**IP-guard用户使用培训-加密模块**

目录

[一、加密概述 1](#_Toc457221002)

[二、术语介绍 2](#_Toc457221003)

[三、工作流程 3](#_Toc457221004)

[1、普通员工 3](#_Toc457221005)

[2、加密管理员 5](#_Toc457221006)

[3、部门管理人员 9](#_Toc457221007)

[a、代理管理员 9](#_Toc457221008)

[b、安全审批 9](#_Toc457221009)

[c、Web审批 18](#_Toc457221017)

[四、其他功能 20](#_Toc457221018)

[1、外发系统 20](#_Toc457221019)

[2、全盘扫描 21](#_Toc457221022)

[3、备用服务器 21](#_Toc457221025)

[4、加密文档备份服务器 23](#_Toc457221028)

# 一、加密概述

1. 加密的过程是自动的
2. 在任何介质中都是加密的
3. 重要文档需要授权后才能解密或带出

# 二、术语介绍

1. **授权软件**

授权软件是用于编辑重要文件的软件，(如Microsoft Word、AutoCAD、Photoshop、C++等) 。

预定义授权库：IP-GUARD默认的授权软件库，不在这个库的软件则不会加密文件。

自定义授权：用户通过进程名，加密文件，过滤文件三项简单定义授权软件。

1. **安全区域和级别**

安全区域和级别，是用来区分企业内部不同的客户端对加密文档的访问权限，可以理解为部门和行政级别。

默认安全区域：公共安全区域，也就是所有人都属于这个区域。

自定义区域：管理员可自定义客户端所属安全区域，如市场部、财务部。

安全级别：普通、内部、秘密、机密和绝密，从普通到绝密，安全等级依次递增。

文档默认安全属性：能访问此文档的安全区域和级别。

例：客户端A具有市场部的普通级别的权限，则他能访问市场部普通级别的加密文档，不能访问财务部普通级别的文档，也不能访问市场部内部级别的文档，B是新启用加密的客户端，未设置默认文档安全属性，所以B生成的加密文档是公共安全区域普通级别，A是可以看得，当我设置B的默认文档安全属性为财务部普通级别的文档，B生成的文档才是财务部普通级别的文档，这时A就不能看了。

1. **在线与离线（客户端状态）**

当客户端能连上服务器时，为在线状态；

当客户端无法连上服务器时，为离线状态。，离线无法正常使用加解密。

1. **紧急模式**

当主服务器存在问题，如停止或崩溃时，备份服务器便启动，显示为紧急模式，代表当前IP-guard加密系统进入紧急模式，客户端此时连接到备份服务器，转变为紧急模式，具备在线时的加解密权限。

1. **解密/外发**

企业内的加密文档有时候需要发给指定的企业外部人员查看，则可以把文档解密或生成外发文件发给对方，没有权限的人通过申请解密或外发，由管理员审批来实现。

解密和外发的区别：

加密文件解密后文件就是明文，可以任意修改和转发；

外发文件还是密文，需要通过外发查看器才能进行查看，生成外发文件时可以对文件的相关权限进行控制。

**f．离线授权**

客户端在离线状态下（出差,笔记本），其离线加解密权限需要登入授权后才能正常使用。离线授权状态可以通过在线进行临时离线申请或者直接由管理员设置长期离线权限

# 三、工作流程

应用加密系统之后会增加工作流程如下：

1、普通员工：

1. 直接解密/外发/变更安全属性
2. 申请解密/外发/变更安全属性/临时离线

2、管理员：

1. 权限设置与审批
2. 代理管理员：
3. 由管理员指定某台加密客户端的代理审批申请
4. 具体在针对不同使用者的培训中在具体介绍

## 1、普通员工

1. **托盘图标**

加密客户端启用后，会出现图标；图标的几种状态

|  |  |
| --- | --- |
|  | 启动； |
|  | 停止； |
|  | 离线； |
|  | 离线授权； |
|  | 紧急模式。 |

1. **托盘图标的菜单说明**

选项-参数设置（安全密码，离线授权登入，数据保存，解密申请浮动窗口）

临时离线申请和导入授权码

本地扫描工具：扫描本地目录文件，可以批量解密，有解密权限的话可以直接加密文档

导入授权文件可以导入离线授权文件实现离线正常使用加解密

查看申请信息（四种申请）：客户端员工可以通过这里查看自己申请的信息，以及是否批准，同时进行批准后的操作。

查看本地加密客户端设置：加密权限，安全区域，授权软件）

登录代理管理员可以登录代理管理员控制台，对各种申请进行审批

1. **文档右键菜单**

解密/申请解密

外发/申请外发

申请变更安全属性

1. **常用工作操作**

加密/解密/外发

申请解密/外发/查看申请信息

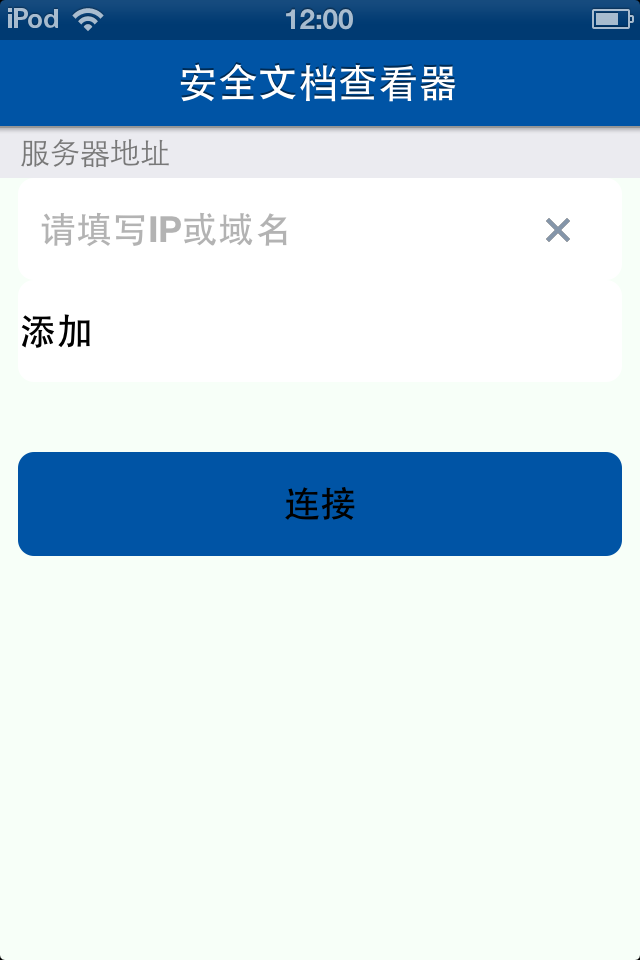
离线申请

流程：申请（查看）-审批-申请后操作

1. **安全查看器**

首次打开APP，需要输入连接的服务器地址，服务器地址支持填写IP或域名，如下图：

输入服务器地址后，点击连接，连接服务器；



输入申请信息

若连接服务器成功，则可以点击“申请授权”进行申请，填写使用者和申请理由，提交申请；填写申请信息页面如下图：



管理员授权后，员工可点击启动安全查看器APP，进入APP后打开文档；也可在在其它APP中， 选中文档，以其它方式打开，选中“安全查看器”打开。

安全文档查看器的主页，如下图：



## 2、加密管理员

1. **控制台管理**

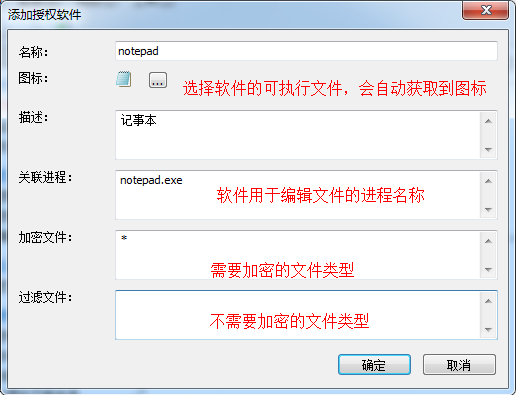
菜单->文档安全管理

1. **加密启用/禁用**

计算机->加密管理功能->启用透明加密

1. **授权软件**

自定义授权软件



1. **安全区域管理**
2. **加密客户端权限设置**

可对单个计算机设置权限，也可对计算机组设置权限；单个计算机没有设置权限时，会继承计算机组的权限。用户模式仅支持域用户。

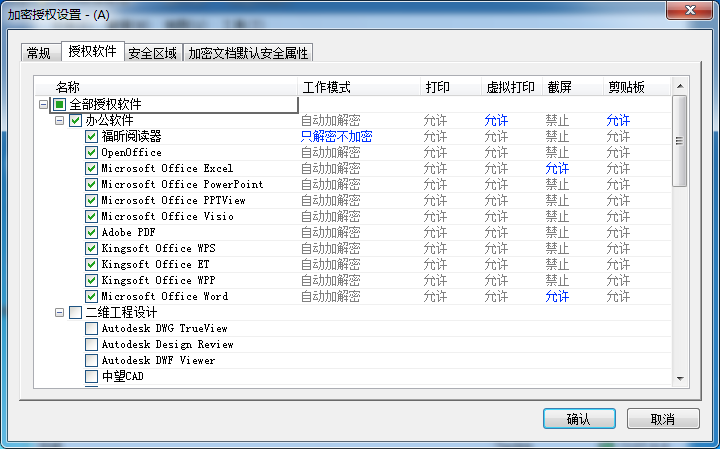
1. **加密常规设置**

可设置客户端允许登录代理管理员，进行申请审批操作。

1. **授权软件工作模式**

自动加解密：打开文件时自动解密，保存文件时自动加密

只解密不加密：打开文件时自动解密，保存文件时不加密



1. **安全区域**

公共安全区域，安全级别。

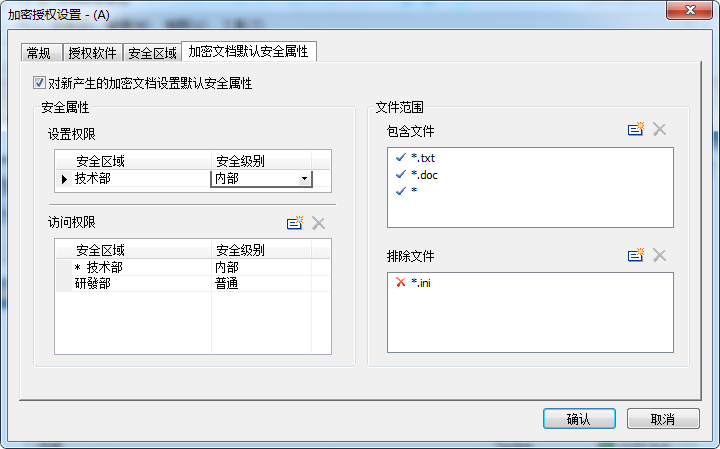
1. **加密文档默认安全属性**

设置权限：修改文档安全属性的权限可为其他部门或其他级别。

访问权限：打开文档的权限，必须有自己安全区域及所处级别以下。

包含文件：需要采用默认安全属性的文档类型。

排除文件：不需要采用默认安全属性的文档类型。



1. **加密参数设置**

容灾时间：加密系统在客户端连不上服务器时，可正常使用的时间。客户端状态为“紧急模式”。

邮件白名单：将加密文档发到指定的邮箱时，自动解密。仅支持普通协议邮件（SMTP协议）。

长期离线与临时离线的区别：长期离线授权的权限可与在线时不同；临时离线是在线权限的延长。

1. **加密文档操作日志**

查询加密操作；可导出备份文档。

1. **控制台本地扫描工具**
2. **备用服务器管理**
3. **远程加密文档管理**
4. **各种申请审批流程**

解密，外发，离线，安全属性变更

## 3、部门管理人员

### a、代理管理员

由管理员指定某一台客户端代理审批工作，一般用在管理员不在公司时指定进行某台 客户端代理审批加密客户端的申请。

审批的账户和密码（账户管理），登陆、代理控制台、设置、审批管理

对于外发申请、临时离线申请、安全属性变更申请的审批也是和解密申请审批一样的操作。

代理管理员审批离线客户端的申请操作。

### b、安全审批

### 登录应用程序

首次启动APP，需要用户填写服务器地址、管理员账号、密码；

* 服务器地址：填写格式为 web服务器IP/域名:端口号/oapprove；
  + 端口号是指web服务器安装时手动设置的端口号（默认是80），默认端口不需要填写亦可；非默认端口，IP后面必须填写端口；
  + 只支持http协议（http可不写），不支持https协议；
* 管理员账号：填写的是IPG管理员的账号

注意：admin和audit账号为限制账号，不可登录

* 密码：对应管理员账号的密码



登录成功后，APP退出登录，APP会自动保存上次登录的服务器地址和账号（不保存密码），下次登录时只需输入正确密码，即可登录；

注意：登录成功，若通过系统自带退出后台的方式，使APP退出后台，不会退出APP当前账号的登录；下次启动APP后，会自动使用上次登录的账号登录；

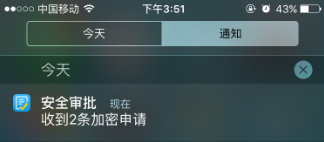
### 查看或审批申请

1.接收新的申请通知

启动安全审批APP并登录成功，保持APP在后台运行，客户端提交桌面安全申请/文档安全申请，则设备即可及时收到新的申请的通知信息；

系统通知栏会显示安全审批的通知：

1. iOS系统的通知：



1. Android系统的通知：



同时APP主页里的菜单栏，也会对应以“红点”标识有新的申请，如下图：



注意：通知栏显示新消息的前提，是系统设置安全审批应用为“允许通知”

### 加密申请管理

加密申请管理页面分为两部分，等待审批和申请总览。等待审批页面显示当前处在审批中的申请，申请总览页面显示全部申请。

其中加密申请管理各申请都支持审批操作（同意/拒绝），解密申请、外发申请和安全属性变更申请还支持文件预览的操作，但不能更改申请的其他信息。

### 查看待审批申请

等待审批页面，显示当前处在审批中的申请记录，能查看仅由当前登录用户审批的所有类型的申请记录（包括解密申请、外发申请、安全属性变更申请、临时离线申请）。



1. 点击该条申请后，会打开该申请的明细页面；
2. 等待审批页面，包括“快速查询”和“查询条件查询”；

**快速查询**：查询字段支持对“流程名”或“文件名”的查询；其他字段不支持；在下图中的搜索框输入流程名或文件名，点击即可完成快速查询；



**查询条件查询**：查询条件，默认是折叠的，点击折叠按钮后可以展开显示查询条件。选择条件，点击【查询】按钮进行完成查询，支持多条件组合搜索，查询条件包括申请类型、时间、文件名以及流程名。点击【重置】，可以重置查询条件为默认情况；（与桌面申请管理的类似）

### 审批申请

支持解密申请、外发申请、安全属性变更申请和临时离线申请的审批。

如果当前登陆的管理员在审批流程中，能执行审批操作（同意/拒绝），不能更改申请的其他信息。以下以解密申请为例，其他申请审批过程类似。

管理员在等待审批页面，点击查看某解密申请，查看申请明细，如下图：



* 点击“同意”，则该申请被批准，如果有下一环节，则会进入下一环节审批。如果没有下一环节，则该审批结果会返回到客户端，客户端收到审批通过的消息，可以进行相关操作，如完成解密操作。
* 点击“拒绝”，则该申请被拒绝，如果有上一环节，则会返回上一环节审批。如果没有上一环节，则该审批结果会返回客户端，客户端收到审批被拒绝的消息，不可以进行相关操作。

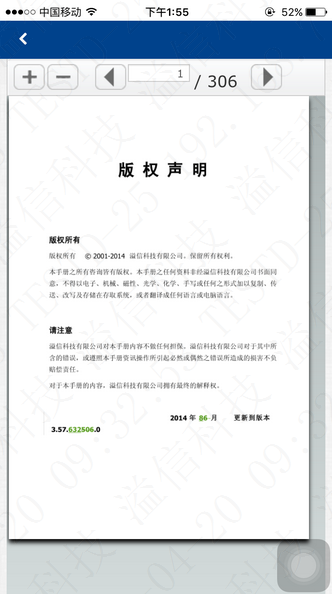
### 预览文件

解密申请、外发申请和安全属性变更申请支持文件预览，目前只支持txt，doc，docx，ppt，pptx，pdf文件的预览，excel文件的转换效果不好，暂时不支持

点击“申请信息-文件信息”中的>，查看文件信息详细情况，默认显示文件名和文件大小；点击可显示文件的安全属性



当客户端在线且文件存在时，点击按钮可以正常预览此文件；预览效果如下图，可点击左上角的<返回上一层界面；



注：大于20M的文件，或不支持的文件格式文件，不提供预览功能，【文件信息】标签页看不到预览按钮。

若客户端已离线，或文件已被修改、重命名、删除，则有相应提示。



**注：如需要使用预览功能，web服务器需要做以下配置操作**

1、安装OpenOffice.org 3.4.1

程序路径：

\\192.168.1.1\setup\Office\Apache\_OpenOffice\_incubating\_3.4.1\_Win\_x86\_install\_zh-CN.exe

(1)安装后需要配置，右键OpenOffice快捷方式--属性，在目标后面添加参数

-headless -accept="socket,host=127.0.0.1,port=8100;urp;" -nofirststartwizard，然后以管理员身份启动OpenOfiice（任务管理器有soffice.bin和soffice.exe进程）。

(2)将已增加参数的OpenOffice快捷方式，放到开始菜单-所有程序-启动中，设置为开机启动；

2、安装java

程序路径：\\192.168.1.1\setup\Develop Tools\JAVA

安装后，需要设置为全局变量或将安装目录bin文件夹下的java.exe拷贝到C:\Windows\SysWOW64\目录下（64位系统）或者C:\Windows\system32\目录下（32位系统）。

### 申请总览

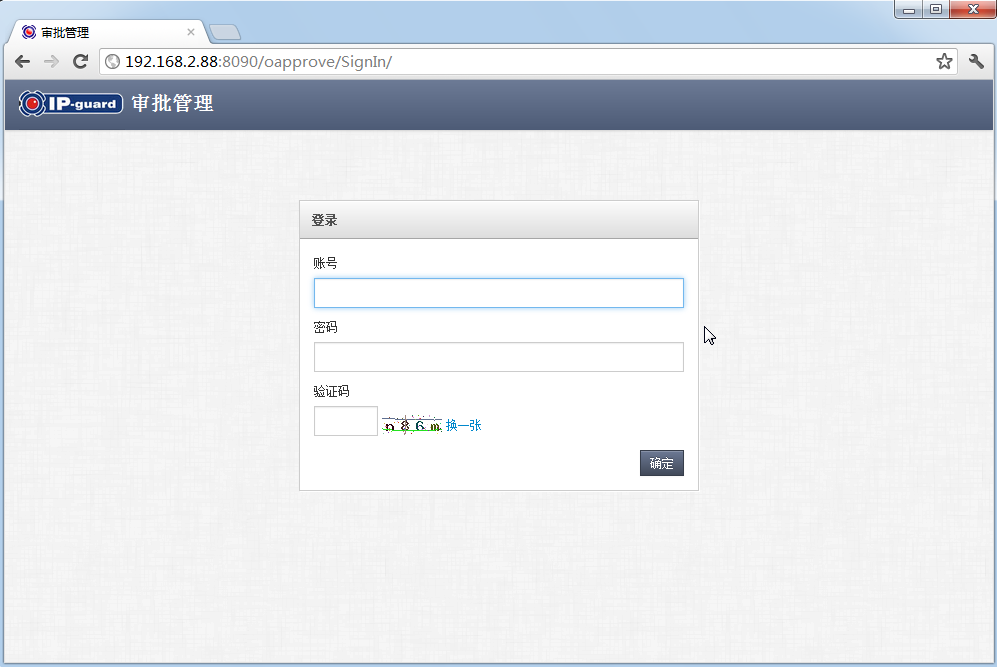
点击申请总览，跳转到全部申请页面，默认显示服务器所在时间的一个月内的申请。

显示当前登陆用户所能查看的所有类型的申请记录。与等待审批界面的查询类似，界面上的查询条件默认是折叠的，点击后可以选择条件进行查询，支持多条件组合搜索，查询条件包括申请类型、申请状态、时间、文件名、审批者以及流程名。如下图：

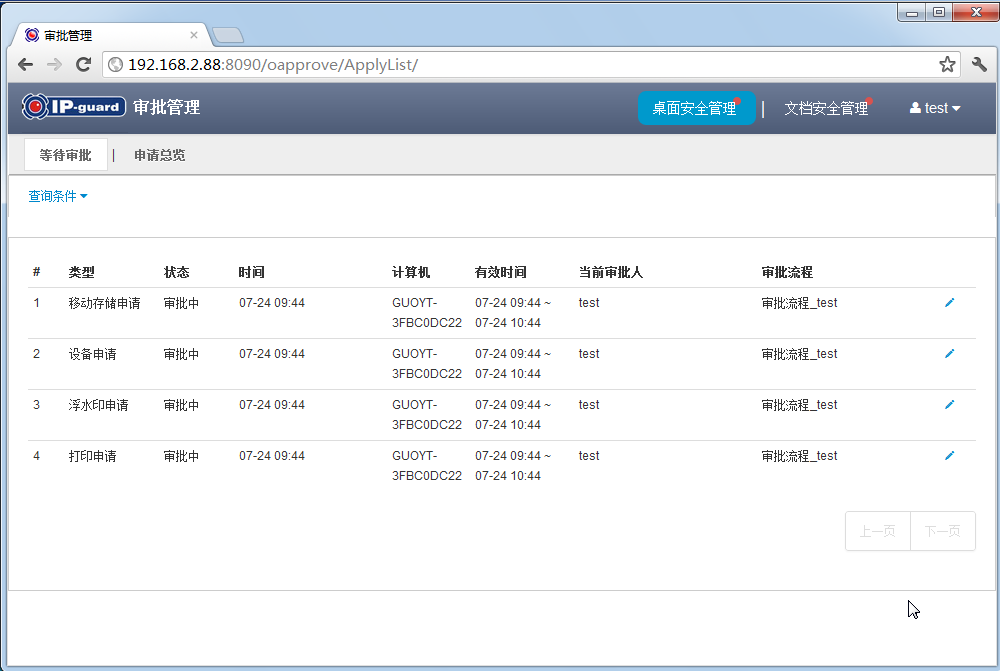


### c、Web审批

在浏览器地址栏输入网上审批系统网址，格式为：<http://网上审批系统服务器IP:端口号> （这个端口号是安装时手动设置的端口号，默认是80，端口号前有冒号），进入登录页面，例如：<http://192.168.2.88:8090>，如下图：



输入正确的管理员帐户、密码和验证码，点击登录，可以成功跳转到网上审批界面，用没有审批权限的管理员也是可以成功登录的，只是登录后看不到任何数据。登录后默认显示桌面安全管理，可以通过点击文档安全管理进行切换，界面如下图：



登录以后能否同时管理普通和加密模块申请，取决于主服务器所注册的模块。其中有普通模块（含打印、移动存储、设备中任意模块）登陆后则能管理普通模块申请。

WEB审批界面显示的语言可以根据系统语言自动调整，支持简体中文、繁体中文、英文显示，也可以手动切换语言。

# 四、其他功能

## 1、外发系统

## 外发查看器安装及注册流程

1. **通用识别码：**

* 直接由管理员在外发对象设置界面，添加外发对象。
* 对这个外发对象创建“通用识别码”。然后对外发对象授权，设置有效时间及导入密码（密码可不设置），导出授权文件，并将授权文件发到安装外发查看器的电脑。
* 安装外发查看器的电脑只要导入这个“通用识别码”生成的授权文件文件就可以授权成功。

1. **绑定识别码：**

* 使用外发查看器的安装程序安装外发查看器，安装完成后，运行外发查看器并进入设置界面。
* 将设置界面的“识别码”发给管理员，管理员在外发对象管理界面，导入“识别码”，然后对外发对象授权，设置有效时间及导入密码（密码可不设置），导出授权文件，并将授权文件发到安装外发查看器的电脑。
* 进入外发查看器的设置界面，导入授权文件，完成外发查看器的注册。

## 外发文档查看

标准外发文档，需要安装外发查看器才能查看；可执行文件的外发文档，可以直接运行查看。

* 如果外发文档，有要求同步标准时间，在打开外发文档时，必须进行时间同步才能正常地打开外发文档。
* 查看外发文档的机器，如果可以直接连接互联网，则会自动进行时间同步；如果不能连网，则需要选择“手动同步时间”，记录下操作码，然后在可以连互联网的机器上运行时间同步工具，输入操作码，生成一个确认码，再将确认码在查看外发文档的机器输入，点击“更新”完成时间同步，打开外发文档查看器，查看外发文档的详细信息。
* 如果外发文档未要求同步标准时间，则可直接打开外发文档查看器，查看外发文档。

## 2、全盘扫描

该功能可通过控制台同时对多台客户端设置扫描任务，实现目标客户端的本地磁盘扫描，并加/解密指定的文件。一台客户端可以设置多个加/解密任务，任务按照创建顺序依次执行。

### 创建全盘任务

1. **创建全盘加密任务：**

* 在全盘扫描界面可以查看显示全部计算机和查看有任务的计算机两种模式。
* 点击右边的加号按钮可以添加任务，举例添加全盘加密任务。
* 选中一台电脑，并对这台电脑的常用办公文档进行扫描加密。
* 加密后的文档安全区域通通为测试部普通级别。
* 性能设置勾选”扫描速度优先”

1. **创建全盘解密任务：**

同全盘扫描加密任务类似，不举例。

注意如果文件正在打开或者为只读状态则跳过文档。

### 查看任务

点击这条任务，在任务的下面窗口的任务信息一栏可以看到任务的详细情况，包括任务的进度（百分比），当前扫描的路径。在任务日志一栏可以看到详细的加密解密的信息。

## 3、备用服务器

备用服务器，主要用于在服务器或网络出现故障客户端无法连接服务器时，临时接管客户端，让客户端处于加密紧急模式，可以正常使用加密系统。

备用服务器不存储加密日志，也不能进行审批操作。

### 备用服务器授权

* 在控制台的文档安全管理界面，选择“工具”🡪“备用服务器管理”，打开备用服务器设置界面，设置允许范围，点击“连接密码”，设置用于备用服务器连接的密码。
* 在任务栏中的备用服务器图标上右键，选择“工具”🡪“设置连接参数”，输入主服务器的IP及连接密码，连接成功后，备用服务器就会获得主服务器的授权信息。
* 设置连接参数之后，还可以设置“主动轮询”，设置之后，当紧急模式时，备用服务器会自动去检测指定范围的客户端（默认为所有网段）。

### 备用服务器设置

1. **备用服务器的运行状态**

未启动、未授权、与服务器连接、紧急模式、无法连接服务器

|  |  |
| --- | --- |
| 图标状态 | 说明 |
|  | 服务未启动； |
|  | 参数未设置，包括服务器IP、连接密码；或未与主服务器进行授权验证； |
|  | 正在与服务器连接； |
| emergency | 与服务器断开连接并进入紧急模式； |
| error | 授权错误，备用服务器无法与主服务器连接； |

1. **备用服务器登录密码**

在任务栏服务服务器图标上右键，选择“工具”🡪“设置登录密码”；

设置登录密码后，使用备用服务器右键菜单“工具”中的功能时，需要输入密码才能操作。

1. **备用服务器得到授权后，可在系统任务栏的备用服务器图标上右键，选择“状态”，查看备用服务器的授权状态。在“工具”菜单中还有其它的设置：**

客户端状态：查看当前主服务器上所有客户端连接的信息

连接列表：当前连接到备用服务器的客户端的信息。

1. **紧急模式授权文件**

由于网络故障导致客户端无法连接主服务器和备用服务器，可以在备用服务器上创建紧急模式授权文件，在客户端导入，让客户端进入紧急模式。

任务栏备用服务器图标上右键，选择“工具”🡪“高级”🡪“创建紧急模式授权文件”，可设置导入密码及有效时间。

1. **超级授权**

在没有部署备用服务器的情况下，主服务器出现故障，无法对备用服务器进行授权，也无法给客户端设置离线权限。此时，可以向厂商申请超级授权。

* 备用服务器图标上右键，选择“工具”🡪“高级”🡪“申请超级授权”，输入产品授权书上的主序列号，点击“创建申请文件”，然后将申请文件发给厂商。
* 收到厂商提供的超级授权文件后，在备用服务器图标上右键，选择“工具”🡪“高级”🡪“设置超级授权”，导入授权文件。如果主服务器有设置检验码，在导入超级授权时，也可以一并输入主服务器的检验码，否则无法连接客户端。如果导入超级授权时忘记输入，也可以在备用服务器上右键，选择“工具”🡪“高级”🡪“设置检验码”，在弹出的对话框中输入主服务器上设置的检验码。
* 超级授权文件与备用服务器是一一对应关系，如果需要授权多个备用服务器，则需要在多个备用服务器上创建申请文件。
* 通过超级授权进入紧急模式的备用服务器，需要开启主动轮询。

## 4、加密文档备份服务器

文档备份功能，主要是为了防止文档加密过程中由于系统或应用程序故障导致文档损坏，或者人为恶意修改加密文档导致重要文件丢失，而无法找回。

### 文档备份服务器授权

* 在加密文档备份服务器图标上右键，选择“工具”🡪“选项”，进入备份服务器设置界面，输入加密服务器的IP，设置备份路径。
* 进入控制台文档安全管理界面，选择“工具”🡪“文档备份服务器管理”，进入文档备份服务器管理界面。可以查看到当前所有连接的文档备份服务器及授权状态。选择刚安装的备份服务器，点击“授权”，这样就完成了文档备份服务器的授权。

### 文档备份服务器状态

文档备份服务器的任务栏图标及对应状态：

|  |  |
| --- | --- |
| 图标状态 | 说明 |
| BHMV}E1CHP2Y`D%)G4HA8GJ | 文档备份器正在启动 |
| WY_9MYOI)CN9(PJV2TF$Q9K | 文档备份服务停止； |
| IWP{~YY~64BU2T2KZQW[NML | 未设置运行参数，包括连接参数、备份设置、空间设置；或未与主服务器进行授权验证； |
| U4A~JX}OXPF6QGTZJ1$HH`K | 与IPG服务器连接成功，已获得授权； |
| HRS}DH2~O63MYOO]ZXOWL3T | 与IPG服务器连接成功，未获得授权； |
| EMFG36KLY`]0HP@SA3X$2%Y | 与IPG服务器断开连接；或是达到空间报警限制； |
| )]CQOT30J7LP`)}YVDY5HJK | 与IPG服务器断开连接，未获得授权 |
| [X[`A0M0I)M4PBB[R$LOL0M | 停止备份；或是通讯错误； |

### 文档备份设置

进入控制台的文档安全管理界面，选择“文档备份设置”，在需要备份的计算机或计算机组上右键，选择“设置权限”，进入“文档备份设置”界面。

勾选“启用加密文档自动备份任务”，有如下设置项：

* 包含文件：需要备份的文件或目录
* 过滤文件：不需要备份的文件或目录
* 备份范围：备份文件的大小范围（0-2000KB）
* 备份间隔：间隔长时间进行备份
* 备份流量：上传备份文档时的流量限制
* 备份时段：指定备份文档的时间段
* 定期备份：按照指定周期的时间扫描客户端加密文档并进行备份
* 允许客户端开启/关闭备份功能：开启后，客户端可以查看自己当前备份的数量，并且可以选择关闭备份功能。

### 备份文件查看

在文档备份服务器，点击文档备份服务器任务栏图标右键，选择“工具”🡪“备份文档管理工具”，打开备份文档查看工具。

文档备份目录格式：备份目录+计算机名称+文档实际路径