目　录

第一章. 安装和部署

1.1 软硬件环境

安装 IP-guard 服务器之前需要先安装数据库，每个模块支持的操作系统以及硬件建议配置如下表：

安装模块	计算机基本要求
数据库	SQL Server 2000 SP4 / MSDE SP4 32/64 位 SQL Server 2005 SP1 / SQL Server 2005 Express SP1 32/64 位 SQL Server 2008/ SQL Server 2008 Express 32/64 位 SQL Server 2012/ SQL Server 2012 Express 32/64 位 SQL Server 2014/ SQL Server 2014 Express 32/64 位 SQL Server 2016/ SQL Server 2016 Express 32/64 位 SQL Server 2019/ SQL Server 2019 Express MySQL 5.7 及更高版本
服务器模块	操作系统 Win2000 SP4 / XP SP2 / 2003 SP1 / Vista / 2008/ Win7/ Win8/ Win2012/ Win10 / Win2019 包含各 32/64 位 Windows 版本 最低配置 Pentium4 2G / 2GB 内存 / 20GB 可用硬盘空间 建议配置 Pentium4 双核或四核 / 4GB 内存 / 120GB 可用硬盘空间
文档云备份服务器模块	操作系统 XP SP3 / Win2003 SP2 / Win2008 R2 SP1 / Vista SP2 / Win7 SP1 / Windows 8 / Win2012 / Win10 包含各 32/64 位 Windows 版本 最低配置 Pentium4 2G / 2GB 内存 / 20GB 可用硬盘空间 建议配置 Pentium4 双核或四核 / 4GB 内存 / 2T 可用硬盘空间
控制台模块	操作系统 Win2000 / XP / 2003 / Vista / 2008 / Win7/ Win8/ Win2012/ Win10 / Win2019 包含各 32/64 位 Windows 版本 最低配置 Pentium III 500/512MB 内存/256MB 可用硬盘空间 建议配置 Pentium4 / 1GB 内存 / 1GB 可用硬盘空间

客户端模块	操作系统 Win2000 / XP / 2003 / Vista / 2008 / Win7 / Win8/ Win2012/ Win10 / Win2019 包含各 32/64 位 Windows 版本 最低配置 Celeron II 433 / 2G 内存 / 512MB 可用硬盘空间 建议配置 Pentium 4 / 4GB 内存 / 1GB 可用硬盘空间

注意 1. 如果服务器模块安装在 Windows 2000 SP4 系统上，请先确认安装“Windows 2000 SP4 更新汇总升级补丁（KB891861）”。

1.2 安装和部署服务器和控制台

1.2.1 安装服务器和控制台模块

服务器模块的数据库使用 SQL Server 2000 SP4 或以上、SQL Server 2005 SP1 或以上，如果没有 SQL Server 可以安装微软免费提供的 MSDE SP4 或 SQL Server 2008 R2 Express。

安装服务器和控制台的具体操作步骤如下：

1) 双击 IPguard3.exe，选择安装界面语言，点击【确定】;

2) 系统会弹出欢迎安装的界面，点击【下一步】继续；

3) 安装程序会提示用户确定安装的路径，用户也可以自己选择安装的路径，可以选择一个存储空间较大的盘符来安装 IP-guard 服务器；

4) 安装程序会提示用户选择安装类型和组件：用户可以根据需要选择安装 IP-guard 的服务器和控制台，点击【下一步】;

5) 选择开始菜单的快捷方式的目录，点击【下一步】;

6) 确认设置无误，点击【下一步】，复制文件结束后系统安装完毕，单击【结束】按钮完成安装，服务器模块自动启动，在托盘有个小图标显示。

安装服务器时，安装程序会判断安装的条件，包括操作系统和 SQL Server 的版本，如果无法正常安装，请按照提示完善安装环境。

管理员也可以在其它机器上单独安装控制台程序，以便查看数据和监视客户端机器的操作。

1.2.2 服务器注册

右键单击【服务控制器】，选择“**工具->注册**”输入管理员密码进入注册界面。

管理员点击【**升级**】按钮，主序列号和加密序列号栏会变为可编辑状态，输入购买的正式主序列号和加密序列号，再单击【**确定**】按钮，系统会提示“**序列号升级成功**”并且提示您需要激活产品。

在产品注册对话框中填写您公司的信息，包括公司名称、联系人、联系电话和邮件地址，点击【**在线注册**】会自动返回注册码，单击【**注册**】按钮，提示“**注册成功**”即可。

1.2.3 设置系统检验码

当第一次安装服务器后，右键单击【服务控制器】选择菜单“**工具->检验码**”，系统会要求输入管理员的账号和密码，才能设置检验码。输入检验码，再次输入，点击【确定】按钮，设置检验码成功。

1.3 部署客户端模块

安装客户端模块需要首先创建客户端安装程序，然后到需要部署的机器上手工运行安装程序，安装客户端程序需要管理员权限。

客户端安装程序需要在服务器机器上打包。

打包客户端安装程序，在安装了服务器的机器，点击“**开始->所有程序->IP-guard V3->创建客户端安装程序**”打开客户端生成工具。

点击【创建客户端安装程序】按钮，客户端安装程序创建成功。

说明 将安装配置信息打包到独立文件中，能使安装程序带上数字签名，避免安装时被杀毒软件误报为病毒。

1.4 卸载

1.4.1 卸载客户端

对于在线客户端，选择“**控制->卸载客户端**”将客户端模块移除，此后客户端模块不再运行，如果您以后需要在该计算机上再运行客户端模块，必须重新安装。

对于离线的客户端，可以在控制台上生成卸载工具，在客户端上运行进行卸载。具体步骤如下：

1) 在控制台选择“**工具->客户端工具->客户端离线辅助工具**”，打开客户端离线辅助工具；

2) 选择“**永久卸载客户端**”，点击【下一步】按钮；

3) 设置参数，包括程序的有效执行次数、有效执行时间、操作密码、导出路径，程序名称，点击【完成】按钮，导出 EXE 格式的可执行程序。

4) 将生成的 exe 程序发给客户端，在客户端运行，则会执行指定的卸载操作。

1.4.2 卸载服务器和控制台

首先关闭 IP-guard 服务器和控制台等应用程序，然后选择 “**开始**”菜单的“**所有程序->IP-guard V3->卸载 IP-guard V3**”进行卸载，也可以选择在“**控制面板->添加/删除程序**”中选择 IP-guard3 进行卸载。

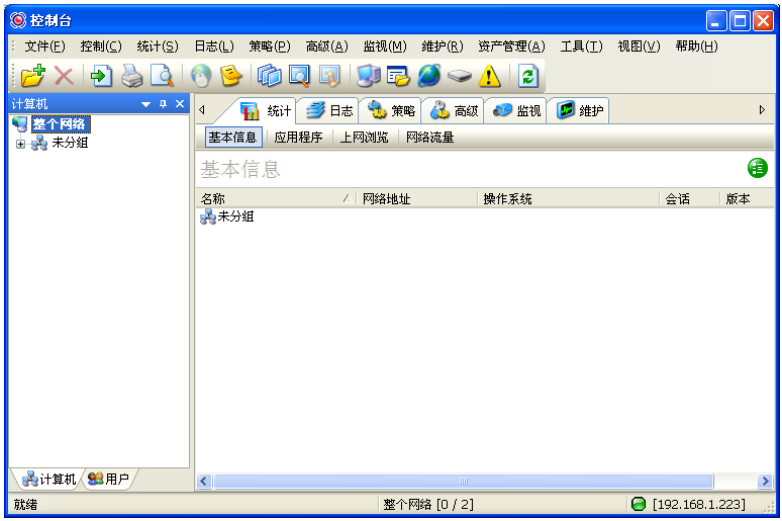
第二章. 控制台

2.1 登录控制台

单击安装目录下的 OConsole3.exe 或者“开始->所有程序->IP-guard V3->IP-guard V3 控制台”启动控制台模块。

在启动控制台模块之前必须先在网络上运行服务器模块，控制台模块在启动后会显示登录窗口。

控制台登录后，将见到如下的界面视图：



2.2 计算机和用户操作

2.2.1 查看基本信息

选择菜单“**统计->基本信息**”，管理员可以查看计算机、计算机组、用户、用户组的基本信息。

2.2.2 分组操作

在计算机栏和用户栏中，所有的客户端机器和用户在首次出现时，默认都会在【未分组】内。为了方便管理，管理员可以新建一些分组，将这些计算机和用户在逻辑上划分到不同的分组中。

新建分组

在计算机栏，选择整个网络或某个分组，选择菜单“**文件->新建组**”，则会在计算机树中出现一个新的组结点，为可编辑状态，输入组名称，将相关的计算机拖到该计算机组。管理员可以按照相同的办法建立多级的分组机构。

切换到用户栏，可以按照相同的方法对用户进行分组管理。

指定分组和改变分组

当需要为计算机和用户指定逻辑的分组时或改变分组时，我们可以选定需要移动的计算机和用户，选择菜单“**文件->移动到**”，选择相应的目标组，这样我们所选择的计算机和用户会移动到我们指定的组内。

我们也可以通过鼠标的拖拽操作来完成。选择我们要操作的对象后，按住鼠标左键不放，然后把它拖到我们所希望的目标组中去，这样我们所选择的计算机(组)或用户(组)就会属于我们指定的组了。

2.2.3 查找

通过查找功能，计算机栏中选择“**文件->查找**”打开查找对话框。输入相关的查询条件，管理员可以快速定位到指定的计算机或用户，并且查看其相关的数据内容。

2.2.4 删除

对于不再需要接受管理和查看其以往数据内容的计算机，可以在控制台上将其删除。选择“**文件->删除**”，可以把计算机栏或计算机列表中选中的计算机(组)删除，如果是计算机组，则包括该组中所有的子组和计算机。

删除操作会卸载该计算机上运行的客户端，并且收回相应的 License 授权。如果删除时，客户端不在线，会在下次上线时卸载。

2.2.5 恢复

对于已删除组里的计算机和用户，可以在控制台上将其恢复。选择“**文件->恢复**”，可以将计算机或用户恢复到原分组。

执行恢复操作后，不管客户端是否已卸载，都会重新占用 License。

2.2.6 重命名

为了方便管理，管理员可以将计算机名称或用户名称改为便于管理和查看的名

称。选择要更改名字的计算机(组)或用户(组)，选择菜单“**文件->重命名**”进行改名，修改后的名称将会显示在控制台上。

2.2.7 数据同步

当客户端较多的时候，难免会出现分类库和策略下发到某些机子快一些，下发到另一些机子慢一些的情况。此时管理员可以对指定的计算机设置数据优先同步。

选择需要优先同步的计算机，右键菜单“**数据同步->优先数据同步**”， 则库信息改变，以及新建或修改策略时，优先对此则该计算机同步这些信息；右键菜单“**数据同步->取消优先同步**”， 则不会再对该计算机优先同步类库和策略信息。

2.3 控制

管理员可以通过控制台对运行客户端模块的计算机进行控制，前提是所要进行控制的计算机必须正在运行客户端模块。控制只能针对计算机，在用户模式下不能进行控制。

2.3.1 发送通知消息

选择目标客户端机器或组（如果是组，则对组内所有计算机发送通知消息），选择菜单“**控制->发送通知消息**”打开一个对话框，输入通知的标题以及通知的内容，点击【发送】按钮。目标计算机的桌面将会弹出通知消息窗口。

2.3.2 锁定/解锁计算机

选中一个或多个计算机，选择菜单“**控制->锁定计算机**”可锁定选中对象。被锁定的计算机将无法再使用键盘和鼠标进行任何操作，只有在菜单“**控制->解锁**”进行解锁，用户才能继续使用键盘和鼠标。被锁定的计算机在基本信息里面会显示锁定的状态。

2.3.3 注销用户、关闭/重启计算机

管理员可以选择“**控制**”菜单的“**注销用户**”、“**重新启动**”和“**关闭计算机**”执行相应的操作。目标计算机会执行控制台下达的命令。

第三章. 统计

各项统计情况，除了可生成统计报表，控制台也会生成统计图表

3.1 应用程序统计

选择菜单“**统计->应用程序**”可查询在某一段时间计算机(组)或用户(组)的应用程序使用情况，系统默认统计当天的应用程序使用情况。

应用程序统计可分 4 种模式：

1. 按应用程序类别统计

在应用程序分类中，管理员可对客户端机器所使用过的所有应用程序进行分门别类，以方便对应用程序类别进行统计。

2. 按应用程序名称统计

假如需要统计具体使用过的应用程序百分比，则可以选择“**模式->按名称统计**”，这种统计模式会列出所选计算机(组)使用过的应用程序的使用的时间总和以及所占工作时间的百分比。

3. 按应用程序明细统计

按应用程序明细统计与按名称统计类似，不是按进程，而是按该应用程序的描述进行统计。

4. 分项统计

分项统计是针对计算机或计算机组分别统计不同的应用程序类别的使用百分比，默认是统计开机时间和工作时间，需要在查询栏的【类别】中增加应用程序类别进行统计。

3.2 上网浏览统计

很多员工会在上班时间浏览工作以外的网站，通过上网浏览统计功能可以查到

用户浏览网站的情况，从而及时的发现问题并采取应对措施。

上网浏览统计可分 3 种模式：

1. 按网站类别统计

按网站类别模式进行统计的前提是，管理员应该预先在“**分类管理->网站**”中添加类别及其网站识别。这种统计模式方便用户针对不同类别的网站进行宏观统计和分析。

2. 按网站明细统计

按网站明细统计查询到所有访问过的网站明细，默认显示所有网站的上网时间，一般按域名来统计。如果想区分类别统计，可以在右边的查询条件中筛选指定的类别。

3. 分项统计

分项统计是以计算机为单位统计一个或多个网站分类的浏览时间，可以对一个计算机组或整个网络进行统计。

3.3 网络流量统计

选择菜单“**统计->网络流量**”查看网络流量使用情况。

网络流量统计可分为 6 种模式：

1. 按地址明细统计

按地址明细统计是按所有 IP 地址统计端口的数据流量，从统计结果中可以看出一段时间范围内，与客户端机器通讯流量最大的对方 IP 地址。

2. 按端口明细统计

按端口明细统计是按照指定的端口范围统计对方 IP 地址范围的流量数据，从统计结果中可以看出客户端机器在哪些端口上的数据流量比较大。

3. 按地址类别统计

按地址类别统计是按照网络地址的分类统计指定网络端口的流量。

4.　按端口类别统计

按端口类别统计是按照网络端口的分类统计指定网络地址的流量，管理员可以在右侧的查询栏中的地址范围和端口范围选择其它的类别进行统计。

5.　按计算机和地址类别统计

按计算机和地址类别统计是以计算机或计算机组为单位统计其在指定网络地址范围内的流量。

6.　按计算机和端口类别统计

按计算机和端口类别是指按计算机或计算机组统计指定端口范围内的流量。

注意　网络流量统计只能根据计算机来统计，不支持对用户进行统计。

第四章. 日志

IP-guard 会记录客户端机器的各种操作日志，包括：用户登录、注销日志，应用程序日志，网站浏览日志，文档操作日志，共享文档日志，文档打印日志，移动存储操作日志，资产变更日志等。通过这些具体的日志，可以查看用户在其机器上的几乎所有操作。

管理员也可以设置各种查询条件，对各项日志进行有选择有目的的查询。

4.1 基本事件日志

选择菜单“**日志->基本事件**”查看基本事件日志，基本事件日志记录客户端系统的启动/停止，用户登录/注销，拨号，补丁管理和软件分发相关日志。

基本事件日志默认显示所有的日志，管理员也可以设置各种查询条件进行有选择有目的的查询。

4.2 应用程序日志

应用程序日志会记录客户端机器打开或关闭的应用程序以及应用程序窗口切换信息。管理员可以通过控制台查看相关日志。选择菜单“**日志->应用程序**”，管理员可以查看所有的应用程序启动/停止和窗口/标题 切换日志。

4.3 上网浏览日志

上网浏览日志会记录客户端计算机上浏览过的网站，方便管理员查看该客户端用户的网页浏览情况。选择菜单“**日志->上网浏览**”，管理员可以查看所有的上网浏览日志。网站浏览日志支持各种常用浏览器的记录。

4.4 文档操作日志

选择菜单“**日志->文档操作日志**”查看文档操作日志，在文档控制策略、IM文件传送策略和敏感信息外传控制策略中可以设置文档备份策略，当客户端机器触发了这些策略，会记录备份文档日志。备份文档日志用一个别针的图标“ ”标志，比如复制的图标为“ ”。

双击备份文档日志，可以查看其详细属性，在文档名称的右侧有个按钮【副本】，点击该按钮，可以查看或保存备份文档。备份文档也支持批量导出，右键菜单“**导出备份文档**”可导出指定或是全部记录的备份文档。

4.5 刻录操作日志

刻录操作日志记录客户端机器用户的使用专用刻录工具进行刻录操作的信息。

选择菜单“**日志->刻录操作日志**”查看刻录操作日志，在文档控制策略中，若勾选操作类型为“**修改**”和“**复制/移动到备份到**”，则当刻录的文件触发此策略，在文档操作日志中可以查到这些文档的刻录备份文档日志，图标为 。

4.6 共享文档操作日志

选择菜单“**日志->共享操作**”查看共享文档操作日志记录。

4.7 文档打印日志

文档打印日志是记录客户端机器上的打印操作，以方便日后查询。选择“**日志->文档打印**”可以查看相关打印日志。

查看和保存打印记录

在打印控制策略中可以设置记录打印内容的策略，当客户端打印指定的文档时，会记录其打印内容。在打印日志中可以查看或保存打印内容。打印日志中会用一个别针的图标“ ”标志，例如共享打印机的图标为“ ”。

双击其中一条日志或右键“属性”查看其详细信息，在计算机右侧有个【副本】

按钮，点击该按钮可以“**查看打印记录**”或“**保存打印记录**”。

4.8 移动存储操作日志

选择菜单“**日志->移动存储操作**”查看所有移动存储的使用日志。

4.9 资产变更日志

选择“**日志->资产变更**”查看所有软硬件的变化日志策略日志。

4.10 策略日志

选择“**日志->策略日志**”可查看到客户端机器触发的策略日志。

4.11 系统事件日志

选择菜单“**日志->系统事件**”，管理员可以查看服务器的启动和停止日志，非法计算机接入网络的报告、服务器和客户端之间的通讯错误日志，服务器时间日志、客户端登录冲突日志，自动删除客户端日志，邮件报告发送日志等。

第五章. 策略

5.1 策略简介

策略通用属性说明

策略的设置包含很多属性，在各种类型的策略属性中，有一些属性是通用的，含义也相同。

策略属性	说明
名称	只是用户自己定义的一种对该条策略的描述。与策略的执行功能无关。当添加一条策略时，控制台会默认添加名称，管理员也可以自定义名称。
时间	指定策略生效的时间范围。系统默认是全天，可以是已定义的时间类型(在“**工具->分类管理->时间类型**”中设置)； 如果没有符合要求的时间类型，可以选择“**自定义**”，在弹出的时间选择框中直接设置时间范围。
模式	是指满足了策略条件后执行的模式，包括禁止、允许、忽略和不操作。详情请参考后面的模式说明。
动作	策略执行的同时产生的动作，包括报警，警告，锁定计算机三种类型。这 3 种动作可以同时设置，也可以设置其中的一种。详情请参考后面的动作说明。
到期时间	指定策略生效的终止时间。默认策略是<始终有效>。如需要设置到期时间，在设置窗口中选中“**启用**”并设置到期时间。不允许设置小于当前系统时间的到期时间。如果此策略已经过期，则此条策略的字体将会以深灰色显示，【到期时间】中的时间值显示成红色。
仅离线生效	当客户端和服务器无法通讯时，则客户端视为处于离线状态。选中“仅离线生效”表示该策略仅当客户端处于离线状态时才生效，主要是计算机使用者出差，回家或网线故障的情况。如果不选中此项，表示该策略始终生效。

策略有 4 种模式：允许、禁止、忽略、不操作。

模式	说明
允许	允许进行某种操作。如果某个操作匹配的策略模式为允许，则允许，并不再继续判断其下面的策略。
禁止	禁止进行某种操作。如果某个操作匹配的策略模式为禁止，则禁止，并不再继续判断其下面的策略。
忽略	对操作既不允许，也不禁止。如果某个操作匹配的策略模式为忽略，会执行本策略所设置的动作，然后继续匹配下面的策略，决定该操作是允许还是禁止。
不操作	既不允许，也不禁止（主要用于基本策略和设备策略中）。如果某个项目或者设备匹配的策略模式为不操作，则不做允许或者禁止，并不再继续判断其下面的策略。

当客户端机器触发了策略，可以产生相应的动作，动作包括：报警、警告、锁定计算机。

动作	说明
报警	当此策略匹配后，客户端会向服务器发送报警信息，在控制台上会弹出报警以提示管理员，同时此报警日志也会作为策略日志记录下来。 可以通过菜单“**工具->选项->实时报警->气泡设置**”选择当前控制台是否弹出报警气泡，通过“**工具->警报**”查看实时报警信息。 报警可以设置为三种级别：低、重要和严重。
警告	当此策略匹配后，在客户端会弹出对话框，警告客户端的使用者执行了某些限制的操作。管理员可以在警告信息中自定义消息框显示的内容。
锁定计算机	当此策略匹配后，客户端计算机会被自动锁定，使用者将不能进行任何操作。 在控制台的“**控制->解锁**”可以对客户端进行解锁。
记录屏幕	当触发策略时会立即记录当下的屏幕信息，可在“**查询屏幕历史**”中查询到，默认触发时每隔 2 秒记录一帧屏幕信息，一共记录三次。

策略的匹配优先级

策略采用类似于防火墙的策略方式，每组策略可由多条策略组合而成，按照先后关系进行匹配，按最先匹配的策略执行规则；同时每个对象还会自动继承父对象的策略。

管理员可以依次设置整个网络策略、组策略、计算机策略和用户策略；策略匹配的优先级由高到低依次为：用户策略 > 用户角色策略 > 用户组策略 > 用

户组角色策略 >计算机策略 > 计算机角色策略 > 计算机组策略 > 计算机组角色策略。

从父组继承的策略都会用浅绿色背景显示，且不能修改父组策略。策略涉及到字符串的输入字段都支持通配符，支持输入多个，中间以半角分号“;”或半角逗号“,”隔开。

5.2 基本策略

通过基本策略可以规范网络内计算机的操作权限，限制客户端机器对计算机系统设置的任意修改，防止恶意或无意的破坏，增强计算机的使用安全性。

策略示例

假如您的需求是：在公司时禁止修改 IP 地址，但是允许回家或出差的时候修改 IP。管理员可以对目标计算机（如整个网络）设置基本策略：

① 先设置一条策略，禁止修改 IP/MAC 属性；
② 再设置一条离线策略，允许 修改 IP/MAC 属性 仅离线生效。

按照策略匹配原则，后设置的策略在上面，因此策略②优先于策略①，当离线状态时，策略匹配，允许修改 IP/MAC；当在线状态时，与策略②不匹配，接着向下匹配策略①，条件满足，执行策略禁止修改 IP/MAC 属性。

注意 基本策略的修改网络 IP/Mac 配置，系统还原，网络共享对计算机有效，对用户是无效的。

5.3 设备控制策略

设备控制策略主要是对与计算机有关的各种设备进行控制，规范企业内计算机对存储设备、通讯设备各种类型的设备使用，防止企业机密资料通过这些计算机外部设备泄露出去，增强企业管理的规范性和安全性。

策略示例

为了保护企业内部的重要文档资料，需要限制员工通过可移动设备或刻录机等设备将内部资料拷走，可设置策略禁止这些设备。

策略：模式选择“禁止”，在设备列表中勾选需要禁止的设备，如：可移动设备、软盘、光盘、刻录机等，则设置了策略的计算机无法使用这些设备。

5.4 应用程序策略

在企业中，可能有些应用软件是管理者不希望员工使用的，例如一些 BT、迅雷下载工具，聊天工具以及游戏类的软件。应用程序控制策略可以限制客户端机器对这些应用程序的使用。

应用程序

新添加的策略，应用程序默认是全部，需要管理员来指定应用程序，应用程序的控制有 3 种方式：

1. 通过进程名称来禁止

管理员直接添加应用程序的名称，如 thunder.exe，此时策略是通过字符串匹配的，如果客户端修改了应用程序名称改为 thunder123.exe，则策略就无法生效；要避免这种情况可以采用第二种方法去控制；

2. 通过应用程序分类来禁止

管理员选择应用程序分类中的一个分类（可以将要禁止的应用程序都放到这个分类中），即使客户端修改了应用程序名称，只要程序本身没有变化，策略依然生效。

3. 通过运行路径来禁止

管理员添加路径名称，如：禁止 APPDIR:e:*.exe，则 e 盘下的所有程序都会被禁止；同理要禁止 H 盘下的所有程序，设置策略为：禁止 APPDIR:h:*.exe 即可。

另外还可以用$UDISK$表示 U 盘，$CDROM$表示 CDROM。如：

APPDIR:$UDISK$:*.exe，禁止运行 U 盘上的程序；

APPDIR:$CDROM$:*.exe，禁止运行 CDROM 中的程序。

服务

此外，通过应用程序策略，还可以对客户端机器上的服务运行情况进行控制。设置策略时，在输入应用程序的名称之处直接输入服务名称，输入格式为

SERVICE:ServerName；

例如：要禁止服务 bthserv，则在应用程序中填写 SERVICE:bthserv。

其中需要注意的是，输入时需为英文半角状态，且“SERVICE”一定要为大写，否则会导致策略不生效；格式中 ServerName 填写的是服务名称，而不是显示名称

警告 禁止全部应用程序会导致大部分进程被禁用，为避免可能的损失，请设置策略时谨慎操作。

5.5 上网浏览策略

上网浏览策略可以有效控制员工访问网页的行为，禁止访问与工作无关的网站或者恶意网站，提高工作效率，保护内网安全。

管理员可以直接添加网站，也可以在网站分类中指定一个网站类别进行控制，对网站分类的设置在“**分类管理->网站分类**”中添加或修改。

网站名称可以是完整的网址，也可以包含通配符，如：“*.baidu.com”，“*mail*”，“*game*”，“*.com/mail/*”等。

策略示例

为了防止员工访问非法的网站，可以设置上网浏览策略禁止访问这些网站或者只允许访问指定的一些网站。假如您的需求是只允许访问指定的网站，可以设置一组策略：

① 先设置一条策略，禁止 <全部> 网站；
② 再设置一条策略，允许 指定网站（将允许的网站都添加进去）。

这样，指定的网站可以访问，而其他所有的网站都无法访问了。

5.6 屏幕记录策略

屏幕历史可以记录客户端机器的所有操作行为，因为数据量较大，系统默认是不记录的，管理员可根据实际需要来设置策略记录屏幕记录。

通过针对不同的应用程序，设定不同的记录频率，可以对一些用户关注的应用做频繁的记录，而对不重要的程序则不记录或少记录。

5.7 日志记录策略

客户端的所有日志默认都是记录的，除了窗口标题日志。企业内可能会有一些需求，并不是所有的日志都希望记录下来，比如拨号日志、即时通讯日志等，此时可通过日志记录策略来控制日志的记录类型。

系统有一条默认策略，除了窗口标题变化日志不记录，其它所有日志都默认记录。

5.8 远程控制策略

通过设置远程控制策略，可以控制客户端机器能否被远程控制或者被远程控制的方式。

远程控制类型有远程控制和远程文件传送两种。

只有选择了上面两项中的至少一项后，才能设置下面其它属性。管理员名称、控制台 IP 地址和控制台名称支持分号“;”或逗号“,”作分隔符，可同时设置多个。

5.9 客户端配置策略

客户端配置策略主要作为其他策略功能的补充，一些新增的小功能可在客户端策略中集中设置。不同的功能具有不同的属性，视具体而定。

5.10 系统报警策略

系统报警功能是针对计算机的软硬件变化以及系统的关键设置变化给出实时报警。

5.11 流量控制策略

流量控制策略是针对客户端机器的网络流量进行合理控制，该策略只对计算机有效，对用户无效。

策略示例

为了限制客户端机器任意访问互联网，严重占用企业带宽，从而给整个企业的网络访问带来影响，可以设置流量控制策略来控制指定机器的流量。

策略：模式选择“限制流量”，指定地址范围，如：互联网，端口范围可以为默认，也可以指定端口，选择流量方向并设置限制速度如 20k/s，则设置策略的客户端机器访问网站或上传/下载的速度被限制在 20k/s。

5.12 网络控制策略

网络控制策略可以有效控制客户端机器与其他非法计算机之间的通讯，同时阻断一些恶意端口或下载端口。网络控制策略是针对计算机的，在用户模式下无效。

策略示例

在整个企业中，有些部门的计算机可能是非常重要的，是不允许部门之外的计算机访问的，通过网络控制策略也能很好的解决这个问题。

对整个部门设置策略：

① 先设置一条策略，禁止 网络地址范围：局域网
② 再设置一条策略，允许 对方是客户端+属于相同分组

这样该部门内的计算机只能和本部门的计算机通讯，设置策略之前，管理员需要将所有该部门的计算机放在同一个分组。如果该部门还有其他没有安装客户端的计算机，请把 IP 地址范围添加到允许的策略中。

5.13 邮件控制策略

邮件控制策略只能对发送邮件进行控制，对接收邮件无法控制。暂时不支持网页邮件和 Lotus 邮件的发送控制。策略属性包括：

策略示例

一些企业可能需要限制邮件的发件人，只允许员工使用指定的内部邮箱发送邮件，使用其它邮箱发送邮件被禁止，规范管理员工使用电子邮件，也方便对外发的邮件进行严格把关。

设置策略：
① 先设一条策略：禁止 全部邮件；
② 再设一条策略：允许 发件人：指定发件人，如：*@teclink.com.hk。

这样只有发件人的邮箱地址包含@teclink.com.hk 的邮件才能发送成功。

5.14 IM 文件传送策略

IM 文件传送策略支持各种即时通讯工具，包括：QQ、ICQ、MSNMessenger、YAHOO、TM、UC、SKYPE、RTX、LSC、ALI、FETION、Google Talk、百度 Hi、263EM、飞秋、MSNLite、营销 QQ、企业 QQ、连我 LINE、群英 CC、LYNC、微信、企业微信、Activity Message 、KK、IMO 班聊、钉钉。

OfficeIM、LIMC 目前仅支持通讯内容记录，不支持 IM 文件传送控制。

策略属性包括：

策略示例

为了保护内部资料的安全，防止员工通过即时通讯工具将文件传送出去，可以设置 IM 控制策略，禁止发送包含指定关键字的文档，并且备份其他发送出去的文档。

设置策略：

① 先设一条策略：允许 勾选备份选项；
② 再设一条策略：禁止 文件名称：*关键字*。

则客户端机器发送包含关键字的文件时会被禁止，而其它文档可以正常发送，但是会自动备份下来,管理员可以到文档操作日志中查看发送的文档是否合法。

5.15 上传控制策略

上传控制策略，可以有效的控制网络上传行为，包括发送网页邮件，论坛发帖和 FTP 上传等。

5.16 文档操作策略

文档控制策略可以有效的限制客户端访问机密文档的权限,防止机密文件外泄,同时文档备份功能也能避免重要文档因为误操作而带来的损失。

策略示例

为了防止用户对一些文档的误操作：删除或修改，管理员可以设置策略针对这种情况备份指定的文档。

设置策略：允许 操作类型：修改和删除，指定文档名称，选择备份， 则用户对这些文档的使用不受限制，但是修改和删除时会自动备份文档，备份的文档到文档操作日志中查看。

5.17 打印控制策略

管理员通过设置打印机的类型及开启打印文档的应用程序，有效地限制员工打印文档。

策略示例

在企业中，需要限制客户端机器的打印操作，以防止资料外泄或滥用打印机的问题。

设置策略：禁止共享打印机、网络打印机 打印机描述：输入打印机名称 应用程序：指定打印的应用程序，默认是<全部>，则使用打印机时被禁止。

5.18 水印控制策略

管理员通过设置水印模板并应用于打印水印策略，可以使打印出来的文件带上自定义水印图片或文字，有效地保护文档版权。

5.19 屏幕水印策略

管理员通过设置水印模板并应用于屏幕水印策略，可以使客户端机器的屏幕带上自定义水印效果，防止截屏拍照等手段泄露重要信息。

5.20 移动存储授权策略

管理员可以通过移动存储策略来授予不同的移动盘不同的权限，同时可以对复制到移动盘的文档进行加密，使其只能在企业授信的环境中才能打开。

5.21 软件安装管理策略

软件安装管理策略，可以限制员工安装无关工作的软件，同时也能制止员工卸载重要的安全软件。该策略不支持用户策略。

第六章. 监视

6.1 即时通讯内容

即时通讯可以记录客户端机器上的聊天内容，及时发现非法的聊天内容。

支持的即时通讯工具

即时通讯记录支持各种聊天工具，包括：QQ、ICQ、MSNMessenger、YAHOO、TM、UC、SKYPE、RTX、LSC、ALI、FETION、Google Talk、百度 Hi、263EM、飞秋、OfficeIM、MSNLite、LIMC、营销 QQ、企业 QQ、连我 LINE、群英 CC、LYNC、微信、企业微信、Activity Message 、KK、IMO 班聊、钉钉。

6.2 邮件内容

邮件记录会将客户端机器上使用邮件工具收发的邮件记录下来，以便管理员统一管理和掌握邮件内容， 邮件记录支持的邮件类型包括：普通邮件、Exchange 邮件、网页邮件、Lotus 邮件，其中普通邮件和 Exchange 邮件可以记录发送和接收，而网页邮件和 Lotus 邮件只能记录发送。

6.3 实时屏幕

选择菜单“**监视->屏幕快照**”，管理员可以实时查看并跟踪某一台计算机或某一个用户的屏幕快照。

6.4 多屏监视

多屏监视可以同时监控多台计算机的实时屏幕，多屏监视显示的是一个屏幕矩阵，这个矩阵的大小范围是（2 x 2）到（4 x 4）。选择菜单“**监视->多屏监视**”开始多屏监视。

6.5 查询屏幕历史

选择“**监视->查询屏幕历史**”默认查询的是当天的屏幕历史记录，设置屏幕记录策略的客户端机器才能查询到屏幕记录。

6.6 屏幕历史查看器

查询出需要查看的屏幕记录后，双击其中的一条记录或点击【查看】按钮打开屏幕历史查看器，查看该计算机的屏幕历史。屏幕查看器不能单独启动，只能从控制台模块中启动运行。

第七章. 远程维护

7.1 远程维护

远程维护实时查看远程计算机的信息，包括：应用程序列表、进程列表、性能、设备管理、系统服务、磁盘管理、共享文件夹、计划任务、用户和组、软件管理、启动项。

管理员可以在远程查看这些计算机的当前状态，并可以根据实际需要远程结束进程等操作，远程维护计算机。

7.2 远程控制

7.2.1 远程控制

远程控制是通过控制台远程操作客户端机器，远程控制有 2 种授权方式：用户授权和密码授权。

用户授权

选定目标计算机，选择菜单“**维护->远程控制**”，向远程用户请求授权，远程用户允许后可对其远程控制。

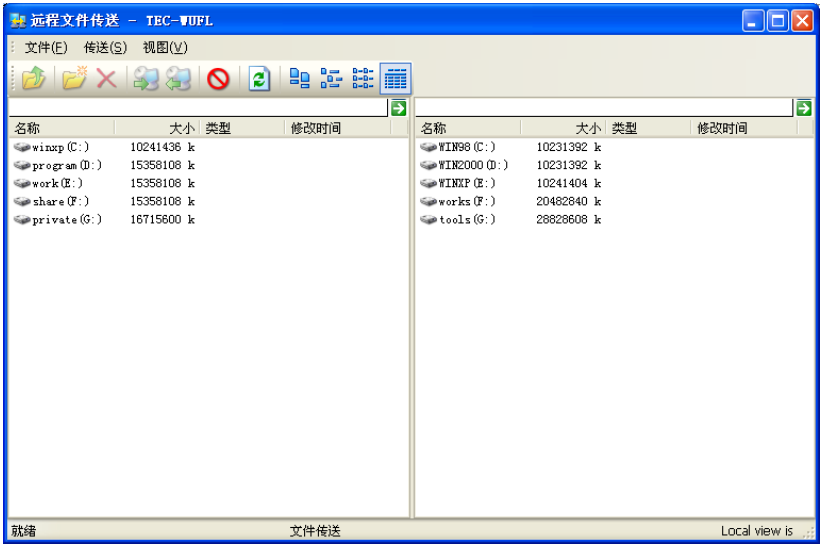
密码授权

选定目标计算机，选择菜单“**维护->远程控制**”，控制台会弹出对话框要求输入密码，密码正确，则进入控制界面，否则控制结束。
远程控制密码要在客户端机器上设置，方法是 shift+alt+ctrl+ “oculartrm” 会弹出密码设置框，输入密码即可。

7.2.2 远程文件传送

远程文件传送是指在控制台机器和目标客户端机器之间的文件传送，远程文件

传送和远程控制一样，有 2 种授权方式：用户授权和密码授权，控制台获得用户授权后，进入远程文件传送窗口。



本地视图和远程视图之间支持拖拽传送文件，可同时选择多个文件进行传送，正在文件传送时不能进行其他操作。

第八章. 敏感信息

管理员通过敏感信息功能可针对性地监控、管理文档， 敏感信息功能支持识别文件内容的文件类型有：OFFICE 文件，包括 doc、docx、xls、xlsx、ppt、pptx，pdf，txt 和所有纯文本文档。

8.1 敏感信息全盘扫描任务

拥有“**功能权限->敏感信息->设置敏感信息全盘扫描任务**”权限的管理员，选择菜单栏“**敏感信息-敏感信息全盘扫描任务**”进入敏感信息全盘扫描任务对话框，进行扫描任务的设置。

设置敏感信息全盘扫描任务的步骤：

1) 点击右上角的添加按钮，弹出创建扫描任务对话框；

2) 在“常规”选项卡中，对常规项目进行设置；

3) 切换至“高级”选项卡中，对高级项目进行设置；

4) 设置完成后，点击“确定”按钮，扫描任务创建成功。

8.2 敏感信息扫描工具

8.2.1 本地敏感信息扫描工具

选择“**敏感信息->本地敏感信息扫描工具**”，可扫描控制台所在计算机上文件，识别其中匹配敏感内容的文件，并可以对识别出的文件执行加密、解密、修改文档属性等操作。

8.2.2 远程敏感信息扫描

在计算机树选择一台计算机，选择右键菜单“**远程敏感信息扫描**”，可以扫描指定客户端的文件，识别其中匹配敏感内容的文件，并可以对识别出的文件远

程执行加密、解密、修改文档属性等操作。

8.3 敏感信息控制策略

8.3.1 敏感信息外传控制策略

管理员可通过设置敏感信息外传控制策略针对性地对文档外传进行管控；外传的文件匹配敏感内容，则文件外传受到策略动作限制并记录下本次操作信息，若外传的文件不匹配的敏感内容，则文件外传不受策略影响。

8.3.2 敏感信息落地控制策略

管理员可通过设置敏感信息落地控制策略针对性地对本地文档进行管控；在策略控制范围中保存时，客户端将自动对文件进行扫描，若文件匹配敏感内容，记录文件信息，同时可加密此文件。

8.4 敏感信息日志

敏感内容全盘扫描得到的匹配敏感内容的文件、触发敏感信息外传控制策略和敏感信息落地控制策略的敏感文档均记录在敏感信息日志中。

选择“**敏感信息->敏感信息日志**”查看所有匹配敏感内容的文件操作日志。

第九章. 资产管理

9.1 资产管理

选择菜单“**资产管理->资产管理**”进入资产管理主窗口。资产管理可以自动搜集客户端计算机上的软硬件信息、以及软硬件变更信息。

切换不同的子功能界面，点击查询按钮“  ”，在查询条件设置框中设置查询条件，添加结果列表，选择需要显示的资产属，设置好后，点击【**确定**】即可查询。

9.2 补丁管理

补丁管理功能可以扫描出所有客户端机器的补丁安装情况。

补丁的扫描、下载和安装

如果希望所有的客户端都自动安装补丁，可以在第一次启动控制台时，在菜单“**工具->选项->服务器设置->补丁选项**”中勾选“**新出现的客户端默认自动安装**”或“**新出现的补丁默认自动下载**” 。

如果不希望安装所有的补丁，可以只选择需要下载的补丁，右键选择“下载”；选择需要安装的计算机，右键选择“安装”。

管理员可以在控制台上选择菜单“**资产管理->补丁管理**”来查看客户端机器的补丁安装情况。

9.3 漏洞检查

安装了客户端的计算机会自动扫描漏洞信息，管理员也可以在控制台上下达扫描命令立即扫描，单击命令按钮“  ”立即执行漏洞检查，单击范围按钮“  ”可以选择查看一个计算机组或单个计算机的漏洞信息。

9.4 软件分发

选择菜单“**资产管理->软件分发**”管理员可以建立分发任务，向客户端自动分发及安装软件，或者复制特定的文件或应用程序到客户端。分发过程分为两步：创建分发程序包和创建分发任务。分发任务会把做好的程序包分发到指定的客户端上。

9.4.1 分发程序包

管理员需要首先创建分发程序包，分发程序包设置了该程序包进行分发时需要的参数信息，保存在服务器上，可以重复使用。

点击新增按钮“  ”新建一个分发程序包，创建分发包需要设置的信息包括：常规信息、文件信息、检测条件和必要条件。

9.4.2 分发任务

创建了分发程序包后，还需要创建分发任务来指派目标计算机。在分发任务视图中点击右上方的新建按钮“  ”创建一个分发任务，在任务列表中可以查看任务分发情况。

9.5 软件卸载

选择菜单“**资产管理->软件卸载**”，管理员可以建立软件卸载任务。可在两种模式下建立任务：软件模式和计算机模式。

9.5.1 软件模式下设置任务

软件模式下设置卸载任务，主要是以所选软件为主体，对已安装或可能安装这些软件的客户端机器下达卸载的任务。可实现对多个计算机卸载多个软件。

设置软件卸载任务

设置任务步骤：

1) 在安装软件列表中选择一个或多个安装软件，右键菜单选择“**卸载**”，或是选中一个安装软件，在下方的安装计算机列表中选中一台或多台计算机，右键菜单选择“**卸载**”，弹出软件卸载任务设置对话框；

2) 左边为计算机列表，可选择执行任务的客户端机器；

3) 右边的上半部分为软件列表，显示所选的软件；

4) 在任务设置中选择任务模式 和任务执行时段；

5) 最后点击【**确定**】按钮，完成任务设置。

9.5.2 计算机模式下设置任务

计算机模式下设置卸载任务，主要是以所选计算机为主体，对该计算机已安装的软件进行卸载。可实现对单台计算机卸载多个软件。

设置软件卸载任务

设置任务步骤：

1) 在客户端机器列表中选择一台客户端，在下方的“**软件安装情况**”中选择一个或多个软件，右键菜单选择“**卸载**”，弹出软件卸载任务设置对话框；

2) 左边为计算机列表，可选择执行任务的客户端机器；

3) 右边的上半部分为软件列表，显示所选的软件；

4) 在任务设置中选择任务模式 和任务执行时段；

5) 最后点击【确定】按钮，完成任务设置。

9.5.3 软件卸载任务管理

查看任务

在计算机模式下，选择一台计算机，选择“**卸载任务**”，可以查看选定计算机的卸载任务信息。内容包括：

删除任务

删除一台计算机的任务

在计算机模式下，选中一台计算机，在下方的“**卸载任务**”选项卡中选择一个或多个软件的卸载任务，右键菜单中选择“**删除任务**”，任务会被删除。

删除一个软件的任务

在软件模式下，选中一个软件，在下方的“**执行卸载任务计算机**” 选项卡中选择一个台或多台计算机，右键菜单中选择“**取消卸载任务**”，任务会被取消。

第十章. 分类管理

为了方便查询、统计和设置策略，管理员可预先在系统中设置好分类，分类管理包括：应用程序分类、网站分类、移动存储分类、软件安装包分类、软件卸载分类、时间类型分类、网络地址分类、网络端口分类、邮件分类、水印模板分类和敏感信息分类库。

10.1 应用程序分类

选择“**分类管理->应用程序**”打开应用程序类别窗口，系统默认定义了两个应用程序类别：系统应用程序和未分类。

“系统应用程序”分类是指与操作系统相关的一些程序。所有的应用程序都是在客户端搜集到的，如果没有匹配到任何分类则被归类为“未分类”。管理员可以新建其它分类并将相关程序从“未分类”移动到新建的分类，但是不能手工增加应用程序。

10.2 网站分类

管理员可以根据企业需要，将网站进行分类，方便管理员按照类别统计和控制员工的上网浏览情况。

点击“**分类管理->网站**”打开网站类别窗口，系统默认分类为空，管理员需要手工添加网站类别库和网站识别，网站识别支持通配符。

10.3 时间类型分类

为查询和统计的方便，管理员可以预先定义好时间段类别。点击“**分类管理->时间类型**”，管理员可以查看现有时间类别。系统默认有四种时间类型：全天，工作时间，休息时间，周末时间。

管理员可以根据企业工作时间去修改这些时间类型，点击一种时间类型，查看时间范围并且对其编辑修改。除了系统定义好的时间类别，管理员可以添加其

它时间类别。

10.4 移动存储分类

移动存储盘可以分为加密盘和非加密盘（普通盘），加密盘是指经过我们产品加过密的移动盘，只能在客户端机器上正常使用，没有安装客户端的机器无法使用该盘，加密盘只能通过控制台来制作。

移动存储信息的获取主要有 2 种方式：

获取方式	说明
客户端获取	所有在客户端机器上使用过的移动存储信息都会放在未分类中，管理员可将这些移动存储移动到其它自定义分类。
控制台获取	管理员可将移动存储直接插入控制台机器来添加移动存储信息，选择“**操作->本地移动存储信息**”查看插入的移动存储信息，其中有标志“ ”的表示该移动存储还没有保存在移动存储库中。

制作加密盘

管理员将需要整盘加密的移动盘依次插入控制台的机器上，制作加密盘。选择“**分类管理->移动存储**”打开移动存储库，选择菜单“**操作->本地移动存储信息**”查看本地移动盘列表。

按图标按钮“ ”将正常的移动盘格式化为加密盘，格式化时可以选择加密盘的文件系统格式（FAT32/NTFS）。格式化为加密盘后，该盘上的所有文件将被删除，并且将只能在安装了本产品客户端的机器上使用，请管理员确认是否执行格式化操作。

格式化成功后，图标将变为“ ”，表示该盘是加密盘，但还没有保存，单击保存按钮后，图标变为“ ”。

注意 加密盘默认不可在客户端上使用，需对客户端设置一条勾选“可读”、“可写”的移动存储授权策略，加密盘方可在此客户端上使用。

加密盘格式化为非加密盘

管理员也可以将加密盘还原为普通盘，也就是非加密盘，格式化加密盘为非加

密盘的方法有 2 种：

在没有安装客户端的机器上手工格式化

1. 加密盘在客户端机器上可以正常打开并且使用，而在没有安装客户端的机器上打开时，会提示需要格式化。如果用户选择了“是”，将手工格式化该盘为非加密盘，同时删除该盘上的所有文件。

2. 对于管理严格的企业，需要提醒员工谨慎操作，如果手工格式化之后，就不再是加密盘了。

通过控制台将加密盘格式化为普通的盘

在控制台机器上插入加密盘，打开移动存储库，查看本地移动存储信息，可以看到该加密盘信息。

选中加密盘，按图标按钮“”，格式化该盘为非加密盘，格式化成功后，该盘的图标又变回“”，并且序列号发生变化，需要重新保存；

加密盘不能通过常规的 Windows 的右下角的即插即用的设备里进行安全拔出，如果需要拔出加密盘，单击该界面中的拔出按钮“”后，可以安全拔出该加密盘。

注意 1.在客户端机器上使用加密盘时，需要单击加密盘后右键选择“Eject device”安全退出；

2.手机磁盘无法被格式化为加密盘。

注册管控

默认不启用移动存储注册管控功能。选择“**分类管理->移动存储**”打开移动存储窗口，选择“**操作->注册管控**”，勾选“**启用**”后，注册管控功能生效。

此时仅有注册过且状态为“正常”的移动存储盘才能在客户端使用，未注册、已挂失、已过期、已注销等移动存储盘无法使用。

注册移动盘时，可填写移动盘的一些相关信息，并指定移动到哪个类别下，默认移动到“已注册”类别下。

注册移动存储设备，有 2 种途径：

本地注册

在控制台机器上插入移动盘，打开移动存储库，选择“**操作->本地移动存储信息**”，可以看到该移动盘信息。选中该移动盘，按图标按钮“”，选择“**注册**”注册该盘，按图标按钮“”保存。

远程注册

在远程客户端机器上插入移动盘，通过控制台打开移动存储库，选择“**操作->远程移动存储信息**”，在“**远程客户端**”选择到插入移动盘的客户端后，可以看到该客户端上插入的移动盘信息，选中该移动盘，按图标按钮“  ”，选择“**注册**”注册该盘，按图标按钮“  ”保存。

10.5 网络地址分类

点击“**分类管理->网络地址**”，管理员可以预定义网络地址类别。系统默认定义了全部，企业网，互联网，局域网和外网。因局域网和外网不可修改，因此在分类管理里无法查看到。

系统会根据服务器 IP 地址自动生成企业网的地址范围，管理员可以修改为企业内部网络的 IP 地址范围，系统会自动生成互联网的 IP 地址范围（除了企业网的 IP 范围之外的 IP 都属于互联网范围）。除了系统定义的地址类别，管理员还可以手工添加新类别，并输入该类别的 IP 地址段。

网络地址分类在流量统计、流量控制策略、网络控制策略等相关策略中会用到。

注意 在网络地址类别中，不能查看局域网和外网，但是在网络流量统计、流量控制策略和网络控制策略中可以看到局域网和外网。实际上，局域网是对单个计算机来说的，是指该计算机所在的网段；外网是相对于局域网来说的。

10.6 网络端口分类

点击“**分类管理->网络端口**”，管理员可以预定义端口类别。系统默认定义了全部，ICMP，TCP，UDP，邮件，网页，网络共享这些类别。其中，全部、ICMP、TCP、UDP 的类别不可添加和修改内容，邮件、网页、网络共享的端口范围可以添加和修改。

除了系统定义的这些常用端口类别，也可以手工添加新的端口类别及其端口范围。系统定义的端口类别无法删除和重命名，而手工添加的端口类别可以删除和重命名。

10.7 软件安装包分类

点击“**分类管理->软件安装包**” ，管理员可以预定义软件安装包类别。打开软件安装包分类窗口，系统默认分类为空，管理员需要手工添加软件安装包类别库和软件安装包。

此外，可以在策略日志中，选中一条软件安装控制记录，单击右键“**添加到分类库->软件安装分类库**”， 将该记录的软件安装包添加到指定的已存在分类库中。

10.8 软件卸载分类

点击“**分类管理->软件卸载**”打开软件卸载分类库窗口，系统默认分类为空，管理员需要手工添加软件卸载类别库和软件。

新增卸载软件可以单击工具栏上的卸载软件导入按钮，从服务器的软件库中选择软件添加，也可以单击工具栏上的添加按钮，手动输入软件名，支持通配符。

10.9 邮箱分类

管理员可以根据企业需要，将邮箱进行分类，方便按照类别对邮箱进行相关控

制。

点击“**分类管理->邮箱分类**”打开邮箱类别窗口，系统默认分类为空，管理员需要手工添加邮箱类别库和邮箱识别，邮箱识别支持通配符。

10.10 敏感信息分类库

为了方便管理员对企业内部的文档进行分类管理，管理员需要先在敏感信息分类库中设置用于识别文档的文字规则，程序使用这些规则自动匹配企业内部文档并对这些文档分类。

选择“**分类管理->敏感信息分类库**”打开敏感信息分类库创建特征规则和信息分类，特征规则用于设置具体匹配文档的信息，信息分类用于将不同的特征规则组合起来识别文档，作为确定文档分类的基准。

10.11 水印模板

点击“**分类管理->水印模板**”，管理员可以预定义水印模板，打开水印模板窗口，可添加打印水印模板和屏幕水印模板。

创建水印模板有两种方式：创建空白模板、从模板中复制。

创建空白模板

以创建打印水印模板为例，步骤如下：

1) 选中“**打印水印模板**”总节点，点击按钮，选择“**创建空白模板**”，点击【**确定**】按钮；

2) 设置水印对象，水印对象包括 1.点阵，2.指定位置，3.平铺；

3) 选择“**点阵**”节点，在右边视图中设置点阵相关参数；

4) 选择“**指定位置**”或“**平铺**”节点，点击按钮可添加水印对象，选择“**创建空白对象**”并指定水印样式和水印类型，或者从已有的水印对象中选择进行复制，点击【**确定**】按钮；

5) 若创建水印对象时选择的水印样式是“**指定位置**”，则新建的水印对象去到“**指定位置**”的节点下方，若创建水印对象时选择的水印样式是“**平铺**”，则新建的水印对象去到“**平铺**”的节点下方；

6) 选择具体的水印对象，在右边视图中设置具体属性；

7) 设置完成后，点击**【确定】**按钮；

设置好水印对象的属性后，可以在最右端的预览水印效果。

从模板中复制

从模板中复制，则是创建时可选择已有的模板，创建的新模板会沿用所选模板的水印对象，可在创建后根据实际进行调整。

第十一章. 桌面安全管理

11.1.1 申请管理

桌面申请管理默认可查看所有申请信息，并可按多种方式查询。

在线审批：

客户端在线时，桌面安全申请及审批的具体步骤如下：

1) 具有“**允许**”申请权限的客户端提交申请；

2) 控制台上有气泡提示，并在“**申请管理->桌面申请管理->申请管理**”中可以查看到申请记录，状态为等待审批；

3) 双击申请记录，可查看申请信息和文件内容；如果管理员认为客户端申请临时解除限制的内容和时效不合适，可对申请内容进行调整；

4) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；

5) 审批通过后，客户端在桌面申请管理申请信息窗口执行“**启用**”操作后申请生效。

离线审批：

客户端离线时，桌面安全申请及审批的具体步骤如下：

1) 具有“**允许**”申请权限的客户端提交申请，并在桌面申请管理申请信息窗口点击“**离线申请**”生成离线申请文件；

2) 管理员拿到申请文件，在桌面申请管理界面，选择右键菜单“**导入申请文件**”，选择申请文件导入；

3) 控制台上有气泡提示，并在桌面申请管理中可以查看到申请记录，状态为等待审批；

4) 双击申请记录，可查看申请信息和文件内容；

5) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；

6) 在桌面申请管理界面选中此条申请记录，选择右键菜单“**导出审批结果**”，并保存文件；

7) 把导出的审批结果文件发给客户端，在客户端申请信息中导入审批结果并启用。

否决申请

选中一个或多个申请，右键菜单中选择“**否决**”或者点击  按钮，输入否决意见，否决审批。

处于流程中的任一具有“**审批否决权限**”的管理员都可以否决申请， 申请一旦被否决，则该条申请结果即为不通过。

快速审批

同时选中多个申请，点击  按钮或是右键菜单中选择“**快速审批**”，进行快速审批，若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮。

删除申请

具有删除申请权限的管理员，可以删除桌面申请管理申请。

11.1.2 审批权限委托

当管理员外出时，可将自身的桌面申请管理审批权限，临时委托给信任的管理员代行审批管理，如果是系统管理员，还可以帮助其他管理员将权限委托给其他人。权限委托时，可设置授权时间区间与审批权限范围，预定时间到期，管理权限自动收回。

具有“**申请管理->桌面申请管理->审批权限委托**”权限的管理员才能将权限委托给其他管理员，具有“加密功能管理权限”的管理员才能接受委托。系统管理员还可以查看所有的委托情况。

权限委托

将委托权限给其他管理员的步骤如下：

1) 选择菜单栏“**申请管理->桌面申请管理->审批权限委托**”进入审批权限委托窗口；

2) 点击  按钮切换至权限委托设置界面，点击  按钮，弹出审批权限委托设置窗口；

3) 在常规选项卡中，勾选“**启用委托**”，选择受委托的管理员、委托的有效

起止时间，填写备注信息；

4) 切换到功能权限选项卡，选择要委托的权限，可以选择全部权限，也可以选择部分权限；完成之后点击【**确定**】按钮。

5) 此时“**申请管理->桌面申请管理->审批权限委托->权限委托设置**”，可以查看委托权限的具体信息。

权限代委托

1) 拥有系统管理员权限，点击桌面申请管理审批权限委托界面的  按钮切换至“**查看所有委托情况**”界面，点击  按钮，弹出审批权限代委托设置窗口；

2) 在常规选项卡中，勾选“**启用委托**”，选择受委托的管理员、委托的有效起止时间，填写备注信息；

3) 切换到功能权限选项卡，选择要委托的权限，可以选择全部权限，也可以选择部分权限；完成之后点击【**确定**】按钮。

4) 此时“**申请管理->桌面申请管理->审批权限委托->查看所有委托情况**”，可以查看委托权限的具体信息。

自动暂停委托

权限委托和权限代委托时，常规选项卡中有“委托人在线时自动暂行委托”选项。勾选此项，则委托人未登录控制台时，被委托人能得到受托的权限，当委托人登录控制台时，该委托将暂停，被委托人的受托权限将被收回。

此处设置只是在委托人登录控制台时暂时收回权限，委托人退出控制台登录后，受托人将再次获得受托权限。想要完全收回权限需要在审批权限委托界面执行删除操作。

11.1.3 审批流程管理

桌面申请管理支持申请流程管理，实现多级审批，保证申请得到各级别管理者复核和审查。

具有“**查看桌面申请和审批情况**”以及“**设置桌面审批流程**”权限的管理员登陆控制台，“**申请管理->桌面申请管理->审批流程管理**”，进入桌面申请管理流程管理界面，可对审批流程进行各项管理操作。

查找流程

点击查找按钮“”，打开查找对话框，输入查询条件，查询条件支持名称、申请类型、申请对象和审批人，支持模糊查询。点击查询按钮将定位到第一条符合条件的，再次点击查询按钮则会定位到下一条查询结果。

新建流程

点击新增按钮“”新建一条流程，新建流程包含基本设置和流程环节设置。新生成的审批流程默认不用。勾选流程名称前的复选框即可启用流程。

点击按钮添加流程环节，可建立多个环节，每个环节建立后都能进行修改、删除、上下移动操作，至少要有一个环节，才能完成流程设置。

编辑流程

点击编辑按钮，进入编辑流程页面，可对选中的流程进行编辑。可对每项流程条件以及流程环境进行修改。

说明 **编辑修改流程后，原先属于此流程的未完成的申请都会失效。**

复制流程

点击复制流程按钮，则选中的流程将会被复制。复制的流程默认在流程列表的最上方，名称为原审批流程名称后加_N，N 指当前流程是流程列表中存在的原流程的第几个复制版本。复制的流程所有设置，包括是否启用都与原流程一致。

删除流程

点击删除流程按钮，则选中流程会被删除。若删除流程是，尚有申请处于流程中未结束，则该申请终止，有相应提示返回给申请者。

替换流程

选中一条或多条流程，点击替换按钮“”，打开替换审批人对话框，在替换审批人窗口中选择原审批人和新的审批人， 点击确定并保存后，所选流程中的审批人将替换为新的审批人。

流程匹配原则

申请会按照审批流程列表中的各流程顺序，自上而下匹配，匹配到一条流程就不会再继续匹配。如果申请不能匹配到任何自定义的流程，则会匹配到默认流程，由管理员 Admin 审批。

一条申请匹配了某一流程后，会按顺序去到流程的每一个环节。每个环节都需

要达到指定审核通过结果时，才会进入下一个环节。只有当前环节的审批人可以审批，其他环节的审批人不能进行审批。申请在经过所有环节批准通过的情况下才算是被批准了。

申请审批处于某一环节 N 时，达到指定人数的审批人审批通过，则去到 N+1 环节；若未达到指定人数的审批人审批通过时，有审批者拒绝，则会回到 N-1 环节。此时，N-1 环节的审批者无需重新审批，只要有一名审批者点击【拒绝】按钮，则该申请会回到 N-2 环节；只要有一名审批者点击【说明】并输入审核通过的解释说明，则审批回到 N 环节。

桌面申请管理有否决操作，对于审批中的申请，流程中任一具有“**审批否决权限**”的管理员都可以否决申请，申请一旦被否决，则该条申请结果即为不通过，不会回到上一环节；对于已批准未执行的申请，被否决则无法执行。

11.2 申请审批权限设置

计算机和用户默认没有申请权限，管理员可在“**申请管理–申请审批权限设置**”中对计算机/用户的桌面申请权限进行管理。

选中设置对象后，在右边的申请审批权限设置视图中，逐个对每项申请权限设置。设置方法如下：

1. 点击“**申请状态**”下的下拉菜单中设置权限。申请状态为空或者禁止时，则不允许客户端申请对应的申请类型，申请状态为允许时，则允许申请对应的申请类型，具体申请范围受高级设置中限制。
2. 设置完申请状态后，点击  修改按钮可进行高级设置。

策略优先级

所有计算机（组）默认继承“计算机”节点的策略，计算机默认继承上一级计算机组的策略；计算机组策略优先于“计算机”节点的策略，计算机策略优先于计算机组策略；

所有用户（组）默认继承“用户”节点的策略，用户默认继承上一级用户组的策略；用户组策略优先于“用户”节点的策略，用户策略优先于用户组策略；

用户策略优先于计算机策略。

11.3 自我备案权限设置

为了减轻频繁申请外发文件给管理员带来的时间损耗，管理员可以给客户端设置自我备案权限，客户端在指定权限内自我审批外传文件，并有对应日志记录。

在“**申请管理-自我备案权限设置**”中对计算机/用户的自我备案权限进行设置，点击“**申请状态**”下的下拉菜单中设置权限。状态为空或者禁止时，则不允许对应类型的申请，状态为允许时，则允许对应类型的申请，点击  修改按钮可进行高级设置。高级设置内容同申请审批权限设置中的高级设置内容。

11.4 自我备案日志

客户端自我备案的申请会有对应的日志记录，管理员可以登录控制台，在“**申请管理-自我备案日志中**”查看。双击日志可以查看申请明细，明细内容包括：申请类型、时间、文件名称、文件路径、有效时间、申请理由、描述等。

11.5 权限查看

11.5.1 查看申请权限

在“**申请管理-查看申请权限**”中，可以查看到当前所有计算机\计算机组、用户\用户组的申请审批和自我备案权限。

11.5.2 查找申请权限

在“**申请管理-查找申请权限**”中，可以在右侧查询条件框中设置查询条件，查询条件包括申请类型、状态、对象类型、对象范围、对象名称；点击“**查询**”后在信息列表中将列出符合条件的申请审批和自我备案权限。

11.6 客户端申请

打印策略、设备控制策略、移动存储策略限制的计算机或用户，当其具有“**允许申请**”权限时可以提交申请在指定的时间内解除限制。

客户端在线时，申请后控制台能马上收到通知并审批。审批通过后，可以在“**查看申请信息**”中进行解密。

客户端离线时，申请后，还需要在“**查看申请信息**”菜单中，导出申请文件，把申请文件发给管理员，管理员在控制台导入后进行审批。审批通过后，从管理员处拿到授权文件，在客户端导入授权文件，并在“**查看申请信息**”中启用。

11.6.1 打印申请

当计算机或用户被设置了禁止打印操作的策略时，可以通过申请请求在特定时间内放开对特定打印机和应用程序的打印控制。

具有“**允许申请**”权限计算机或用户，右键单击客户端图标，选择“**申请->打印**”，选择想要解除限制的打印机以及应用程序，设置时间，填写申请理由后点击【**申请**】即完成申请。

11.6.2 打印时不加水印申请

当计算机或用户被设置了打印添加水印的策略时，可以通过申请请求在特定时间内对特定打印机和应用程序进行打印时不添加水印。

打印时不加水印申请的操作步骤，类同于打印申请操作步骤。

11.6.3 使用设备申请

当计算机或用户被设置了禁止使用设备的策略时，可以通过申请请求在特定时间内可使用指定的设备。

具有“**允许申请**”权限计算机或用户，右键单击客户端图标，选择“**申请->使用设备**”，会显示当前客户端环境所有被禁用的设备和预设的设备分类（与控制台“**设备控制**”一致），选择想要解除禁止的设备，设置时间，填写申请理

由后点击【**申请**】即完成申请。

11.6.4 使用移动存储设备申请

当计算机或用户被设置了禁止使用移动存储设备的策略时，可以通过申请请求在特定时间内可使用指定的移动存储设备。

具有“**允许申请**”权限计算机或用户，右键单击客户端图标，选择“**桌管申请->使用移动存储设备**”，会显示当前客户端环境所有移动存储设备，选择需要放开控制的移动存储以及读写权限，设置时间，填写申请理由后点击【**申请**】即完成申请。

11.6.5 发送邮件

当计算机或用户被设置了禁止发送邮件的邮件控制策略时，可以通过申请请求在特定时间内发送带附件的邮件。

具有“**允许申请**”权限计算机或用户，右键单击客户端图标，选择“**桌管申请->发送邮件**”，设置收件人和文件信息，设置时间，填写申请理由后点击【**申请**】即完成申请。

11.6.6 聊天工具传送文件

当计算机或用户被设置了禁止文件控制的 IM 文件传送策略时，可以通过申请请求在特定时间内使用聊天工具传送文件。

具有“**允许申请**”权限计算机或用户，右键单击客户端图标，选择“**桌管申请->聊天工具传送文件**”，设置文件信息和聊天工具，设置时间，填写申请理由后点击【**申请**】即完成申请。

11.6.7 上传文件和数据

当计算机或用户被设置了禁止上传文件的上传控制策略时，可以通过申请请求在特定时间内上传文件到指定网站。

具有“**允许申请**”权限计算机或用户，右键单击客户端图标，选择“**桌管申请**

->**上传文件和数据**”，设置文件信息和网站信息，设置时间，填写申请理由后点击【**申请**】即完成申请。

11.6.8 复制到移动盘\网络盘\刻录光盘

当计算机或用户被设置了禁止修改、删除可移动盘、网络盘、光盘的文档控制策略时，可以通过申请请求在特定时间内修改、删除可移动盘、网络盘、光盘的内容。

具有“**允许申请**”权限计算机或用户，右键单击客户端图标，选择“**桌管申请->复制到移动盘\网络盘\刻录光盘**”，设置申请的文件或文件夹信息，设置时间，填写申请理由后点击【**申请**】即完成申请。

11.6.9 查看申请情况

在客户端桌面安全管理托盘，选择右键菜单“**查看桌管申请情况**”，可查看申请和审批情况。双击申请记录，可查看申请的详细信息，包括：申请信息、申请内容、审批状态、审批流程、审批历史、有效时间。

11.7 客户端自我备案

打印策略、设备控制策略、移动存储策略、IM 文件传送策略、上传控制策略、文档控制策略限制的计算机或用户，当其具有“**允许申请**”的自我备案权限时可以在指定权限内自我审批申请，审批外传文件等。

客户端自我备案操作可参考客户端申请的操作，通过右键客户端托盘图标选择“**桌管申请**”，弹出申请向导，选择对应申请类型进行申请，最后在申请向导界面中点击“**自我备案**”按钮进行自我备案，完成后即可直接执行对应申请的操作。

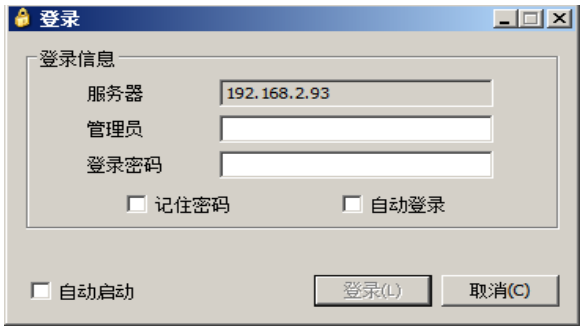
11.8 代理管理员

管理员设置某一客户端可以登录代理管理员后，则可在该客户端所在计算机上

登录代理控制台，进行审批桌面安全管理申请。

11.8.1 登录

控制台“**桌面申请->申请审批权限设置**”或“**桌面申请->自我备案权限设置**”中存在申请状态为“允许”的申请项的计算机或用户，可在系统托盘的客户端图标上，选择右键菜单“**审批管理平台**”，并输入管理员帐户和密码，即可登录代理控制台。代理控制台支持自动启动。



登录代理控制台时，勾选“**自动启动**”，则下次客户端启动并且连上服务器后，代理控制台自动启动，弹出登录对话框。也可在代理控制台选择菜单“**申请管理->选项**”进行设置，在“**基本设置->登录设置**”中勾选“**自动启动**”。

11.8.2 审批管理

代理控制台的审批管理功能和控制台一样，可以查看桌面安全管理申请，可以审批申请、导入申请文件和导出审批文件，可以查看审批权限委托情况、进行权限委托。

11.8.3 锁定

为防止他人使用代理控制台进行审批，管理员离开时可锁定代理控制台。锁定后代理控制台仍能收到解密申请和外发申请的气泡通知，需要输入密码登录才能进行审批。锁定有三种方式：直接锁定、离开后锁定和最小化锁定

直接锁定：

选择菜单“**操作->锁定**”进行锁定。

离开后锁定：

选择菜单“**申请管理->选项**”进行设置，勾选“**用户离开后自动锁定**”，并可设置离开后多少分钟进行锁定，默认为 15 分钟。

最小化锁定：

选择菜单“**申请管理->选项**”进行设置，勾选“**最小化到托盘后锁定**”。

第十二章. 网络接入检测

网络接入检测功能可以发现是否有非法的计算机接入网络，并且对其进行网络阻断。 选择菜单“**工具->网络接入检测**”打开网络接入检测窗口。

12.1 启动接入检测

启动接入检测

网络接入检测默认并没有打开，所以刚开始接入检测窗口的内容为空。要启动接入检测，选择“**系统->设置**”设置接入检测策略。

在设置对话框中勾选“启动接入检测”，则客户端会启动接入检测功能，安装了客户端计算机的网段内所有在线的计算机都会被扫描出来。在每个网段内会有一个客户端机器作为检测代理，用小红旗标识，作为检测代理的计算机会扫描其所在网段内所有的计算机。

接入规则设置

管理员可对计算机的 IP、MAC、IP/MAC 设置接入规则，包括：授权、保护、阻断、常规。

12.2 启动接入控制

启动接入控制功能

设置好计算机的类型后，可以启动接入控制功能。选择“**操作->设置**”打开策略设置对话框。

1. 启动接入控制功能

如果选中此项，代理计算机将启动接入控制功能，阻止“阻断”的计算机访问“保护”的计算机。

管理员可将不允许访问“保护”的计算机都设置为“阻断”。

2. 阻断所有未安装客户端的计算机接入网络

如果勾选此项，未安装客户端并且没被设为“授权”或“保护”的计算机，不能访问“保护”的计算机。请确认所有未安装客户端的计算机都需要被阻断，否则，请手工指定为“授权”或者“保护”。

一般来说，外来接入的计算机未安装客户端的，因而无法访问“保护”的计算机，达到保护企业机密资料的目的。

3. 阻止 IP 地址范围

如果不设置阻止 IP 地址范围，代理计算机会对网段内所有需要被阻断的计算机进行阻断；如果指定了 IP 地址范围，则只会对设置范围内需被阻断的计算机进行阻断。

第十三章. 数据备份

13.1 使用数据库备份

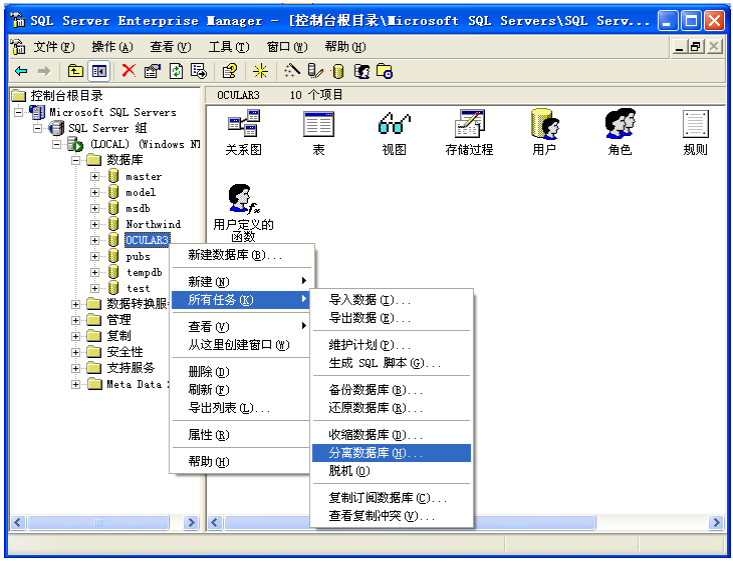
主数据库备份

主数据库的备份，主要操作下列步骤：

1) 首先停止 IP-guard Server 以及其他一切使用 OCULAR3 数据库的程序；

2) 打开 SQL Server 2000 的企业管理器或 SQL Server 2005 的 Management Studio；

3) 右键点击“OCULAR3”数据库，选择菜单“**所有任务->分离数据库**”



4) 分离数据库成功后，管理员可以将主数据库文件 OCULAR3.mdf、OCULAR3_Log.LDF 两个文件一起复制到备份目录下；

5) 分离完成后，企业管理器中的 OCULAR3 目录会被清除，管理员需要通过选择菜单“**所有任务->附加数据库**”还原 Server 安装目录下的主数据库。

上面是通过分离数据库然后复制数据库文件来备份的，也可以先把 MSSQLSERVER 服务停止，然后复制数据库文件到备份目录，再启动 MSSQLSERVER 服务和 IP-guard 服务，同样可以达到备份的目的。

日志数据库备份

日志数据按天存储在 DATA 目录，默认存放在安装程序的 DATA 文件夹中。按日期命名，例如：2009-6-20 这一天的文件名为
OCULAR3_DATA.20090622.MDF
OCULAR3_DATA.20090622_Log.LDF
OCULAR3_DATA.20090622.X.MDF
OCULAR3_DATA.20090622.X_Log 等共有 2 到 10 个文件。

日志数据库的备份，主要操作下列步骤：

1) 首先停止 IP-guard Server 以及 MSSQLSERVER 服务；

2) 把数据库文件.mdf 和.ldf 文件复制到备份目录下；

3) 启动 MSSQLSERVER 服务和 IP-guard 服务。

13.2 控制台备份管理

13.2.1 备份数据

管理员可以使用控制台提供的备份数据功能定期备份客户端的数据，将数据存放在其它盘符或移动存储设备中，以防止数据量太大，磁盘空间不足而引发的问题。

选择菜单“**工具->服务器管理->数据库备份管理**”打开备份数据与查看窗口。

图标状态	说明
	新建备份任务；
	取消备份任务；

 　　设定定期备份计划；

创建备份任务

点击工具栏的【新建任务】图标，新建一个备份任务，具体步骤如下：

1) 选择需要备份的数据类型，包括：基本事件日志、文档操作日志、文档操作副本、网页浏览日志、打印日志、邮件和屏幕历史等十几种数据类型；

2) 选择需要备份的数据的日期范围，设置起始时间和结束时间；

3) 选择保存备份数据的路径；

   勾选“**将备份数据存储到 SQL-SERVER 所在的计算机**”，选择路径，则备份数据会保存到 SQL-SERVER 所在计算机对应的路径；

   勾选“**将备份数据存储到网络路径**”，输入具体的路径地址，如：\\192.168.1.1\backupdata ，支持域名，同时需要输入对该网络路径有读写权限的用户名以及密码，点击“**测试连接**”按钮，连接成功后，届时备份数据会保存到指定的网络路径；

4) 为了清理数据库空间，管理员可以勾选“**删除原始的数据**”自动清除已经备份的数据，否则备份的数据不会从数据库中删除；

5) 点击【确定】，启动备份任务。

添加备份计划

点击工具栏的【备份计划】图标，打开“备份计划管理”窗口。再点“新建”图标，新建备份任务，具体步骤如下：

1) 设置备份周期，可以选定日、月、周为单位。例如，每 3 天备份一次，每个月备份一次，每 3 个月备份一次，每 2 周备份一次等。最长支持每 10 年备份一次，即 120 个月或 520 个周。

2) 选择首次备份时间；

3) 设定备份的时间范围，填入起始日期和终止日期，其中终止日期必须填写，单位会保持与备份周期选定的单位一致。设置之后，从备份开始的时间算起，前后对应的时间范围内进行备份；

4) 选择需要备份的数据类型，包括：基本事件日志、文档操作日志、文档操作副本、网页浏览日志、打印日志、邮件和屏幕历史等十几种数据类型；

5) 根据实际情况勾选“**删除原始数据**”，勾选后会自动清除已经备份的数据；

6) 选择保存备份数据的路径；

7) 点击【确定】，会在备份计划列表中查看到这条新建的备份计划。

到了指定的任务执行时间，系统会按照设定新建一条备份任务并启动该任务。

注意 备份任务只能同时执行一个，如果已经存在正在执行的备份任务则不能再增加新的备份任务。

13.2.2 加载和卸载备份数据

选择菜单“**工具->服务器管理->备份管理**”打开备份管理窗口，可以直接查看已加载的备份数据列表，也可以加载和卸载备份数据。

加载备份数据

选择菜单“**备份管理->加载**”，单击工具栏的【加载备份】按钮，选择备份数据文件所在的目录，勾选需要加载的数据，单击【加载】和【确定】加载指定的备份数据。

卸载备份数据

假如不需要查看某个备份数据，也可以将备份数据从服务器中卸载。选择需要卸载一个或者多个的备份数据，单击【卸载备份】按钮“  ”，可以查看待卸载的备份列表，再单击【确定】，对应的备份数据列表将被删除，在控制台上也不能再查看到这些备份数据。

第十四章. 工具

14.1 账户管理

系统管理员具有最高权限，他可以使用系统内的所有功能。系统管理员可以通过新建管理员的方式来使其他的管理者执行某些管理功能。

选择菜单“**工具->账户**”，系统管理员可以查看管理员信息，并可以添加/删除、启用/禁用管理员账号，同时也可以修改管理员密码。

14.2 计算机管理

选择菜单“**工具->客户端管理->计算机管理**”进入计算机管理窗口，可查看计算机授权信息列表以及计算机识别信息列表。

在计算机授权信息列表中点击任意一条记录，即可在计算机管理窗口下面的计算机识别信息列表中查看到该记录的相关识别信息。

14.3 警报信息

警报信息记录了实时报警日志，在“**工具->警报**”中查看。如果控制台设置了“弹出报警气泡”，出现满足报警的情况时，会在控制台机器上弹出报警气泡进行通知，通过点击报警气泡查看所有的实时报警记录。

警报信息主要有：策略触发报警信息、服务器报警信息、以及客户端异常报警信息。

14.4 邮件报告设置

实时报警信息可以通过邮件服务器，发送到指定的邮箱，管理员可以通过邮件及时地了解和处理报警。

使用邮件报告功能前，系统管理员必须在“**工具->选项->邮件报告服务器设置**”中配置邮件报告服务器。

配置邮件报告服务器之后，才开始进行邮件报告设置。选择菜单“**工具->邮件报告设置**”，管理员可以查看、添加和修改邮件报告设置。

14.5 策略应用查询

点击“**工具->策略应用查询**”，可查询到已设定的所有策略。通过策略库，管理员可以清楚的知道当前哪个客户端上设置了哪一个策略，以及策略的具体设置，如策略是否启用，应用的对象是计算机还是用户等。管理员可以根据策略名称进行查找。

14.6 水印编码查询

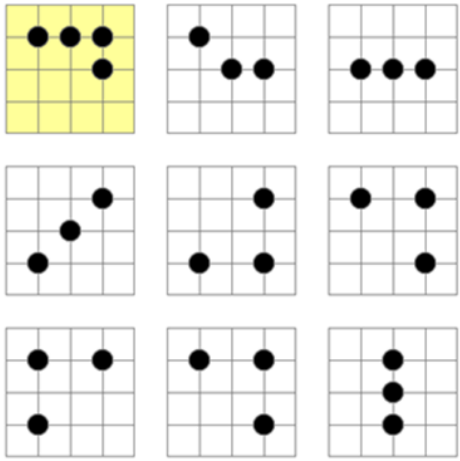
点击“**工具->水印编码查询**”，可根据获取到的点阵水印信息，查询到对应的计算机信息。

点阵含义

点阵水印是在打印文档或者电脑屏幕上覆盖上一层包含计算机信息的圆点图

案，以 9 个为一组（九宫格形式），重复排列而成。

一组点阵的示意图如下：



说明 1.第一个点阵图案为起始位图案，不包含信息；

水印编码查询

查询步骤如下：

1) 在对应的水印中找到起始位图案，以起始位图案为起点，往右算三个图案位，往下算三个图案位，获取到一组九宫格点阵图案；

2) 除去起始图案，按从左到右，从上到下的顺序，逐个将图案对照码表得到对应的字母或数字，组成编码字符串；

3) 选择此次查询的水印类型，输入已得到的编码字符，点击【**查询**】按钮，即可查询出此点阵图案代表的计算机信息。

14.7 服务器时间

选择“**工具->服务器管理->服务器时间**”，可以查看服务器当前时间。如果管理员确认服务器当前时间没有问题，点击【信任】按钮，控制台就不会再弹出报警气泡。

14.8 类库同步管理

在类库信息发生改变时，服务器会将最新的类库信息同步到客户端计算机，

选择“**工具->服务器管理->类库同步管理**”，可以查看各客户端计算机同步类库信息的时间，包括应用程序类别、应用程序识别、网站类别，网站识别、网络地址类别、网络端口类别、时间类别、移动存储库、移动存储识别的同步时间、邮箱类别、邮箱识别。

14.9 组织架构同步

组织架构同步功能，可以将 AD 域的组织结构同步至 IP-guard 服务器，实现 AD 域中未接入服务器的计算机和用户预先配置分组，当客户端接入服务器后，可自动分配到其所属分组中。选择“**工具->服务器管理->组织架构同步**”，进入组织架构同步管理界面。

14.9.1 同步配置

选择“**组织架构同步->同步配置**”，可以对 AD 域服务器或 LDAP 服务器的同步配置进行添加/修改/删除/立即执行等操作，也可对同步配置信息进行查看。

说明　查看同步配置时，如果该配置的目标设置是到用户，则执行完配置后，可以直接在查看同步配置中看到其同步情况；

添加配置

点击图标，或者在同步配置界面右键菜单选择“**新增配置**”，新增一条同步配置。新增配置时需要设置 AD 连接设置和同步的对象设置。

14.9.2 同步日志

选择“**组织架构同步->同步日志**”，管理员可以查看组织架构同步日志。

14.9.3 例外对象

对于需要分配到特定分组，无需保持和域组织架构同步的计算机或用户，可以设置为例外对象，则手动或自动同步时，例外对象均不会同步。

选择“**组织架构同步->例外对象**”，可以添加、修改、删除例外对象。

14.10 邮件报告服务设置

使用邮件报告功能前，系统管理员必须在“工具->选项->邮件报告服务器设置”中配置邮件报告服务器。

邮件服务器设置按照从上到下匹配，如果规则匹配得上，则使用此设置发送邮件，如果所有设置都不匹配，则不发送邮件。

策略示例

假如企业内部使用的邮件系统不能收发外网的邮件，内部邮箱和外部邮箱都需要接收报警邮件。此时需要设置两个邮件服务器，一个发送给内部邮箱，一个发送到外部邮箱。

① 设置一个邮件服务器，匹配邮箱为：@companyname.com；
② 再设置一个邮件服务器，匹配邮箱为：@163.com，再把此服务器设为默认服务器。

第十五章. 用户系统管理

若公司已存在 AD 域或 LDAP，需要在客户端机器上做统一的身份验证和管理，可使用用户系统管理功能。

选择“**工具->服务器管理->用户系统管理**”进入用户系统管理界面。

15.1 服务器配置

选择“**用户系统管理->服务器配置**”，需要添加对应的 AD 域服务器或 LDAP 服务器配置。

点击图标，打开服务器设置界面，选择服务器类型，输入域服务器的域名以及域服务器的 IP 地址。其中，服务器类型可以选择“LDAP **服务器**”或“**域服务器**”，若选择了“LDAP **服务器**”，则需要点击“**高级设置**”按钮，进入 LDAP 服务器的高级设置界面，设置 LDAP 服务器的端口、协议版本号、是否使用 SSL、是否使用匿名连接。

完成对应的服务器参数后，可点击“**测试登录**”按钮，弹出测试连接窗口，输入所设服务器中的用户名称和密码。最后点击“**确定**”按钮，会新增一条服务器配置。

15.2 登录验证

15.2.1 控制台设置策略

选择“**用户系统管理->登录验证**”，进入登录验证界面，可设置是否启用登录验证。

点击图标，打开登录验证配置界面，进行相应参数设置：

参数	内容
强制验证	勾选强制验证，启用强制登录验证功能；
包含范围	设置包含的客户端范围，在该范围内的客户端会执行强

	制验证；
排除范围	设置排除的客户端范围，在该范围内的客户端不会执行强制验证；
非强制验证	勾选非强制验证，启用非强制登录验证功能；
包含范围	设置包含的客户端范围，在该范围内的客户端会执行非强制验证；
排除范围	设置排除的客户端范围，在该范围内的客户端不会执行非强制验证。

注意 若对客户端同时设置强制登录验证和非强制登录验证，则强制登录验证优先级高于非强制登录验证。

15.2.2 客户端登录验证

登录验证

强制验证

对于启用了强制验证的客户端：

若登录 Windows 系统的账户名并非“**服务器配置**”中指定的域服务器存在的用户，则进入 Windows 系统后会弹出用户系统登录对话框，此时无法关闭该对话框，需要输入“**服务器配置**”中指定的域服务器存在的用户名和正确密码，方可以正常使用计算机；

若登录 Windows 系统的账户名为“**服务器配置**”中指定的域服务器存在的用户，进入 Windows 系统后不会弹出用户系统登录对话框，自动会使用当前登录的用户登录用户系统，可正常使用计算机。

非强制验证

对于启用了非强制验证的客户端：

不论登录 Windows 系统的账户名是否为“**服务器配置**”中指定的域服务器存在的用户，进 Windows 系统后都不会弹出用户系统登录对话框，自动会使用当前登录的用户登录用户系统，可正常使用计算机。若是手动调出登录登录对话框，可以直接关闭该对话框。

说明 客户端托盘菜单中，选择“**登录用户**”或“**注销**”，可以手动登录或退出用户系统。

申请取消强制登录

在强制登录验证策略下，客户忘记域账户或者离线客户端，可以申请取消强制登录验证，直到下次重启计算机之前暂时使用计算机。

客户端在用户登录验证第一次失败后，界面上会有“**申请取消强制登录**”按钮，点击后弹出“**检验操作码**”界面；

在控制台“**工具->客户端工具->确认码计算器**”，将客户端“**校验操作码**”中的原始操作码复制到“**确认码生成器**”中的客户端操作码处，点击“**解析**”，再点击“**生成确认码**”。在客户端“**校验操作码**”中填入控制台生成的确认码，即可取消强制登录验证。

切换用户

对于启用了强制登录验证或非强登录验证的客户端，若使用域账号登录操作系统，会自动使用此域账号登录用户系统，此时右键客户端托盘，会出现一个"**切换用户**"的选项，点击后，可以弹出用户系统登录窗口，填写其它用户登录，可将用户系统切换至其它用户。成功切换为其它用户后，再右键客户端托盘，"**切换用户**"的选项会变为"**注销**"，选择"**注销**"后，用户将自动登回原先操作系统登录的域用户。

15.3 关联验证

15.3.1 控制台设置策略

选择“**用户系统管理->关联验证**”，进入关联验证设置界面，可选择是否启用关联验证，以及进行相应的参数配置；

点击图标，打开关联验证配置界面，进行相应参数设置：

参数	内容
强制验证	勾选强制验证，启用强制用户关联验证功能；
包含范围	设置包含的客户端范围，在该范围内的客户端执行强制验证；
排除范围	设置排除的客户端范围，在该范围内的客户端不执行强制验证。
非强制验证	勾选非强制验证，启用用户非强制关联功能；

包含范围	设置包含的客户端范围，在该范围内的客户端执行非强制验证；
排除范围	设置排除的客户端范围，在该范围内的客户端不执行强制验证；
不关联用户	客户端使用此设置中的用户账号登录验证成功后，可以验证成功并正常使用计算机，但该用户名不会变为本机的关联用户。支持用户名和域名\用户名的格式输入；
禁止关联用户	客户端使用此设置中的用户账号登录或验证后，无法验证成功，计算机保持锁定。支持用户名和域名\用户名的格式输入；

15.3.2 客户端关联验证

强制关联验证

对于启用了强制关联验证的客户端：

若该机器已经存在关联用户且关联用户为“**服务器配置**”中指定的域服务器存在的用户，则不会弹出“**用户关联认证**”窗口，可正常使用计算机；

若该机器不存在关联用户，或者存在的关联用户并非“**服务器配置**”中指定的域服务器存在的用户，则会弹出“**用户关联认证**”窗口，窗口无法关闭，需输入“**服务器配置**”中指定的域服务器存在的用户和正确的密码，方可通过验证，继续正常使用计算机，此时新输入的用户自动成为本机的关联用户。

非强制关联

对于启用了非强制关联验证的客户端：

若该机器已经存在关联用户且关联用户为“**服务器配置**”中指定的域服务器存在的用户，则不会弹出“**用户关联认证**”窗口，可正常使用计算机；

若该机器不存在关联用户，或者存在的关联用户并非“**服务器配置**”中指定的域服务器存在的用户，则会弹出“**用户关联认证**”窗口，此时可输入“**服务器配置**”中指定的域服务器存在的用户和正确的密码（则此时输入的用户自动成为本机的关联用户），或者直接关闭对话框，均可正常使用计算机，若输入了新的用户则该用户指定成为本机的关联用户。

15.4 关联信息

当设置同步配置时，若来源为用户，目标为计算机，则系统会根据首次登录的用户去匹配来源的用户，匹配成功则该计算机会被同步到该来源用户所在的分组。此时，我们把这个用户称做“计算机关联用户”。

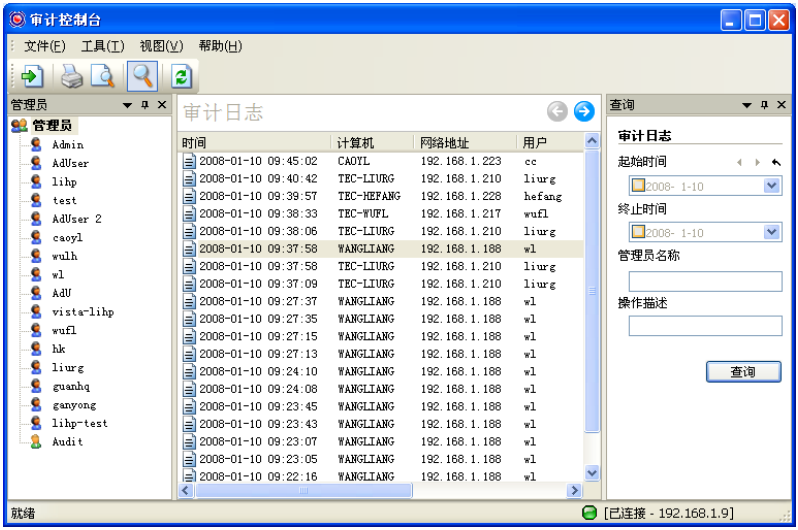
选择“**用户系统管理->关联信息**”，可以查看计算机关联了哪个用户。

第十六章. 审计控制台

16.1 登录审计控制台

单击安装目录下的 OConsole3.exe 或者“**开始->所有程序->IP-guard V3->IP-guard V3 控制台**”启动控制台模块。

输入服务器 IP 或服务器机器名称，使用系统审计员的帐号“**audit**”，初始密码为空，登录到审计控制台。



16.2 使用审计控制台

审计日志内容

审计日志包括控制台登录情况，管理员的操作日志、修改删除策略、查看实时屏幕、远程控制、设置管理员的账户与权限等。

第十七章. 文档安全管理

17.1 操作流程

启用加密功能

1) 安装客户端
2) 在控制台启用加密授权
3) 在控制台设置加密权限，含授权软件、安全区域和级别等

申请与审批

1) 客户端申请解密/外发
2) 控制台进行审批
3) 客户端执行解密/外发

外发查看器

1) 安装外发查看器
2) 控制台对外发查看器进行授权
3) 外发查看器导入授权
4) 客户端生成外发文档
5) 外发查看器查看外发文档

17.2 启用/禁用加密授权

对于 Windows 客户端，加密授权分为两种模式：透明加密模式以及只读加密模式。两种加密模式不能同时启用。

在 IP-guard 控制台的计算机栏中，选择目标计算机或组（如果是组，则对组内所有计算机），右键选择“**加密管理功能->启用透明加密**”，或者是“**启用只读授权**”，则目标计算机启用了相应的加密授权模式。若选择“**加密管理功能**

->禁用加密授权”，即取消目标计算机的加密授权。

说明 以下的操作说明，如无特别指出，皆默认是启用了透明加密模式。

17.3 授权软件管理

选择菜单栏“**文档安全管理**”进入加密管理主窗口。再选择文档安全管理窗口的菜单“**管理->授权软件**”可查看当前支持的授权软件。

如果需要使用的授权软件，在授权软件库不存在，可点击添加自定义授权软件。

17.4 安全区域管理

在针对客户端进行加密权限设置之前，应该先根据企业部门的分类，设置好加密安全区域。

在文档安全管理窗口，可查看和修改安全区域。默认有一个公共安全区域，无法修改和删除。可点击添加安全区域。

授权软件自动加密生成的文件，默认为公共安全区域普通级别。为了方便信息交流，所有的启用加密的计算机都拥有公共安全区域普通级别的访问权限。

17.5 外发对象管理

外发对象是指可以在加密系统环境外可以打开外发文档的对象。

在文档安全管理窗口，可查看和修改外发对象。

授权情况

目前支持三种外发对象授权方式：通用授权、绑定计算机授权、绑定外发 usbkey 授权。

通用授权

具体步骤如下：

1) 添加一个外发对象，默认为启动状态；

2) 在授权情况处右键选择“**创建通用识别码**”，创建成功，通用识别码为已认证状态；（此步骤可以省略，如直接对外发对象授权，会自动生成一个通用识别码。）

3) 选中该外发对象，右键菜单中选择“**授权**”；

4) 在弹出的授权窗口中，填写授权设置，包括到期时间、是否设置密码，完成后点击**【生成授权文件】**按钮 ，生成授权通用授权文件；

5) 在外发查看器中导入该授权文件，则通用识别码为启用状态时，该外发查看器能查看发给此外发对象的所有外发文件。

绑定计算机授权

具体步骤如下：

1) 添加一个外发对象，默认为启动状态；

2) 在授权情况处右键选择“**导入外发计算机识别码**”；

3) 弹出的导入窗口中填入计算机的识别码，名称以及描述信息，完成后点击**【确定】**，生成绑定的识别码，默认为未认证；

4) 选中该识别码，右键菜单中选择“**认证**”；

5) 选中该外发对象，右键菜单中选择“**授权**”；

6) 在弹出的授权窗口中，填写授权设置，包括到期时间、是否设置密码，完成后点击**【生成授权文件】**按钮 ，生成授权通用授权文件

7) 在外发查看器中导入该授权文件，则能查看发给此外发对象的所有外发文件。

8) 绑定授权可以先导入通用授权证书，再获取识别码进行绑定；也可以先根据识别码绑定，导入生成的绑定授权证书进行绑定

绑定外发 USBKey 授权

具体步骤如下：

1) 在控制台的登录的机器上插入外发 USBKey；

2) 添加一个外发对象，默认为启动状态；

3) 在授权情况处右键选择“**导入外发 USBKey 识别码**”；

4) 弹出的导入窗口中，自动载入 USBKey 的识别码，如果插入多个外发 USBKey，则需要选择对应要授权的外发 USBKey，输入名称以及描述信息，完成后点击【**确定**】，生成绑定的外发 USBKey 识别码；

5) 选中生成的外发 USBKey 识别码，右键菜单中选择“**认证**”；

6) 选中该外发对象，右键菜单中选择“**授权**”；

7) 在弹出的授权窗口中，填写授权设置，包括到期时间、是否设置密码，完成后，点击【**授权 USBKey**】，则该 USBKey 授权成功，插入该 USBKey 的机器能查看发给此外发对象的所有外发文件。

说明 若是授权时控制台所在机器没有插着外发 USBKey，则需要点击【**生成授权文件**】，在插着外发 USBKey 的机器中导入该授权文件完成授权。

17.6 外发配置模板管理

控制台菜单“**文档安全管理**”->“**外发配置模板管理**”，管理员可以设置外发配置模板并进行统一管理，方便地使用常用设置。

每个管理员只能使用、管理自己创建的外发配置模板，无法查看到其他管理员创建的，可以导入其他管理员导出的模板。

17.7 加密权限设置

控制台菜单“**文档安全管理**”->“**加密授权设置**”，是对启用加密授权的客户端在连上服务器时的权限设置，包括设置授权软件、安全区域、加密文档默认安全属性。

可以对计算机和域用户设置加密。如果某计算机或域用户有自己的权限，在图标右上角有个星号表示。如果计算机和域用户没有自己的权限，则会继承其所在组的权限。用户权限优先于计算机权限。

17.8 加密参数设置

在加密参数设置界面中，可设置整个网络、指定分组或指定客户端的容灾时间及是否需要在客户端的资源管理器中隐藏加密文档上的加密标记。

可点击进行各项设置加密参数各项设置，完成后需要保存才可以生效。

17.8.1 安全密码设置

必须设置安全密码

设置了“**必须设置安全密码**”的客户端上，安全密码不能为空，必须要设置。

密码必须符合复杂性要求

设置了“**密码必须符合复杂性要求**”的客户端上，设置的安全密码必须符合复杂性要求。其中，复杂性要求需同时满足以下三点：

1、长度至少为六个字符

2、包含来自以下四个类别中的至少三种字符

英文大写字母（从 A 到 Z）

英文小写字母（从 a 到 z）

10 个基本数字（从 0 到 9）

非字母字符（例如,!、$、#、%）

3、密码强度为中及以上。

管理员可以通过设置**密码最长使用期限**指定安全密码可以使用的天数。

17.8.2 邮件白名单

设置邮件白名单的客户端，可以实现发送指定邮件时，附件中的加密文件会自动解密成普通文件。目前只支持 SMTP 协议非 SSL 加密的邮件。

点击邮件白名单设置单元格末端的…后，可设置邮箱地址规则、附件文件名、是否备份解密的附件文件。

邮箱地址规则设置说明

点击邮件白名单设置单元格末端的…，点击，可添加邮箱地址规则。可设置多条邮箱地址规则，通过调整邮箱规则顺序。

邮箱地址规则匹配原则

规则匹配自上而下匹配，一封邮件匹配到一条有效的规则后将不会匹配之后的规则，当所有规则都无法匹配时，则此邮件的加密附件将不会被解密。

邮件白名单规则使用示例

企业相关情况

1.公司设立文控部，文控部作为明文的出口，对于一些要发往公司外网的邮件，经过公司相关的流程后，统一由文控部门使用外部邮箱发送出去；

2.外部邮箱的后缀统一为@outerdept.com。

需要实现：

文控部门使用外部发出去的邮件，附件密文都需要解密，但前提是该邮件必须有抄送文控部门的主管（chen@outerdept.com）

针对以上要求，可以如此设置

设置一条邮件白名单规则，具体设置如下

模式：解密附件

接收邮箱：包含邮箱 chen@outerdept.com，排除邮箱为空，勾选"允许排除范围外的收件人解密"

发送邮箱：包含*@outerdept.com，排除邮箱为空

17.9 长期离线授权设置

长期离线权限设置可指定允许离线使用的时间范围，在此时间范围之内可打开加密文档。长期离线权限还能设置解密、外发、授权软件和安全区域等权限，具体操作同加密权限设置。

当客户端在线时，设置长期离线权限，权限能直接传达给客户端。
当客户端离线时，设置长期离线权限，还可以导出离线授权文件，把离线授权文件发给客户端，在客户端导入授权文件。

17.10 加密文档操作日志

加密文档操作日志可记录：客户端加密文件，解密文件，生成外发文件，修改文档属性，解密申请和外发申请等相关日志。

加密文档操作日志默认显示所有的日志，管理员也可以设置各种查询条件进行查询。双击日志可查看详细信息。有设置备份的操作日志，可在详细信息中查看文档副本。

17.11 全盘扫描

拥有“**加密功能-任务管理**”权限的管理员，选择菜单栏“**文档安全管理**”进入加密管理主窗口，再选择 “**全盘扫描**”，进行全盘扫描加解密任务的设置。

全盘扫描加密任务

设置全盘扫描加密任务步骤：

1) 选中一台或多台客户端机器，点击右上角的添加按钮，在出现的菜单中选择“创建加密任务”，弹出创建加密任务对话框；

2) 在“常规”选项卡中，对常规项目进行设置；

3) 切换至“高级”选项卡中，对高级项目进行设置；

4) 设置完成后，点击“确定”按钮，扫描加密任务创建成功。

全盘扫描解密任务

设置全盘扫描解密任务步骤：

1) 选中一台或多台客户端机器，点击右上角的添加按钮，在出现的菜单中选择“创建解密任务”，弹出创建解密任务对话框；

2) 在“常规”选项卡中，对常规项目进行设置；

3) 切换至“高级”选项卡中，对高级项目进行设置；

4) 设置完成后，点击“确定”按钮，扫描解密任务创建成功。

17.12 解密申请管理

解密申请管理默认查看所有解密申请信息，包括已审批和未审批的。并可按多种方式查询。

在线审批：

客户端在线时，解密申请及审批的具体步骤如下：

1) 客户端使用右键菜单或扫描工具申请解密；
2) 控制台上有气泡提示，并在解密申请管理中可以查看到申请记录，状态为等待审批；
3) 双击申请记录，可查看申请信息和文件内容；
4) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；
5) 审批通过后，客户端在申请信息窗口进行解密。

离线审批：

客户端离线时，解密申请及审批的具体步骤如下：

1) 客户端使用右键菜单或扫描工具申请解密，并在申请信息菜单中生成申请文件；
2) 管理员拿到申请文件，在解密审批管理界面，选择右键菜单“**导入申请文件**”，选择申请文件导入；
3) 控制台上有气泡提示，并在解密申请管理中可以查看到申请记录，状态为等待审批；
4) 双击申请记录，可查看申请信息和文件内容；
5) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；
6) 在解密申请管理界面选中此条申请记录，选择右键菜单“**导出审批结果**”，并保存文件；
7) 把导出的审批结果文件发给客户端，在客户端申请信息中导入审批结果文件并解密。

快速审批

同时选中多个解密申请，选择右键菜单“**快速审批**”，若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮。

17.13 外发申请管理

外发申请管理和解密申请管理类似。

在线审批：

客户端在线时，外发申请及审批的具体步骤如下：

1) 客户端使用右键菜单或扫描工具申请外发；
2) 控制台上有气泡提示，并在外发申请管理中可以查看到申请记录，状态为等待审批；
3) 双击申请记录，可查看申请信息和文件内容。多层目录时，双击文件夹可以可以进入子级目录查看，点击 … 或者 可以返回上层目录；
4) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；
5) 审批通过后，客户端在申请信息窗口生成外发文档。

离线审批：

客户端离线时，外发申请及审批的具体步骤如下：

1) 客户端使用右键菜单或扫描工具申请外发，并在申请信息窗口中生成申请文件；
2) 管理员拿到申请文件，在外发审批管理界面，选择右键菜单“**导入申请文件**”，选择申请文件导入；
3) 控制台上有气泡提示，并在外发申请管理中可以查看到申请记录，状态为等待审批；
4) 双击申请记录，可查看申请信息和文件内容；
5) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；
6) 在外发申请管理界面选中此条申请记录，选择右键菜单“**导出审批结果**”，并保存文件；

7) 把导出的审批结果文件发给客户端，在客户端在申请信息窗口中导入审批结果文件，并生成外发文件。

快速审批

同时选中多个外发申请，选择右键菜单“**快速审批**”，若要批准，点击【批准】按钮，反之点【拒绝】按钮。

17.14 安全属性变更申请管理

安全属性变更申请管理与解密申请类似。

在线审批：

客户端在线时，安全属性变更申请及审批的具体步骤如下：

1) 客户端使用右键菜单或扫描工具申请变更安全属性；

2) 控制台上有气泡提示，并在安全属性变更申请管理中可以查看到申请记录，状态为等待审批；

3) 双击申请记录，可查看申请信息和文件内容；

4) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；

5) 审批通过后，客户端在申请信息窗口修改文档安全属性。

离线审批：

客户端离线时，安全属性变更申请及审批的具体步骤如下：

1) 客户端使用右键菜单或扫描工具申请变更安全属性，并在申请信息窗口中生成申请文件；

2) 管理员拿到申请文件，在安全属性变更申请管理界面，选择右键菜单“**导入申请文件**”，选择申请文件导入；

3) 控制台上有气泡提示，并在安全属性变更申请管理中可以查看到申请记录，状态为等待审批；

4) 双击申请记录，可查看申请信息和文件内容；

5) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；

6) 在安全属性变更申请管理界面选中此条申请记录，选择右键菜单“**导出审**

批结果”，并保存文件；

7) 把导出的审批结果文件发给客户端，在客户端在申请信息窗口中导入审批结果文件，并修改文档安全属性。

快速审批

同时选中多个安全属性变更申请，选择右键菜单“**快速审批**”，若要批准，点击【批准】按钮，反之点【拒绝】按钮。

17.15 临时离线申请管理

客户端短时间内出差，如几天之内便可以完成出差任务时，建议使用临时离线

临时离线申请管理默认查看所有临时离线申请信息。

在线审批：

客户端在线时，临时离线申请审批流程如下：

1) 客户端申请临时离线；

2) 控制台上有气泡提示，并在临时离线申请管理中可以查看到申请记录，状态为等待审批；

3) 双击申请记录，进入审批窗口，可查看客户端的申请理由及申请离线到期时间；如果管理员认为客户端申请的临时离线时间不合适，可通过修改申请离线到期时间进行调整；

4) 若要批准，点击【**批准**】按钮，在审批窗口中即生成授权码；在反之点【**拒绝**】按钮，拒绝时需要填入拒绝理由；

5) 审批通过后，客户端离线，从离线后一刻开始，在到期时间之前，客户端进入备用模式，执行在线加解密策略。

6) 客户端查看申请审批情况时，可在申请信息中查看。

离线审批

客户端离线时，无法申请临时离线，而由管理员在控制台创建申请。具体步骤如下：

1) 在临时离线审批页面，点击  创建申请按钮；

2) 选择离线计算机或计算机分组，点击【**确定**】;

3) 选择到期时间，点击【**批准**】;

4) 这时离线申请对话框关闭，临时离线申请管理窗口中自动增加一条已批准的记录;

5) 管理员双击该记录，再次打开离线申请对话框，获取授权码，以电话或其他形式告知离线客户端，客户端导入授权码后，即可进入备用模式，在管理员设定的到期时间之前，执行在线加解密策略;

17.16 审批权限委托

当管理员外出时，可将自身的审批权限，临时委托给信任的权限管理人代行审批管理，如果是系统管理员，还可以帮助其他管理员将权限委托给其他人。权限委托时，可设置授权时间区间与审批权限范围，预定时间到期，管理权限自动收回。

具有“**流程管理—审批权限委托**”权限的管理员才能将权限委托给其他管理员，具有“**加密功能管理权限**”的管理员才能接受委托。系统管理员还可以查看所有的委托情况。

权限委托

将委托权限给其他管理员的步骤如下：

1) 选择菜单栏“**申请管理**”进入管理主窗口，再选择菜单“**申请管理->加密申请管理->审批权限委托**”;

2) 点击  按钮切换至权限委托设置界面，点击  按钮，弹出审批权限委托设置窗口;

3) 在常规选项卡中，勾选“**启用委托**”，选择受委托的管理员、委托的有效起止时间，填写备注信息;

4) 切换到功能权限选项卡，选择要委托的权限，可以选择全部权限，也可以选择部分权限；完成之后点击【**确定**】按钮。

5) 此时“**申请管理->加密申请管理->审批权限委托->权限委托设置**”，可以查看委托权限的具体信息。

权限代委托

1) 拥有系统管理员权限，点击审批权限委托界面的按钮切换至“**查看所有委托情况**”界面，点击 按钮，弹出审批权限代委托设置窗口；

2) 在常规选项卡中，勾选“**启用委托**”，选择受委托的管理员、委托的有效起止时间，填写备注信息；

3) 切换到功能权限选项卡，选择要委托的权限，可以选择全部权限，也可以选择部分权限；完成之后点击【**确定**】按钮。

4) 此时“**申请管理->加密申请管理->审批权限委托->查看所有委托情况**”，可以查看委托权限的具体信息。

17.17 审批流程管理

多级审批功能，可以满足办公多级别审批流程的要求，保证申请得到各级别管理者复核和审查。多级审批中，负责各级别审批的角色均称为“**加密审批者**”。加密审批者其实就是具有加密管理功能权限的管理员。

具有“**查看加密审批流程**”以及“**设置加密审批流程**”权限的管理员登陆控制台，“**文档安全管理->流程管理->审批流程管理**”，进入审批流程管理界面，可对审批流程进行各项管理操作。

新建流程

点击新增按钮“”新建一条流程，新建流程设置了流程条件和流程环节。新生成的审批流程默认不用。勾选流程名称前的复选框即可启用流程。

说明 新建流程时，部分页面仅对指定的申请类型有效（对应页面有提示说明），当新建流程选择的申请类型不包含某种类型时，其仅生效的页面将直接不显示。

流程匹配原则

申请会按照审批流程列表中的各流程顺序，自上而下匹配，匹配到一条流程就不会再继续匹配。如果申请不能匹配到任何自定义的流程，则会匹配到默认流程，由拥有该类型审批权限的管理员或系统管理员进行审批。默认流程不能进行修改、移动、删除等操作。

一条申请匹配了某一流程后，会按顺序去到流程的每一个环节。每个环节都需要达到指定审核通过结果时，才会进入下一个环节。只有当前环节的审批人可以审批，其他环节的审批人不能进行审批。申请在经过所有环节批准通过的情况下才算是被批准了。

17.18 文档管理

控制台本地扫描

在文档安全管理窗口，选择菜单“**工具->本地扫描工具**”，可扫描控制台所在计算机的加密文件，并可以执行加密、解密、生成外发、修改文档属性等操作。

远程文档管理

在 IP-guard 控制台主窗口，在计算机栏选择一台计算机，选择右键菜单“**加密管理功能->远程加密文档管理**”，可以扫描指定客户端的加密文件，并可以远程直接执行加密、解密、生成外发、修改文档属性等操作。只能对在线的客户端进行操作。

17.19 备用服务器设置

控制台菜单“**文档安全管理**”->“**备用服务器管理**”选项，包括两个子项：“**设置**”和“**修改连接密码**”。

设置

点击“**设置**”，可进入备用服务器设置对话框中，进行备用服务器接入范围的设置。具体步骤如下：

1) 控制台菜单“**文档安全管理**”->“**备用服务器管理**”->“**设置**”，进入备用服务器设置窗口。

2) 设置备用服务器的 IP 允许范围，点击【**提交**】。如设置允许的 IP 范围 为：192.168.0.1-192.168.0.100，则在该 IP 地址段以外的备用服务器无法与主服务器关联。

在备用服务器设置对话框中，可看到当前主服务器上的所有备用服务器列表。

17.20 加密文档备份

用户可部署加密文备份服务器，将各个客户端中的加密文件统一以明文的方式备份到文档备份服务器上，即使客户端上的加密文件丢失或损坏，都能在服务器上找回来。

文档备份服务器使用步骤如下：

1) 双击运行安装程序进行安装文档备份服务器；

2) 在加密文档备份服务器的运行图标上点击右键，在右键菜单“**工具**”->“**选项**”，弹出服务器参数设置对话框，进行对应的参数设置，其中，服务器地址填入所要连接的 IP-guard 服务器地址；

3) 控制台“**工具**”->“**服务器管理**”->“**文档备份服务器管理**”，在列表中选中对应的文档备份服务器，点击【**授权**】。点击【**设置范围**】，弹出选择对象窗口，勾选要收集备份的计算机或计算机组，点击【**确定**】。点击【设置模式】，选择“**明文备份**”；

4) 计算机默认不启用加密文档自动备份任务。登录控制台“**文档安全管理**”->“**其他权限设置**”-> “**文档备份设置**”，文档备份设置可以启用或停止计算机的加密文档自动备份任务，并设置备份的条件。

5) 以上设置完成后，有备份策略的客户端，修改加密文档、把非加密文档加密，对应的加密文件均为进行备份。

   管理员可在加密文档备份服务器的运行图标上点击右键，在右键菜单“**工具**”->“**备份文档管理工具**”，可以查看各客户端机器的备份文档。

第十八章. 加密客户端

客户端启用加密功能后，在系统托盘处显示  图标。禁用加密授权并重启客户端后，系统托盘处的加密图标将会消失。

18.1 加密文档扫描工具

客户端系统托盘处，选择右键菜单“**扫描本地文件**”，可启动扫描工具。

在扫描工具选择扫描路径、文件类型、是否扫描子文件夹、是否仅扫描加密文件等条件，再点击“**扫描**”，可以扫描出本地的加密和非加密文件。加密文件的图标有个小锁标志。

在扫描结果中，选择一个或多个加密文件，使用右键菜单可执行加密、解密、申请解密、外发、申请外发、外发提取和修改文档属性等操作。

18.2 加密

在资源管理器中，选择一个非加密文件，右键菜单，选择“**文档加密系统**”->“**加密**”，可以把此文件加密，并设置此文件的文档安全属性。扫描工具中对非加密文件直接右键“**加密**”，亦可加密文件并指定默认安全属性。

18.3 解密

在资源管理器中，选择一个加密文件，右键菜单，选择“**文档加密系统**”->“**解密**”，就能对此加密文件进行解密。

扫描工具中对加密文件直接右键“**解密**”，亦可解密文件。

18.4 申请解密

没有解密权限的客户端，可以使用右键菜单或扫描工具，或者将加密文件拖拽

入解密申请浮动窗口，进行解密申请，填写申请理由并提交。客户端在线时，申请解密后控制台能马上收到通知并审批。审批通过后，可以在“**查看申请信息**”中进行解密。

客户端离线时，申请解密后，还需要在“**查看申请信息**”菜单中，导出申请文件，把申请文件发给管理员，管理员在控制台导入后进行审批。审批通过后，从管理员处拿到授权文件，在客户端导入授权文件，并在“**查看申请信息**”中进行解密。

18.5 只读打开

对于启用了只读加密授权的客户端，选择一个加密文件，选择右键菜单“**文档加密系统**”->“**只读打开**”，直接打开该文档进行查看，也可以通过右键菜单“**文档加密系统**”-> “**只读打开方式**”，选择相应的程序打开该文档进行查看，不能修改加密文档。

18.6 外发

有直接外发权限的客户端，可以使用右键菜单或扫描工具生成外发文档。

外发操作步骤：

1) 选择外发目标文件，点击右键，在右键菜单中选择“**外发**”；
2) 在弹出的创建外发文档窗口中，可查看到添加的文件信息。如还有需要添加的文件，可点击“**文件信息**”标签页上的添加文件按钮或添加文件夹按钮进行文件的添加操作（可添加加密文件，也可添加非加密文件）。
3) 确定目标文件后，切换到“**外发对象**”标签页，选择外发对象；可以在右上角的查询框中输入查询条件，快速定位到指定的外发对象，查询条件支持模糊查询。
4) 确定外发对象后，切换到“**外发配置**”标签页，设定外发文档的操作权限。其中，外发配置可以点击按钮在已有的客户端外发模板中选择，手动设置的配置可以点击按钮保存成客户端外发模板。
5) 所有信息选择填写完毕之后，点击【**创建**】，选择外发方式以及保存位置，点击【**确定**】即可完成外发

18.7 申请外发

没有直接外发权限的客户端，可以使用右键菜单或扫描工具，选择申请外发。申请外发时需填写申请理由，并指定发外对象和文档的使用权限。

客户端在线时，申请外发后控制台能马上收到通知并审批。审批通过后，可以在“**查看申请信息**”中进行生成外发。

客户端离线时，申请外发后，还需要在“**查看申请信息**”菜单中，导出申请文件，把申请文件发给管理员，管理员在控制台导入后进行审批。审批通过后，从管理员处拿到授权文件，在客户端的“**查看申请信息**”中导入授权文件，并在“**查看申请信息**”中生成外发文件。

18.8 修改加密文档安全属性

文档的安全属性，包含两个权限，即设置权限和访问权限。

设置权限，是指能修改文档安全属性的权限。只能有一个安全区域和级别。

访问权限，是指能打开、编辑此加密文档的权限。可以有多个安全区域和级别。

有直接修改加密文档安全属性权限的客户端，可以在资源管理器的文件属性加密选项卡中，和扫描工具的右键菜单“**修改文件安全属性**”中，修改加密文档的安全属性。

18.9 申请修改加密文档安全属性

具有申请修改加密文档安全属性权限的客户端，可以使用右键菜单或扫描工具申请变更文档属性。

操作步骤：

1) 选择目标文件，点击右键，在右键菜单中选择“**申请变更安全属性**”；
2) 在弹出的申请窗口中，可查看到添加的文件信息。如还有需要添加的文件，可点击“**文件信息**”标签页上的  添加文件按钮或  添加文件夹按钮进行文件的添加操作。

3) 确定目标文件后，切换到“**安全区域**”标签页，设置变更后的文档安全属性。

4) 随后切换至“**申请理由**”标签页，填写申请理由。

5) 所有信息设置填写完毕之后，点击【**申请**】，完成操作。

客户端在线时，申请变更文档安全属性后，控制台能马上收到通知并审批。审批通过后，可以在“**查看申请信息**”中进行安全属性修改。

客户端离线时，申请变更文档安全属性后，还需要在“**查看申请信息**”菜单中，导出申请文件，把申请文件发给管理员，管理员在控制台导入后进行审批。审批通过后，从管理员处拿到授权文件，在客户端的“**查看申请信息**”中导入授权文件，并在“**查看申请信息**”中进行安全属性修改。

18.10 申请临时离线

客户端短时间内出差，如几天之内便可以完成出差任务时，建议使用临时离线申请功能：

1) 在客户端系统托盘，选择右键菜单“**临时离线**”->“**申请**”;

2) 在弹出的临时离线策略时间信息设置对话框中，填写开始时间，离线到期时间，并输入理由，点击【**确定**】。

3) 管理员收到申请信息并审批后，客户端离线，即可进入备用模式，依照在线加解密策略执行加解密操作。

如果客户端还未申请临时离线，便已离开公司的网络环境，则需要以邮件或电话等形式通知管理员，让管理员生成临时授权码返回给客户端导入。

导入方法：在客户端系统托盘，选择右键菜单“**临时离线**”->“**导入**”，输入临时离线授权码，点击【**确定**】即可。

说明 申请时如果不勾选“**开始时间**”，则临时离线申请通过后，客户端一离线立刻进入临时离线状态。若申请时勾选“**开始时间**”并设置了具体的时间,则客户端离线了也需设置的时间点才会进入临时离线状态。

18.11 查看申请信息

在客户端系统托盘，选择右键菜单“**查看申请情况**”，可查看解密、外发和临时离线的申请和审批情况。

解密申请

双击申请记录，可查看申请的详细信息。并可执行解密、生成离线申请文件、取消申请等操作。

已批准的申请，可点击【**解密**】按钮进行解密，可选择解密到原文件，也可以到其他目录。

离线时提交的解密申请，点击【**生成离线申请文件**】按钮，生成申请文件，发给控制台进行审批。

外发申请

双击申请记录，可查看申请的详细信息。并可执行创建外发、生成离线申请文件、取消申请等操作。

已批准的申请，可点击【**创建外发**】按钮生成外发文件，可选择生成目录。

离线时提交的外发申请，点击【**生成离线申请文件**】按钮，生成申请文件，发给控制台进行审批。

安全属性变更申请

双击申请记录，可查看申请的详细信息。并可执行安全属性修改、生成离线申请文件、取消申请等操作。

已批准的申请，可点击【**修改安全属性**】按钮修改文件的安全属性。

离线时提交的外发申请，点击【**生成离线申请文件**】按钮，生成申请文件，发给控制台进行审批。

临时离线申请

双击申请记录，可查看申请的详细信息，包括申请时间、申请的离线到期时间、审批管理员、审批时间等信息。

客户端在离线状态下，所发起的临时离线申请，必须在重新连接上服务器时，管理员才可进行审批。因此，在客户端离线时，如需要使用临时离线功能，请

已电话或邮件等联系方式通知管理员，由管理员生成授权码发给客户端进行导入。

18.12 加密系统信息

在客户端系统托盘，选择右键菜单“**加密系统信息**”，可查看当前授权进程、当前安全对象、加密系统信息。

18.13 文档安全属性

在资源管理器的文件属性加密选项卡中，和扫描工具的右键菜单“**修改文件安全属性**”中，可以查看和修改加密文档的安全属性。

设置权限，是指能修改文档安全属性的权限。只能有一个安全区域和级别。

访问权限，是指能打开、编辑此加密文档的权限。可以有多个安全区域和级别。

18.14 离线授权登陆

客户端在离线状态下，其离线加解密权限需要登入授权后才能正常使用。在客户端系统托盘，选择右键菜单“离线授权登入”，输入安全密码后点击确定，即可登入离线授权模式。

18.15 导入授权文件

在系统托盘的客户端图标处，选择右键菜单“**导入授权文件**”，选择一个由控制台生成的离线授权文件导入，即可获得离线权限。

也可以导入备用服务器生成的紧急授权文件，即可获得紧急授权。

18.16 加密系统的登入与注销

有允许注销加密系统权限的客户端，在系统托盘的客户端图标上，选择右键菜单“**注销加密系统**”，注销后，所有加密功能不可使用，无法打开加密文件。

在系统托盘的客户端图标上，选择右键菜单“**登入加密系统**”，登入时需要输入安全密码，成功登入后加密功能正常使用。

18.17 参数设置

在系统托盘的客户端图标处，选择右键菜单“**选项**”，可设定安全密码、加密系统的登入、系统日志存储时间、是否显示解密申请浮动窗口以及申请管理设置。

18.17.1 安全密码设置

设置安全密码

安全密码初始状态为空。点击“选项”对话框中的“安全密码输入设置”，填入原密码及新密码进行修改。

清除安全密码

用户如果忘记了自己的安全密码，可以在管理员的协助下，使用客户端工具来清除客户端的安全密码。具体操作步骤：

1) 在客户端机器按住“**Ctrl+Alt+Shift**”，然后依次输入“**oculara**t”字符串，打开客户端工具；
2) 选择“**清除加密安全密码**”，点击【**生成操作码**】按钮；
3) 会弹出一个“**检验操作码**”对话框，请把原始操作码报告给管理员；
4) 管理员在控制台“**工具-客户端工具-确认码生成器**”输入客户端的操作码，会解析出该客户端的操作以及相应的客户端信息；
5) 管理员确认后点击【**生成确认码**】；
6) 管理员将确认码告诉客户端，在客户端工具中输入正确的确认码，即可清

除安全密码。

18.17.2 申请管理设置

默认情况下，解密申请和安全属性变更申请审批通过之后，需要手动去完成解密和安全属性变更操作。

可设置自动完成安全属性变更和自动完成解密申请，则审批通过之后自动完成对应的操作。

18.18 代理管理员

管理员设置某一客户端可以登录代理管理员后，则可在该客户端所在计算机上登录代理控制台，进行审批解密申请、外发申请、临时离线申请。

18.18.1 登录

有允许登录代理管理员权限的客户端，可在系统托盘的客户端图标上，选择右键菜单“**登录代理管理员**”，并输入管理员帐户和密码，即可登录代理控制台。代理控制台支持自动启动。

登录代理控制台时，勾选“**自动启动**”，则下次客户端启动并且连上服务器后，代理控制台自动启动，弹出登录对话框。也可在代理控制台选择菜单“**申请管理->选项**”进行设置，在“**基本设置->登录设置**”中勾选“**连上服务器后自动启动**”。

18.18.2 审批管理

代理控制台的审批管理功能和控制台一样，可以查看解密/外发/临时离线申请/安全属性变更申请，可以审批申请、导入申请文件和导出审批文件，可以查看审批权限委托情况、进行权限委托。

18.19 强制更新策略

当 lisence 数量多时，可能会出现策略下发变慢的情况，此时客户端机器可以在系统托盘的客户端图标处，选择右键菜单“**强制更新策略**”，强制更新服务器上最新的策略，策略更新成功后会有相应的气泡提示。

第十九章. 外发查看器

外发查看器是安装在企业外的计算机上，用来查看外发文档的工具。

19.1 安装

运行安装程序，选择安装目录，直到程序安装完毕。

19.2 授权

授权外发查看器

具体步骤：

1) 运行安装目录下的 OEAViewer.exe，“开始”->“所有程序”->“**IP-guard OeaViewer**”->“**IP-guard 外发加密文档查看器**”启动外发文档查看器。

2) 点击外发查看器界面右下角的【**设置**】，进入外发查看器设置窗口。

3) 点击【加载】，导入通用授权文件，并填写公司信息。

4) 在授权列表中可看到此外发查看器获得了哪些公司的授权，和授权有效期。

识别码获取

点击外发查看器界面右下角的【**设置**】，进入外发查看器设置窗口；在授权管理页面中找到识别码，在 USBKey 管理页面找到外发 USBKey 的识别码，将识别码发给管理员便可进行计算机或者外发 USBKey 绑定授权。

19.3 查看外发文件

外发文档后缀名为.oeax 时，打开有两种方式：

1）双击外发文档，会启动外发文档查看器，在文件列表中选择文件，双击打开文档，或是点击“打开方式”按钮选择应用程序打开文档。

2) 先启动外发查看器文件，将外发文档拖入外发查看器中，在文件列表中双击打开，或是选择打开方式打开想要查看的外发文档。

外发文档后缀名为.exe。双击该文件，会启动外发查看器，接下来的查看方式同.oeax 格式。

第二十章. 加密备用服务器

备用服务器用于在主服务器运行出错，如主服务器被停止时，保证加密客户端的在线加解密策略权限正常。

20.1 安装与运行

备用服务器可与主服务器装在同一台机器上，也可以装在不同机器上。

运行后，在系统托盘处显示运行图标。

注意 备用服务器应该与主服务器一样长期运行，而不是等主服务器出问题才启动。

20.2 备用服务器设置

备用服务器安装成功后，默认不与任何主服务器关联。在为主服务器部署备用服务器时，必须先在控制台上设置备用服务器的接入范围及连接密码。

在控制台上设定了备用服务器的接入范围及连接密码后，需继续在备用服务器上进行对应的参数设置。

具体步骤如下：

1) 在备用服务器托盘图标上点击右键“**工具**”->“**设置连接参数**”，选择“**服务器连接**”选项卡；

2) 填入主服务器的 IP 地址、连接密码，点击【**确定**】。

根据以上步骤依次设置，备用服务器即可连接上对应的主服务器，成功获取备用授权。

20.3 查看客户端状态

备用服务器已连接上主服务器，且已同步客户端及计算机组的信息，则在备用

服务器的右键菜单“**工具**”->“**客户端状态**”，可以查看到当前主服务器上所有的客户端信息，包括客户端名称和客户端 IP。

如果客户端曾经连接上备份服务器，在客户端连接状态信息中，能查看到客户端与备用服务器连接的最新时间。

20.4 查看连接列表

当主服务器出现异常时，已获取到备用授权的备用服务器即进入备用模式，主服务器上的客户端也进入到备用模式中，连接到备用服务器上。

此时，在备用服务器托盘图标上点击右键“**工具**”->“**连接列表**”中，可查看当前连接到备用服务器的客户端信息。

注意 若主服务器停止前，备用服务器与主服务器断开连接（备用服务器被人为停止或网络不通所致）时间超过 30 分钟，则默认该备用服务器未获得正确的备用授权，客户端不会连接到该备用服务器上。

第二十一章. 文档云备份服务器

文档云备份服务器，可备份指定类型的文档，防止重要数据丢失。管理员可通过 WEB 管理界面进行数据的查看与管理，也可以对用户进行权限分级管理，让用户也可登录文档云备份服务器查看权限内的备份数据。

21.1 安装与部署

文档云备份服务器具体安装部署步骤如下：

1) 双击运行安装程序进行安装文档备份服务器；

2) 在浏览器中输入服务器地址，弹出初始化界面填入信息完成初始化，重启文档云备份服务器。

3) 登录云备份服务器 WEB 管理界面，“**设置**”->“**参数设置**”中设置备份相关参数

4) 控制台“**工具**”->“**服务器管理**”->“**文档备份服务器管理**”，在列表中选中对应的文档云备份服务器，点击【授权】。点击【设置范围】，弹出选择对象窗口，勾选要收集备份的计算机或计算机组，点击【确定】，则选定的计算机的文档将会备份到此文档云备份服务器。

5) 控制台“**工具**”->“**服务器管理**”->“**组织架构同步**”中进行过域组织架构同步，在客户端机器上首次登录的域用户将会自动成为该台计算机的关联用户。也可在控制台“**工具**”->“**服务器管理**”->“**用户系统管理**”->“**关联信息**”中，手动为客户端设置关联用户

6) 控制台“**高级**”->“**文档云备份**”，设置策略启用计算机的文档备份，并设置备份的条件

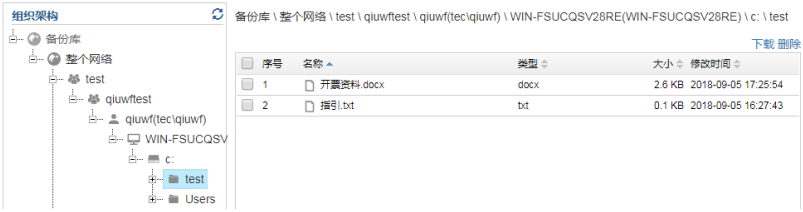
7) 以上设置完成后，有备份策略的客户端，重命名、修改文档内容、复制到覆盖、拖拽到覆盖；新增文档包括：创建文件、另存为、复制到、拖拽到、移动到等修改文档的操作均为进行备份。

21.2 WEB 管理端

通过浏览器登录文档云备份服务器后，进入 WEB 管理端界面，查看备份、管理用户和设置参数。

备份浏览

在左侧的组织架构树中选择对应的用户，右侧视图可以查看各用户的备份文档，可查看文件详细信息、也可下载、删除文件。



角色管理

角色管理用于分角色管理和设置域用户的权限。点击上方视图中的✚，下方视图的各设置项变为可编辑状态，设置好各项参数后，点击即可保存并添加成功。

当用户被分配多个角色时，相同管理范围内若出现用户权限冲突，则按以下优先级执行：禁止>允许>不设置。

管理员黑白名单设置

管理员黑白名单设置，用于限制管理员登录文档云备份服务器， 点击进行设置，勾选对应的设置项，并输入管理员名称，完后点击保存。

参数设置

“设置”->“参数设置”中设置各项参数，可点击进行编辑，编辑完后点击**“保存”**按钮保存，可设置参数有授权设置、域账号密码验证设置、组织架构同步设置、备份存储设置、端口映射设置和域名。

21.3 WEB 审计端

具有“**文档云备份服务器**”权限的审计管理员，可以登录文档云备份服务器查看审计日志。

审计日志

审计管理员可以查看审计日志，审计日志包括文档云备份服务器登录情况，管理员的操作日志等。

审计管理员可以通过时间范围、操作类型、文件名称来查询需要的日志信息。

审计员黑白名单设置

审计员黑白名单设置，用于限制审计管理员登录文档云备份服务器，点击进行设置，勾选对应的设置项，并输入审计管理员名称，完后点击保存。

21.4 文档云备份扫描工具

拥有“**功能权限-文档云备份服务器-扫描任务管理**”权限的管理员，登录控制台，选择菜单栏“**工具-文档云备份扫描任务**”，进行全盘扫描备份任务的设置。

设置文档云备份扫描任务步骤：

1) 点击右上角的添加按钮，弹出创建任务的对话框；
2) 在“常规”选项卡中，对常规项目进行设置；
3) 切换至“高级”选项卡中，对高级项目进行设置；
4) 设置完成后，点击“确定”按钮，文档云备份扫描任务创建成功。

21.5 文档云备份操作日志

控制台“**日志**”->“**文档云备份操作**”，可查看文档备份操作日志。

第二十二章. 报表系统

报表系统提供各项记录日志的查询统计，支持多种组合的统计条件，以图表结合的方式呈现各项统计结果，帮助管理员全方位掌握各种计算机操作使用情况，为策略部署提供充足的依据，同时对策略的执行情况进行实时追踪。

22.1 报表控制台

登录控制台，选择菜单“**工具->登录报表系统**”，启动报表控制台。登录后报表控制台，数据显示区默认进入首页，首页显示整个网络特定日志的统计信息。

统计的数据包括：打印页数，发件邮件大小，写入移动磁盘文件大小，上传文件大小。统计的时间区间为：当日 00:00 至当前界面右上角显示的统计时间。首页同时还会显示最新生成的 10 个报表信息。

报表控制台的界面如下：

22.2 预设报表和查询

系统为支持的报表类型预设了周期报表和查询，分别包含对应的统计表和趋势表，并按报表类型分组，统计表预设为标准月表，趋势报表预设为标准季度表。

报表系统支持以下报表类型：

报表类型	说明
打印报表	打印日志统计；
即时通讯报表	即时通讯日志统计；
上网浏览报表	上网浏览日志统计；
文档操作报表	文档操作日志统计；
移动存储报表	移动存储日志统计；
应用程序报表	应用程序日志统计；
邮件报表	邮件日志统计；
策略日志报表	策略日志统计；
加密文档操作报表	加密文档操作日志统计；
征兆报表	征兆事件日志统计，即符合征兆条件的事件日志统计； 征兆条件可在“**报表->征兆条件设置**”中设置；
综合报表	综合日志统计，包括以上除征兆报表外其他所有日志的综合统计。


说明

1.预设的报表不包含策略日志报表；

2.预设的报表、分组等可以进行修改、删除；

3.综合报表仅有统计表，没有趋势表。

22.3 模板管理

模板包含条件设置和统计设置。点击“**报表->模板管理**”，管理员可以预定义报表模板。系统默认定义了每种模块的统计表和趋势表（综合报表只有统计表）模板。

系统预定义的模板只能查看，不可修改和删除。

22.4 周期管理

周期管理包含报表数据的时间范围、报表生成时间，以及是否进行预统计的设置。

点击“**报表->周期管理**”，管理员可以自定义周期报表的周期。

默认预设标准的年度、季度、月、周、日周期。系统默认周期可以修改，但不可删除。选中任一周期，点击  按钮可恢复为对应周期类型的标准设置。

22.5 征兆管理

征兆即为预先设置的指标，根据指定时间内对各项操作的限制来定义征兆级别，征兆级别分为严重、重要、一般。以打印操作为例，征兆可设置一天内打印超过 100 页为严重级别，打印超过 50 页为重要级别，打印超过 20 页为为一般级别。

点击“**报表->征兆条件管理**”，管理员可以预定义征兆报表的征兆条件。系统默认定义的征兆条件可以修改，可以删除。

22.6 周期报表

周期报表位于导航栏的“**报表**”节点处。周期报表中的预定义报表，统计报表都是标准月表，趋势报表则为标准的季度表。预定义报表不能满足要求时，可以修改预定义报表，也可以新建自定义报表。

22.6.1 创建报表

创建周期报表有三种方式：从模板创建、从报表创建、从查询条件创建。

从模板创建

从模板创建周期报表，创建时可选择模板，创建的报表会沿用所选模板的条件设置和统计设置，也可自行修改。

以创建打印报表统计表为例说明

1) 选择导航栏处“**报表**”，右键菜单中选择“**新建报表->从模板创建**”，弹出创建报表界面；

2) 选择“**打印报表模板->标准打印统计表**”，也可选择其他自定义打印统计表模板，点击【**下一步**】；

3) 条件设置，包括通用的计算机范围、用户范围，以及高级条件设置。默认显示所选模板的条件设置，可修改，设置完成后，点击【**下一步**】；

4) 统计设置，包括统计类型选择和具体统计设置，默认显示所选模板的条件设置，可修改。设置完成后，点击【**下一步**】；

5) 设置生成报表的周期，点开下拉菜单会显示所有已有周期，选定周期后，如果想要调整部分数值，可以点击右侧的【**修改设置**】进行调整。设置完成后，点击【**下一步**】；

6) 设置报表的一些基本信息，包括报表名称，报表位置，以及备注。设置完成后，点击【**完成**】；

说明 1.从模板生成报表，默认使用所选模板的条件设置和统计设置，可以修改，修改仅对当前报表生效，所选模板不会改动。

2.所有方式生成报表时，选择已有周期后，对选定周期的部分数值进行的修改，也仅对当前报表生效，所选周期不会改动。

从报表创建

从报表创建周期报表，创建时可选择已有周期报表，创建的报表会沿用所选周期报表的条件设置、统计设置、周期设置，以及显示设置，也可自行修改。

选择导航栏处“**报表**”，右键菜单中选择“**新建报表->从报表创建**”，创建步骤类似于从模板创建。

从查询条件创建

从查询条件创建周期报表，创建时可选择已有查询，创建的报表会沿用所选查询的条件设置、统计设置以及显示设置，但也可自行修改。

选择导航栏处“**报表**”，右键菜单中选择“**新建报表->从查询条件创建**”，创建步骤类似于从模板创建。

22.6.2 查看报表

在导航栏出的“**报表**”节点下选中一个报表，右边的数据显示区即可查看报表数据。

22.6.3 修改报表

报表创建后，若想修改报表的设置，则可选中目标报表，右键菜单中选择“**修改报表**”进行修改。

选中报表，右键菜单中还可进行重命名、删除、移动操作。

22.7 查询

22.7.1 创建查询

以创建打印查询为例说明创建查询步骤：

1) 选择导航栏处“**查询**”，右键菜单中选择“**新建查询**”，弹出创建查询界面；
2) 选择“**打印报表模板->标准打印统计表**”，也可选择其他自定义打印统计表模板，点击【**确定**】；

查询新建成功后，会沿用所选模板的条件设置和统计设置。右键菜单中可进行重命名、删除、移动操作。

22.7.2 查询

在导航栏的“**查询**”出选中一个查询，右边的数据显示区上方，可以修改查询条件和统计类型。修改后点击右上方的【**保存**】，下次再选中该查询时会默认出现本次保存的查询条件和统计类型。

选择好查询条件和统计类型后，点击【**统计**】按钮，开始进行统计。统计完成显示统计图和统计表。双击统计表中的一条数据，可查看具体的日志明细内容。选中数据列头，右键可增加或减少显示的数据列。

22.8 历史报表

22.8.1 生成历史报表

历史报表，即已过去时间范围的报表。周期报表默认从创建报表之后才开始定期生成报表，过去的历史报表不会自动生成。生成历史报表功能可以生成过去时间的报表。

菜单“**报表->生成历史报表**”，选择数据的起始时间和结束时间，选择报表，选择是否“**重新生成已生成过的报表**”，点击“**保存**”。

不勾选“**重新生成已生成过的报表**”，则只对未生成过报表的周期生成报表；勾选“**重新生成已生成过的报表**”，则过去已经生成过报表的周期，也再重新生成报表。

22.8.2 历史任务管理

设置了生成历史报表后，可以在“**报表->历史任务管理**”中对已有生成历史报表任务进行管理。

点击按钮可新建历史报表任务，建立完后即刻执行生成报表任务，状态为“**进行中**”。

22.9 邮件报告

周期报表可以通过邮件服务器，发送到指定的邮箱，管理员可以通过邮件及时地了解各项报表的最新结果。

使用邮件报告功能前，系统管理员必须在控制台“**工具->选项->邮件报告服务器设置**”中配置邮件报告服务器。

配置邮件报告服务器之后，才可以进行邮件报告设置。在报表控制台，菜单“**报表->邮件报告**”，管理员可以查看、添加和修改邮件报告设置。

点击  按钮，添加邮件报告配置，选择需要邮件发送的周期报表，以及设置好其他参数即可。

22.10 数据中心

菜单“**报表->数据中心**”，可查看系统生成的报表，包括周期报表每一次的统计报表、查询中点击“**保存结果**”生成的报表。

技 术 支 持

感谢您对我们产品的支持和信赖，为客户提供优质的技术支持是我们的承诺。如果您有任何本手册无法解决的技术问题请发电子邮件到我们的技术支持部门，我们将尽快回答您的问题：

techsupport@ip-guard.net

您也可以直接致电我们垂询：

电话（广州）：+86-20-86001438

传真（广州）：+86-20-86001438-807

您的意见和建议对我们很重要，我们会根据您的建议对我们的产品不断地进行改进。