目录

[1. 基本机制介绍 3](#_Toc53508561)

[2. 检查客户端是否安装成功 3](#_Toc53508562)

[2.1. Windows系统 3](#_Toc53508563)

[2.2. Mac系统 3](#_Toc53508564)

[2.3. Ubuntu系统 4](#_Toc53508565)

[3. 文档安全区域和密级 4](#_Toc53508566)

[3.1. 文档默认安全区域和密级 4](#_Toc53508567)

[3.2. 文档安全区域和密级查看 4](#_Toc53508568)

[3.2.1. Windows系统 4](#_Toc53508569)

[3.2.2. Mac和Ubuntu系统 4](#_Toc53508570)

[3.3. 文档安全区域和密级修改 5](#_Toc53508571)

[3.3.1. Windows系统 5](#_Toc53508572)

[3.3.2. Mac和Ubuntu系统 5](#_Toc53508573)

[3.4. 计算机可访问的文档安全区域和密级 5](#_Toc53508574)

[3.4.1. 权限申请及变更 6](#_Toc53508575)

[4. 加密文档申请解密 6](#_Toc53508576)

[4.1. Windows和Mac系统 6](#_Toc53508577)

[4.2. Ubuntu系统 7](#_Toc53508578)

[5. 客户端菜单操作说明 8](#_Toc53508579)

[5.1. Windows - 客户端托盘图标右键菜单 8](#_Toc53508580)

[5.1.1. 审批管理平台 8](#_Toc53508581)

[5.1.2. 临时离线申请 8](#_Toc53508582)

[5.1.3. 查看加密申请情况 8](#_Toc53508583)

[5.1.4. 扫描本地文件 8](#_Toc53508584)

[5.1.5. 加密系统信息 9](#_Toc53508585)

[5.1.6. 导入授权 11](#_Toc53508586)

[5.1.7. 常规选项 11](#_Toc53508587)

[5.1.8. 加密功能选项 11](#_Toc53508588)

[5.2. Windows – 文件右键快捷菜单 13](#_Toc53508589)

[5.2.1. 对于加密的文档 13](#_Toc53508590)

[5.2.2. 对于未加密的文档 15](#_Toc53508591)

[5.3. Mac系统 – 客户端托盘图标右键菜单 15](#_Toc53508592)

[5.3.1. 选项 16](#_Toc53508593)

[5.3.2. 高级 – 策略更新 16](#_Toc53508594)

[5.3.3. 扫描本地文件 16](#_Toc53508595)

[5.3.4. 查看申请情况 17](#_Toc53508596)

[5.3.5. 语言 17](#_Toc53508597)

[5.4. Mac系统 – 文件右键快捷菜单 17](#_Toc53508598)

[5.4.1. 对于加密的文档 18](#_Toc53508599)

[5.4.2. 对于未加密的文档 18](#_Toc53508600)

[5.5. Ubuntu系统 – 客户端UI界面菜单 18](#_Toc53508601)

[5.5.1. 选项 18](#_Toc53508602)

[5.5.2. 高级 – 策略更新 19](#_Toc53508603)

[5.5.3. 扫描本地文件 19](#_Toc53508604)

[5.5.4. 查看申请情况 19](#_Toc53508605)

[5.5.5. 语言 20](#_Toc53508606)

[6. 移动端安全文档查看器 20](#_Toc53508607)

[6.1. 下载安装 20](#_Toc53508608)

[6.2. 申请授权 22](#_Toc53508609)

[6.2.1. 连接服务器 22](#_Toc53508610)

[6.2.2. 申请授权 23](#_Toc53508611)

[6.2.3. 授权状态查看 23](#_Toc53508612)

[6.3. 功能使用 24](#_Toc53508613)

[6.4. 安全文档查看器支持打开的文件格式 26](#_Toc53508614)

[6.4.1. iOS系统 26](#_Toc53508615)

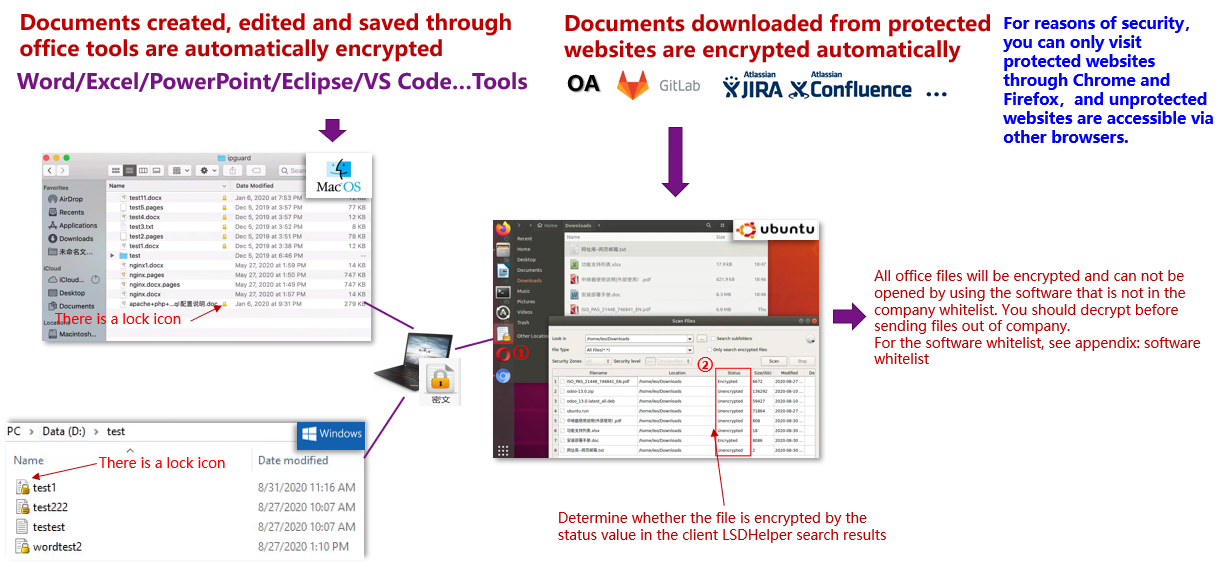
[6.4.2. Android系统 27](#_Toc53508616)

[7. 附录： 27](#_Toc53508617)

[7.1. 附录1：角色权限对照表 27](#_Toc53508618)

[7.2. 附录2：软件白名单 27](#_Toc53508619)

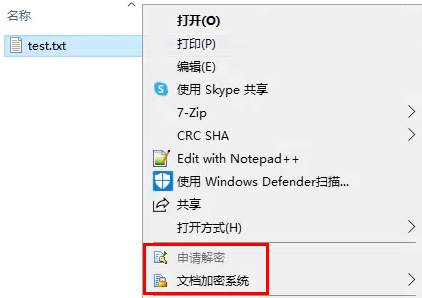
1. 基本机制介绍



1. 检查客户端是否安装成功
   1. Windows系统

任务栏显示如下终端安全图标，同时右键菜单里出现如下终端安全菜单项，表示安装成功：

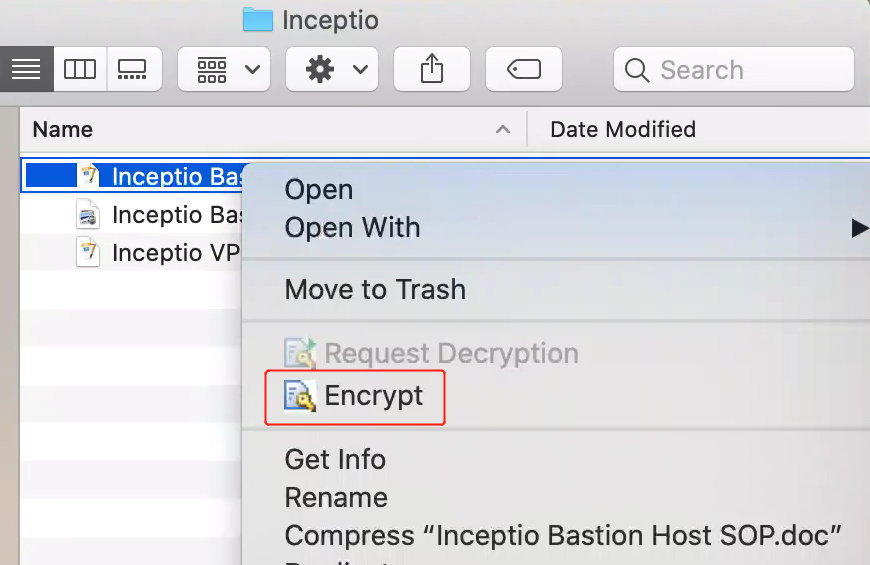




* 1. Mac系统

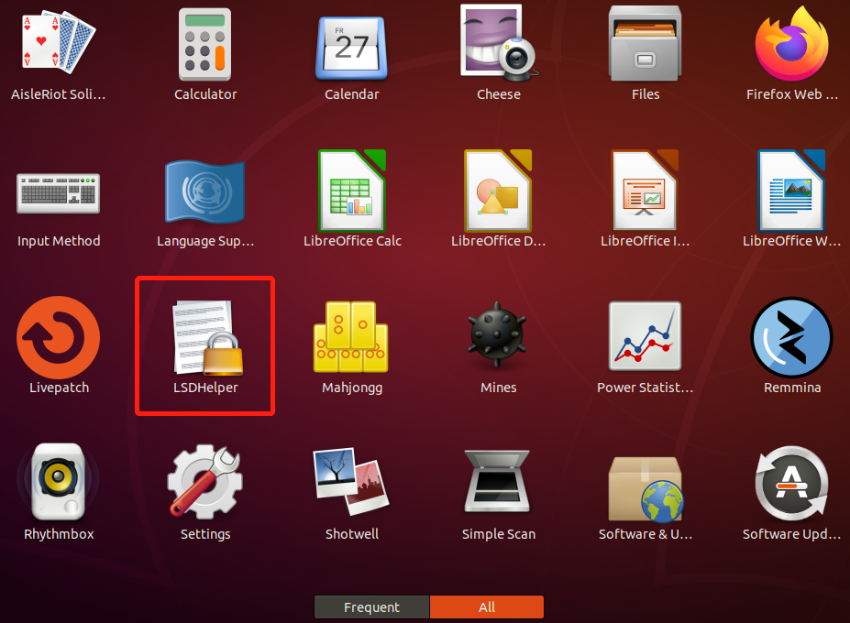
任务栏显示如下终端安全图标，同时右键菜单里出现如下终端安全菜单项，表示安装成功：





* 1. Ubuntu系统

应用程序列表中显示如下终端安全图标，表示安装成功：



1. 文档安全区域和密级
   1. 文档默认安全区域和密级

文档被加密时会设置默认的安全区域和密级，可按需手工调整；每台计算机有自己的文档默认安全区域和密级规则（由计算机所属终端安全角色决定），基于文件需要协同分享的最常见范围进行默认设置，在分享给他人时，按需调整区域和密级；各角色文档默认安全区域和密级见附录1：角色权限对照表。

* 1. 文档安全区域和密级查看
     1. Windows系统

可以通过 右键菜单 – 属性 – 加密 – 访问权限 查看文档的安全区域和密级：



* + 1. Mac和Ubuntu系统

暂不支持查看文档的安全区域和密级。

* 1. 文档安全区域和密级修改

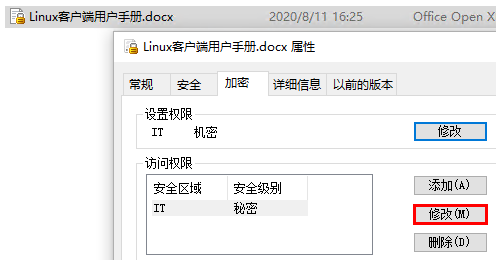
需要特殊保密的文档可手动提升文档的安全级别。

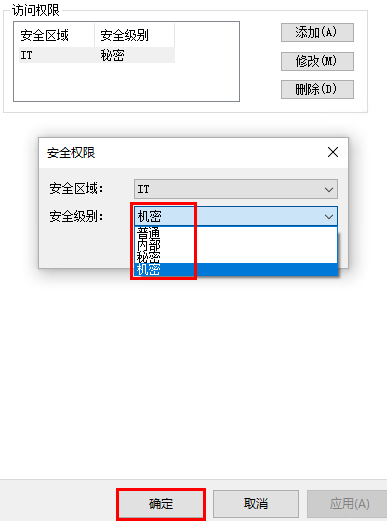
内部进行文档共享要确保对方有访问权限，没有权限的需要文档创建者降低文档的安全级别。

* + 1. Windows系统

可以通过 右键菜单 – 属性 – 加密 – 访问权限 – 修改 来修改文档的安全区域和密级：

降低“访问权限”时，无需修改“设置权限”；提升“访问权限”时，需要同步将“设置权限”提升到相同的区域和密级。





* + 1. Mac和Ubuntu系统

暂不支持修改文档的安全区域和密级。

* 1. 计算机可访问的文档安全区域和密级

每台计算机可访问自己权限范围内的安全区域和密级的加密文档（由计算机所属终端安全角色决定），各角色计算机的安全区域和密级的访问权限见附录1：角色权限对照表。

对于Windows系统，可以通过客户端菜单 加密系统信息 – 显示当前安全对象 – 安全区域 来查看当前计算机可访问的安全区域和密级（Mac和Ubuntu暂不支持该功能）：





* + 1. 权限申请及变更

员工在入职时由部门负责人在“OA入职流程”中指定该员工所属的终端安全的角色。

员工在转岗时由转入部门负责人在“OA转岗流程”中指定该员工所属的终端安全的角色。

员工若想要进行终端安全角色变更，可通过“OA权限申请流程”发起申请，由部门负责人审批通过后方可变更。

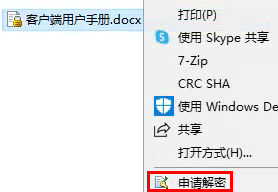
1. 加密文档申请解密

外部合作伙伴无法打开加密文档，如文档需要外发进行交流，需先申请解密。

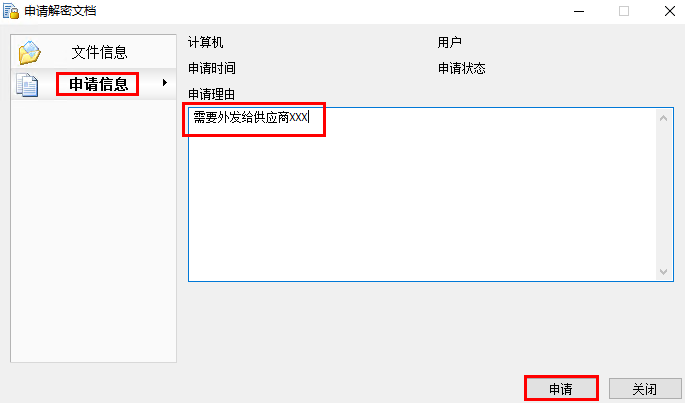
基于工作便捷性的考虑，申请解密流程暂不设置审批人，申请后文档自动解密，服务器上会保留申请解密记录。

* 1. Windows和Mac系统

1. 选中要解密的文件，右键 – 申请解密：



1. 填写申请理由：



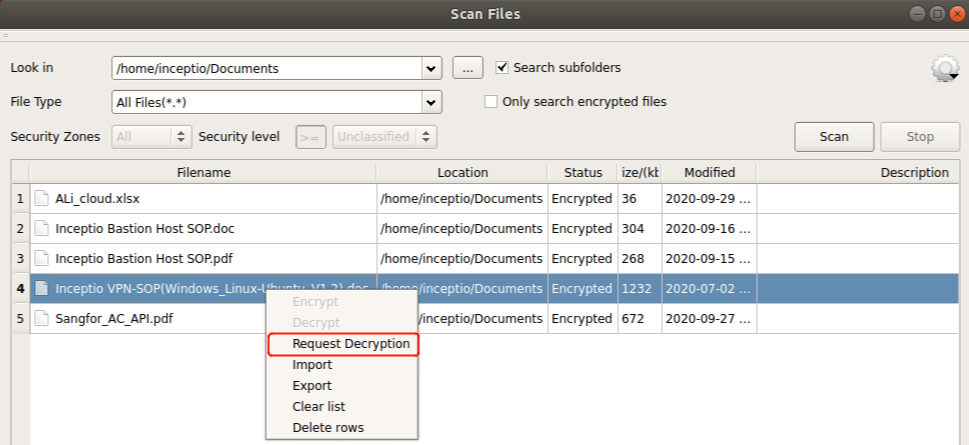
1. 文档自动解密，并在服务器上保留申请解密记录：



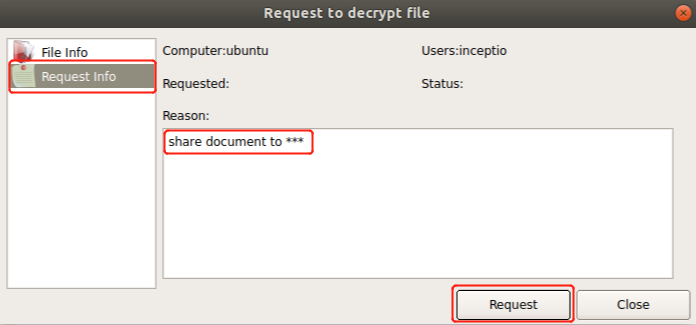


* 1. Ubuntu系统

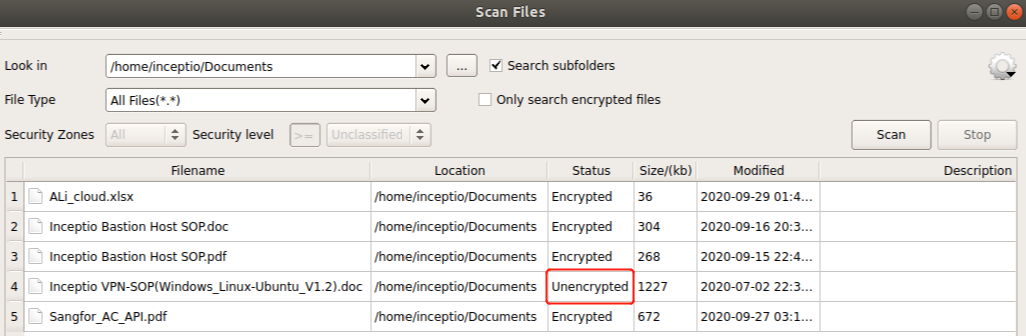
1. 通过终端安全客户端搜索出要解密的文件，选中文件 - 右键 – 申请解密：

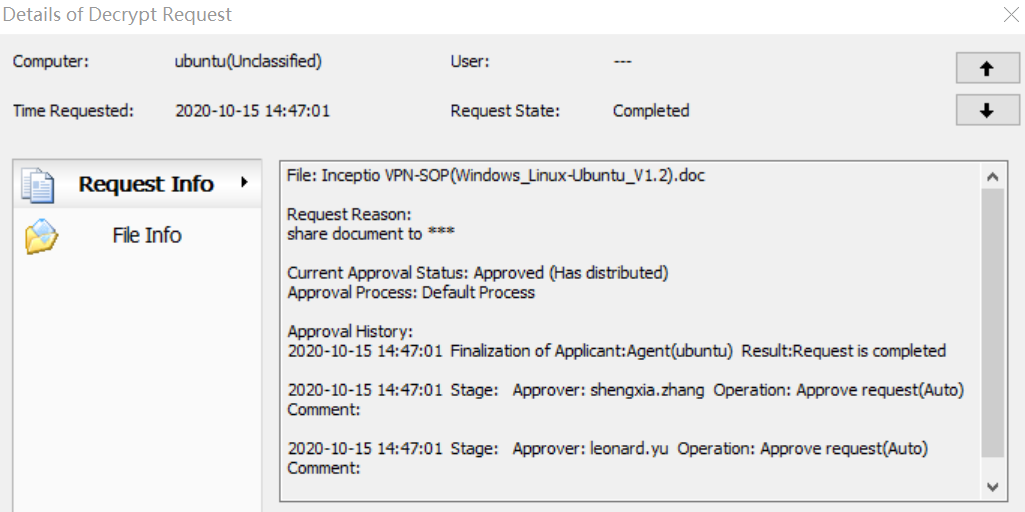


1. 填写申请理由：



1. 文档自动解密，并在服务器上保留申请解密记录：





1. 浏览器使用规则

访问公司如下受保护的应用系统只能使用Firefox浏览器：

Confluence：https://confluence.inceptio.tech

JIRA：https://jira.inceptio.tech

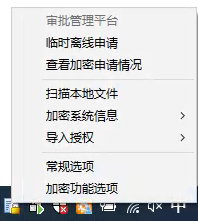
GitLab北美：https://gitlab.rd.inceptioglobal.ai

GitLab上海：https://inceptio-tech.com

访问其它网站推荐使用Chrome等其它浏览器（Firefox也可以访问但是不能上传附件，且有些页面因为安全原因会出现无法加载或无法连接服务器的情况）。

1. 客户端菜单操作说明
   1. Windows - 客户端托盘图标右键菜单

右击客户端托盘图标，弹出如下菜单：



* + 1. 审批管理平台

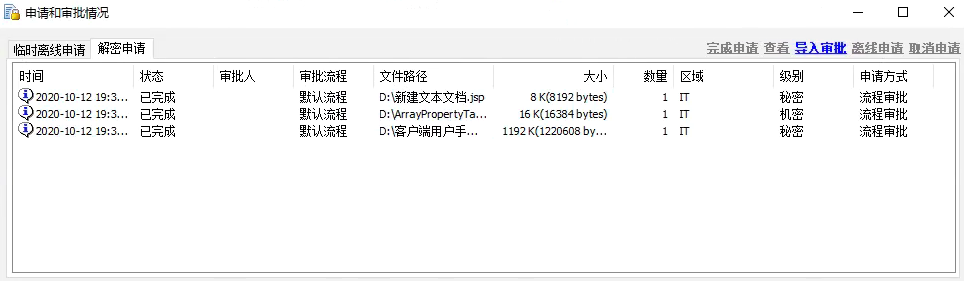
用于对解密申请进行审批，暂不开启该功能。

* + 1. 临时离线申请

当长期在无法连接网络的环境中使用办公电脑时，需要进行此项申请，由于已经有了容灾措施，不需执行该操作。

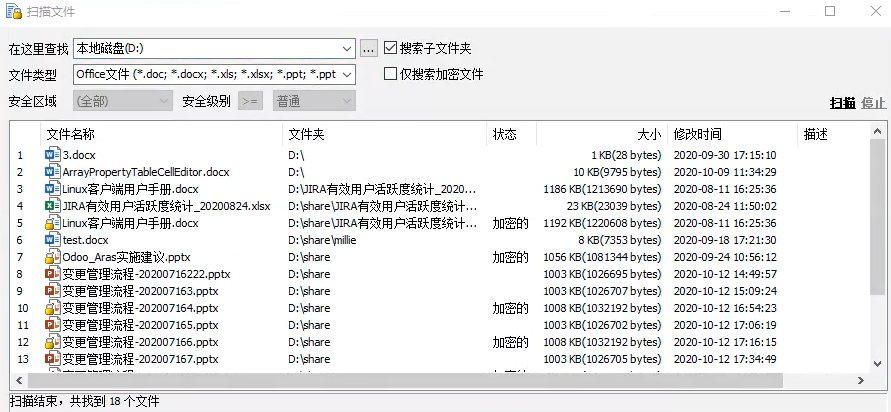
* + 1. 查看加密申请情况

查看自己的解密申请和临时离线申请的审批进展，由于目前启用了自动审批功能，不需在此进行查看：



* + 1. 扫描本地文件

根据目录和文件类型搜索查看文件的加密情况：



* + 1. 加密系统信息
* 显示当前授权进程

管理员排查问题时使用，无需执行此操作。

* 显示当前安全对象

客户端允许进行的操作：



白名单授权软件：



允许访问的文档安全区域和密级：



加密文档的默认安全区域和密级：



* 查看加密系统日志

管理员排查问题时使用，无需执行此操作。

* 查看离线信息

管理员排查问题时使用，无需执行此操作。

* 强制更新策略

当服务器端策略进行了更新时，可通过该操作强制触发策略配置更新到客户端。日常使用不需执行该操作。

* + 1. 导入授权
* 导入长期离线授权文件

管理员排查问题时使用，无需执行此操作。

* 导入USBKEY授权文件

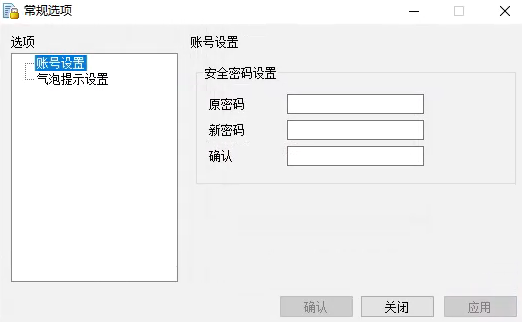
管理员排查问题时使用，无需执行此操作。

* 导入临时离线延时码

管理员排查问题时使用，无需执行此操作。

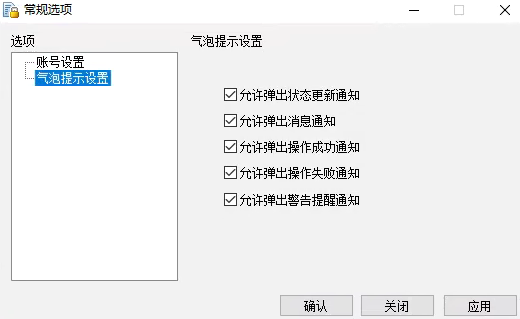
* + 1. 常规选项
* 账号设置：安全密码设置

与 加密功能选项 - 安全密码输入设置 配合使用，如果设置客户端操作需要输入密码，则此处需设置密码。从操作便捷性考虑，不建议设置密码，建议离开办公电脑时对电脑进行锁屏，防止恶意操作：



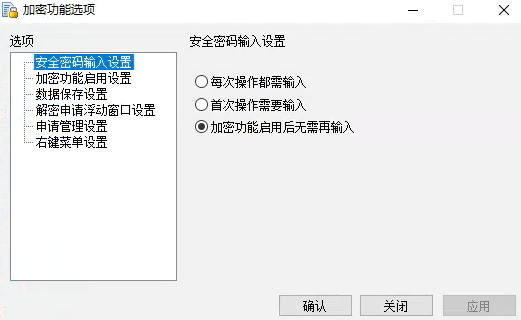
* 气泡提示设置

设置客户端的哪些行为会弹出气泡提示，可按需进行设置：



* + 1. 加密功能选项
* 安全密码输入设置

设置客户端操作是否需要输入密码进行验证，从操作便捷性考虑，建议使用默认设置“加密功能启用后无需再输入”，建议离开办公电脑时对电脑进行锁屏，防止恶意操作：



* 加密功能启用设置

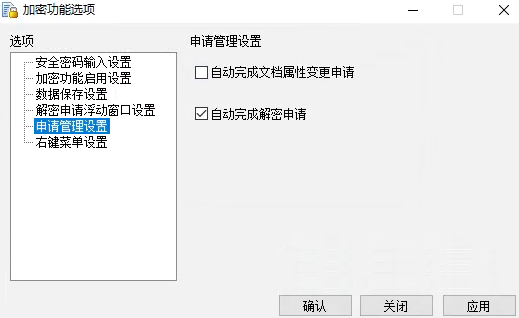
已统一进行了设置，无需手工进行设置。

* 数据保存设置

加密系统日志的时间，保持默认即可，无需进行设置。

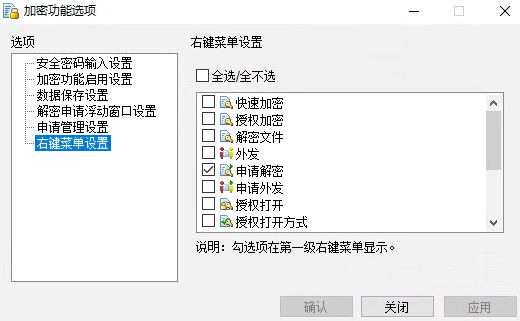
* 解密申请浮动窗口设置
* 申请管理设置

设置申请是否自动完成，保持默认即可，无需进行设置：

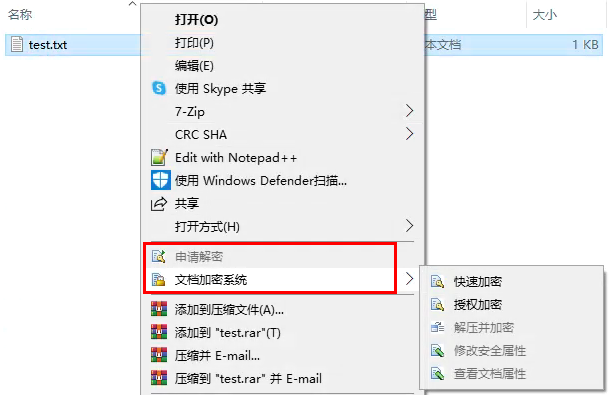


* 右键菜单设置

设置在右键菜单中，哪些操作项在一级菜单显示，哪些在二级菜单显示：



未勾选的会在“文档加密系统”下的二级菜单显示：

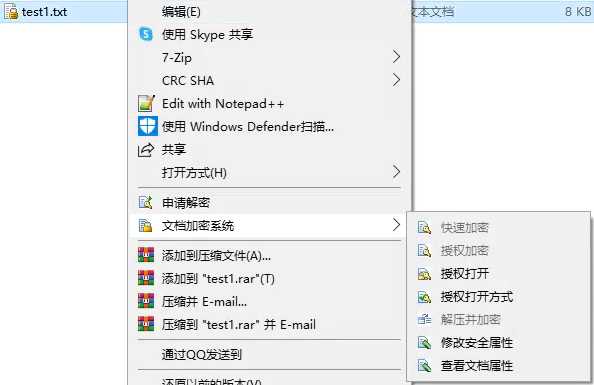


* 1. Windows – 文件右键快捷菜单

右击文件，在快捷菜单中会出现终端安全相关操作项。

* + 1. 对于加密的文档

可执行的操作有：申请解密、授权打开、授权打开方式、修改安全属性、查看文档属性：



* 申请解密

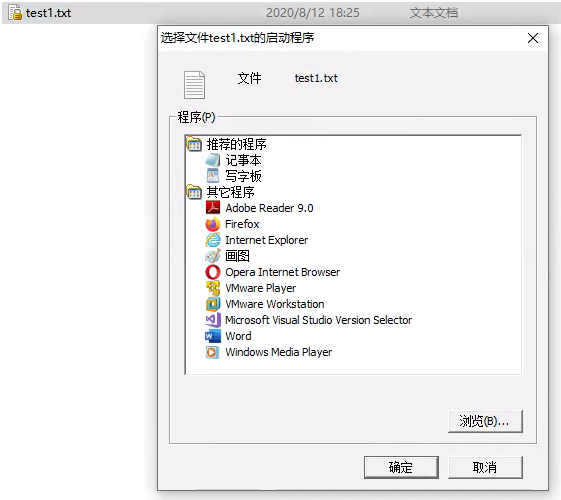
对加密文件申请解密（申请后文档自动解密，服务器上会保留申请解密记录）。

* 授权打开

功能同Windows右键快捷菜单中的“打开”，使用当前文档类型对应的默认的应用程序打开。

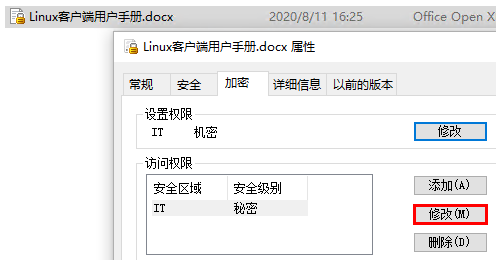
* 授权打开方式

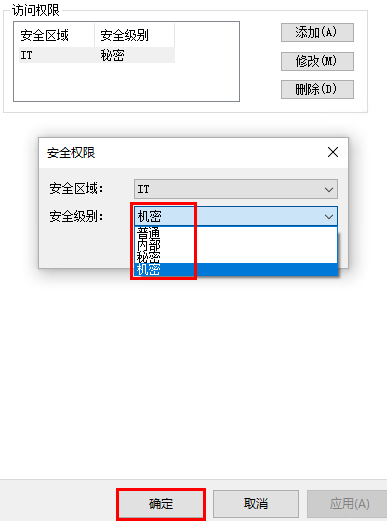
功能同Windows右键快捷菜单中的“打开方式”，选择应用程序打开当前文档：



* 修改安全属性

修改文档的安全区域和密级：





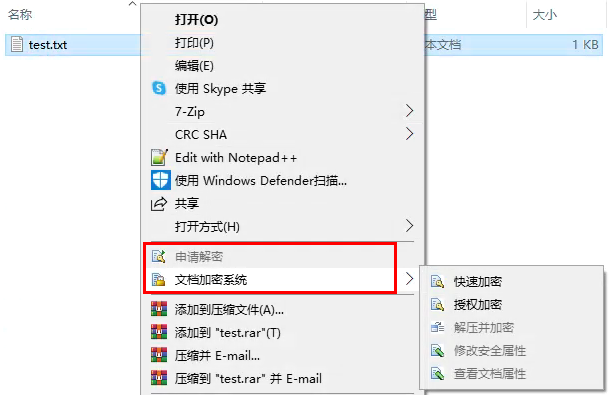
* 查看文档属性

查看加密文档的安全区域和密级：



* + 1. 对于未加密的文档

可执行的操作有：快速加密、授权加密：



* 快速加密

对选中的文档进行加密。

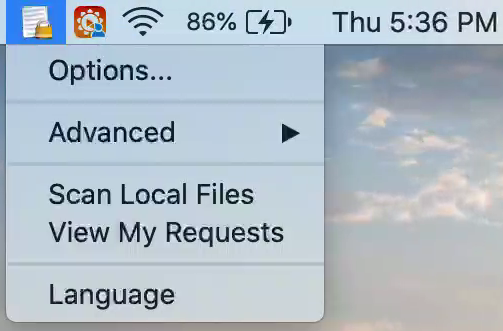
* 授权加密

对选中的文档进行加密，同时弹出文档加密属性窗口，可在该窗口中修改文档的安全区域和密级：



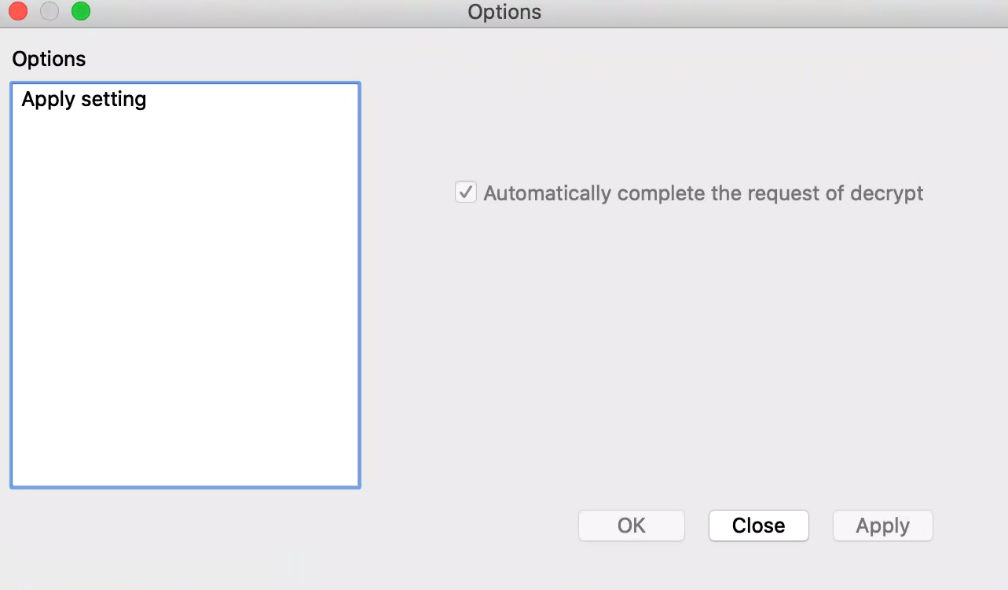
* 1. Mac系统 – 客户端托盘图标右键菜单

右击客户端托盘图标，弹出如下菜单：



* + 1. 选项

解密申请相关设置，该设置无需修改：

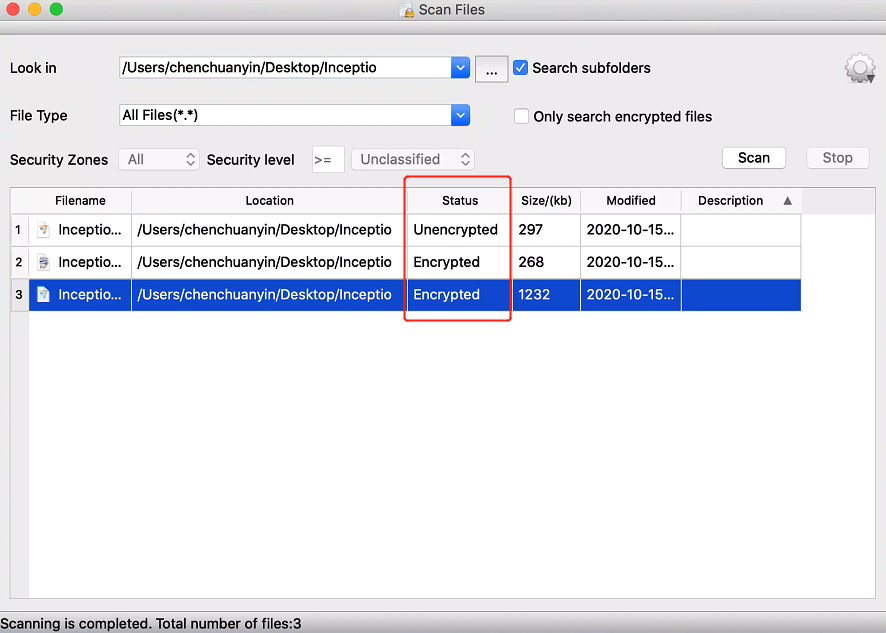


* + 1. 高级 – 策略更新

当服务器端策略进行了更新时，可通过该操作强制触发策略配置更新到客户端。日常使用不需执行该操作。

* + 1. 扫描本地文件

根据目录和文件类型搜索查看文件的加密情况：



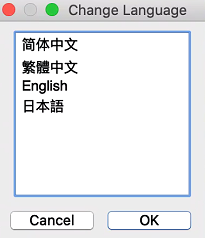
* + 1. 查看申请情况

查看自己的解密申请的审批进展，由于目前启用了自动审批功能，不需在此进行查看：



* + 1. 语言

用于切换中英文语言，切换后需重启客户端方可生效：

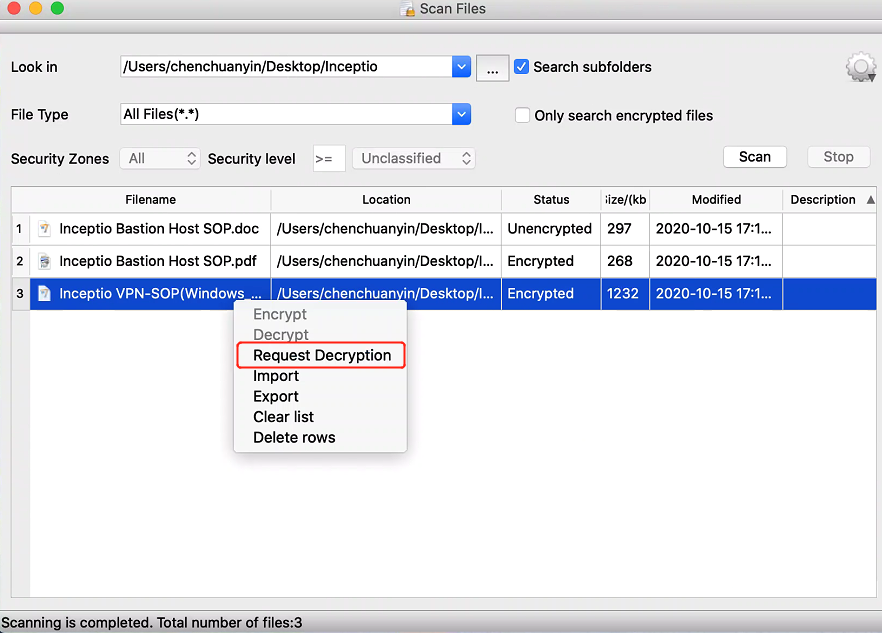


* 1. Mac系统 – 文件右键快捷菜单

右击文件，在快捷菜单中会出现终端安全相关操作项。

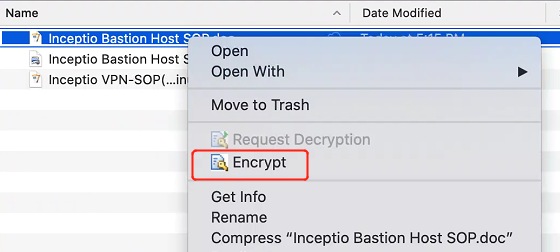
* + 1. 对于加密的文档

可申请解密（申请后文档自动解密，服务器上会保留申请解密记录）：



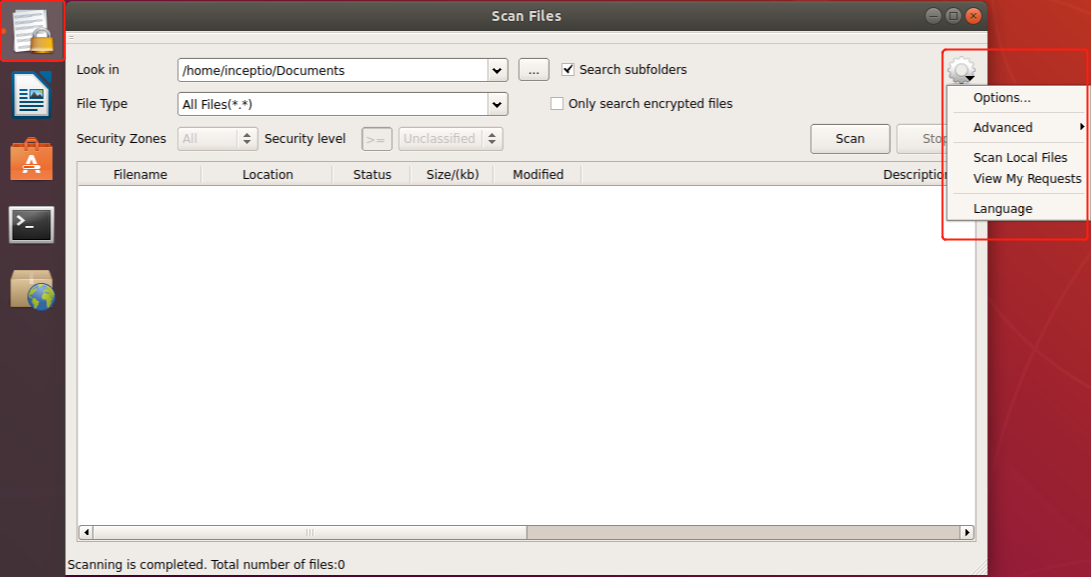
* + 1. 对于未加密的文档

可执行加密操作，对选中的文档进行加密：



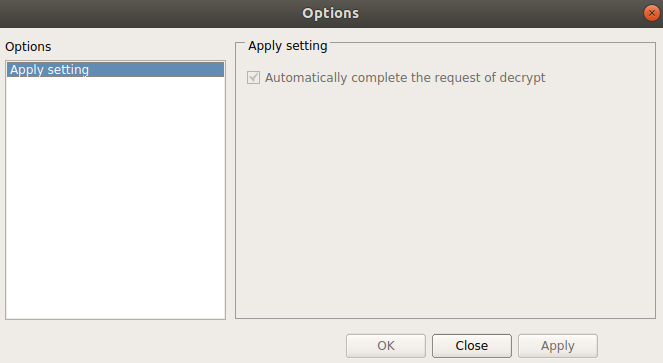
* 1. Ubuntu系统 – 客户端UI界面菜单

打开客户端，单击右上角齿轮图标，弹出如下菜单：



* + 1. 选项

解密申请相关设置，该设置无需修改：



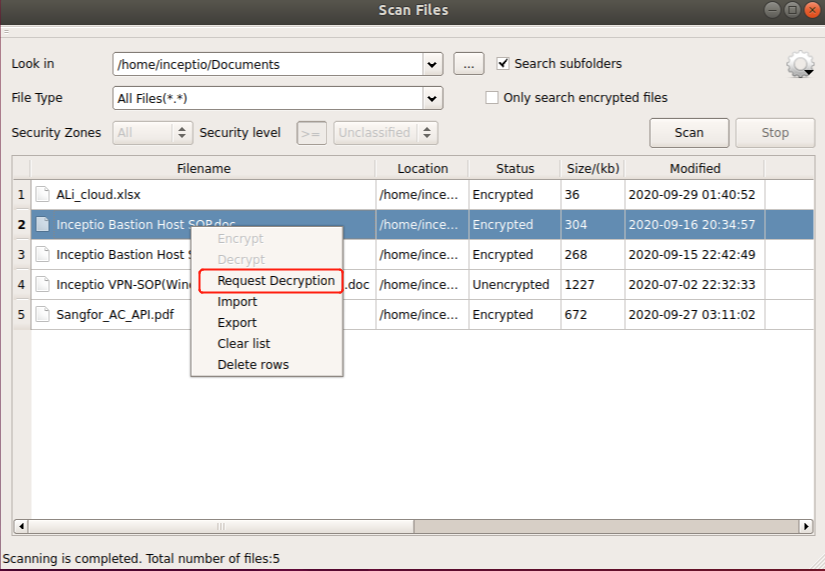
* + 1. 高级 – 策略更新

当服务器端策略进行了更新时，可通过该操作强制触发策略配置更新到客户端。日常使用不需执行该操作。

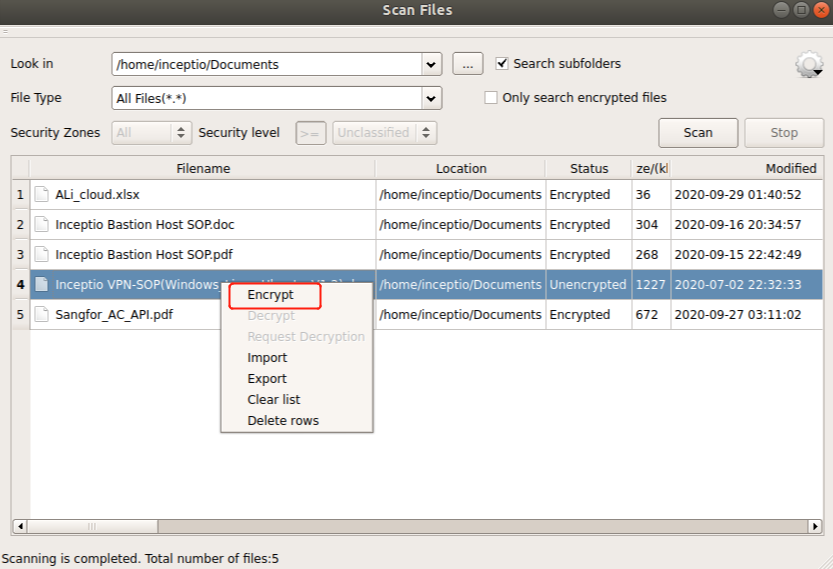
* + 1. 扫描本地文件

根据目录和文件类型搜索查看文件的加密情况。

右键单击加密文档，可以对其进行申请解密操作：

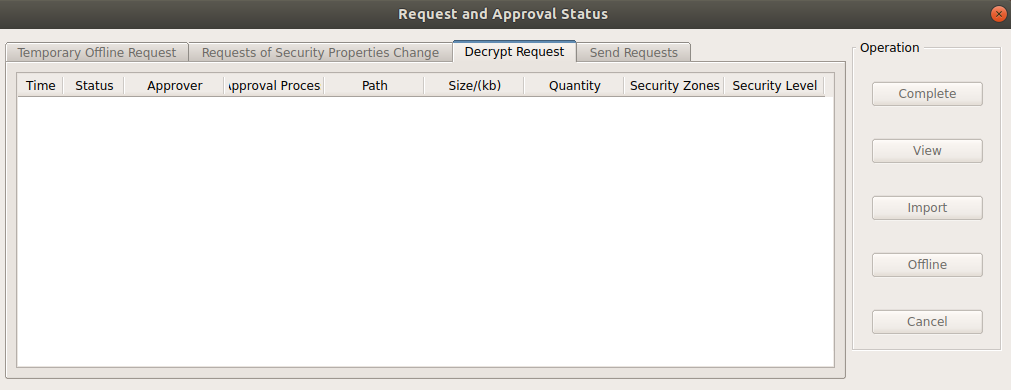


右键单击加密文档，可以对其进行加密操作：



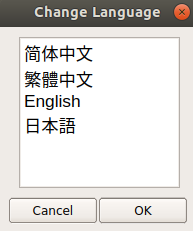
* + 1. 查看申请情况

查看自己的解密申请的审批进展，由于目前启用了自动审批功能，不需在此进行查看：



* + 1. 语言

用于切换中英文语言，切换后需重启客户端方可生效：



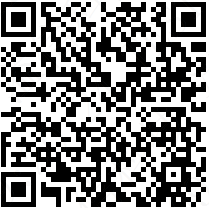
1. 移动端安全文档查看器

安全文档查看器可以实现移动设备在授权情况下能够正常查看加密的文档（不会对加密文档进行解密，移动设备上的其它软件也无法查看加密文档）。

* 1. 下载安装

可通过下载链接地址或扫描二维码的方式进行下载：

* 下载地址：<http://www.tec-development.com/apps/download.html>
* 下载二维码：



根据移动设备的系统自行选择下载安装Android系统APP或者iOS系统APP：



安装完成后，移动设备的桌面会生成一个新的APP图标，即安全查看器，如下图：



**注意：iOS系统安装APP后需要对应用进行“信任”操作**

* iOS 9.0以上的系统：安装APP后打开，会弹出以下提示“未受信任的企业级开发者”：



需要用户自行去“设置-通用-描述文件”信任该应用，如下图：





* iOS 8.0以上的系统：安装APP后打开，会直接弹出提示是否信任该应用，直接点击“信任”即可打开APP。
  1. 申请授权
     1. 连接服务器

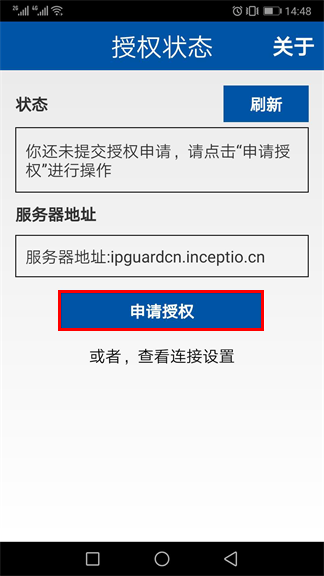
首次打开APP，需要进行服务器连接。

输入连接的服务器域名ipguardcn.inceptio.cn，然后点“连接”：

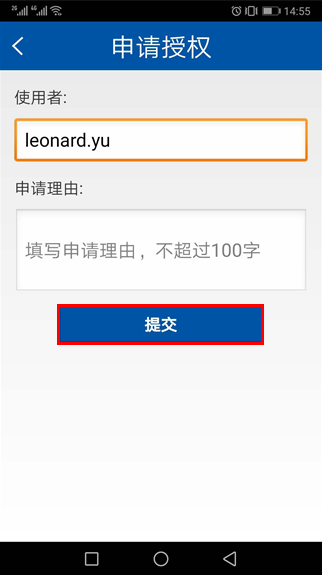


* + 1. 申请授权

若连接服务器成功，则可以点击“申请授权”进行权限申请：



“使用者”填写自己的AD域账号（同OA账号），以便管理员能准确识别申请者；“申请理由”不需填写：

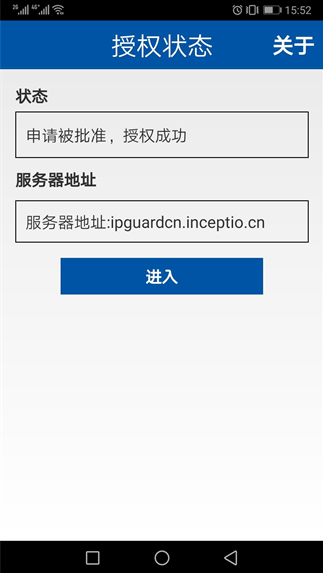


* + 1. 授权状态查看

申请提交成功后，会自动跳到授权状态页面，提示“你的申请已提交，正在等待审批中”：



若此时管理员已批准申请，则授权状态页面会提示“申请被批准，授权成功”，安全文档查看器的使用无需进入APP内，确认授权成功后退出即可：

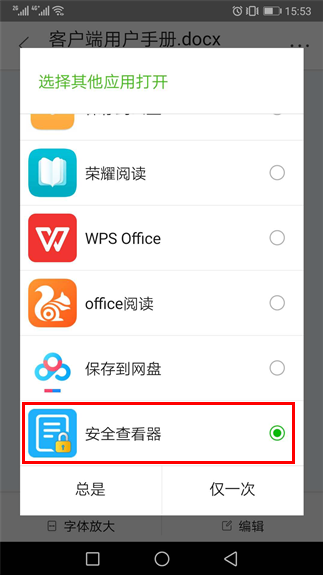


* 1. 功能使用

对于加密文件，若不使用安全文档查看器则无法打开，提示“文件预览失败”或“文档加载失败”：



选择使用安全查看器打开则可以正常查看（基于信息安全角度考虑，会在文档查看界面添加水印）：





安全文档查看器仅可访问自己权限范围内的加密文档（权限同员工计算机）。

无法打开超出自己权限的加密文档，会提示“没有权限打开该文件”：



* 1. 安全文档查看器支持打开的文件格式
     1. iOS系统

Office文件：doc，docx，ppt，pptx，xls，xlsx；

纯文本文件：txt，c，h，cpp，hpp等；

图片文件：bmp，png，jpg，gif；

网页文件：htm，html；

iWork文档：pages，key，numbers（不支持2013 iWork文档）；

其它文件：PDF，RTF；

* + 1. Android系统

Office文件：doc，docx，ppt，pptx，xls，xlsx；

纯文本文件：txt，c，h，cpp，hpp等；

图片文件：bmp，png，jpg；

网页文件：htm，html；

其它文件：PDF；

1. 附录：
   1. 附录1：角色权限对照表
   2. 附录2：软件白名单