密码输入错误处置。**密码输入超时时间(秒)必须为5到59的整数**，默认为20秒。如果输入的数值不在合法范围内将弹出相应错误提示：



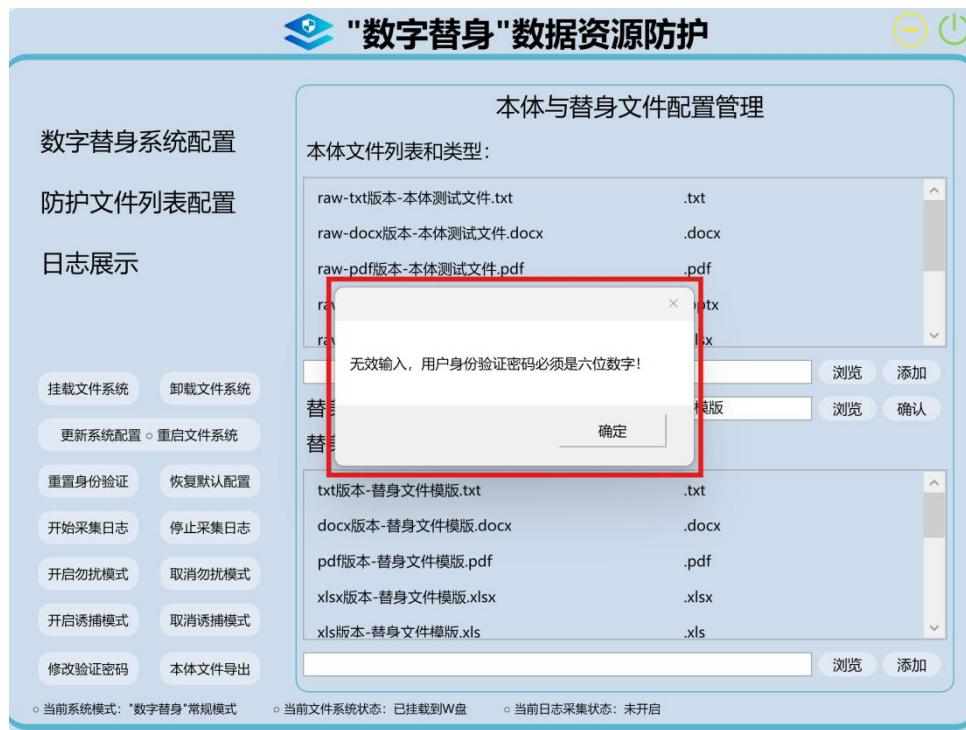
用户可以设置点击防护文件时进行身份验证的密码，这个密码在点击本体文件弹窗时输入，目前限制密码为 6 位纯数字，默认密码为“123456”。点击“修改身份验证密码”按钮，将弹窗提示“请输入原身份验证密码”，点击确认后，如果原密码正确，将进一步弹窗显示“输入新的身份验证密码”。用户仍需输入 6 位纯数字密码，并重复输入以避免错误。点击确认后提示“修改身份验证密码成功”，信息将以 base64 编码后的字符串存储到相应配置文件中。





如用户输入的原身份验证密码错误或取消输入，将提示“输入的原始密码错误，无法重置用户身份验证密码”。如果用户两次输入的新密码不一致或输入不合法，也将弹出相应错误提示：





### (3) 设置日志采集信息

用户可以设置对文件系统路径进行日志监控和采集的关键字，目前支持多组关键字，以逗号分隔，默认值为“敏感文件资料”。



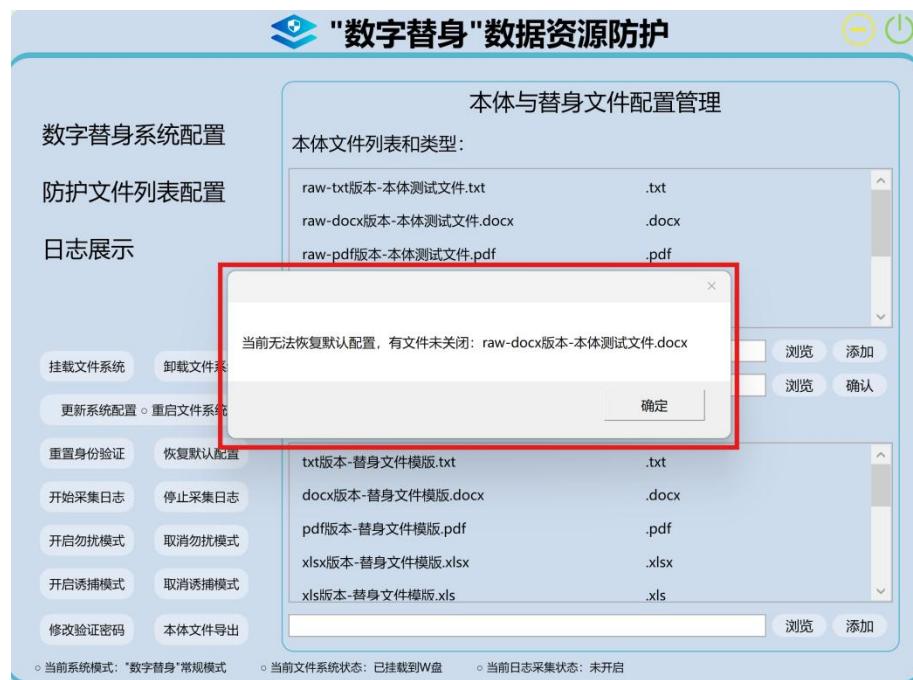
- ❖ 注意：用户修改系统挂载信息、身份验证信息、日志采集信息等相关配置信息后，需要点击“更新系统配置·重启文件系统”按钮方可生效。

#### (4) 恢复默认系统配置

此外，用户可点击“恢复默认配置”按钮，可以将“防护文件列表配置”、“数字替身系统配置”界面参数以及系统状态全部恢复为默认值。“防护文件列表配置”、“数字替身系统配置”GUI界面中显示的配置取值在切换刷新后生效。点击“恢复默认配置”后将弹出密码验证框，输入正确身份验证密码后才能够成功恢复，否则将提示“身份验证失败，无法恢复默认配置”。



当用户通过点击“恢复默认配置”时，如有文件通过WPS或Office Word/Powerpoint/Excel程序打开，会提示“当前无法恢复默认配置，有文件未关闭”，需用户关闭相应文件才能恢复默认配置，避免切换模式导致的文件查看、写入、保存错误或与模式状态存在不一致。（此功能目前仅适用于WPS和Office Word/Powerpoint/Excel应用打开本体情况。）



## 4.3 系统虚拟加密盘挂载与文件查看

### (1) 挂载文件系统

完成以上配置后，点击“挂载文件系统”，会将加密文件目录解密挂载为虚拟盘符。弹出提示信息后，在文件系统中找到新盘符（如W盘），如果未出现刷新一下文件目录列表即可。点击进入新盘，可以看到解密后的文件目录树列表。



完成系统挂载后，可点击 GUI 界面右上角左侧最小化按钮，将程序最小化到托盘，日常中无需开启 GUI。需要修改配置信息或卸载文件系统时，单击托盘中图标即可恢复原始 GUI 界面。点击界面右上角右侧关闭按钮即可退出 GUI 界面程序。

## (2) 查看文件

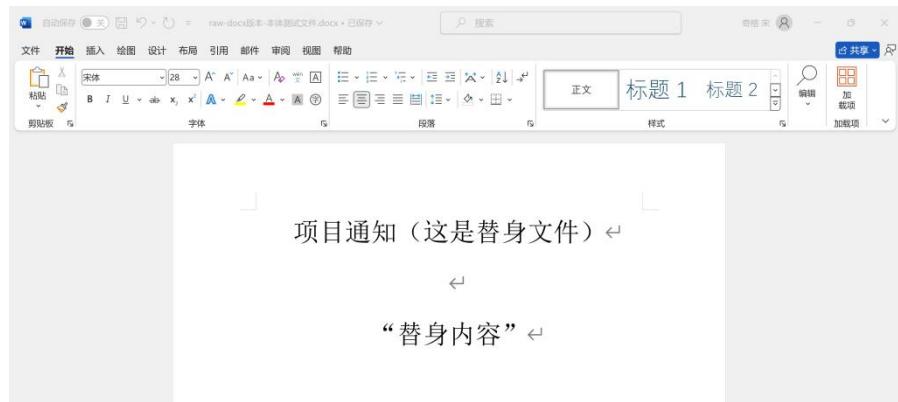
当用户通过应用程序访问 W: 盘中文件，命中被防护的本体文件名时，如果该应用程序是当日新挂载文件系统后首次访问被防护文件，会弹出“数据看门狗”密码验证窗口，需要用户输入 6 位身份验证密码。如果密码正确则打开本体文件真实内容：



同时，该进程后续的身份验证将通过私钥签名验证的方式在后台完成。

如果用户输入错误密码，或点击“取消”按钮，或超时未输入密码（如10秒），则打开该文件类型对应的替身文件模版内容：



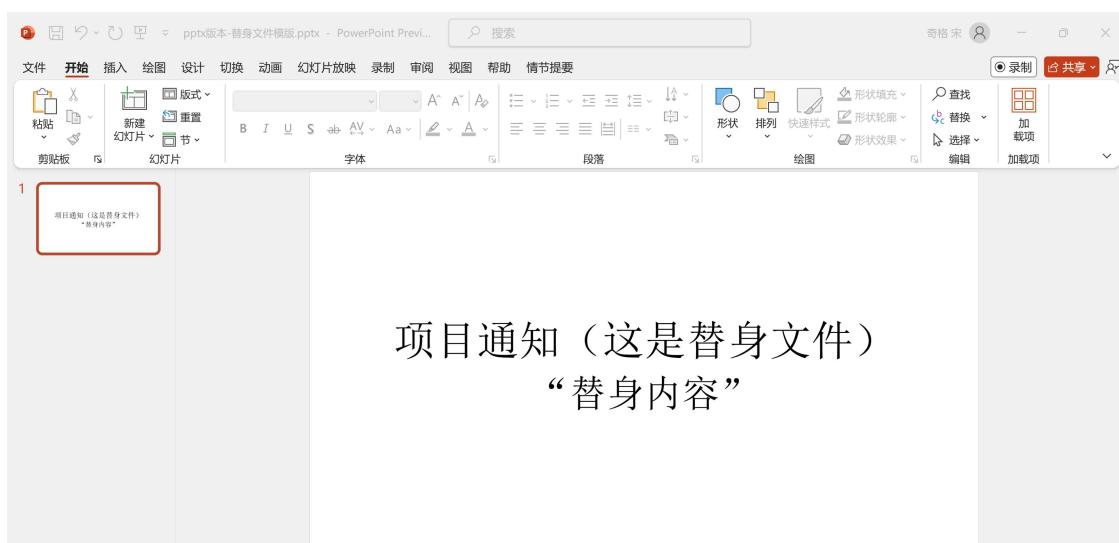
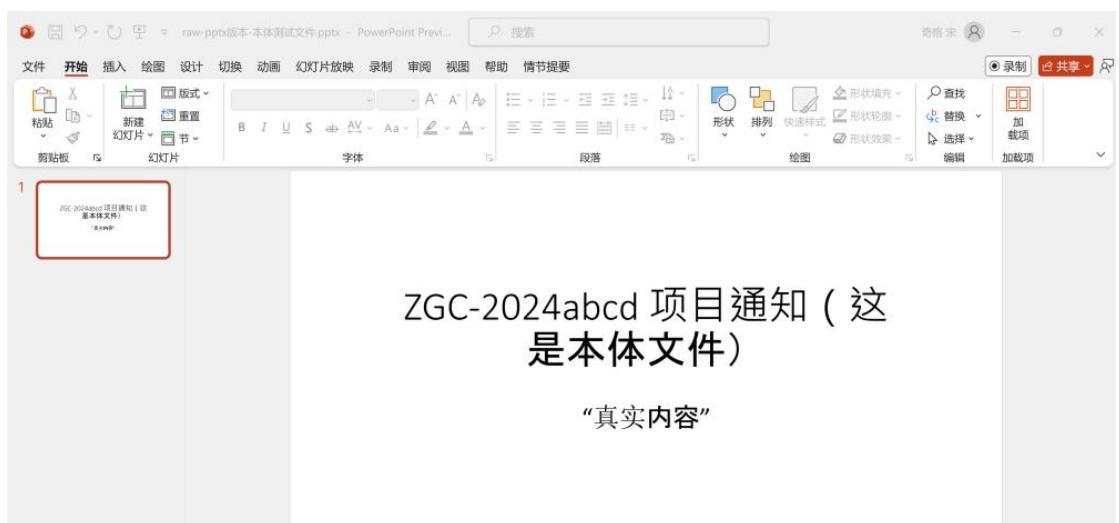


同时，该进程后续的身份验证仍将弹出密码验证框，直至用户输入正确密码。

当未超过该进程身份验证的有效时间（如 1 分钟）时，再次点击打开本体文件，不会重新发起身份验证，而是根据上一次身份验证的结果打开真实本体文件或替身文件模版。超过身份验证有效时间后打开本体文件，则会发起身份验证。

目前 doc、docx、ppt、pptx、xls、xlsx、pdf 等文件类型在 WPS、Office-Word/PowerPoint/Excel 应用程序中均可正常使用。

A screenshot of the PDFelement application showing a PDF document titled "ZGC-2024abcd 项目通知(这是本体文件)". The content of the document is "“真实内容”". The PDFelement interface includes various tools for editing, converting, and protecting PDF files.



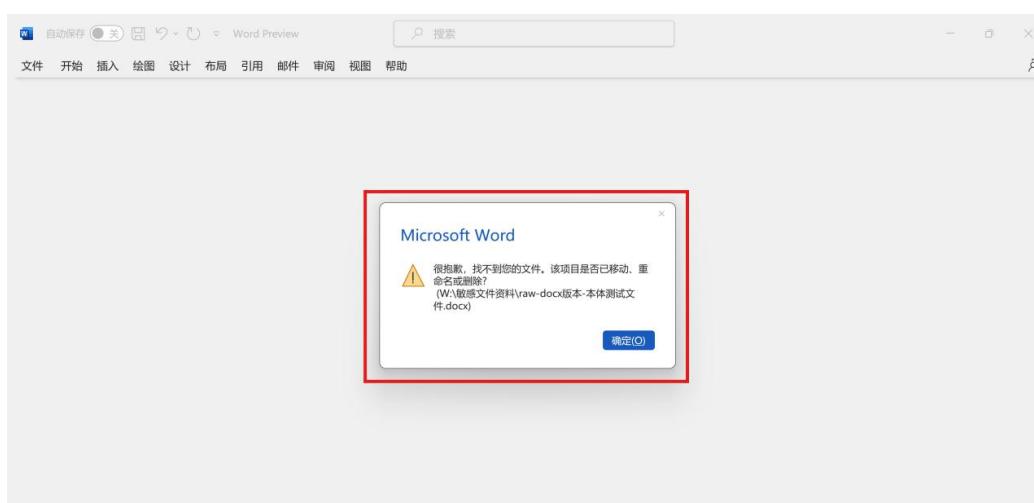
The screenshot shows two Excel windows side-by-side. The left window, titled 'raw-xlsx版本-本体测试文件.xlsx - Excel Preview', contains a table with data starting from row 1. The right window, titled 'xlsx版本-替身文件模板.xlsx - Excel Preview', also contains a table with data starting from row 1. Both tables have columns for Name, Age, Gender, Phone Number, and Education Level.

这是本体文件					
	姓名	年龄	性别	手机号	学历
1	张三	34	男	13800138000	本科
2	李四	29	女	13900139000	硕士
3	王五	45	男	13700137000	博士
4	赵六	38	女	13600136000	本科
5	周七	50	男	13500135000	硕士
6					
7					
8					
9					

这是替身文件					
	姓名	年龄	性别	手机号	学历
1	张**	3*	男	1380013****	本科
2	李**	2*	女	1390013****	硕士
3	王**	4*	男	1370013****	博士
4	赵**	3*	女	1360013****	本科
5	周**	5*	男	1350013****	硕士
6					
7					
8					

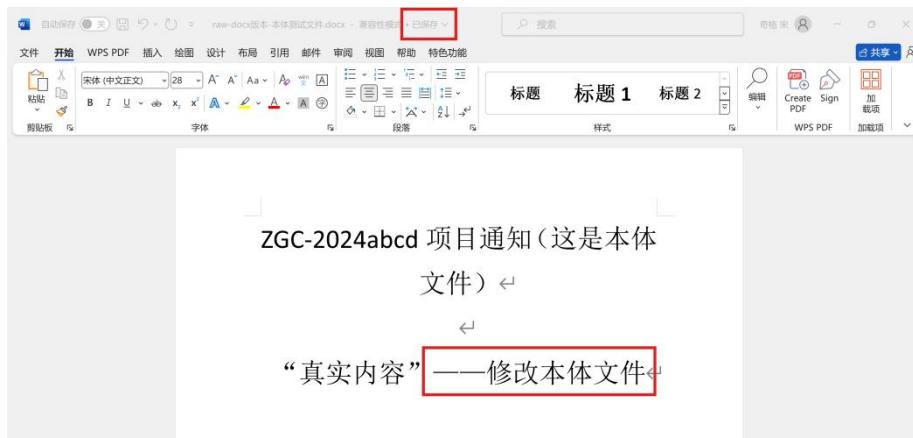
如果对于某文件类型，其替身模版文件在 GUI 界面“替身模版列表和类型”中没有被配置，或者配置后替身文件被删除，当用户打开该类型某个本体文件后输入错误验证密码时，将显示“找不到文件”相关效果：





### (3) 修改文件

用户通过应用程序打开本体文件，该进程首次访问本体需要用户输入正确密码，然后对文件进行更新，保存时，如果已经超过身份验证有效期（默认 1 分钟），将通过私钥签名验证的方式在后台重新进行身份验证，无需用户重新输入密码。



如果用户或攻击者打开本体文件后输入错误密码并查看替身文件，此时修改文件内容并保存，修改的内容将正确存储到对应的替身模版文件中。用户给对本体文件的修改和保存不会影响替身文件内容，同样的，对于替身文件的修改和保存也不会影响本体文件内容。

#### ❖ 注意：

- (1) 每次重新挂载文件系统后，替身文件将被恢复为初始状态内容（与“C:\SZTSPProgramInstaller\SZTSConfig\目录树模版\敏感文件资料\temp\替身文件模版”目录下 11 个替身模版文件内容相同）。
- (2) 当使用 wps、Office Word/Powerpoint/Excel 程序查看并修改

doc/docx/ppt/pptx/xls/xlsx 等文件时，文件修改操作涉及多种临时文件创建、写入、重命名等操作，程序对此进行了特殊处理。临时文件创建和命名机制可能受到 wps 和 Office 程序版本影响。目前替身文件修改保存并且不影响本体文件内容的功能在 wps 程序 2024 夏季更新-17827 版本、2024 夏季更新-15320 版本、11.1.0.9912 版本、11.1.0.7693 版本以及 Office 程序 LSTC 专业增强版 2024 preview、Office 家庭和学生版 2021 版本、Office 365 2407 版本已测试通过。

#### (4) 删除文件

当用户删除虚拟盘符中的本体文件时，会弹出密码验证窗口，验证结果正确则能够删除真实本体文件，否则将删除替身文件。

对于密码验证失败后删除替身文件的情况，如果操作后目录下本体文件消失，刷新文件夹则能够重新看到本体文件。**如果此时本体文件无法正常打开，用户需点击“更新系统配置·重启文件系统”按钮重新挂载虚拟盘符，同时能够补充被删除的替身模版文件。**

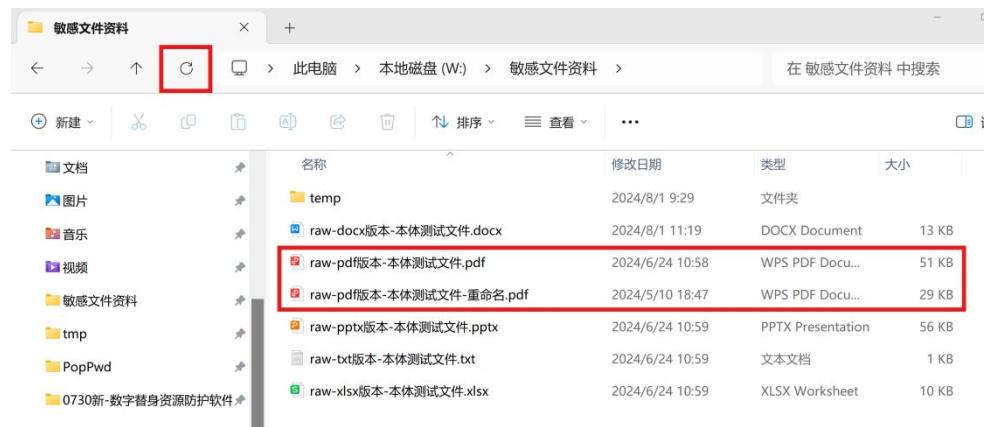
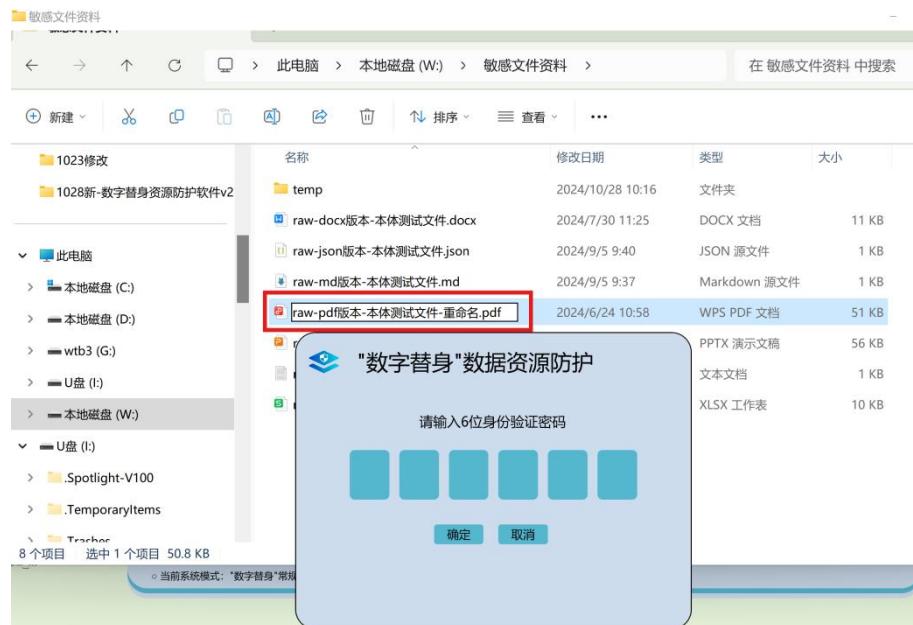
本体文件删除操作每次超过身份验证周期后再次执行都会弹出密码验证框，需要用户输入身份验证密码，不会通过私钥签名验证方式在后台完成。



## (5) 重命名文件

当用户重命名虚拟盘符中的本体文件时，会弹出密码验证窗口，验证结果正确则能够重命名真实本体文件，否则将重命名替身文件。

对于密码验证失败后重命名替身文件的情况，如果操作后目录下本体文件消失，刷新文件夹则能够重新看到本体文件。如果此时本体文件无法正常打开，用户需点击“更新系统配置·重启文件系统”按钮重新挂载虚拟盘符，同时能够补充被重命名后消失的替身模版文件。

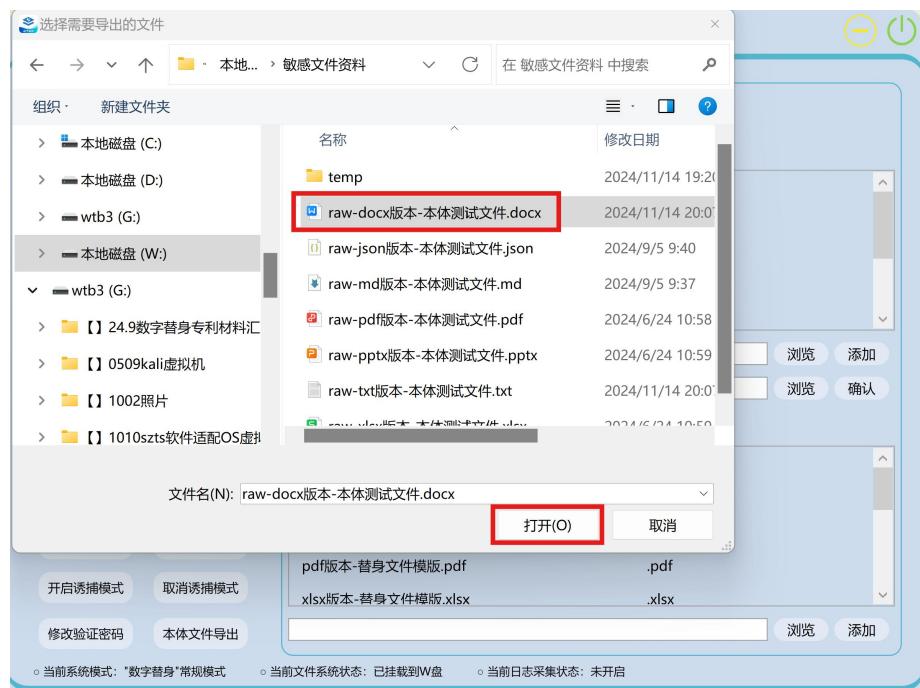


❖ 注意：用户在上述使用过程中遇到问题时，均可点击“更新系统配置·重启文件系统”按钮重启文件系统。

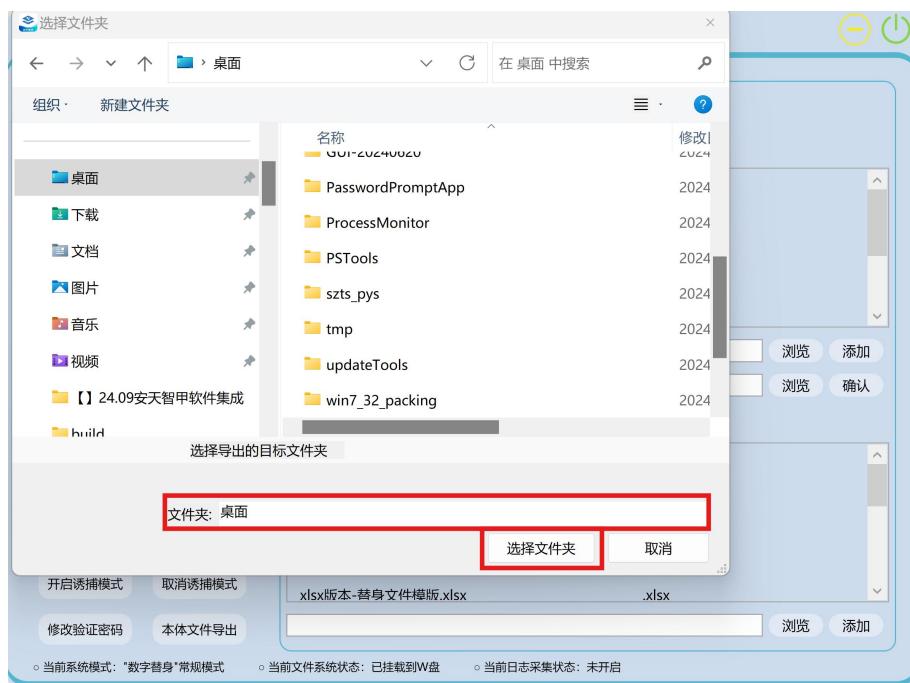


## (6) 导出文件

“数字替身”数据资源防护软件只对放置在虚拟盘内的本体文件实施防护。当用户需要将被防护文件从虚拟盘（如 W: 盘）拷贝到设备其他磁盘中时，需通过软件 GUI 界面操作。点击“本体文件导出”按钮，将弹出第一个文件目录浏览框，用户选择 W 盘中需要导出的文件（如 raw-docx 版本 - 本体测试文件.docx）：



选中文件并点击“打开”后，将弹出第二个文件目录浏览框，用户选择要导出的目标文件夹（如桌面），点击“选择文件夹”后，弹出密码验证框。输入正确密码后，弹窗提示“文件已成功导出到目标文件夹”，W 盘中 raw-docx 版本-本体测试文件.docx 文件被正确导出到桌面，可以直接打开查看。**本体文件复制到虚拟盘之外的文件将不会被防护。**

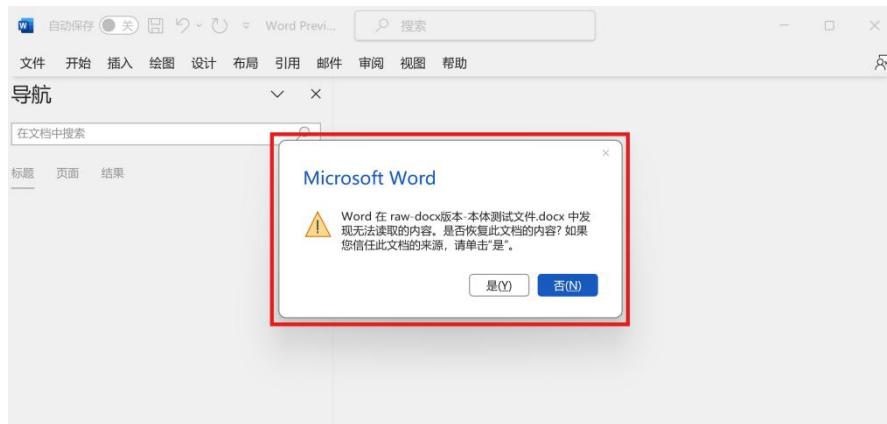




如果输入错误密码，将弹窗提示“身份认证失败，无法导出文件”。

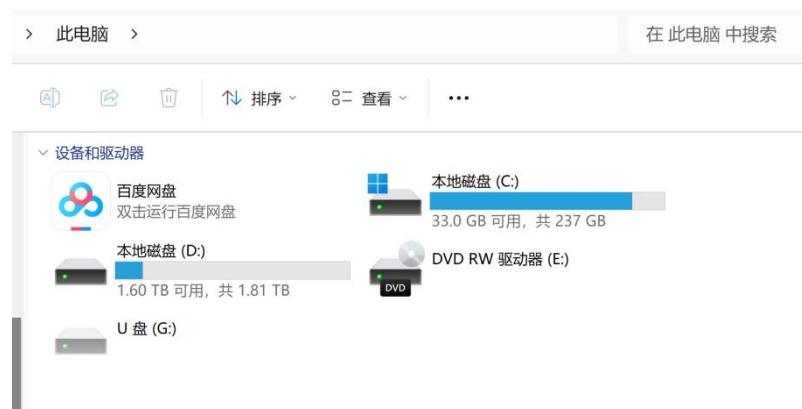


如果当用户直接将文件从虚拟盘（如 W: 盘）拷贝到设备其他磁盘中，被复制出来的文件将无法正确打开。使用记事本、WPS、Office 等应用打开 txt/docx/pptx/pdf/xlsx 等格式文件将显示空文件或文件格式无效等相关提示。



## (7) 卸载文件系统

点击“卸载文件系统”，弹出提示信息后，新盘符将消失。



## 4.4 日志采集与展示

### (1) 日志采集与停止

点击“开始采集日志”按钮，将启动针对虚拟磁盘的文件系统操作日志采集程序：



采集的日志文件内容经过解析处理后读入到数据库文件 C:\SZTSPProgramInstaller\SZTSPProgram\test.db 中，用于 GUI 界面展示文件系统、网络、进程、可疑文件等日志信息，随日志采集持续追加更新。系统设置每日上午 8 时对 test.db 文件进行备份，并清空现有日志信息。每日备份后的日志存储在 C:\SZTSPProgramInstaller\SZTSCConfig\database\_backups 文件夹下：

在 database_backups			
名称	修改日期	类型	大小
2024-06-25-test.db	2024/6/25 11:36	Data Base File	5,620 KB

点击“停止采集日志”，终止日志记录程序：



## (2) 日志信息表展示

点击进入“日志展示”子页面，可以查看文件操作行为、进程网络行为、进程详细信息、可疑文件信息、触发替身事件、用户操作行为六组数据库表信息，每项展示最多 500 条最新数据。

- ❖ 注意：触发替身事件日志、用户操作行为日志两个子页面中的日志信息无需用户点击“开始采集日志”也会持续记录并实时更新，GUI 界面中展示的为当日的触发替身事件和用户操作行为。
- ❖ 软件安装后，如果用户从未点击过“开始采集日志”，GUI 界面中将展示文件操作行为、进程网络行为、进程详细信息、可疑文件信息四组日志的示例日志内容。当用户点击过“开始采集日志”之后，GUI 界面中将不再展示这四组日志的示例日志内容。



点击查看“文件操作行为日志”，包含“序号、时间、进程名称、进程号、文件路径、操作行为”6个字段，展示应用程序进程对本体文件列表中的文件执行的读写等操作信息：

序号	时间	进程名称	进程号	文件路径
1	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-xlsx版本-本体测试文件.xlsx
2	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-xlsx版本-本体测试文件.xlsx
3	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-txt版本-本体测试文件.txt
4	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-txt版本-本体测试文件.txt
5	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-pptx版本-本体测试文件.pptx
6	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-pptx版本-本体测试文件.pptx
7	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-pdf版本-本体测试文件.pdf
8	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-pdf版本-本体测试文件.pdf
9	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-docx版本-本体测试文件.docx
10	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\raw-docx版本-本体测试文件.docx
11	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\aaa.txt
12	3:29:19 上午	powershell.exe	13704	W:\敏感文件资料\aaa.txt
13	3:29:16 上午	powershell.exe	13704	W:\敏感文件资料\temp
14	3:29:16 上午	powershell.exe	13704	W:\敏感文件资料\temp
15	3:29:16 上午	powershell.exe	13704	W:\敏感文件资料
16	3:29:16 上午	powershell.exe	13704	W:\
17	3:28:36 上午	powershell.exe	13772	W:\敏感文件资料\raw-pdf版本-本体测试文件.pdf
18	3:28:32 上午	powershell.exe	13772	W:\敏感文件资料\raw-pdf版本-本体测试文件.pdf
19	3:28:29 上午	powershell.exe	13772	W:\敏感文件资料
20	3:28:27 上午	powershell.exe	13772	W:\

点击查看“进程网络行为日志”，包含“序号、时间、进程名称、进程号、网络行为、四元组、详细信息、进程命令信息”8组字段：

 "数字替身"数据资源防护

进程网络行为日志

序号	时间	进程名称	进程号	网络行为	四元组
1	3:28:55 上午	powershell.exe	13772	TCP Receive	bogon:50573 -> bogon:4459 ^
2	3:28:55 上午	powershell.exe	13772	TCP TCPCopy	bogon:50573 -> bogon:4459
3	3:28:55 上午	powershell.exe	13772	TCP Send	bogon:50573 -> bogon:4459
4	3:28:55 上午	powershell.exe	13772	TCP Connect	bogon:50573 -> bogon:4459
5	3:28:55 上午	powershell.exe	13772	TCP Disconnect	bogon:50572 -> bogon:4459
6	3:28:55 上午	powershell.exe	13772	TCP Receive	bogon:50572 -> bogon:4459
7	3:28:55 上午	powershell.exe	13772	TCP TCPCopy	bogon:50572 -> bogon:4459
8	3:28:55 上午	powershell.exe	13772	TCP Send	bogon:50572 -> bogon:4459
9	3:28:55 上午	powershell.exe	13772	TCP Connect	bogon:50572 -> bogon:4459
10	3:28:55 上午	powershell.exe	13772	TCP Disconnect	bogon:50571 -> bogon:4459
11	3:28:55 上午	powershell.exe	13772	TCP Receive	bogon:50571 -> bogon:4459
12	3:28:55 上午	powershell.exe	13772	TCP TCPCopy	bogon:50571 -> bogon:4459
13	3:28:55 上午	powershell.exe	13772	TCP Send	bogon:50571 -> bogon:4459
14	3:28:55 上午	powershell.exe	13772	TCP Send	bogon:50571 -> bogon:4459
15	3:28:55 上午	powershell.exe	13772	TCP Connect	bogon:50571 -> bogon:4459
16	3:28:55 上午	powershell.exe	13772	TCP Disconnect	bogon:50570 -> bogon:4459
17	3:28:55 上午	powershell.exe	13772	TCP Receive	bogon:50570 -> bogon:4459
18	3:28:55 上午	powershell.exe	13772	TCP TCPCopy	bogon:50570 -> bogon:4459
19	3:28:55 上午	powershell.exe	13772	TCP Receive	bogon:50570 -> bogon:4459
20	3:28:55 上午	powershell.exe	13772	TCP TCPCopy	bogon:50570 -> bogon:4459
21	3:28:55 上午	powershell.exe	13772	TCP Send	bogon:50570 -> bogon:4459
22	3:28:55 上午	powershell.exe	13772	TCP Connect	bogon:50570 -> bogon:4459
23	3:28:55 上午	powershell.exe	13772	TCP Disconnect	bogon:50569 -> bogon:4459
24	3:28:55 上午	powershell.exe	13772	TCP Receive	bogon:50569 -> bogon:4459

返回

点击查看“进程详细信息日志”，包含“序号、时间、进程名称、父进程号、操作行为、进程命令信息、用户账号、路径”8组字段：

 "数字替身"数据资源防护

进程详细信息日志

序号	时间	进程名称	进程号	父进程号	操作行为	进程命令信息
1	3:29:19 上午	powershell.exe	13704	13772	Process Exit	powershell -nop -ex^
2	3:29:19 上午	powershell.exe	13704	13772	Thread Exit	powershell -nop -ex^
3	3:29:19 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
4	3:29:19 上午	powershell.exe	13704	13772	Thread Create	powershell -nop -ex^
5	3:29:19 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
6	3:29:17 上午	powershell.exe	13704	13772	Thread Exit	powershell -nop -ex^
7	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
8	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
9	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
10	3:29:16 上午	powershell.exe	13704	13772	Thread Create	powershell -nop -ex^
11	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
12	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
13	3:29:16 上午	powershell.exe	13704	13772	Thread Create	powershell -nop -ex^
14	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
15	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
16	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
17	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
18	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
19	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
20	3:29:16 上午	powershell.exe	13704	13772	Thread Create	powershell -nop -ex^
21	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
22	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
23	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^
24	3:29:16 上午	powershell.exe	13704	13772	Load Image	powershell -nop -ex^

返回

系统将对日志进行实时分析研判，提取可能针对替身文件发起窃密攻击行为的可疑样本、文件、脚本等，并关联相关进程信息，生成相应的可疑文件信息表。点击查看“可疑文件信息日志”，包含“序号、时间、进程名称、进程号、可疑文件路径、操作行为、进程命令信息”7组字段：

"数字替身"数据资源防护

文件操作行为日志
进程网络行为日志
进程详细信息日志

可疑文件信息日志

触发替身事件日志

用户操作行为日志

查看可疑文件

序号	进程号	可疑文件路径
hell.exe	13704	& "C:\file_stal2.ps1"
r.EXE	7184	C:\Users\Lenovo\Desktop\24_working_tmp\关于开放课题申请的相关通知.pdf\
r.EXE	7184	C:\Users\Lenovo\Desktop\24_working_tmp\关于开放课题申请的相关通知.pdf\
r.EXE	7184	C:\Users\Lenovo\Desktop\DBeaver.Ink
r.EXE	7184	C:\Users\Lenovo\Desktop\DBeaver.Ink

返回
<
>

点击查看“触发替身事件日志”，包含“序号、时间、进程名称、进程号、原始文件路径、替身文件路径”6个字段，具体展示应用程序在访问本体文件时，由于未通过身份验证导致触发替身模版文件访问行为的信息：

"数字替身"数据资源防护

文件操作行为日志
进程网络行为日志
进程详细信息日志

可疑文件信息日志

触发替身事件日志

用户操作行为日志

查看可疑文件

序号	时间	进程名称	进程号	原始文件路径
1	2024-10-28 5:56:19 下午	DllHost.exe	21708	/敏感文件资料/raw-pptx版本-本体 ^
2	2024-10-28 5:56:18 下午	POWERPNT.EXE	21124	/敏感文件资料/raw-pptx版本-本体
3	2024-10-28 5:56:17 下午	POWERPNT.EXE	21124	/敏感文件资料/raw-pptx版本-本体
4	2024-10-28 5:56:17 下午	DllHost.exe	21632	/敏感文件资料/raw-pptx版本-本体
5	2024-10-28 5:56:16 下午	DllHost.exe	21632	/敏感文件资料/raw-pptx版本-本体
6	2024-10-28 5:56:16 下午	Explorer.EXE	7640	/敏感文件资料/raw-pptx版本-本体
7	2024-10-28 5:56:16 下午	DllHost.exe	21632	/敏感文件资料/raw-pptx版本-本体
8	2024-10-28 5:56:16 下午	Explorer.EXE	7640	/敏感文件资料/raw-pptx版本-本体
9	2024-10-28 5:56:14 下午	DllHost.exe	9908	/敏感文件资料/raw-pptx版本-本体
10	2024-10-28 5:56:14 下午	Explorer.EXE	7640	/敏感文件资料/raw-pptx版本-本体
11	2024-10-28 5:56:11 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体
12	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体
13	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体
14	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体
15	2024-10-28 5:56:10 下午	wpscloudsvr.exe	10000	/敏感文件资料/raw-docx版本-本体
16	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体
17	2024-10-28 5:56:10 下午	wpscloudsvr.exe	10000	/敏感文件资料/raw-docx版本-本体
18	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体
19	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体
20	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体
21	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体
22	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体
23	2024-10-28 5:56:10 下午	wps.exe	8172	/敏感文件资料/raw-docx版本-本体
24	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体

返回
<
>

“触发替身事件日志”的原始日志记录文件位于“C:\SZTSPProgramInstaller\SZTSCConfig\sztfs-trigger-replacement-log”

目录下，每日生成的触发替身事件日志记录文件以日期开头命名（如 2024-09-02\_sztsfs\_trigger-replacement-log.txt），用户也可以通过文件查看完整记录信息。

点击查看“用户操作行为日志”，包含“序号、时间、用户操作、操作结果”4个字段，展示用户在程序 GUI 界面执行过的操作记录：

The screenshot shows a software window titled "数字替身"数据资源防护. On the left, there is a sidebar with several log categories: 文件操作行为日志 (File Operation Behavior Log), 进程网络行为日志 (Process Network Behavior Log), 进程详细信息日志 (Detailed Process Information Log), 可疑文件信息日志 (Suspicious File Information Log), and 触发替身事件日志 (Triggered Impersonation Event Log). The "User Operation Behavior Log" button is highlighted with a red rectangle. Below it is a "View Suspicious Files" button. At the bottom of the sidebar are "Return" and navigation arrows. The main area displays a table of user operations:

序号	时间	用户操作
1	2024-10-28 5:58:14 下午	用户终止日志采集
2	2024-10-28 5:58:00 下午	用户启动日志采集
3	2024-10-28 5:57:58 下午	用户添加文件"aaa.doc"到本体文件列表，该文件位于W:\敏感文件
4	2024-10-28 5:57:29 下午	用户添加文件"doc版本-替身文件模版.doc"到替身模版列表
5	2024-10-28 5:57:20 下午	用户从替身模版列表中删除"doc版本-替身文件模版.doc"
6	2024-10-28 5:56:25 下午	用户关闭诱捕模式
7	2024-10-28 5:56:08 下午	用户开启诱捕模式
8	2024-10-28 5:56:04 下午	用户关闭勿扰模式
9	2024-10-28 5:55:49 下午	用户开启勿扰模式
10	2024-10-28 5:55:07 下午	用户添加文件"精简版-2024-09-18-数字替身资源防护系统-windows版.exe"到本地文件列表
11	2024-10-28 5:53:02 下午	用户挂载文件系统到 W: 盘

“用户操作行为日志”的原始日志记录文件位于“C:\SZTSPProgramInstaller\SZTSConfig\sztsfs-gui-logs”目录下，每日生成的用户操作行为日志记录文件以日期开头命名（如 2024-09-05\_sztsfs-gui-log.txt），用户也可以通过文件查看完整记录信息。

有时查看以上日志信息时会提示“日志数据正在入库，请等待一分钟左右再进行查看！”，请用户根据提示等待后查看：

文件操作行为日志

进程网络行为日志

**进程详细信息日志**

可疑文件信息日志

触发替身事件日志

用户操作行为日志

在文件夹中显示

返回

序号	时间	进程名称	进程号	网络行为	四元组
1	8:19:32 下午	QQMusic.exe	10916	UDP Receive	DESKTOP-3UIF: ^
2	8:19:32 下午	QQMusic.exe	10916	UDP Send	DESKTOP-3UIF: ^
3	8:19:32 下午	QQMusic.exe	10916	UDP Receive	DESKTOP-3UIF: ^
4	8:19:32 下午	QQMusic.exe	10916	UDP Send	DESKTOP-3UIF: ^
5	8:19:29 下午	QQMusic.exe	10916	TCP Receive	DESKTOP-3UIF: ^
6	8:19:29 下午	QQMusic.exe	10916	TCP TCPCopy	DESKTOP-3UIF: ^
7	8:19:29 下午	QQMusic.exe	10916	TCP Send	DESKTOP-3UIF: ^
8	8:19:29 下午	QQMusic.exe	10916	TCP Send	DESKTOP-3UIF: ^
9	8:19:29 下午	QQMusic.exe	10916	TCP Receive	DESKTOP-3UIF: ^
10	8:19:29 下午	QQMusic.exe	10916	TCP TCPCopy	DESKTOP-3UIF: ^
11	8:19:29 下午	QQMusic.exe	10916	TCP Send	DESKTOP-3UIF: ^
12	8:19:29 下午	QQMusic.exe	10916	TCP Send	DESKTOP-3UIF: ^
13	8:19:29 下午	QQMusic.exe	10916	TCP Receive	DESKTOP-3UIF: ^
14	8:19:29 下午	QQMusic.exe	10916	TCP TCPCopy	DESKTOP-3UIF: ^
15	8:19:29 下午	QQMusic.exe	10916	TCP TCPCopy	DESKTOP-3UIF: ^
16	8:19:29 下午	QQMusic.exe	10916	TCP Send	DESKTOP-3UIF: ^
17	8:19:28 下午	QQMusic.exe	10916	TCP Receive	DESKTOP-3UIF: ^
18	8:19:29 下午	QQMusic.exe	10916	TCP TCPCopy	DESKTOP-3UIF: ^
19	8:19:28 下午	QQMusic.exe	10916	TCP Receive	DESKTOP-3UIF: ^
20	8:19:28 下午	QQMusic.exe	10916	TCP TCPCopy	DESKTOP-3UIF: ^
21	8:19:28 下午	QQMusic.exe	10916	TCP Send	DESKTOP-3UIF: ^
22	8:19:28 下午	QQMusic.exe	10916	TCP Connect	DESKTOP-3UIF: ^
23	8:19:28 下午	QQMusic.exe	10916	TCP Send	DESKTOP-3UIF: ^
24	8:19:28 下午	QQMusic.exe	10916	TCP Receive	DESKTOP-3UIF: ^

日志数据正在入库，请等待一分钟左右再进行查看！

确定

“可疑文件信息”数据库表中的样本将持续存储到 C:\SZTSProgramInstaller\SZTSProgram\malicious\_file 文件夹中。点击“查看可疑文件”，将自动打开可疑文件所在文件夹路径：

文件操作行为日志

进程网络行为日志

**进程详细信息日志**

可疑文件信息日志

触发替身事件日志

用户操作行为日志

**查看可疑文件**

返回

序号	时间	进程名称	进程号	原始文件路径
1	2024-10-28 5:56:19 下午	DllHost.exe	21708	/敏感文件资料/raw-pptx版本-本体 ^
2	2024-10-28 5:56:18 下午	POWERPNT.EXE	21124	/敏感文件资料/raw-pptx版本-本体 ^
3	2024-10-28 5:56:17 下午	POWERPNT.EXE	21124	/敏感文件资料/raw-pptx版本-本体 ^
4	2024-10-28 5:56:17 下午	DllHost.exe	21632	/敏感文件资料/raw-pptx版本-本体 ^
5	2024-10-28 5:56:16 下午	DllHost.exe	21632	/敏感文件资料/raw-pptx版本-本体 ^
6	2024-10-28 5:56:16 下午	Explorer.EXE	7640	/敏感文件资料/raw-pptx版本-本体 ^
7	2024-10-28 5:56:16 下午	DllHost.exe	21632	/敏感文件资料/raw-pptx版本-本体 ^
8	2024-10-28 5:56:16 下午	Explorer.EXE	7640	/敏感文件资料/raw-pptx版本-本体 ^
9	2024-10-28 5:56:14 下午	DllHost.exe	9908	/敏感文件资料/raw-pptx版本-本体 ^
10	2024-10-28 5:56:14 下午	Explorer.EXE	7640	/敏感文件资料/raw-pptx版本-本体 ^
11	2024-10-28 5:56:11 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体 ^
12	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体 ^
13	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体 ^
14	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体 ^
15	2024-10-28 5:56:10 下午	wpscloudsvr.exe	10000	/敏感文件资料/raw-docx版本-本体 ^
16	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体 ^
17	2024-10-28 5:56:10 下午	wpscloudsvr.exe	10000	/敏感文件资料/raw-docx版本-本体 ^
18	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体 ^
19	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体 ^
20	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体 ^
21	2024-10-28 5:56:10 下午	wps.exe	20432	/敏感文件资料/raw-docx版本-本体 ^
22	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体 ^
23	2024-10-28 5:56:10 下午	wps.exe	8172	/敏感文件资料/raw-docx版本-本体 ^
24	2024-10-28 5:56:10 下午	wps.exe	11184	/敏感文件资料/raw-docx版本-本体 ^

