版 权 声 明

版权所有

请注意

溢信科技有限公司对本手册内容不做任何担保。溢信科技有限公司对于其中所含的错误，或遵照本手册资讯操作所引起必然或偶然之错误所造成的损害不负赔偿责任。

对于本手册的内容，溢信科技有限公司拥有最终的解释权。

2020 年 02 月　　更新至版本 4.35.903.0

目　录

第一章. 简介

1.1 前言

日新月异的信息科技，既给企业的发展带来了前所未有的便利，也给企业的信息维护及管理带来了风险和挑战：

信息数据安全如何保障

由普华永道与 CIO、CSO 举办，130 个国家和地区、7200 多名管理人员参与的全球信息安全调查显示，企业信息安全要“对症下药”，首先必须考虑数据的安全防护。56%的受访者表示自己的企业缺乏数据丢失防护能力。而接近半数的中国受访者表示，数据丢失保护的同时，没有实行数据访问授权控制的措施。

在今天，企业的信息和数据大多以为电子文档的形式进行存储和传递。从设计图纸到客户信息，从财务数据到无纸化公文，电子文档大大加快了信息的流动与共享，加速了组织的业务流程。但是，电子文档本身所具有的易获取、易复制、易传播的开放性特征，以及发达的互联网应用，随处可见的移动存储设备，都是电子文档安全防护过程中不可回避的难题。

系统应用效率难以评估和控制

最近公布的一项调查结果表明，在工作中使用 MSN、QQ 等聊天的人数高达 89.2%，网页浏览中新闻网页占 65.9%居于首位。一个月薪 2000 元的员工，每天“隐性旷工”2 小时，每年为企业带来的直接损失高达 6000 元。一个拥有 50 人的企业仅此一项每年将损失 30 万。并且滥用网络和系统资源还可能将暗藏于互联网的安全隐患带入企业网络内，威胁系统安全。

系统维护及资产管理繁琐

Gartner 及 Forrester Research 的研究指出，IT 部门接近一半的工作时间用于为计算机安装及升级软件，IT 人员为 PC 做简单的日常维护工作占其总工作量的 70-80%，大大增加计算机网络的综合管理成本。如果问题没有得到及时有效的处理，也会极大影响企业的业务连续性。

IP-guard 正是一个为企业解决上述问题的有力工具。IP-guard 运用系统管理思

想，采用功能模块式设计，充分利用行为审计，分级授权，访问控制、集中管理和文档透明加解密等技术手段，为企业提供信息安全、应用效率和系统管理的全面解决方案。

其中，IP-guard 文档透明加解密模块，采用多种先进技术保证文档的完整性和可用性；同时，高速缓冲技术的加入也使其对系统性能的损耗微乎其微。其高安全性、高稳定性、高可用性的特点，适合各种规模的商业企业、政府机构、事业单位、科研院所等保护其机密信息。

1.2 功能介绍

IP-guard 基于系统管理思想和安全实践经验，全面考虑可能造成信息破坏及外泄的各个方面，保护企业信息不被人为外泄、非法盗取、恶意篡改，帮助企业对信息安全进行系统规划及管理。
IP-guard 通过灵活有力的管理，在保持企业活力的前提下规范终端行为，提升企业执行力；管理人员通过单一控制台随时了解各台计算机运行状态，并进行系统安全管理及资产管理。

IP-guard 的主要功能包括：

应用程序管控

记录应用程序使用的日志；
统计应用程序使用时间和百分比；
控制应用程序的运行。

网页浏览管控

记录浏览网页的网址和标题；
统计网页浏览的时间和百分比；
控制访问指定的网站或网页。

文档操作管控

记录所有文档的操作信息，包括不同类型存储设备以及各种文档操作；
记录其他计算机对本机共享目录的删除和修改操作；
可设定灵活的多种操作权限，控制文档的读取，修改和删除操作；

重要文档的复制和删除操作，可对文档进行备份。

打印内容管控

记录所有打印任务的日志；
完整记录文档打印映像；
控制打印操作。

设备管控

控制各种计算机设备的使用；
对任何新增加的设备进行控制。

网络控制

根据客户端类别以及网络地址和端口的类别进行网络通讯控制；
检测网络内的非法计算机，阻止非法计算机接入网络。

网络流量管控

记录网络通讯流量，并按照不同的口径进行统计；
根据不同的地址和端口范围，在不同时间段内实现流量控制。

屏幕监控

实时查看客户端的屏幕快照；
记录客户端的历史屏幕记录，根据不用的应用程序采用不同的记录频率；
可将屏幕历史转换为通用视频文件进行播放。

邮件管控

记录邮件收发的日志以及邮件的完整内容和附件的；
根据策略控制邮件的发送。

即时通讯控制

完整记录流行的即时通讯工具的对话时间，联系人和对话内容；
控制通过即时通讯工具向外发送文档；
对向外发送的文档进行备份。

资产管理

自动扫描每台终端的软硬件资产信息，详尽记录资产变更情况；
可自定义资产属性和类别对软硬件资产和非 IT 资产进行管理；

自动扫描微软产品补丁安装情况，对补丁进行自动分发和安装；
自动扫描客户端的安全漏洞，提供分析报告和解决方案；
自动部署和安装软件、指定程序或派送文档。

远程维护

实时查看客户端的运行信息，可执行远程操作；
远程连接到客户端桌面，进行远程协助；
支持进行远程文件传送。

移动存储控制

记录移动存储设备在网络内的使用，设定不同的访问权限，控制移动存储读取；
对移动存储设备中的文档进行自动加解密，在未经授权的计算机上无法读取。

文档透明加解密

重要文档自动强制加密；
设定加密文档的截屏、打印、复制/粘贴、拖拽、邮件发送等操作权限；
根据企业部门分级设定文档使用的分级授权管理权限；
解密外发申请审计；
离线权限控制、外发文档权限控制；
加密文档操作审计与备份。

第二章. 安装和部署

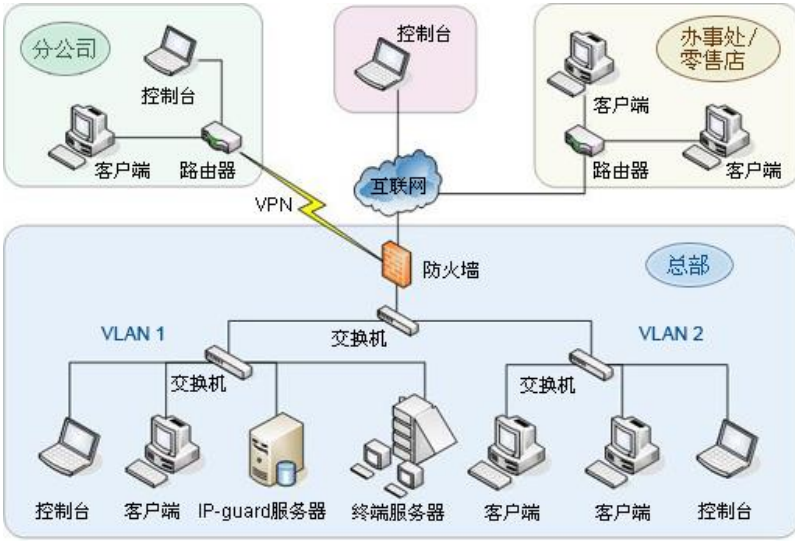
2.1 基本运行框架

IP-guard 基本系统由三个模块组成：客户端模块、服务器模块和控制台模块，用户可以根据管理的需要将它们安装在网络中的计算机上。

客户端模块用于收集数据和执行系统管理策略，安装在每台需要被管理的计算机上；
服务器模块用于存储系统数据和管理规则策略，一般安装在性能较高、存储容量较大的计算机上；
控制台模块用于查看系统数据、设定管理策略和进行实时维护，一般安装在企业相关管理人员的计算机上，也可以和服务器模块安装在同一台计算机上。

基本框架

系统的基本框架如下图所示：

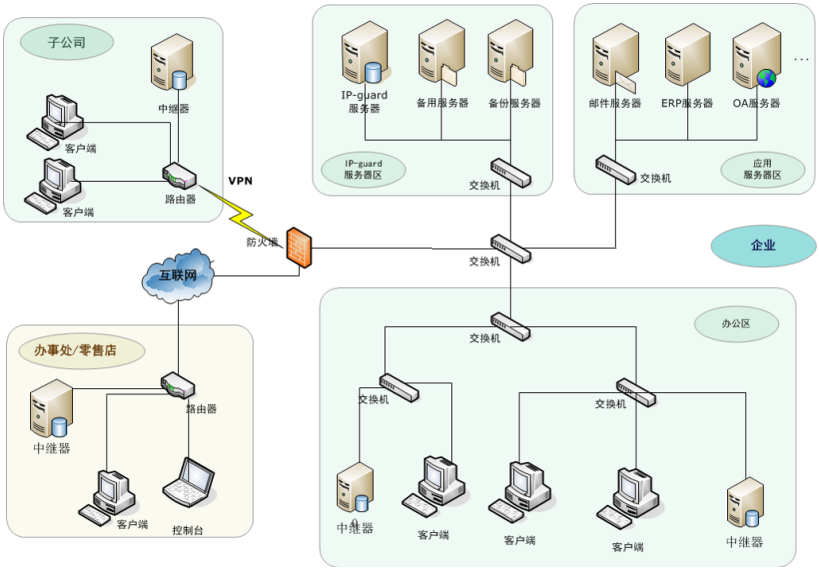


IP-guard 基于 TCP/IP 协议的网络架构，可以灵活地从本地网络扩展到远程网络和异地网络。服务器通过虚拟专用网（VPN）或互联网连接远程的计算机，实现对大规模复杂网络的集中管理。控制台也可以通过互联网连接异地的服务器，实现对分支机构的远程监控。

中继器框架

如果网络更大更复杂，可在基本系统的基础上，部署中继器框架。在各个子网络部署中继器，由中继器接管客户端，中继器连接主服务器，保证客户端之间与主服务器正常通讯，各项策略能正常下发，各种日志也能正常上传至服务器。部署多台中继器可实现扩展主服务器的处理能力，让系统能更好的应用于大规模跨地域的网络环境。

系统的中继器框架如下图所示：



服务器模块的基本功能包括：

管理所有客户端计算机，并向其传递相关的规则和指令
收集客户端采集的数据并保存
提供方便灵活的记录管理、查看、归档、搜索等功能

中继器模块的基本功能包括：

连接主服务器并获得授权，将主服务器的相关规则和指令传递至其所连接的客户端
收集客户端数据并上传至主服务器

控制台模块的基本功能包括：

查看和审计客户端的数据
数据统计，分析和导出
对客户端计算机实时监控和系统维护
设置监控规则和管理策略

客户端模块的基本功能包括：

执行系统设定的各种管理策略
采集客户端运行的各项数据
定时将采集的数据传送到服务器
根据控制台发出的指令进行监控操作

2.2 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
中继器模块	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
WEB 服务器模块	操作系统 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 / 1GB 内存 / 20GB 可用硬盘空间 建议配置 Pentium4 双核或四核 / 2GB 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）"。

2.3 安装和部署服务器和控制台

2.3.1 安装数据库

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。

如果使用免费的数据库时，建议使用 SQL Server 2008 R2 Express，因为它的容量限制要比 MSDE 大，同时也有自带的管理工具界面，可以比较方便地进行数据库维护。

注意　MSDE 的数据库容量有 2G 的限制，2008 R2 Express 容量有 10G 的限制，而且对服务器的性能也会有一定的限制，所以如果数据量比较大，建议尽量使用 SQL Server 2000 或 2005 标准版（或以上版本）数据库。

安装 SQL Server 2000 请确认安装 SP4 补丁，安装 SQL Server 2005 请确认安装 SP1 补丁。如果导致服务器无法启动，请先在系统的"**计算机管理->事件查看器->应用程序日志**"查看是否属于 SQL Server 版本问题。

SQL Server 2008 R2 Express 的安装

我们推荐安装“SQL 2008 R2 Expres”版本。

在安装 SQL 2008 R2 Express 前，操作系统需要先安装：
1. Windows Installer 4.5
2. .NET Framework 3.5
3. Windows PowerShell 1.0

在安装光盘上，已经包含有 Windows Install 4.5，.Net Framework 3.5，Windows PowerShell 1.0 和 SQL Server 2008 R2 Express 的安装程序。

SQL Server 2008 R2 Express 安装步骤：

1) 运行 SQL Server 2008 R2 Express 的安装程序，进入 SQL 安装中心；
2) 在“安装”步骤中，选择“全新安装或向现有安装添加功能”，等待处理后接受用户许可条款。并点击【下一步】
3) 安装 SQL Server 之前需要安装一些组件，单击【安装】按钮安装这些内容，安装成功后点击【下一步】
4) 在功能选择中，按照默认，点击【下一步】;
5) 在实例配置中，请选择默认实例，如果选择其他实例，会导致服务器不能正常启动。其余设置默认即可，点击【下一步】；
6) 在磁盘空间要求中，点击【下一步】；
7) 在服务器配置中，选择 SQL Serer Database Engine 的帐户名为“NT AUTHORITY\SYSTEM”，点击【下一步】；
8) 在数据库引擎配置中，账户设置处选择身份验证方式为“混合验证方式”，并为 sa 设置密码，其余默认，点击【下一步】；
9) 在错误报告中，按照默认，点击【下一步】；
10) 进入安装过程，等待安装完毕即可。

2.3.2 安装服务器和控制台模块

安装数据库完成后，就可以开始安装服务器和控制台了，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。

2.3.3 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。

第一次安装服务器后，IP-guard 会自动生成一个有 30 天试用期的演示序列号，演示序列号不含有加密功能。

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，如果您输入的序列号无误，系统会提示“**序列号升级成功**”并且提示您需要激活产品。您必须通过产品注册得到注册码来激活您的产品。

如果 IP-guard 所在服务器可以连接互联网，有 2 种注册方法：

在线注册

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；

邮件注册

您也可以使用邮件注册。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【**发送邮件**】，系统会弹出发送邮件窗口，请确认填写信息无误后发送邮件。
我们会将注册码发到您填写的电子邮件地址，收到后请将注册码复制到相应地方，点击【**注册**】按钮，系统提示“**注册成功**”就完成了整个注册的过程。

如果因为网络或别的问题，无法在线注册或即时发送邮件获得注册码，您也可以在其他可上网的机器上将注册信息和识别码发送邮件给我们进行处理。

注意　　**第一次注册时填写的电子邮箱地址是非常重要的，以后因其他原因需要再次注册时，新的注册码我们仍然会发到第一次注册时填写的电子邮箱内。**

2.3.4 设置系统检验码

检验码是服务器和客户端除了序列号外唯一的识别码，其目的是增加系统内的安全性。服务器上的检验码必须和客户端的检验码一致，该客户端才能被服务器所管理。所以建议您先在服务器上设置检验码，再打包客户端安装程序，这样就会把服务器的序列号和检验码一起打包到客户端安装程序，防止外来非法的服务器接管企业内的客户端。

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。

系统默认检验码为空，如果客户端没有检验码，第一次设置检验码后，服务器会自动更新所有连接上的客户端的检验码，使客户端的检验码与服务器保持一致。

如果服务器再次设置新检验码，只要客户端识别到服务器之前设置的检验码中有一个与客户端现在的匹配，客户端就会主动将检验码更新为服务器现在的检验码。

警告　　管理员请务必牢记自己设置的检验码，以便服务器重装之后或者换了系统后可以顺利接管以前的客户端，否则您可能需要重新部署客户端。

如果发现客户端有运行但是无法在控制台显示，请在 IP-guard 控制台“**日志->**

系统事件”中查看是否属于检验码验证失败的问题。

2.3.5 服务器日志

右键单击【服务控制器】选择菜单“**工具->日志**”会自动链接到操作系统的【事件查看器】。选择【应用程序】可以查看 OSERVER3 的运行日志，包括：服务器程序的启动和停止、错误日志等。管理员通过这些日志信息可以分析服务器的运行情况。

2.4 安装和部署中继器

部署中继器的计算机需要安装数据库。

2.4.1 安装中继器模块

安装完数据库后便可开始安装中继器，具体操作步骤如下：

1) 双击 IPguardRelay.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 中继器；
4) 选择数据库，点击【确定】;
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【安装】，复制文件结束后系统安装完毕，单击【完成】按钮完成安装，中继器模块自动启动，由于此时中继器并未连接任何主服务器，未得到授权，所以在托盘有图标显示为  。

2.4.2 连接主服务器

在中继器的托盘图标上点击右键，在右键菜单“**工具->设置连接参数**”，弹出连接参数设置框，设置主服务器信息和申请者相关信息。

参数	内容
主服务器地址	主服务器的地址，可以是 IP 或域名；
申请者	申请者名称。

中继器连接主服务器后，需要在控制台“**工具->服务器管理->中继服务器管理**”中对中继器进行授权。

2.4.3 查看中继器状态

中继器的运行图标，显示当前中继器运行时的状态，具体状态有：

图标状态	说明
	中继器当前状态未知；
	中继器未连接服务器，或者已连接服务器但未获得授权；
	中继器正在启动；
	中继器与服务器连接成功，并获得授权；
	中继器停止运行；

在中继器的运行图标上点击右键，在右键菜单“**状态**”，可以查看中继器更加详细的状态情况。

属性名称	说明
名称	控制台“**工具->服务器管理->中继服务器管理**”中显示的中继器名称，默认为中继器所在机器的计算机名。可在控制台上进行重命名；
计算机	中继器所在机器的计算机名称；
申请者	中继器设置连接参数时所设置的申请者；

网络地址	中继器所在计算机的 IP 地址；
运行状态	包括：“未授权，与主服务器断开连接”、“连接成功，未获得授权”、“连接成功，已获得授权”
启动时间	中继器启动的时间；
运行时间	中继器从启动后运行的时间；
主服务器地址	中继器所连接的主服务器 IP 地址；
连接状态	中继器与主服务器的连接状态。若是能正常连接，则显示“连接成功”，若连接异常，则显示“连接失败”；
最后连接时间	中继器与主服务器最后连接的时间；
授权状态	主服务器是否对其进行授权，包括：“已授权”、“未授权”；
授权更新时间	主服务器最新一次更新授权的时间；
客户端连接数	连接上该中继器的在线客户端数量。

2.4.4 中继器日志

右键单击【中继器控制器】选择菜单“**工具->日志**”会自动链接到操作系统的【事件查看器】。选择【应用程序】可以查看中继器的运行日志，包括：中继器程序的启动和停止、错误日志等。管理员通过这些日志信息可以分析中继器的运行情况。

2.5 安装和部署 WEB 服务器

IP-guard 支持基于 B/S 的管理方式，通过部署 WEB 服务器，可以实现在任何机器上使用浏览器登录服务器，实现控制台相关管理操作，如查看日志、报表、进行各项审批等。

部署 WEB 服务器的计算机不需要安装数据库。

安装的具体操作步骤如下：

1) 双击 IPguardWebServer.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；

4) 设置服务器 IP 和端口。其中服务器 IP 为 WEB 服务器所要连接的 IP-guard 服务器 IP，如果两者安装在同一台机器上，可保持默认的 127.0.0.1 不改；端口为访问 WEB 服务器时的端口号，默认为 80；

5) 安装程序会提示用户选择安装组件，用户可以根据需要选择安装。其中：
WebConsole — WEB 控制台
WebReport — WEB 报表
WebApprove — WEB 审批
JAVA — WEB 审批必要组件
OpenOffice — WEB 审批必要组件
建议安装全部组件，点击【下一步】；

6) 选择开始菜单的快捷方式的目录，点击【下一步】；

7) 确认设置无误，点击【安装】，复制文件结束后系统安装完毕，单击【完成】按钮完成安装。过程中如果弹出提示 Windows 防火墙阻止了 Apache HTTP Server，请点击【允许访问】。

安装完成后，WEB 服务器模块自动启动，在托盘有图标显示为  。

2.6 部署客户端模块

客户端模块的部署有多种方式：直接安装、远程推送、域登录脚本安装，您可根据实际需要完成对客户端机器的部署。

2.6.1 直接安装客户端

直接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。

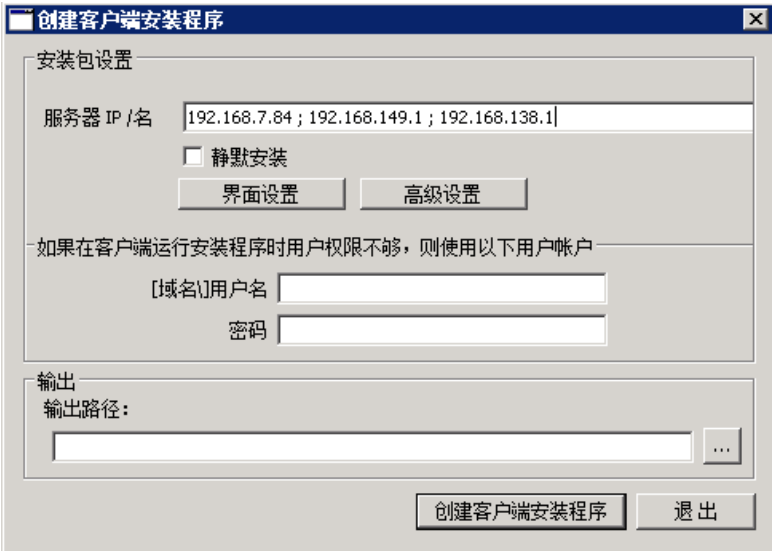
打包 Windows 客户端安装程序，在安装了服务器的机器，点击“**开始->所有程序->IP-guard V4->创建客户端安装程序**”打开 Windows 客户端生成工具。

打包 Mac 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 V4->创建客户端安装程序（Mac）**”打开 Mac 客户端生成工具。

打包 Linux 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 V4->创建客户端安装程序（Linux）”打开 Linux 客户端生成工具。

三种客户端的生成工具界面一致，使用方法也类同，下面以 Windows 客户打包工具为例说明。



客户端安装程序的参数包括：

名称	说明
服务器 IP 地址	系统默认是当前计算机的 IP 地址，如果服务器有多个 IP 地址，请输入一个有效 IP 地址。
静默安装	选中该复选框，客户端安装程序为静默安装，没有安装界面；不选中该复选框，则为非静默安装包。
界面设置	点击此按钮进行安装包界面设置；
安装包标题设置及图标设置	设置安装包运行时显示的窗口标题，可选择设置安装包标题包含版本号、安装包名称。 勾选安装包名称时，可以在内容输入框中输入自定义的标题文字内容，支持多语言。

自定义标题设置说明如下：

1.设置所有语言系统的标题内容

直接输入需要显示的内容即可，如输入“agent”，则在任何语言系统下，生成的安装包标题均显示为“agent”；

2. 设置指定的语言系统的标题内容，其他语言系统下标题内容使用默认。

格式为“语言代码=设置内容”。

目前支持的语言代码为：chs 表示中文简体、cht 表示中文繁体、enu 表示英文、jpn 表示日文、kor 表示韩文、rus 表示俄文。

例如：输入“chs=客户端;cht=用户端;enu=agent”，则在简体中文系统下,安装包的标题显示为“客户端”，在繁体中文系统下，安装包的标题显示为“用户端”，在英文系统下，安装包的标题显示为“agent”，在其他语言系统下显示为默认标题。

3.设置指定的语言系统的标题内容，其他语言系统统一设置标题内容（即不使用默认）

此时参照 2 中的例子，将设置改成“agent ;chs=客户端;cht=用户端;enu=agent”即可，则其他非指定的语言系统下，安装包的标题显示为“agent”。

设置安装包显示的图标，可选择图标项，点击 … 按钮选择文件，文件格式只支持.ico。

安装包属性设置　设置安装包属性中显示的文件说明和产品名称。

高级设置　点击此按钮进行高级设置；

将安装配置信息打包到独立文件中　不勾选此项，则安装配置信息一同打包到安装程序中；勾选此项，则安全配置信息独立打包到 AgentSetup.dat 文件中，安装时需将打包好的安装程序和 AgentSetup.dat 文件放在同一目录中。

提升 UAC 权限　设置提升运行安装包的 UAC 权限，勾选此项，执行安装包时则以管理员身份运行。

安装包密码　设置安装包的使用密码，则运行安装包时需输入正确密码才可以成功安装。

用户许可设置　设置安装包包含用户许可协议，则运行安装包时需接受协议条款后才能继续安装过程。

导入客户端策略　设置安装包包含的客户端策略，点击 … 按钮选择从控制台导出的客户端策略 ipz 文件(详见控制台章节中的“**策略导出**”小节)，客户端安装后会自动导入策略；

	客户端连上服务器后会自动同步服务器上的策略。，
安装包过期时间	超过设置的时间，则安装包不可用。
用户名和密码	安装客户端需要管理员权限，如果计算机上登录的用户是 user 权限，可能会无法成功安装，这种情况下，可以在创建客户端安装包时，在这里输入具有计算机管理员权限的用户名和密码，这样创建的客户端在 user 权限下也能安装成功。
输出路径	客户端安装程序的文件名、保存类型以及存放路径。其中，保存类型有 exe 以及 msi 格式可选。

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 1.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。

2.打包 Mac 客户端和 Linux 客户端时，不支持静默安装和高级设置。

3.无法同时设置“静默安装”和“提升 UAC 权限”选项。

2.6.2 远程推送客户端

对于较大的企业，计算机数量较多，分布的较广，不方便在计算机上进行手工安装，逐台计算机进行安装也会消耗大量的精力。此时，我们可以通过远程安装的方式来解决这个问题，既可以批量安装客户端程序，也省去了亲自到该计算机上安装的麻烦。

在安装了 IP-guard Server 的机器，点击“**开始->所有程序->IP-guard V4->远程安装客户端模块**”运行远程安装工具。

该工具能对 Windows NT 4.0/2000/XP(X86/X64)/2003(X86/X64) /2008(X86/X64) /Vista(X86/X64) /win7(X86/X64)的机器进行安装，要安装 Windows 9x/ME 的计算机请直接在所需的计算机上安装。

扫描设置：

系统默认扫描本网段内的所有计算机，如果需要扫描其它网段的计算机，请选择菜单“**文件->扫描设置**”打开扫描设置对话框，添加其它网段的 IP 范围，

也可以对扫描包的时间间隔进行设置。

在计算机列表中各种图标代表的含义：

图标	颜色	Window NT4 / 2000 / XP	Window 95 / 98 / Me	是否在线	是否安装 Agent
	深蓝	是	否	是	否
	深蓝	否	是	是	否
	灰色	是	否	否	否
	灰色	否	是	否	否
	浅蓝	是	否	是	是
	浅蓝	否	是	是	是

远程推送

选择需要安装客户端模块的计算机，可同时选择多个计算机，点击“**操作->开始安装**”开始客户端模块的安装，在安装状态栏可以查看每台计算机的安装状态，在下面的安装日志窗口可以查看所有计算机的安装日志。

【常见问题】

- ✧ 当前登录的用户没有操作目标计算机的权限，此时会弹出一个安装出错的窗口，请输入具有目标计算机管理员权限的用户名和密码；
- ✧ 目标计算机没有打开 admin 共享，这时需要到目标计算机上开启 admin 共享，打开命令提示符 cmd.exe，net share 查看 ADMIN$共享是否开启，如果没有打开，net share ADMIN$ 打开 admin 的共享；
- ✧ 目标计算机无法访问本机共享文件，可能是本机的 admin 共享没有打开，目标计算机没有权限访问本机共享文件。

注意

1. Mac 客户端和 Linux 客户端不支持远程推送安装。

2.由于 Windows NT 网络内部的一些安全权限的设定影响程序正常运行，所以可能某些时候并不能使您有足够的权限在远程的计算机上执行远程安装。在这种情况下，请您用 IP-guard 客户端的安装程序到所需的计算机直接安装。

2.6.3 域登录脚本安装

如果网络中有域环境，可以通过修改域脚本来安装客户端。通过修改登录脚本，Windows 用户登录域时，执行登录脚本，将 IP-guard 客户端安装到本机上。

具体步骤如下：

1) 在安装光盘中找到 LogonScript 目录，将整个目录复制到域服务器机器上；

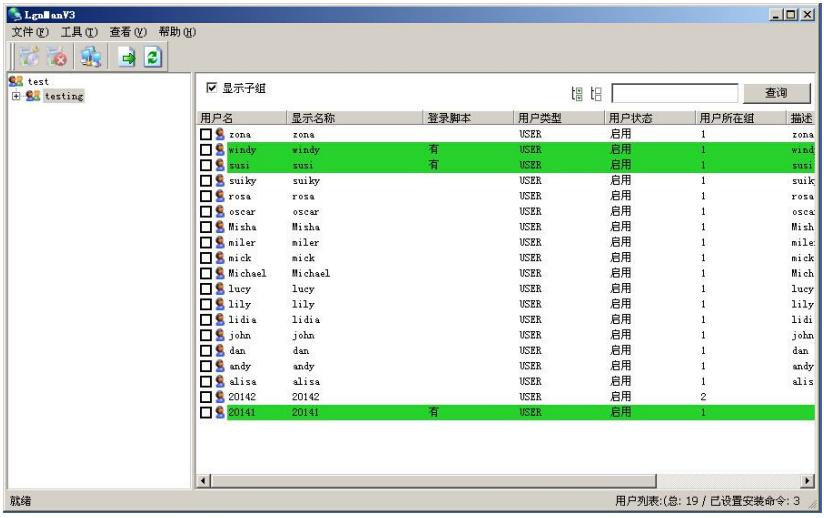
2) 在 IP-guard 服务器上创建客户端安装程序，并命名为 OAgentInst.exe；

3) 将 OAgentInst.exe 复制到域服务器上的 LogonScript 目录下；

4) 运行域服务器上 LogonScript 目录下的 LgnManV3.exe 程序进行域登录脚本的设置。

使用说明：

1) 运行 LgnManV3.exe 后出现以下的界面，LgnManV3.exe 会自动扫描并排序显示域服务器上的用户分组信息列表，显示各个用户的登录脚本状态。其中，用户图标底色为绿色表示该用户的登录脚本已经包含我们的安装命令。



2) 管理员可以点击列表表头进行排序，并结合 CTRL， SHIFT 等键选择多个要操作的用户，在“**菜单栏->工具**”中或者是点击功能按键设置安装命令、删除安装命令等操作。

3) 设置了安装命令的用户在登录域时，相关的域脚本将会运行，IP-guard 客户端会自动安装到指定用户的计算机。

4) 当 IP-guard 客户端成功安装到所需的计算机，你可以删除有关用户的安装命令，从而将用户的登录脚本还原为原来的登录脚本。

功能按钮说明

图标按钮	说明
	设置安装命令，将在选定用户的登录脚本中添加我们的安装命令；；
	删除安装命令，将在选定用户的登录脚本中删除我们的安装命令；；
	设置安装范围，可通过 IP 地址和计算机名称来设置域登陆脚本安装的计算机范围，包括安装范围和排除范围，支持跨网段地址；
	导出，可导出域脚本安装工具列表，能保存为 Web 文件格式、Microsoft Excel 文件格式以及文本文件格式
	刷新视图列表信息。

注意　Mac 客户端和 Linux 客户端不支持域脚本安装。

2.7 制作 U 盘加密客户端

2.7.1 注册

使用 U 盘加密客户端功能，首先需要注册。联系厂商并提供主序列号、U 盘加密客户端授权数，由厂商生成注册授权文件 USBALicenseCertFile.dat。

登录控制台，选择菜单“**工具->客户端管理->U 盘加密客户端管理**”，在弹出的 U 盘加密客户端管理窗口中，点击【**导入**】按钮，选择 USBALicenseCertFile.dat 文件，导入后可在窗口下方看到授权点数以及授权有

效期。

2.7.2 制作

制作 U 盘加密客户端主要为两大步骤

1.创建 U 盘加密客户端程序文件；

2.将指定 U 盘制作成 U 盘加密客户端。

下载 U 盘加密客户端压缩包文件，解压后将 AInstGen_SDUDisk.exe 和 AKernel3U.e32 拷贝到服务器安装目录下，将 UDiskSetup 文件夹复制到要插入 U 盘制作 U 盘加密客户端的机器上。

创建 U 盘客户端程序文件

在安装服务器的机器上运行 AInstGen_SDUDisk.exe，制作程序界面图如下。

参数如下：

名称	说明
服务器 IP/名	系统默认是当前计算机的 IP 地址，如果服务器有多个 IP 地址，请输入一个有效 IP 地址。也支持输入可有效访问的计算机名称；
输出路径	U 盘加密客户端安装程序的文件名以及存放路径。生成后的安装程序文件的文件类型为 ipk 文件。

点击【**创建客户端安装程序文件**】按钮，U 盘加密客户端安装程序文件创建成功。

使用 U 盘制作加密客户端

在计算机上插入 U 盘，运行 UdiskSetup 文件夹里的 SDUDiskFormatter.exe，可移动盘处选定 U 盘，选择已生成的 U 盘加密客户端安装程序文件，点击【**开始制作**】按钮，等待制作完成即可。

2.7.3 授权

U 盘制作成便携式加密客户端后，需要授权该 U 盘，不授权无法启用加密相关功能。

打开已制作好的 U 盘，运行其中的 USDconf.exe，弹出 U 盘加密客户端策略更新工具，点击下方的【**导出可移动盘信息**】按钮，可将此 U 盘的信息保存成. uea 文件导出。

登录控制台，选择菜单“**工具->客户端管理->U 盘加密客户端管理**”，在弹出的 U 盘加密客户端管理窗口中，点击按钮，添加 U 盘加密客户端授权，选择 U 盘信息文件.uea 文件进行授权。

授权后，在计算机树中选定的分组里会新增一个 U 盘加密客户端节点。此时该节点由于并未在任何计算机上使用过，所以节点为灰色。此时该客户端会继承对应的分组加密策略，也可以对其设置特定的加密策略。

2.8 系统升级

2.8.1 更新维保码

维保服务期

用户享受维保服务的期限。

维保码

用户享受维保服务的凭证。

用户进行续保之后，需要更新维保码，以便升级至产品的最新版本使用最新功能以及享受其他的维保服务。用户的维保服务期包含在维保码里。

首次安装服务器时，如果不能获取到维保码，在无维保码的情况下，可以使用

15 天。超过 15 天仍未能获取到维保码，则控制台无法登录。获取维保码后，会验证版本的合法性，如果版本的出厂日期不在维保服务期内，会禁止产品的使用。

查看维保期服务

控制台“**帮助->关于**”中，可以查看维保服务期，其中维保服务期会根据当前时间和到期时间呈现不同的颜色：

颜色	说明
红色	维保服务期已过；
紫色	维保服务期即将过期，离到期日还有 1 到 30 天；
蓝色	维保服务期未过期，且离到期日超过 30 天；

如果维保服务期即将过期或者已经过期，有“**产品维保升级**”权限的帐户在登录控制台时会收到维保服务期即将到期或者过期提醒。

没有维保码或者维保服务期有变动，需要更新维保码，可以通过服务器和控制台来更新维保码。

更新维保码

更新维保码，有两种方式。

方式一：服务器自动更新。如果服务器能正常连接互联网，则会定期自动更新维保码；否则，无法更新。

方式二：控制台更新。控制台“**帮助->维保服务期更新**”，或者菜单“**帮助->关于**”中点击更新维保服务期，进行维保码更新。

设置	说明
在线更新	运行控制台的计算机可正常连接网络，选择此项在线更新维保码；
手动更新	运行控制台的计算机无法正常连接网络，可通过商务途径取得维保码，手动填入完成更新；

2.8.2 下载升级包

检查新版本

检查新版本分为自动和手动两种方式。

方式一：自动检查新版本。控制台登录后，会自动检查是否有新版本可以升级。如果有新版本，会弹出窗口提示。另外，管理员可以在控制台“**工具->选项->升级维护->自动检查产品升级**”中，设置是否进行自动检查。

方式二：管理员可以在控制台“**帮助->检查产品升级**”处，手动检查新版本。

下载升级包

检查到有新版本时,会弹出新版本更新日志以及下载链接。点击下载链接，可以下载最新版本的升级包。

注意　　如果升级包的出厂日期在维保服务期外，则无法下载。

2.8.3 升级服务器和控制台

升级服务器和控制台可以通过升级包来完成，可以直接在控制台菜单“**帮助->检查产品升级**”下载新版本的升级包，也可以联系我们获取升级包。

升级服务器和控制台的具体步骤如下：

1) 运行升级程序，列表中会显示当前版本和升级版本，单击【升级】按钮进行升级；
2) 手工启动服务 OCULAR V3 SERVER 和 OCULAR V3 UPDATE（如果直接覆盖安装，不需要手工启动）

注意　　如果升级程序的出厂日期在维保服务期外，会禁止升级。

2.8.4 升级中继器

控制台“**工具->服务器管理->中继服务器管理**”中，左侧中继器树中的中继

器带有（#）的标识，则说明此中继器当前可升级为新版本。选中需要升级的中继器，右键菜单中选择“**升级**”，等待完成升级即可。

2.8.5 升级客户端

客户端默认不会自动升级，选择“**工具->服务器管理->客户端升级管理**”，根据实际管理需要进行升级设置。

2.9 卸载

2.9.1 卸载客户端

对于不再需要安装客户端模块的计算机，管理员可以将客户端模块卸载，卸载客户端有 2 种方式：

控制台卸载

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。

客户端工具卸载

对于离线状态的客户端机器，也就是无法与服务器连接的客户端机器，我们提

供了另外一种卸载客户端的方法，具体步骤如下：

1) 在客户端机器的“**开始->运行**”中输入命令“agt3tool ocularadv”，打开客户端工具；

2) 选择“**卸载客户端**”，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，输入正确的确认码执行指定的操作。

注意　卸载客户端和删除客户端的区别：卸载客户端仅仅是移除客户端模块，并不减少 license 数，在控制台上可以显示该计算机并查看日志；而删除客户端包括卸载客户端和减少 license 数。

2.9.2 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 V4->卸载 IP-guard V4**”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。

第三章. 控制台

3.1 登录控制台

3.1.1 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 V4->IP-guard V4 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。

登录的对话框中包含以下内容：

字段	说明

服务器	输入服务器的 IP 地址或计算机名称；
账户	初始时预设了系统管理员为“admin”，系统审计员为“audit”，管理员也可以根据不同的权限设置多个管理员账户，在“**工具->账户**”中添加；
密码	管理员的初始密码均为空，登录控制台后可以修改管理员密码，在“**工具->修改密码**”中修改密码，管理员需要保管好自己设置的密码。
记住密码	勾选此项，则登录控制台时会记住此次登录用户的密码。 登录控制台后，可以在“**工具->选项->控制台设置->基本设置->清除记住的密码**”中，点击【**立即清除**】按钮，下次登录控制台时将需要输入密码；
自动登录	勾选此项，则下次启动控制台程序时，使用上一次的用户名和密码自动登录。 若在“**工具->选项->控制台设置->基本设置->清除记住的密码**”中点击【**立即清除**】按钮，下次登录控制台时不会自动登录。

当需要重新连接服务器或者连接到其它的服务器，或需要以不同的管理者身份进入控制台时，可以选择“**工具->重新登录**”功能重新登录控制台。

3.1.2 修改密码

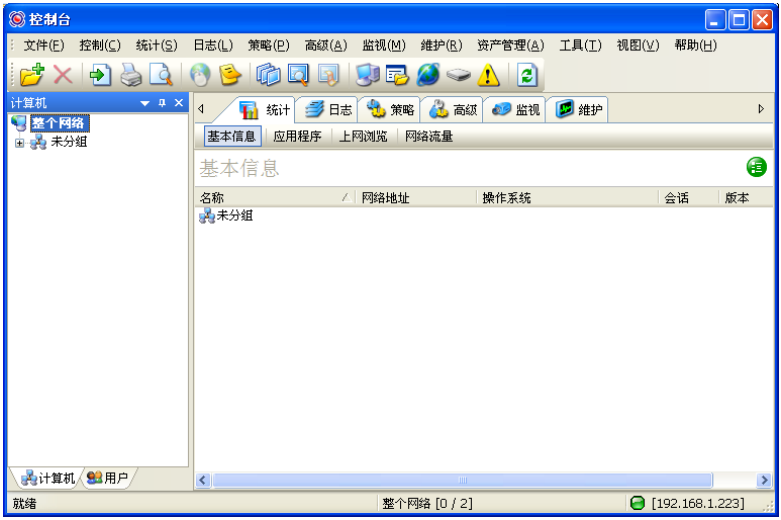
为了保密，用户可以修改自己的密码，以防止他人盗用您的用户帐号登录到系统中执行非法的操作。

登录控制台后，选择“**工具->修改密码**”打开修改密码对话框。输入旧密码，再输入新密码，并在密码确认框中再输入一次，保证两次输入的密码一样，单击【确定】，修改密码成功。注意这里的修改密码只能对当前登录的管理员用户密码进行修改，在这里的第一行会显示当前登录控制台的帐户。

经过服务器模块认可后新密码就生效了。

3.2 控制台简介

控制台登录后，将见到如下的界面视图：



控制台界面包括：

界面区域	说明
菜单栏	包含了本系统的所有菜单，是各功能窗口的入口；
工具栏	包含了一些常用的功能；
计算机栏	位于窗口的左边，显示所有安装了客户端的计算机列表和以及分组信息；
用户栏	位于窗口的左边，显示所有客户端机器登录的用户列表以及分组信息；
导航主菜单	位于工具栏的下方，可以快速导航主要功能；
导航子菜单	对导航主菜单的补充，快速导航到具体的功能；
功能按钮区	位于导航子菜单的下方，该视图也包含了当前功能的标题，功能按钮在标题的右侧；

数据显示区	是本系统的核心视图，所有的数据都在数据显示区查看；
图表栏	只有统计功能包含图表栏，是显示统计图的区域；
查询栏	在统计、日志、即时通讯、邮件记录中均有查询栏，并且有一些通用查询条件，在下面详细说明；
属性栏	只有策略控制功能中包含属性栏，是设置策略属性的区域；
状态栏	位于窗口的最下方，显示当前功能的状态信息。

计算机栏中各图标的含义

图标	颜色	含义
	亮蓝色	客户端模块正常运行
	灰色	客户端模块没有运行，可能是该计算机没有开机或没联网，也可能是防火墙阻断了通讯
	深灰色	客户端模块已被卸载
	亮蓝色带小时钟标志	客户端模块正常运行，但客户端的使用者离开

用户栏中各图标的含义

图标	颜色	含义
	亮蓝色	该用户的客户端模块正常运行
	灰色	该用户的客户端模块没有运行，可能是该用户没有登录

系统通用的日志属性和查询条件

在日志记录中（包含各种事件日志、邮件日志、即时通讯日志），会包含一些通用日志内容：

字段名称	说明
时间	记录该日志的详细时间；
计算机	记录该日志属于的客户端机器，这里的计算机是指在计算机栏中显示的名称；
用户	记录该日志发生的用户，这里的用户是指用户栏中显示的名称。

对于日志和统计数据，我们的通用查询条件包括：

查询条件	说明
时间范围	指定查询的时间范围， 默认终止时间为当天，起始时间为一个月前，即默认查询前一个月内的日志。
◀	单击该图标直接查看上一时间段的日志，一个时间段可以是一天、一个星期、一个月等，取决于当前设置的起始时间和终止时间；
▶	单击该图标直接查看下一时间段的日志，也是取决于设置的时间范围；
↰	单击该图标自动恢复到系统默认的时间范围。
时间类型	在“**分类管理->时间类型**”中系统预定义了工作时间、休息时间和周末时间，管理员需根据实际情况修改这些时间类型，并可以自定义时间类型进行查询；
范围	单击右边按钮打开范围选择窗口，可以选择单个计算机或单个组(包括整个网络)进行查询。

3.3 计算机和用户操作

3.3.1 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。

1） 计算机基本信息

在计算机栏中选择一台计算机，在数据显示区会显示该计算机上客户端模块的运行状态：

字段名称	说明
名称	客户端在计算机树中显示的名称，为了方便管理，该名称可以更改。如果不更改，名称和计算机名称相同；
计算机	客户端所在计算机的真实名称；

字段名称	说明
网络地址	计算机与服务器通讯的 IP 地址；
状态	客户端的运行状态，包括：正在运行、离线、客户端已被卸载；
离线天数	客户端离线天数；
版本	客户端的版本号；
操作系统	客户端所在计算机的操作系统版本；
开机时间	当前客户端的启动时间，只有客户端状态为“正在运行”才有该字段；
最后在线时间	客户端最后一次与服务器的通讯时间；
最后活动时间	显示客户端机器的最后活动时间；
安装时间	该版本客户端的安装时间；
IP/MAC 地址	该计算机的所有网卡的 IP/MAC 地址；
最后登录用户	该计算机的当前登录用户，空闲和锁定的状态也会在这里显示。

如果计算机登录多个用户，在最后登录用户的下方，控制台会显示该计算机当前登录的所有用户及登录时间。

2） 计算机组基本信息

在计算机栏中选择一个计算机组，在数据显示区会显示该组下所有的计算机和组的状态列表。

如果选择整个网络，会显示所有的计算机组，单击数据显示区右上角的【展开】按钮 “  ”，可以查看这些组下所有计算机的状态列表。

3)　用户基本信息

在用户栏中选择一个用户，在数据显示区会显示该用户的运行状态。

字段名称	说明
名称	客户端在用户树中显示的名称，为了方便管理，该名称可以更改。如果不更改，名称和用户名称相同；
用户	客户端所登录的用户的真实名称，如果是本地系统用户，即显示该用户名；如果是域用户，即显示为域名\用户名；
状态	客户端的运行状态，包括：在线，离线等；
最后在线时间	客户端的在线更新时间；
最后活动时间	客户端所在的用户的活动更新时间；

最后登录的计算机	该用户最后登录的计算机。

如果该用户在不同的计算机上登录，在最后登录计算机的下方，控制台会显示该用户登录的所有计算机和登录时间。

4) 用户组基本信息

在用户栏中选择一个用户组，会显示该组下所有用户和组的状态。同样在整个网络下，单击数据显示区右上角的展开按钮“  ”，可以查看所有用户的状态信息。

3.3.2 显示

在计算机栏中，所有客户端机器默认会显示计算机名，可以根据需要设置客户端在计算机栏中显示的信息。

选择整个网络，右键菜单选择“**显示**”，在信息显示设置对话框中，勾选需要显示的内容，则重启控制台后，计算机栏上的客户端将显示勾选的信息内容。可选择的显示内容为：名称、计算机、IP、最后登录用户。

说明 该设置为管理员行为，即：某管理员登录控制台更改了计算机栏的显示信息，则他在任何计算机上登录都显示此信息。其他管理员都显示与他不同。

3.3.3 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。

提示　计算机组和用户组都有一个默认分组 “**未分类**”组，新出现的计算机和用户都被归类为“**未分类**”组。“**未分类**”组不能删除，不能重命名，也不能在“**未分类**”内新建子组。

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。

提示　为了方便分组，可以同时拖动多个计算机或用户到指定的分组，如选择“未分组”，查看“统计->基本信息”，按住 CTRL 或 SHIFT 键，选择多个计算机或用户到指定分组。

3.3.4 查找

通过查找功能，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。

查找计算机

在计算机栏中选择“**文件->查找**”打开查找对话框。输入查询条件，查询条件支持名称（计算机栏中显示的名称）、计算机名（真实的计算机名称）、网络 IP 地址、网卡地址，支持模糊查询和多关键字查询，多个关键字用分号隔开。还可根据计算机的分组和状态进行筛选查找，状态包括在线、离线、空闲、锁定等。

查找出来的计算机在下面的列表中显示，双击其中一台计算机可直接跳转到该计算机的数据显示画面。选中结果列表中一台或多台计算机，右键“**移动到**”，弹出分组窗口，可批量移动计算机到其他分组。

查找用户

从计算机栏切换到用户栏，选择“**文件->查找**”，打开查找对话框。输入查询条件，查询条件支持用户名称，包括管理员自定义的用户名和真实的用户名，支持模糊查询和多关键字查询，多个关键字用分号隔开。还可根据用户的分组和状态进行筛选查找，状态包括在线、离线、空闲。

和查询计算机的操作相同，双击结果列表中的用户可以直接跳转到该用户的数据显示画面。选中结果列表中一个或多个用户，右键“**移动到**”，弹出分组窗口，可批量移动用户到其他分组。

3.3.5 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。

被删除的计算机会被归类至“已删除组”中，能查询历史日志，但不能查询实时维护信息。

删除用户(组)只是删除用户的信息，并不影响 License 授权。被删除的用户被归类至“已删除组”中。当该用户再次登录后，会从“已删除组”自动回到原分组中。

3.3.6 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。

3.3.7 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

3.3.8 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。

3.3.9 策略导出

当需要对离线客户端下发新的策略时，管理员可选中对应的客户端节点，更新相关策略后，右键菜单“**策略导出**”，选择导出文件存放的路径，点击确定，等待导出完成；即可导出计算机的所有策略内容，导出的文件类型为.ipz 格式；选择整个网络或者计算机组，则会导出对应的组策略。

3.3.10　清除子节点的策略

当存在组策略，同时分组下的计算机（用户）又分别被设置了单独的计算机（用户）或策略时，计算机（用户）会优先执行自身的计算机（用户）策略。若管理员想收回单独的计算机（用户）策略，统一执行组策略时，则可以使用清除子节点策略功能，避免逐个计算机（用户）去删除其计算机（用户）策略的麻烦。

控制台切换到具体策略，选中需要清理策略的计算机分组或用户分组，右键菜单“**清除子节点的策略**”，弹出对话框，选择需要清除策略的对象，可批量删除此分组下拥有此类策略的子节点上的策略。

3.4 策略角色

3.4.1 术语介绍

策略集

策略集，即多条策略的集合。管理员可根据实际需求，把一些常用的策略做成策略集，再把策略集应用于各种对象上，如计算机、用户和角色。

角色

角色，是具有相同策略的一组对象的集合。一个对象可以属于多个角色。管理员通常可以按部门划分角色，如市场部员工、销售部员工等，或按职位等级设置角色，如普通员工，部门主管等。一个计算机可以属于多个角色，既属于市场部员工，又属于部门主管，则同时有这两个角色的策略。

3.4.2 基本操作

新建

策略集和角色需要手动新建。在角色栏，选择**策略集**节点，右键菜单中选择“**新建策略集**”，可新建策略集并设置策略集名称。选择菜单“**文件->重命名**”可对选定的策略集进行改名。可按照同样的方法对角色进行新建和重命名操作。

查看基本信息

在角色栏，选择菜单“**统计->基本信息**”，管理员可以查看策略集和角色的基本信息。

1）策略集基本信息

在角色栏中选择一个策略集，在数据显示区会显示该策略集的基本信息：

字段名称	说明
名称	该策略集的名称；
组	该策略集所在的策略集组；

字段名称	说明
备注	该策略集的备注信息；
角色	已分配的角色；

2）策略集组基本信息

在角色栏中选择一个策略集组，在数据显示区会显示该策略集组下所有的策略集和策略集组信息。

3）角色基本信息

在角色栏中选择一个角色，在数据显示区会显示该角色的基本信息：

字段名称	说明
名称	该角色的名称；
组	该角色所在的角色组；
备注	该角色的备注信息；
策略集	该角色包含的策略集；

4）角色组基本信息

在角色栏中选择一个角色组，在数据显示区会显示该角色组下所有的角色和角色组信息。

分组操作

1）新建分组

在角色栏，选择**策略集节点**，选择菜单“**文件->新建组**”，则会在策略集树中出现一个新的组节点，为可编辑状态，输入组名称，将相关的策略集拖到该组。管理员可以按照相同的办法建立多级的分组机构。

选择**角色节点**，可以按照相同的方法对角色进行分组管理。

2）指定分组和改变分组

当需要为策略集和角色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策略集和角色，选择菜单“**文件->移动到**”，选择相应的目标组，这样我们所选择的策略集和角色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，这样我们所选择的策略集(组)或角色(组)就会属于我们指定的组了。

提示 为了方便分组，可以同时拖动多个策略集或角色到指定的分组，如选择某个分组，查看“统计->基本信息”，按住 CTRL 或 SHIFT 键，选择多个策略集或角色到指定分组。

调整策略集优先级

单个策略集中的策略，同一种策略的优先级按照先后关系进行匹配，按最先匹配的策略执行规则。多个策略集中的策略，按对应策略集所处的策略集树结构顺序，自上而下优先级从高至低，即位置在上面策略集，其所拥有的策略优先级高。

选择菜单“**统计->基本信息**”，选择策略集分组节点，在右边显示视图中可以看到当前层级下的策略集和策略集组，点击上移按钮和下移按钮调整顺序，从而调整优先级。

说明 调整顺序后需要点击保存按钮保存。

复制策略集

在角色栏策略集树中选中策略集，选择右键菜单“**复制策略集**”可将选定的策略集复制，复制出的策略集继承原策略集的常规属性以及所拥有的策略，但不继承分配的角色和对象。

查找

通过查找功能，管理员可以快速定位到指定的策略集或角色，并且查看其相关的信息。

在角色栏中，选择“**文件->查找**”打开查找对话框。输入查询条件，查询条件支持名称（计算机栏中显示的名称），支持模糊查询。查询出来的结果包含策略集和角色。

删除

对于不再需要使用的策略集，可以在控制台上将其删除。选择“**文件->删除**”，可以把策略集树或策略集列表中选中的策略集(组)删除，如果是策略集组，则包括该组中所有的子组和策略集。删除了策略集，分配给其的角色和对象将不再具有该策略集所拥有的策略。

可以按照相同的方法删除角色（组）。删除角色，则该角色与分配给其的对象

之间的关系也一并解除。

导入和导出

在策略集树中选中“**策略集**”节点，选择右键菜单“**导出**”，可将当前所有的策略集保持层级结构导出；选择右键菜单“**导入**”，可将事先导出的策略集导入到“**策略集**”节点下。

在角色树中选中“**角色**”节点，可以按照相同的方法对角色进行导入导出操作。

说明　　导入策略集和角色时，对于已存在的同名策略集或角色，均不会导入。

3.4.3 设置策略集

在角色栏选中一个策略集，选择菜单“**统计->策略角色**”， 在右边显示视图中可以查看该策略集已分配的对象，包括计算机、用户。

字段名称	说明
名称	已分配的计算机、用户的名称；
分组	对应计算机和用户所在的分组；

点击编辑按钮，可以编辑策略集属性。

点击导出按钮，可以导出所有策略集下的全部计算机对象和用户对象。

常规

显示该策略集的名称以及所在分组，可在此处对该策略集设置备注。

计算机用户

在列表中显示该策略集分配的计算机和用户。点击添加按钮，即可把该策略集分配给此处选中计算机和用户。分配之后，这些计算机和用户会被赋予该策略集所拥有的策略。点击导出按钮，即可导出所有策略集下的全部计算机对象和用户对象。

角色

在列表中显示该策略集分配的角色。点击添加按钮，即可把策略集分配给此处选定的角色。分配之后，这些角色将带有该策略集所拥有的策略。

3.4.4 设置角色

在角色栏选中一个角色，选择菜单“**统计->策略角色**”， 在右边显示视图中可以查看该角色已分配的对象，包括算机、用户。

字段名称	说明
名称	已分配的计算机、用户的名称；
分组	对应计算机和用户所在的分组；

点击编辑按钮，可以编辑角色属性。

点击导出按钮，可以导出所有角色树下的全部计算机对象和用户对象。

常规

显示该角色的名称以及所在分组，可在此处对该角色设置备注。

计算机用户

在列表中显示该角色分配的计算机和用户。点击添加按钮，即可把该角色分配给此处选中计算机和用户。分配之后，这些计算机和用户会被赋予角色包含的策略集所拥有的策略。点击导出按钮，即可导出所有角色树下的全部计算机对象和用户对象。

策略集

在列表中显示该角色分配的策略集。点击添加按钮，即可把策略集分配给此处选定的角色。分配之后，该角色将带有这些策略集所拥有的策略。

说明　计算机（组）和用户（组）通过策略集或角色分配对象获得的策略，以下统称为计算机（组）角色策略和用户（组）角色策

略。

策略角色功能使用示例

公司内部由于管理需要，需要对不同部门的员工区分资产使用权限，部分资产各部门均可使用，部分资产只有特定的部门方可使用，如实现测试研发部员工禁止使用 U 盘和打印机，销售部员工禁止使用 U 盘，允许使用打印机，则可按照以下步骤进行设置：

1. 建立策略集“禁止使用 U 盘”，以及策略集“禁止使用打印机”；

2. 分别对两个策略集设置指定的策略，如对策略集“禁止使用 U 盘”设置禁止使用全部或指定 U 盘的策略，对策略集“禁止使用打印机”设置禁止使用全部或指定打印机的策略；

3. 按照部门建立角色，如“研发部员工”、“销售部员工”等；

4.将策略集“禁止使用 U 盘”分配给角色“研发部员工”和“销售部员工”；将策略集“禁止使用打印机”分配给角色“研发部员工”.

5. 将角色分配给对应人员的计算机或者用户；

3.5 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。

3.5.1 发送通知消息

当需要对客户端用户发送一些通知消息或下达某些命令时，可以直接通过控制台的发送通知消息功能进行通知。

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。

可以对通知消息进行预设管理。点击  按钮，在弹出的菜单中，可看到预设好的内容，选中的内容会添加到通知内容框。点击菜单中的“管理”，进入预设内容管理界面，可进行添加、删除、修改操作。

说明　　发送通知消息时离线的客户端，下一次连接服务器时会收到

该通知消息。

3.5.2 锁定/解锁计算机

当发现运行客户端模块的计算机有异常举动或有其它原因时，管理员可以将该计算机或多个计算机进行锁定，阻止用户继续使用键盘和鼠标进行操作。

选择菜单“**控制->锁定计算机**”进行锁定。被锁定的计算机将无法再使用键盘和鼠标进行任何操作，只有对它进行解锁，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。

当需要对已锁定的计算机解锁时，选择菜单“**控制->解锁**”进行解锁，目标计算机就可以继续使用键盘和鼠标了。

对于离线的客户端，也可以对其发送锁定命令，则客户端下次连上服务器时会被锁定。

3.5.3 注销用户、关闭/重启计算机

当需要关闭运行客户端模块的计算机，可以使用此项功能。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。当然执行此操作后该客户端模块将退出直到下次重新登录后才会开始运行。

3.6 辅助功能说明

在控制台的使用中，还有一些其它的通用功能，在很多功能模块中都会用到，下面将做简单说明。

3.6.1 导出和导入

数据的导出

控制台上的所有数据视图均可以导出保存为电子文档，包括：统计、日志、策略、即时通讯内容、邮件内容、资产管理等等。部分模块的导出可能会有细微的差别。

导出本页记录

在数据视图中单击右键“**导出->导出本页记录**”只会导出当前页的日志，默认是 20 条记录，管理员可以在控制台“**工具->选项->控制台设置->日志查看**”中修改每页显示的最大记录数；

导出所有满足条件的记录

在数据视图中单击右键“**导出->导出所有满足条件的记录**”会导出所有记录。导出的文档可以保存为 3 种格式：文本文件(.CSV)、HTML 文件、EXCEL 文件（前提是机器安装了 Microsoft 的 Excel 程序）。

策略的导出/导入

只有策略模块提供导入功能，策略的导出/导入是为了方便管理员设置策略。

选择需要导出的策略，单击右键“**导出**”或“**导出选中的策略**”保存为 xml 格式文件，“**导出**”是导出当前所选计算机(组)或用户(组)的当前模块的所有策略，不包括继承的策略。“**导出选中的策略**”只导出其中选中的策略，可以是一条，也可以是多条。

选择需要导入策略的计算机(组)或用户(组)，单击右键“**导入**”选择策略文件导入策略，保存生效。导入的策略必须与当前的策略类型一致，否则无法导入。

3.6.2 打印、打印预览

控制台上的所有数据视图均可打印出来存档，留作日后参考。选择菜单“**文件->打印**”，用户可以将运行统计报告及日志等打印输出，选择“**文件->打印预览**”可以做打印预览。

第四章. 统计

IP-guard 会生成管理人员所关心的公司员工各项应用程序、上网浏览和网络流量的统计报告以及统计图表，以供对员工的工作情况进行评估。

4.1 应用程序统计

应用程序统计提供了强大的统计功能，针对计算机每天的工作情况和应用程序使用的情况进行人性化统计和分析，为管理者评估员工工作效率提供了可靠的依据，并且提供了导出统计列表的功能。

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。应用程序统计界面分 4 块：计算机(用户)树栏、数据显示栏、统计图、查询栏。

功能按钮说明

图标按钮	说明
	模式按钮，管理员可以选择应用程序统计的模式；
	展开按钮，如果应用程序类别有子类，可展开子类；对分项统计，可展开组内计算机或用户。对应用程序明细统计无效，图标变为灰色；
	显示 top 项，定义显示统计列表内容的条数，包括全部、前 10 条、前 20 条、自定义。当按应用程序类别统计设置展开列时，显示 top 项图标为灰色。

在统计中，开机时间和工作时间是系统默认的统计项。开机时间是指客户端机器开机后的运行时间，工作时间是指客户端机器的键盘和鼠标的操作时间。

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。通过统计结果可以知道员工每日的工

作情况，各个部门每日的工作情况等。

单击功能按钮区的模式按钮，选择“**模式->按类别合计**”，默认会统计所有的应用程序类别，统计结果分 3 列显示：

字段名称	说明
类别	应用程序分类中自定义的分类；
时间	客户端机器使用该分类中的应用程序的时间合计，系统默认按使用时间从长到短排列显示；
百分比	该分类中的应用程序使用时间占整个工作时间的百分比，默认是按照从大到小的顺序显示。

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。按应用程序名称统计实际上是按应用程序的进程进行统计，统计出的结果一目了然，清楚的显示出用户大部分的工作时间是使用哪些应用程序，从而知道用户的工作效率。

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。比如用户使用了 2 个不同版本的 QQ 程序，进程却都是 qq.exe，则按明细统计，会分别统计这 2 个不同版本的 QQ，而按名称统计，会把这 2 个版本的使用时间一起统计为 qq.exe。

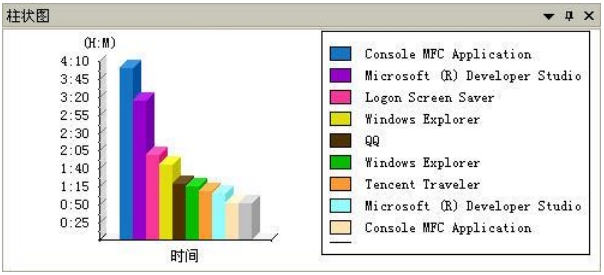
4. 分项统计

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。

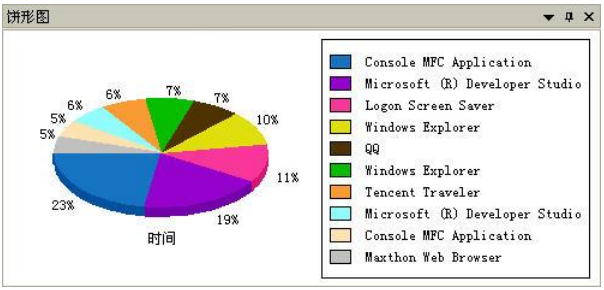
比如需要统计一个计算机组内所有计算机使用 IM、浏览器等分类的使用情况，先选中这个分组，选择统计模式为分项统计，在右边的查询栏中增加应用程序类别：IM、浏览器等预先定义好的应用程序类别，单击【查询】得到统计结果。如该组下还有子组，单击【展开】按钮，查看子组下所有计算机的统计结果。

除了生成统计报表，控制台也会生成统计图表：

柱状图：



饼状图：



4.2 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。

功能按钮说明

图标按钮	说明
	模式按钮，管理员可以选择网站统计的模式。
	展开按钮，对网站明细无效，图标为灰色；如果网站类别包含有子类，可展开子类；对分项统计，可展开组内计算机或用户。
	显示 top 项，定义显示统计列表内容的条数，包括全部、前 10 条、前 20 条、自定义。当按网站类别设置展开列时，显示 top 项图标为灰色。

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。

按类别统计默认统计所有类别的上网时间，不属于任何一个网站分类的网站识别会被自动统计到“未分类”，统计列表默认按上网时间的长短进行排序，浏览网站时间长的排在前面。

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。如果一个网站在网站库中设置了网站名称，会以“网站名称 – 网站”的格式显示，如果没设置网站名称，直接显示该网站域名。

按明细统计时，展开列的功能无效，默认是统计全部网站，也可以单击【显示】按钮选择 Top 项。

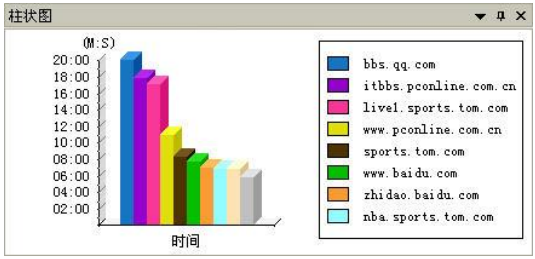
3. 分项统计

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。

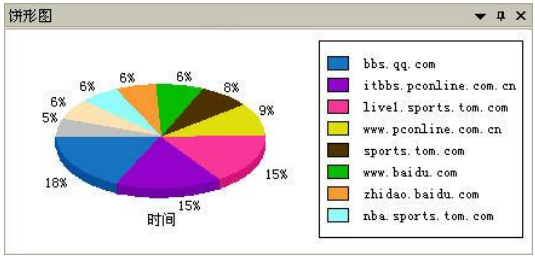
选择需要统计的计算机组，默认统计的是未分类的网站浏览时间，管理员可根据需要在右边查询栏中添加和修改网站分类。单击【展开】按钮，展开所有的子组，显示所有计算机的统计结果。

除了生成统计报表，控制台也会生成统计图表：

柱状图：



饼状图：



4.3 网络流量统计

通过查询网络流量，管理员可以快速定位网络阻塞等问题，从而做出相应的应对措施。网络流量统计包含了通讯双方的网络地址，端口，流量大小等详细信息，以帮助网络管理员查看网络使用状态并排查问题。

选择菜单“**统计->网络流量**”查看网络流量使用情况。

功能按钮说明

图标按钮	说明
	模式按钮，管理员可以选择网络流量统计的模式；
	方向按钮，包括合计、发送、接收三种流量方向；
	展开按钮，选择按计算机统计时有效，可展开组内子组的计算机 ；
	显示 top 项：定义显示统计列表内容的条数，包括全部、前 10 条、前 20 条、自定义。当按网站类别设置展开列时，显示 top 项图标为灰色。

统计条件

字段名称	说明
时间和范围	公共的查询条件
地址范围	地址范围是指通讯对方的 IP 地址，管理员可以在网络地址类别中选择地址范围进行统计，也可以直接在输入框中输入要查询的 IP 地址，如：192.168.1.1 等；
端口范围	是指通讯过程中服务方的端口，管理员可以在端口类别管理中选择端口范围进行统计，也可以直接在输入框中输入要查询的端口，输入端口需加上协议类型：TCP or UDP，如 TCP:139，如果直接输入端口号，系统默认为 TCP。

网络流量统计可分为 6 种模式：

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，从而了解该客户端机器的网络行为。

统计结果包括网络地址及其与该 IP 地址的通讯流量。

字段名称	说明

网络地址	该列会显示所有通讯对方的 IP 地址列表，如果右侧的查询栏->地址范围中指定了一个 IP 地址范围，则只会列出指定 IP 地址范围内的 IP 地址；
全部(合计)	全部表示与该 IP 地址通讯的所有端口的流量，默认还分别统计 TCP(合计)和 UDP(合计)的流量，如果在右侧查询栏->端口范围中指定一个或多个端口类别，则会统计指定端口类别的流量；括号中的“合计”表示流量方向，单击流量方向按钮选择流量方向：合计、发送、接收。

在实际使用中，管理员可根据管理要求设置合适的地址和端口的统计范围，得到需要的网络流量统计图表。

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，如果发现不正当的一些端口流量很大，可以即时采取措施关闭一些非法端口。

统计结果包括端口明细及在该端口的所有流量。

字段名称	说明
网络协议	该列会显示指定的端口范围以及协议类型，统计这些端口的数据流量；
全部(合计)	全部表示所有的 IP 地址范围在这个端口上的流量，系统默认还统计企业网(合计)和互联网(合计)的流量，合计表示流量方向，可以单击流量方向按钮选择流量方向：合计、发送、接收。

在实际使用中，管理员可根据管理要求设置合适的地址和端口的统计范围，得到需要的网络流量统计图表。

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，系统默认统计通讯协议在 TCP 和 UDP 下，通讯地址分别为企业网和互联网的网络流量。

管理员可在右侧的查询栏的地址范围和端口范围中选择其它的类别进行统计。

通过这种统计模式，管理员可以从宏观上分析和比较该计算机(组)在不同网络地址范围内的流量。

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，系统默认统计通讯地址在企业网和互联网中，通讯协议分别为 TCP 和 UDP 的网络流量，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。

通过这种统计模式，管理员可以从宏观上分析和比较该计算机(组)在不同网络端口范围内的流量。

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。通过这种统计模式，管理员可以快速分析和比较计算机(组)之间在指定地址范围的流量不同。

如果是统计计算机组，可单击【展开】按钮展开计算机组内所有计算机，对比组内计算机在指定地址范围内的流量。

管理员可以在右侧的查询栏中更改查询范围以及地址范围，查询到有用的流量统计结果。

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，通过这种统计模式，管理员可以快速分析和对比计算机(组)之间在指定端口的流量不同。

如果是统计计算机组，单击【展开】按钮可以展开计算机组内所有的计算机，对比组内计算机在指定端口的流量。

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。

第五章. 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。

在所有的日志视图中，都可以做以下几种操作：

操作	说明
打印/打印预览	每个日志视图都可以打印保存、打印预览。
导出日志	根据需要导出各种日志。
删除日志	在数据视图中单击右键选择“**删除**”，管理员可根据需要选择一种删除模式：删除选中的记录、删除本页记录、删除所有满足条件的记录。
查询屏幕历史	在查看日志记录的过程中，管理员可以随时查看某条记录的屏幕历史，选择一条日志记录，单击右键“**查看屏幕历史**”会自动打开屏幕历史查看器，并且快速定位到指定日志操作当时的屏幕历史。 没有设置记录屏幕历史的客户端机器无法查询屏幕历史。

5.1 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。

记录的日志操作类型包括以下几种：

操作类型	说明
系统启动/关闭	这里的系统是指客户端系统，因为客户端的启动/关闭和操作系统的启动/关闭对应，也可大致理解为操作系统的启动/关闭；

用户登录	每一个登录到该计算机的用户的登录日志。
用户注销	每一个登录到该计算机的用户的注销日志。
会话连接	使用远程桌面连接与该计算机连接的日志。
会话中断	使用远程桌面连接与该计算机中断的日志。
拨号	当用户拨号连接时，客户端会记录下拨号/挂断日志。
补丁管理	当管理员设置了安装补丁，客户端机器会自动安装补丁，补丁安装的所有日志会记录下来，以方便查询补丁的安装情况。
软件分发	当管理员建立了软件分发任务，会自动在目标计算机上执行，分发任务的执行日志会记录下来，以方便查询分发任务情况。
客户端安装	安装客户端的日志，全新安装客户端会记录新安装的客户端版本信息，覆盖安装客户端会记录安装前后的版本信息；
客户端卸载	卸载客户端的日志，控制台上卸载客户端会记录客户端卸载前的版本信息；
客户端升级	客户端自动升级的日志，记录版本变更情况。
软件卸载	客户端执行软件卸载任务时卸载软件的日志。

基本事件日志包含的内容：操作类型、时间、计算机、用户、描述等信息。操作类型是记录的日志类型，如系统启动、用户登录等，描述该日志的详细信息。

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。

查询条件	说明
时间和范围	通用查询条件。
类型	类型是指基本事件日志的操作类型，默认是全部，也可在下拉框中指定一个或者多个类型进行查询，比如查询客户端机器登录过的用户以及补丁安装情况等。
描述	按照日志记录的描述信息进行查询，这是一个输入字段，支持通配符，也支持模糊查询。

5.2 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。

应用程序日志类型包括：启动/停止、切换窗口、切换标题。

日志类型	说明
启动/停止	记录客户端机器上启动/停止应用程序的情况；
切换窗口	用户切换应用程序时，会记录下切换窗口的日志；
切换标题	用户在使用同一个应用程序时，也可能有多个窗口或多个标题，例如浏览器 maxthon.exe 打开多个标签页互相切换时会记录为切换标题。

注意 由于数据量较大，切换窗口和切换标题默认不记录，您可以通过“**基本策略->日志记录策略**”设置记录窗口标题变化。

应用程序日志记录包含的属性有：操作类型、时间、计算机、用户、应用程序、路径/标题等信息。

属性名称	说明
操作类型	应用程序启动/停止和窗口标题切换；
应用程序	应用程序的进程名称；
文件路径	当操作类型是启动/停止时，记录应用程序在客户端机器上的详细路径；
窗口标题	当操作类型是切换窗口/切换标题时，记录当前的应用程序的窗口标题。

系统默认显示所有的应用程序日志，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。

查询条件	说明
路径/标题	按照应用程序日志的路径或标题来查询；
应用程序	按应用程序的进程名称查询，既可以手工输入名称进行查询，也可以直接在应用程序类别中选择一个类别或一个应用程序进行查询。

按应用程序进行查询包括：手工输入应用程序名称查询、按应用程序分类查询。

1) 手工输入应用程序名称

可直接在输入框中输入需要查询的应用程序名称，例如 qq.exe 或 *game*.exe 等进行查询。

2) 通过应用程序分类

单击右边的“...”按钮打开应用程序分类窗口，左边是应用程序类别，右边是该类别中包含的所有的应用程序。

如果需要查询一个类别，左边选中【应用程序类别】，在右边选择需要查询的应用程序类别，点击【确定】选择该分类进行查询；如果只需要对其中指定的一个应用程序进行查询，左边选中该程序所在的类别找到该程序，在右边选中该程序单击【确定】进行查询。

5.3 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，包括：IE、TT、遨游、Firefox、Netscape 、opera 等。

网页浏览日志包含的内容有：时间、计算机、用户、标题、网址等信息。

属性名称	说明
标题	浏览的网站标题；
网址	浏览的网站的详细网址；

提示 单击右键“**打开网页**”，管理员可以快速链接到选中日志中的浏览网址，以查看该网站的详细信息。

单击右键“**添加到网站类别**”，管理员可以该条日志的网址识别信息添加到指定的网站类别中。

系统默认显示所有的应用程序日志，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。

查询条件	说明

时间和范围	通用查询条件；
网址	按输入的网址查询指定网址的浏览情况，管理员可以直接输入一个网址进行查询，也可以在网站分类中指定一个类别或一个网站识别进行查询。 手工输入网址支持模糊查询。
窗口标题	根据浏览网站的窗口标题查询，如输入“娱乐”查询到所有网站标题包含娱乐的网站浏览日志。

5.4 文档操作日志

文档操作日志记录客户端机器用户对文档的操作信息，管理员通过查看日志记录可以发现用户的文档操作行为，同时为事后追查资料泄密事件提供可靠线索，增强电子文档管理的安全性。

选择菜单“**日志->文档操作日志**”查看文档操作日志，日志记录的内容包括：

属性名称	说明
操作类型	包括：创建、访问、修改、重命名、复制、移动、删除、恢复、上传、下载以及刻录；
源文件	用户操作的文档名称；
文件大小	用户操作的文档的大小；
路径	用户操作的文档的详细路径，当操作类型为复制、移动、重命名时，路径会记录文档的源路径和目的路径；
盘符类型	用户操作的文档所在的盘符类型，包括：硬盘、软盘、光盘、可移动盘、网络盘。 当操作类型为复制、移动时，会显示源和目的盘符类型；
应用程序	操作该文档使用的应用程序进程名称；
标题	操作该文档时的窗口标题。

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。

系统默认显示所有的应用程序日志，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。

查询条件	说明
时间和范围	通用查询条件
文档	
操作类型	默认是全部操作类型，也可通过下拉框选择其中一种或多种操作类型进行查询，比如，查询修改和复制的所有文档；
源	
盘符类型	默认是全部盘符类型，也可通过下拉框中选择其中一种或多种盘符类型进行查询，只查询到指定盘符类型的文档日志；
文件	操作文档的名称； 通过类型查找时，可在给出的默认类型中选择，也可以手动添加类型名称；
路径	操作的文档所在的路径；
目标	只有涉及到有源路径和目标路径的操作，如复制、剪切等，目标盘符类型、文件、路径才有效。
盘符类型	默认是全部盘符类型，也可通过下拉框中选择其中一种或多种盘符类型进行查询，只查询到指定盘符类型的文档日志；
文件	操作文档的名称； 通过类型查找时，可在给出的默认类型中选择，也可以手动添加类型名称；
路径	操作文档所到的目标路径；
大小	指定一个文件大小范围，进行查询，可查询到一定范围大小的文档操作记录；
应用程序	操作文档的应用程序名称，可手工输入名称，也可在应用程序分类中指定一个类别或一个应用程序进行查询；
标题	操作文档的窗口标题；
有备份文档	默认不勾选，查询到所有日志（包括有备份文档和无备份文档），勾选此复选框查询，查询到的日志都有备份文档。

5.5 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。管理员通过查看日志记录可以发现用户的刻录操作行为，同时为事后追查刻录泄密提供审计线索。

选择菜单“**日志->刻录操作日志**”查看刻录操作日志，日志记录的内容包括：

属性名称	说明
操作类型	包括：任务开始、刻录、刻录成功\失败、任务完成； 对于一次包含 N 个文件的刻录操作来说，则会产生以下刻录操作日志： ①一条操作类型为“任务开始”； ②N 条操作类型为“刻录”； ③一条操作类型为“刻录成功（或刻录失败）”； ④一条操作类型为“任务结束”。
光盘名称	刻录的光盘名称；
光盘类型	刻录的光盘类型，CD 或 DVD；
文件大小	刻录的文件大小；
源文件	刻录操作的源文件名称；
应用程序	刻录该文档的应用程序进程名称；
文件总个数	本次刻录的文件的总个数，类型为“刻录”日志为单个文件的刻录，不含有文件总个数；
刻录份数	本次刻录的份数，类型为“刻录”日志为单个文件的刻录，不含有刻录份数。
刻录机描述	刻录机的描述信息；
详细信息	日志的详细信息。

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。

系统默认显示所有的刻录操作日志，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。

查询条件	说明
时间和范围	通用查询条件；
类型	默认是全部类型，也可通过下拉框选择其中一种或多种操作类型进行查询，包括：任务开始、刻录、刻录成功、刻录失败、任务完成；
文件	刻录操作文档的名称； 通过类型查找时，可在给出的默认类型中选择，也可以手动添加类型名称；
路径	刻录操作文档所在的源路径；
大小	指定一个文件大小范围，进行查询，可查询到一定范围大小的文档刻录操作记录；
应用程序	刻录操作的应用程序名称，可手工输入名称，也可在应用程序分类中指定一个类别或一个应用程序进行查询；
光盘名称	刻录的光盘名称；
光盘类型	默认是全部类型，可选包括：CD、DVD；
刻录机描述	刻录机的描述信息；
文件总个数	本次刻录的文件的总个数；
刻录份数	本次刻录的份数。

5.6 共享文档操作日志

共享文档操作日志记录的是客户端机器上的共享文档被其它机器的用户操作的日志，通过查看这些日志，管理员可以知道外来计算机对本地的文档做了哪些操作。

选择菜单“日志->共享操作”查看共享文档操作日志记录。

共享文档日志包括的内容有：

属性名称	说明
操作类型	包括：创建、重命名、修改、删除。访问、复制和移动的操作暂不支持。
远程主机	是指访问本机共享文件的外来计算机的 IP 地址；
源文件	是指远程计算机操作的本地文档的名称；
路径	是指远程计算机操作的本地文档的详细路径。

共享文档日志可以按以下条件进行查询

查询条件	说明
时间和范围	通用查询条件；
共享文档	
操作类型	根据共享文档操作类型进行查询，默认是全部，也可在下拉框中选择其中一种或多种操作类型进行查询；
源	
文件	查询远程机器对指定的文档进行了哪些操作，输入要查询的文档名称，支持模糊查询；
路径	远程操作文档的路径；
目标	只有共享文件重命名时，目标文件和路径才有效果
文件	操作文档的名称；
路径	操作文档所到的目标路径；
名称	查询远程机器对指定的文档进行了哪些操作，输入要查询的文档名称，支持模糊查询；
远端地址或名称	按照访问本机共享的远程计算机的 IP 地址或计算机名称进行查询。

5.7 远程桌面日志

远程桌面日志是记录客户端连接远程桌面的操作。管理员通过查看日志记录可以发现用户的远程操作行为。远程桌面日志默认不记录，需要在“**策略->日志记录**”中添加策略来启用记录。

管理员需要有“**工具->账户->功能权限->日志->远程桌面日志**”的功能权限，才能查看客户端的远程桌面日志。

选择菜单“**日志->远程桌面日志**”查看远程操作日志，日志记录的内容包括：

属性名称	说明
操作类型	包括：连接、断开、远程创建、远程访问、远程复制到本地、本地复制到远程、远程复制到映射盘、远程修改、远程重命名、远程删除；
网络地址	客户端使用远程桌面连接到的主机的网络地址；

远程主机	客户端使用远程桌面连接到的主机的 IP 及计算机名；
源文件	用户远程操作的文档名称；
文件类型	用户远程操作的文档类型；
文件大小	用户远程操作的文档的大小；
路径	用户远程操作的文档的详细路径；
应用程序	远程操作该文档使用的应用程序进程名称；
标题	远程操作该文档时的窗口标题。

远程操作类型属性说明：

类型名称	说明
连接	记录客户端使用远程桌面连接到某一主机上的操作。
断开	记录客户端断开与某一主机的远程桌面的操作。
远程创建	记录远程桌面通过磁盘映射方式在本地客户端上中创建文档的操作。
远程访问	记录远程桌面通过磁盘映射方式在本地客户端中访问文档的操作。
远程复制到本地	记录远程桌面通过复制、剪切将文档直接复制到本地客户端机器的操作。
本地复制到远程	记录本地客户端机器通过复制、剪切将文档直接复制到远程桌面的操作。
远程复制到映射盘	记录远程桌面通过磁盘映射方式复制、剪切文档到本地客户端的操作。
远程修改	记录远程桌面通过磁盘映射方式在本地客户端修改文档的操作。
远程重命名	记录远程桌面通过磁盘映射方式在本地客户端重命名文档的操作。
远程删除	记录远程桌面通过磁盘映射方式在本地客户端删除文档的操作。

5.8 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。

打印日志记录包括的内容有：

属性名称	说明
打印机类型	包括：本地、共享、网络和虚拟打印机。
打印任务	打印任务记录了打印日志的核心内容，通常包含了打印的文档名称；
打印机名称	打印时所用的打印机的名称；
打印页数	打印出来的文档页数；
记录页数	打印的一份文档的页数；
标题	执行打印操作时的窗口标题；
应用程序	执行打印操作的应用程序名称。

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**”。

单击【副本】按钮，选择“**查看打印记录**”打开打印内容查看器。可以放大、缩小、拖动进行查看，在有多页打印内容时，可以翻页查看，可以将图片另存为 JPG 格式保存。

单击【副本】按钮，选择“**保存打印记录**”可将打印内容保存到指定的目录。打印内容是以图片格式保存的，每页都会保存为一个 JPG 文件，如果一个打印任务有多页内容，会保存为多个图片文件。打印内容也支持批量导出，右键菜单“**导出内容**”可导出指定或是全部记录的内容。

文档打印日志可以按以下条件进行查询：

查询条件	说明
时间和范围	通用查询条件；
打印机类型	默认是全部，也可在下拉框中选择其中一种打印类型，只查询一种打印机类型的打印情况；

打印机	根据打印机的名称进行查询，方便对指定的打印机进行打印情况的统计；
计算机	是指打印机所在的计算机，假如是本地打印机，则计算机就是本机的计算机名称，如果是共享打印机，则是远程计算机即打印机所在的计算机，一般是 IP 地址；
任务名称	根据打印任务进行查询，可查询指定文档的打印情况，支持模糊查询；
页数	根据打印页数查询，方便统计滥用打印机的情况；
应用程序	根据打印时的应用程序进行查询，查询指定格式的文档的打印情况。
标题	根据执行打印操作时的窗口标题进行查询；
有打印记录	默认不选择，代表全部；如果选择该项查询，则表示查询有打印记录的打印日志。

5.9 移动存储操作日志

移动存储日志记录了客户端机器上所有移动存储设备的插入拔出情况，对其在网络内的使用情况进行全面监控和记录，提高文档保密的安全性。

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，内容包括：

属性名称	说明
操作类型	移动盘相关的操作，包括：插上、拔出、创建、复制到、移动到、重命名、恢复、删除、访问、修改、上传、下载、刻录、复制出、移动出、启动 XExplore、关闭 XExplore、升级成功、升级失败；
网络地址	使用可移动设备的客户端 IP 地址；
移动存储分类	移动盘所属的移动存储分类；
移动存储类型	移动盘的类型，分别为加密盘，非加密盘，安全 U 盘；
UDiskID	每一个可移动设备都有一个 UDiskID，UDiskID 是一个移动存储设备的唯一标识信息，格式化也不会发生改变；
卷序列号	每一个可移动设备都有一个序列号，格式化后卷序列号可能发生改变。

设备描述	对这个移动存储的描述信息。
卷标	移动存储盘的卷标。
源文件	移动存储操作的源文件名称。
文件类型	移动存储操作的文件类型。
路径	移动存储操作的文件路径，如果文件位置发生变化会显示为“**源路径->目标路径**”
磁盘类型	本次操作的移动存储磁盘类型，分为：硬盘，光盘，软盘，可移动盘。
应用程序	执行操作时的应用程序名称。
标题	执行操作时的应用程序的窗口标题。
备注信息	为了方便查看和区分移动盘，可以添加一些注释信息，默认为空，单击右键“**修改备注**”输入备注信息，比如：使用者，资产编号等。
设备名称	移动存储设备的名称信息；
设备编号	移动存储设备的编号信息；
部门	移动存储设备所属部门信息；
设备使用人	移动存储设备的使用人名称；
职位信息	移动存储设备的使用人的职位信息；
联系方式	移动存储设备的使用人的联系方式信息；
主机信息	仅针对对安全 U 盘交互区操作日志，若上传安全 U 盘交互区的机器是台非客户端，则主机信息中会记录该台非客户端机器的 IP 地址，其他情况为空。；

移动存储操作日志可以按以下查询条件进行查询：

查询条件	说明
时间和范围	通用查询条件；
移动存储	
移动存储	在移动存储分类中指定一个分类或一个移动盘进行查询；
移动存储操作类型	默认是全部，也可在下拉列表中选择插上或拔出进行查询，可以快速查询客户端机器所有插入过的移动盘日志；

移动存储类型	按是否加密盘来查询，默认为全部，可以在下拉列表中选择加密盘或非加密盘进行查询；
文档源	
盘符类型	默认是全部盘符类型，也可通过下拉框中选择其中一种或多种盘符类型进行查询，只查询到指定盘符类型的移动存储日志；
文件	操作文档的名称； 通过类型查找时，可在给出的默认类型中选择，也可以手动添加类型名称；
路径	操作的文档所在的路径；
目标	只有涉及到有源路径和目标路径的操作，如复制、剪切等，目标盘符类型、文件、路径才有效。
盘符类型	默认是全部盘符类型，也可通过下拉框中选择其中一种或多种盘符类型进行查询，只查询到指定盘符类型的移动存储日志；
文件	操作文档的名称； 通过类型查找时，可在给出的默认类型中选择，也可以手动添加类型名称；
路径	操作文档所到的目标路径；
大小	指定一个文件大小范围，进行查询，可查询到一定范围大小的文档操作记录；
应用程序	根据应用程序名称进行查询，可手工输入名称，也可在应用程序分类中指定一个类别或一个应用程序进行查询；
标题	根据执行操作时的应用程序的窗口标题进行查询，默认为空，代表查询所有标题内容；
注册信息	
设备名称	根据注册时对移动盘备注的设备名称进行查询；
设备编号	根据注册时对移动盘备注的设备编号进行查询；
所属部门	根据注册时对移动盘备注的所属部门进行查询；
设备使用人	根据注册时对移动盘备注的设备使用人进行查询；
职位信息	根据注册时对移动盘备注的职位信息进行查询；
联系方式	根据注册时对移动盘备注的联系方式进行查询；

5.10 资产变更日志

资产变更日志记录的是客户端机器上硬件和软件的变化情况，以帮助管理员维护和管理企业内的资产信息。

选择“**日志->资产变更**”查看所有软硬件的变化日志，包括：

属性名称	说明
操作类型	资产的增加、删除、变化；
类型	属于硬件变更还是软件变更；
描述	对发生变化的资产的描述信息。

资产变更日志可以按以下条件进行查询：

查询条件	说明
类型	按照资产类型查询，查询到所有的硬件变更或软件变更，方便管理员分别查看这 2 种资产的变化情况；
操作类型	变更的方式，管理员可查询到增加的资产、删除的资产以及变化的资产；
描述	根据资产的描述信息进行查询，查询资产的变更情况。

5.11 Windows 系统日志

Windows 日志会记录客户端的系统事件日志情况，以方便日后查询客户端的系统日志。Windows 系统日志默认不记录，需要在“**策略->日志记录**”中添加策略来启用记录。

管理员需要有“**工具->账户->功能权限->日志->Windows 系统日志**”的功能权限，才能查看客户端的 Windows 系统日志。

选择“**日志->windows 系统日志**”可查看到策略日志，包括：

属性名称	说明
类型	系统日志的类型，包括：应用程序、安全、系统；
来源	系统日志的事件来源，不支持模糊查询；

记录数	系统日志的记录数；
事件 ID	系统日志的事件 ID，不支持模糊查询；
级别	系统日志的级别情况，包括：关键字、警告、详细、错误和信息。
关键字	系统日志的关键字；
任务类别	系统日志的任务类别，不支持模糊查询；
详细内容	系统日志的详细描述内容；

注意 1.设置策略后在 windows 系统日志中只能查看到最近 5 天的日志；

2.“关键字”只能获取显示审核成功、审核失败、经典，其他值显示为空。

5.12 策略日志

策略日志会记录所有客户端机器触发的策略日志，以方便日后查询员工的操作行为。

选择“**日志->策略日志**”可查看到策略日志，包括：

属性名称	说明
报警级别	报警级别有 3 种：低、重要、严重，管理员在设置策略的时候可以选择报警的级别；
涉及策略	客户端机器的操作触发的策略类型；
描述	客户端机器的操作行为以及触发的策略描述。

策略日志可以按以下条件进行查询：

字段名称	说明
最低级别	默认是全部，查询到所有报警级别的日志，如果选择低，则查询低、重要、严重的日志；选择重要，只查询重要和严重的日志；
策略类型	默认是全部，也可指定其中一种策略类型进行查询，只查询该策略的日志；
内容	根据描述内容进行查询，支持模糊查询。

5.13 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。

系统事件日志包括的内容有：

属性名称	说明
类型	包括：系统状态、系统设置、邮件报告、客户端冲突、发现新客户端、客户端前期检查、客户端管理信息、补丁下载信息。
描述	对应类型事件的现象描述；

注意 客户端连不上服务器或通讯不正常时，可查看系统事件日志，以便发现错误原因。

第六章. 策略

6.1 策略简介

管理员可以通过策略限制客户端对计算机和网络的使用，有效规范员工的电脑使用，提高生产效率。

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“**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。

策略的图标按钮说明

图标按钮	说明
	新建，点击该按钮新增加一条策略；
	上移，将选中的策略上移一个位置；
	下移，将选中的策略下移一个位置；
	删除，点击该按钮删除选中的策略；
	恢复，取消新建或修改策略时点击该按钮；
	保存，设置或修改策略后需保存才会生效。
	表示该策略的模式是“允许”；
	表示该策略的模式是“禁止”；
	表示该策略的模式是“忽略”；
	表示该策略的模式是“不操作”；
	表示该策略设置了报警；
	表示该策略设置了警告；
	表示该策略设置了锁定计算机；
	表示该策略设置了到期时间。

6.2 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。

基本策略主要是通过修改注册表值来实现的。基本策略和设备控制策略与其他的策略不同，是一种状态维持的策略，而不是实时的触发策略；因此对策略的

修改，删除等处理和其他的策略不同。

基本策略支持的项目包括：控制面板，计算机管理，系统，网络，IP/MAC 绑定，ActiveX 控件。

控制面板包括以下 5 项：

基本策略项	说明
控制面板	包括控制面板上的各个功能；
设置屏幕属性	限制客户端设置桌面，屏幕保护程序以及桌面外观等；
添加打印机	限制客户端添加打印机；
删除打印机	限制客户端删除打印机；
快速切换用户	禁止在 Windows 系统里通过切换用户的方式同时登录多个用户（仅 XP 系统有效）；
修改计算机名称	禁止客户端修改计算机名称。

计算机管理包括以下 5 项：

基本策略项	说明
设备管理器	限制客户端机器使用设备管理器；
磁盘管理	限制客户端机器使用磁盘管理；
本地用户和组	限制客户端机器使用本地用户和组的控制面板管理项；
系统服务管理	限制客户端机器使用系统服务管理；
其它计算机管理	限制包括：电脑管理、事件查看器、磁盘碎片整理和共享文件夹。

系统包括以下 5 项：

基本策略项	说明
任务管理器	限制客户端使用任务管理器；
注册表编辑器	限制客户端使用注册表；
命令提示符	限制客户端使用命令提示符，9x 系统下是 command 程序，NT 及以后版本操作系统下是 cmd 程序；
运行注册表中 Run 下的程序	如果模式为禁止，Run 下的程序会在系统开机的时候不会启动，需注销或重启计算机生效；

运行注册表中 RunOnce 下的程序	RunOnce 是指在开机的时候启动一次，下次开机就不会运行了，如果模式为禁止，则 RunOnce 下的程序不会启动，需注销或重启计算机生效。

网络包括以下 6 项：

基本策略项	说明
修改网络属性	限制客户端修改网络属性；
显示“网络邻居”	模式为禁止时，桌面上的网上邻居会隐藏，需要注销或重启生效；
修改 Internet 选项	限制客户端修改 Internet 选项设置；
默认网络共享	如果模式为禁止，客户端上的默认共享被禁止；
使用网络共享	如果模式为禁止，客户端不能共享本机文档；
增加网络共享	如果模式为禁止，客户端新增的网络共享会被禁止。

IP/MAC 绑定

基本策略项	说明
修改网络 IP/MAC 配置	限制客户端修改网络属性； 为了禁止用户随意修改 IP，可使用该功能禁止修改网络 IP/MAC 配置。设置策略后，客户端会保存当前的 IP 和 MAC 信息，一旦发现用户有修改，立即会改回保存的 IP/MAC。 如果用户需要修改 IP，需要先去掉该策略。

ActiveX 控件包括以下 4 种控件：

基本策略项	说明
聊天类 ActiveX 控件	限制客户端使用聊天类 ActiveX 控件，用户使用聊天控件时会被禁止；
影音类 ActiveX 控件	限制客户端使用影音类 ActiveX 控件，一般在互联网上听歌或看视频文件会用到该类控件，禁止该项，用户无法听歌或播放视频；
游戏类 ActiveX 控件	互联网上的一些小游戏可能需要安装游戏类控件，禁止该项，此类小游戏无法正常运行；
FLASH 类 ActiveX 控件	播放 FLASH 文件会用到该类控件，禁止该项，FLASH 文件无法正常播放。

其它

基本策略项	说明
系统还原	为了防止客户端机器通过系统还原来卸载客户端，可以禁止该项，则系统还原功能被禁止。
使用 Print Screen 键复制屏幕	为了防止客户端机器通过使用 Print Screen 键复制屏幕，发现泄密风险，可以禁止该项，则 Print Screen 键无法使用
Windows 自动更新	禁止该项，则 Windows 自动更新功能被禁止；

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。

6.3 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。

设备控制策略支持的设备列表包括：存储设备、通讯接口设备、拨号、USB 设备、网络设备、其它设备。

存储设备包括：

设备类型	说明
软盘驱动器	软盘驱动器，禁止该项，则软驱也被禁止；
光盘驱动器	DVD/CD-ROM 驱动器；
光盘刻录机	对光盘刻录行为做控制；
磁带驱动器	对磁带驱动器做控制；
可移动设备	除硬盘（ide、scsi、sata 接口）外的存储设备，包括 U 盘，移动硬盘，记忆棒，智能卡，MO，Zip；
非系统驱动器	系统盘所在驱动器之外的驱动器；
便携设备	如智能手机。

光盘刻录主要指刻录工具，可控制其进行刻录操作。支持控制的刻录工具包括:

设备类型	说明
专用刻录工具	IP-guard 专用刻录工具；
其他刻录工具	IP-guard 专用刻录工具之外的其他刻录工具。

移动智能终端主要指智能手机，可控制其接入客户端机器，支持控制的接入方式包括：

设备类型	说明
以便携设备方式访问	移动智能终端接入时选择以便携设备方式访问；
以 U 盘存储方式访问	移动智能终端接入时选择以 U 盘存储方式访问（部分设备可能称为以大容量存储方式访问）；
用手机助手访问	移动智能终端使用第三方手机助手软件接入。

通讯接口设备包括：

设备类型	说明
串口	COM 端口；
并口	LPT 端口；
USB 控制器和连接器	通用串行总线控制器和连接器（HUB）；
SCSI 接口	scsi 和 raid 控制器，scsi 硬盘会用到该接口；
1394 控制器	IEEE 1394 总线主控制器，1394 接口，通俗的说就是 1394 插槽，同 USB 控制；
红外线	红外线设备；

PCMICA 卡	一个 PCMCIA 接口，通俗的说就是 PCMCIA 插槽，同 USB 控制器；
蓝牙设备	蓝牙设备；
MODEM	拨号设备；
直接电缆连接	用 usb 线、com 口对连线或并口对连线直接把两台计算机连接起来的行为。

蓝牙设备包括：

设备类型	说明
蓝牙鼠标	控制蓝牙鼠标的使用
蓝牙耳机	控制蓝牙耳机的使用；
蓝牙文件传送	控制通过蓝牙设备传送文件。

拨号包括：

设备类型	说明
拨号连接	对拨号连接做控制。

USB 设备包括：

设备类型	说明
USB 键盘	控制 USB 键盘的使用；
USB 鼠标	控制 USB 鼠标的使用；
USB Modem	控制 USB Modem 的使用；
USB 映像设备	控制 USB 接口的摄像头、扫描仪、数码相机；
USB CDROM	控制 USB 接口的 CDROM；
USB 存储	控制 USB 接口的存储设备；
USB 硬盘	控制 USB 硬盘的使用；
USB 网卡	控制 USB 网卡的使用；
USB 其他设备	控制非以上 USB 接口的其它设备。

网络设备包括：

设备类型	说明
无线网卡	控制无线网卡的使用；

PnP 网卡(USB，PCMICA)	可热插拔的网卡；
虚拟网卡	非物理连接主板或非主板自带的网卡。

其它设备包括：

设备类型	说明
声音设备	声音、视频和游戏控制器；
虚拟光驱	控制虚拟光驱的使用；
无线网络	控制对指定无线网络的访问，通过设备描述来指定具体的网络，不填设备描述则代表所有的无线网络。 设备描述信息格式为：SSID=无线网络名| BSSID=网络地址。SSID 和 BSSID 可只写一个，也可同时写。支持通配符，多个网络设备描述以分号隔开。 如：SSID=teclink_11|BSSID=aa-77-dd-00-88; SSID=teclink_10; BSSID=aa-ee-dd-00-88;
任何新设备	任何一个插入计算机的新设备，如果模式为禁止，所有的新插入的设备都被禁用。

策略示例 1

在一些企业，上班时间不允许听歌、视频等行为，此时可以设置设备控制策略禁止声音设备。

策略：时间范围选择工作时间”，模式选择禁止，在设备列表中勾选“声音设备”，则设置了该策略的计算机的声卡被禁用。

策略示例 2

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。

策略示例 3

一些企业由于管理上的需要，只允许员工使用公司内部的无线网络，不允许使用其他无线网络，此时可设置策略禁止连接到这些无线网络。

策略：模式选择“禁止”，在设备列表中的勾选无线网络，在设备描述中填入该无线网络的信息，如：

SSID=teclink_11|BSSID=aa-77-dd-00-88;SSID=teclink_10;BSSID=aa-ee-dd-00-88

设置成功后，则客户端无法连接①无线网络名为 teclink_11 同时 AP 网络地址为 aa-77-dd-00-88 的无线网络②无线网络名为 teclink_11 的无线网络③AP 网络地址为 aa-ee-dd-00-88 的无线网络。

6.4 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。

6.5 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。在应用程序项中直接添加应用程序或指定一个应用程序类别进行控制，设置后使用对应的应用程序访问指定网站会受到控制。

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。

6.6 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。

策略的属性包括：

策略属性名称	说明
应用程序	设置需要记录的应用程序，默认是<全部>，可以指定管理员关心的应用程序进行记录；
时间间隔	设置记录屏幕快照的时间间隔，默认是 15s，也就是说每隔 15s 截一次屏幕。时间间隔的有效范围是 1-99999，只有在【记录】模式下有效。

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。

注意 屏幕记录的时间间隔越小，产生的数据量越大，管理员需要根据实际需要适当的调节屏幕记录的时间间隔。

6.7 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、windows 系统日志和远程桌面日志。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、windows 系统日志和远程桌面日志不记录，其它所有日志都默认记录。

假如您需要不记录一些日志，可以添加一条策略，设置为不记录，勾选不需记录的日志项，保存策略即可。

日志记录项	说明

日志记录项	说明
系统启动/关闭	基本事件日志中的系统启动或关闭日志；
用户登录/注销	基本事件日志中的用户登录或注销日志；
拨号	基本事件日志中的拨号日志；
策略控制	策略报警日志；
硬件变更	资产变更日志中的硬件变化日志；
软件变更	资产变更日志中的软件变化日志；
Windows 系统日志	Windows 系统日志默认是不记录的，可以添加策略设置记录该项。
类别	记录系统日志的类别，包括：应用程序、安全、系统。
级别	记录系统日志的级别，包括：关键字、警告、详细、错误和信息。
应用程序	应用程序日志可以针对指定的应用程序设置为记录或不记录，也可针对有可视窗口的应用程序进行设置。
仅可见窗口	是指有前台窗口的应用程序。
应用程序	管理员可以手工指定应用程序，也可以在应用程序分类中选择类别，支持通配符。
窗口标题变化	窗口标题变化默认是不记录的，可以添加策略设置记录该项，并可以对指定的应用程序进行记录。
应用程序	管理员指定窗口标题变化的应用程序名称，可手工输入，也可在应用程序分类中选择类别，支持通配符。
网页浏览	管理员可以设置不记录网页浏览日志，并且针对指定的网站记录或不记录。
网站	手工输入网站地址，支持通配符，也可以预先在网站分类中分好类别，选择网站类别。
文档操作	文档操作日志，管理员可以设置不记录某些文档日志，确保记录下来的日志是有用的。
盘符类型	包括：硬盘、软盘、光盘、可移动盘、网络盘和未知盘符。比如可以设置不记录硬盘上的文档日志。
文件名称	设置需要记录或不记录的文件名称，支持通配符，比如设置不记录*.txt；*.log 等。
应用程序	指定文档操作的应用程序。
打印操作	客户端的文档打印日志
打印机类型	选择需要记录或不记录的打印机类型。
应用程序	设置打印文档时的应用程序。
共享文档	共享文档操作日志

日志记录项	说明
文件名称	共享操作的文档名称，支持通配符。
网络地址范围	远程访问该客户端共享文档的计算机 IP 地址范围，管理员可以针对性的设置不记录部分机器的访问记录。
远程桌面日志	记录客户端连接远程桌面的操作日志。远程桌面日志默认是不记录的，可以添加策略设置记录该项。
类型	选择需要记录或不记录的远程操作类型。包括：连接、断开、远程创建、远程访问、远程复制到本地、本地复制到远程、远程复制到映射盘、远程修改、远程重命名、远程删除。
邮件	邮件内容，对于不想记录下来的邮件类型，可以设置不记录某些邮件。
邮件类型	选择邮件的类型，普通邮件、网页邮件、Exchange 邮件、Lotus 邮件。
发送/接收	选择邮件的方向，发送或接收。
发件人	设置邮件的发件人的地址，支持通配符，则发件人符合的邮件会根据策略去记录或不记录。
收件人	设置邮件的收件人的地址，支持通配符。
仅匹配一个收件人	勾选此项时，只要有一个收件人存在于设置的收件人中，都能匹配策略。 不勾选此项，则需要所有的收件人都存在于设置的收件人中，才能匹配策略。
邮件大小（>=KB）	邮件大小>=该值的邮件被记录或不记录
不记录附件	只有在策略模式为“记录”时有效，如果勾选该项，则邮件的附件不会被记录，在控制台上显示是带有附件的，只是无法查看和保存其内容。
不记录正文	只有在策略模式为“记录”时有效，如果勾选该项，则邮件的正文不会被记录，在控制台上无法查看邮件内容。
即时通讯	即时通讯内容，管理员可以根据需要设置记录其中的一些聊天工具的内容。
聊天工具	选择聊天工具。
不记录内容	只有在策略模式为“记录”时有效，如果勾选该项，则聊天的内容不会被记录，在控制台上无法查看聊天内容。
移动存储	移动存储的文档操作日志内容

日志记录项	说明
移动存储类型	选择移动存储类型，有加密盘和非加密盘可选。
应用程序统计	应用程序统计数据。
网页浏览统计	网页浏览统计数据。
网络流量统计	网络流量统计数据。

6.8 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：

策略属性名称	说明
需要强制确认	此项只有在策略模式为【允许】时有效。勾选此项，表示只能通过用户授权的方式进行远程控制；不勾选此项，表示可以通过用户授权和密码授权这 2 种方式进行远程控制。 关于这 2 种授权方式可参照后面的“**维护->远程控制**”。
管理员名称	对登录当前控制台的管理员用户进行控制。比如：可以限制某些管理员用户对指定客户端机器的远程控制方式，需要强制确认。管理员账户在“**工具->账户**”中设置。
控制台 IP 地址	对当前控制台所在计算机的 IP 地址范围进行控制。比如： 限制一个 IP 范围内的所有计算机通过登录 IP-guard 控制台使用远程控制功能。 如果输入是 0.0.0.1-255.255.255.255，或什么也不输入，或不是有效 IP 地址段，会认为是所有的 IP 地址，用<全部>表示。
控制台名称	对登录控制台的计算机名称进行控制。

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。

6.9 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。

新建一条策略，在提供的关键字中选择目标功能，确定后在右边的属性栏中根据要求设置相应的值，备注内容为选填，最后保存。若指定的功能尚未包含于已有的类别关键字中，可在创建策略时选择类别为“自定义”，关键字中输入指定功能代表的名称，确定后在右边的属性栏中的“内容”中输入对应的值。

注意 1.客户端配置策略中的各策略互相独立；
2.客户端配置策略涉及到的功能点较多，尚未包含于已有的类别关键字中功能及其对应值，请咨询我们的售后技术人员。

6.10 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，方便管理员及时发现网络内计算机的变化，并做出应对措施，增加局域网内计算机的可维护性。

系统报警策略支持的报警项包括：

系统报警项	说明
硬件变化	硬件资产中任意一个资产的变化都会报警，方便管理员对网络内计算机硬件资产的维护；
锁定计算机	勾选此项，则硬件发生变化时，会锁定计算机
插入设备	插入计算机外部设备的报警，会记录该设备的名称；
拔出设备	拔出计算机外部设备的报警，与插入对应；
插入存储设备	对存储设备的使用情况报警，会记录存储设备的名称，提醒管理员，防止使用非法外来存储设备；
拔出存储设备	跟插入存储设备报警对应；
插入通讯设备	对计算机通讯设备的使用报警，会记录通讯设备的名称，以提醒管理员，防止使用非法外来通讯设备；

系统报警项	说明
拔出通讯设备	跟插入通讯设备报警对应；

系统报警项	说明
软件变化	软件资产的增加、删除、变化，方便管理员对网络内计算机软件资产的维护；
系统服务变化	客户端机器的系统服务的增加和删除报警，帮助管理员查找病毒或系统问题；
启动项变化	客户端机器的系统启动项的增加、删除和变更报警，协助管理员查找病毒或系统问题；
系统时钟改变	客户端机器的系统时钟的变化；
计算机名称变化	客户端的计算机名称更改报警，提醒管理员，阻止客户端的非法操作；
网络配置变化	客户端机器的网络属性的变化，帮助管理员发现网络问题。
磁盘空间不足	客户端机器的系统盘空间不足，可设置报警时的空间剩余量；
磁盘通电异常	客户端机器的磁盘通电次数出现异常，帮助管理员发现私拆硬盘使用的问题。

系统报警的内容包括报警类型以及具体的描述信息，帮助管理员快速定位问题发生的位置并很好的解决问题。

6.11 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，避免部分机器任意的使用网络资源造成网络堵塞，影响整个企业内的正常工作，同时也可以限制指定端口的流量，禁止员工的任意下载行为。

网络流量策略只对计算机有效，对用户无效。策略属性包括：

策略属性名称	说明
网络地址范围	设置通讯对方的 IP 地址范围。默认地址范围是{全部}，可以手工逐个添加，也可以在网络地址分类中指定类别，指定的类别用{...}表示；

端口范围	设置通讯中用到的端口范围。默认端口范围是{全部}，包括：TCP：0-65535；UDP：0-65535；ICMP。可以手工添加端口或端口范围，也可以在端口分类中指定端口类别，用{…}表示。 输入自定义端口时要在前面加上“TCP：”或“UDP：”来区分 TCP 端口和 UDP 端口，如果不加，则认为是 TCP 端口。
流量方向	通讯过程中的网络流量方向，由客户端机器到对方计算机的流量为发送流量，反之为接收流量。发送流量+接收流量=合计流量；
限制速度	设置流量的限制大小，单位是 KB/s，模式为不限流量时不可用。

如果策略模式为限制流量，则当客户端在指定 IP 范围，指定端口范围和指定的方向的流量超过设置的限制速度时，客户端便会暂停下载/上传，直到平均流量低于指定值，从而达到限制流量的目的。

如果策略模式为忽略，但没有设置任何动作，则限制速度的属性无效，如果设置了动作（报警，警告，锁定计算机），当客户端在指定 IP 范围，指定端口范围和指定的方向的流量超过设置的限制速度时，便会触发所设的动作，但是不会限制该流量。

策略示例 1

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。

策略示例 2

通过流量控制策略，也可以禁止客户端机器与指定 IP 或指定端口之间的通讯，假如需要禁止 FTP 下载，可以设置策略：模式选择“限制流量”，IP 地址范围可以是{全部}，设置端口为 TCP:21，限制速度为 0KB/s。

6.12 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，防止病毒入侵，保护内网安全。

网络控制策略是针对计算机的，在用户模式下无效。策略属性包括：

策略属性名称	说明
通讯方向	有双向，出站和入站三种(是指物理上的通讯方向)。出站和入站是相对于客户端机器来说的，也就是客户端机器主动连接其他计算机，即为出站。
端口范围	与流量控制策略中的端口范围含义相同。
网络地址范围	与流量控制策略中的网络地址范围含义相同。
对方是客户端	判断通讯对方机器是不是客户端计算机，只有勾选了该项，下面的属性才有效。如果不勾选，则表示不判断对方是否客户端。
属于相同分组	对于属于相同分组的客户端机器之间的通讯做控制，这里的相同分组是指当前设置策略的客户端机器所在的分组，不包含子组，也不包含上一层的分组；
属于指定分组	对于指定分组的计算机之间的通讯做控制，分组的指定在下面“所属分组”中设置，只有勾选了该项，“所属分组”才有效；
所属分组	指定通讯对方计算机所属的分组，只有指定了分组，才能选择“包含子组”；
包含子组	选择是否包含指定分组中的子组；
应用程序	指定网络访问的应用程序。

策略示例 1

为了保护内网安全，企业需要禁止一些恶意端口或下载端口，可以通过网络控制策略来实现。

策略：选择模式为“禁止”，设置需要阻断的地址范围，设置需要禁止的端口，如：80 端口，21 端口等。如果设置了 80 端口，则客户端机器无法访问网页，如果设置了 21 端口，则客户端机器无法使用 FTP 下载。

策略示例 2

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。

策略示例 3

在实际运用中，网络控制策略也可以和接入检测策略结合起来使用，防止外来的计算机和内部的计算机通讯。

对于网内安装了客户端的计算机，可以设置网络控制策略，只允许与企业内的计算机通讯，这样外来的计算机就无法访问设置了该策略的客户端机器。

对于网内没有安装客户端的计算机，管理员可以在接入检测中，设置这部分机器为“保护”，并启动接入控制功能，这样外来的计算机将被视为“非法”的计算机，不能与这部分“保护”的计算机通讯。

6.13 邮件控制策略

邮件控制策略是为了防止企业内部重要资料通过邮件的方式泄露出去，在不影响员工正常使用邮件的前提下规范邮件的发送内容，保障企业的内部资料安全。

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：

策略属性名称	说明
发件人	对发件人的邮箱地址做控制，支持通配符，支持输入多个，以“,”“;”作为分隔符；
收件人	对收件人的邮箱地址做控制，收件人也包括抄送人和密送人的邮件地址，输入规则同“发件人”；
仅匹配一个收件人	勾选此项时，只要有一个收件人存在于设置的收件人中，都能匹配策略。 不勾选此项，则需要所有的收件人都存在于设置的收件人中，才能匹配策略。

主题	对发送邮件的主题名称进行控制，输入规则同“发件人”；
包含附件	对发送的邮件是否包含附件做控制。勾选此项，只对包含附件的邮件做控制；不勾选此项，对所有满足条件的邮件做控制(包含附件和不包含附件)；
附件名称	如果勾选了“包含附件”，可以在这里输入附件名称，对指定附件名称进行控制，输入规则同“发件人”；
邮件大小(>=KB)	对发送的邮件大小进行控制，默认是 0，也就是全部，输入要控制的邮件大小，则>=输入值的邮件受控制

策略示例 1

为了防止企业内计算机通过邮件的方式将内部机密资料发送出去，一般需要对发送的附件进行控制，附件名称包含指定关键字的邮件将被禁止发送出去。

设置策略：禁止 包含附件 附件名称：如 *关键字*，则客户端机器上发送的邮件中，包含了附件，且附件名称中包含了“关键字”的邮件被禁止发送。

策略示例 2

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。

6.14 IM 文件传送策略

IM 文件传送策略可以有效控制企业内计算机通过即时通讯工具将企业内部资料传送出去，从而保障了内部资料的安全性。

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：

策略属性名称	说明
文件控制	选择此项则对通过 IM 工具发送的文件进行控制
文件名称	设置需要控制的 IM 传送的文件名称，支持通配符，支持“;”“,”作为分隔符；
限制文件大小	只有当模式为“禁止”时，此属性有效。意为：禁止传送大于此值的文件。此值的范围为：0 – 4000000 KB；
是否备份	选择是否对指定的发送文件备份。备份的文件在“日志->文档操作”中查看或保存；
备份文件最小大小(>=KB) 备份文件最大大小(<=KB)	如果选择了备份文件，则可以限制备份文件的大小这里可以设置备份文件大小的一个范围，分别设置一个最小值和最大值。在此范围内的文档将被备份，否则不备份。
图片控制	选择此项则对通过 IM 工具发送的图片进行控制；
是否备份	选择是否备份发送的图片；
聊天工具	支持的聊天工具列表，可选择受控制的聊天工具

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。

6.15 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。

上传控制策略的属性包括：

策略属性名称	说明
传送方式	默认为上传，无其他可选；
应用程序	指定网络访问的应用程序，可输入多个应用程序，使用“;”分隔；
Http(s)协议	勾选此项，则可对 Http 协议和 Https 协议进行上传控制；
限制大小(>=Byte)	指定上传数据的大小范围，默认为 102400Byte，超过此大小的数据上传将被控制；
网站	指定上传数据的网站，则上传文件、发帖到该网站时将受控。 默认为所有网站，输入格式为“www.baidu.com”,而不是“http://www.baidu.com/”，支持通配符，支持“;”“,”作为分隔符；
Ftp 协议	勾选此项，则可对 Ftp 协议进行上传控制；
限制大小(>=Byte)	指定上传数据的大小范围，默认为 102400Byte，超过此大小的数据上传将被控制；
文件名称	指定文件名称，支持通配符，支持“;”“,”作为分隔符；
网络地址范围	指定网络地址范围，则上传文件到该范围内 FTP 站点时将受控；支持“;”“,”作为分隔符；
其他协议	勾选此项，则可对 TCP 协议进行上传控制；
限制大小(>=Byte)	指定上传数据的大小范围，默认为 102400Byte，超过此大小的数据上传将被控制；
端口范围	与流量控制策略中的端口范围含义相同；
网站或网络地址	指定网站或网络地址，默认为*，即对所有网站所有网络地址控制。支持输入 IP 或 IP 段，支持通配符，支持“;”作为分隔符； 例如： 192.168.3.1;192.168.1.1-192.168.2.255;www.company.net;*baidu*

6.16 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。

文档操作策略的属性包括：

策略属性名称	说明
操作类型	为了方便理解和控制，把文档操作类型简单的分为：读取、修改、删除这 3 种。其中，允许修改就一定可以读取，允许删除就一定可以读取和修改。
读取	即访问文档；
修改	包含了访问和删除之外的所有操作，包括创建、重命名、修改、复制、移动和恢复。只有选中了该项，“修改前备份”和“复制/移动到备份”才有效；
删除	删除文档，只有选中了该项，“删除前备份”才有效。
盘符类型	默认是全部盘符类型，至少要选择一种盘符类型，否则自动识别为全部。选中“盘符类型”，可以用 Ctrl + A 对其所有子项进行全选或全不选；
文件名称	指定需要控制的文件名称，可以包含路径，如 E:\work*，则 work 这个文件夹下的所有文件都生效。文件名称支持通配符，支持“;”“,”作为分隔符；
修改前备份	备份修改的文件，只会备份修改之前的源文件，以防止重要文件被恶意或无意修改；
复制/移动到备份	复制/移动到指定盘符类型时备份文件，方便检查客户端机器是否将重要文件复制/移动到非法的盘符；
复制/移动出备份	复制/移动出指定盘符类型时备份文件，方便检查客户端机器是否将重要盘符内的文件复制/移动到其他盘符
删除前备份	备份客户端删除的文件，避免重要资料被误删除而带来的损失；
备份文件最小大小(>=KB)，备份文件最大大小(<=KB)	指定要备份的文档大小范围，与 IM 文件传送策略中含义相同；
应用程序	指定文档操作的应用程序。

说明 文档操作策略中，盘符类型选择“光盘”时，只针对使用专用刻录工具进行刻录操作生效。

策略示例 1

可能有些重要文件不允许所有用户任意修改，需要限制一部分员工的权限，只允许访问，不允许修改和删除。

设置策略：禁止 操作类型：修改和删除 指定文档名称 选择备份方式，则用户对指定的文档只有访问的权限。

策略示例 2

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。

注意 如果文档策略中设置了备份，可能会导致备份的文档数据量很大，建议在设置策略时，尽量精确定位，避免备份大量无用的文档。

6.17 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，既保障机密文档不外泄，也极大地节约企业资源。

打印控制策略的属性包括：

策略属性名称	说明
打印机类型	有共享、网络、本地和虚拟打印机四种类型。 如果四种类型都不选择，则认为是所有类型的打印机，即相当于四种打印机全部选中，在保存后，这个属性中的四种类型会全部被选中。
打印机描述	设置打印机名称。可以指定网内某台计算机上的打印机，如：“\\server*”表示\\server 上的所有打印机；“SomePrinter”为名称为 SomePrinter 的打印机。
打印任务	设置打印任务名称，支持通配符。
应用程序	指定进行打印的应用程序。
记录打印内容	模式为允许或忽略时可选；模式为“禁止”时不可选。 如果选择该项，策略匹配该条策略，记录或不记录打印内容；如果不选择该项，则继续匹配下一条策略，决定是否记录打印内容。
记录模式	默认不记录，如果需要记录打印内容，可在下列表中选择“记录”。

最大记录页数	记录模式为“记录”时有效，设置记录打印文档的最大页数，管理员可以根据实际情况设置该项，记录的页数越多，则占用的空间会越大。 记录的打印内容到控制台的“**日志->文档打印日志**”中查看。

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。

注意 只有打印机类型和打印机描述都匹配，“打印机”条件才算匹配。

6.18 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。打印水印策略的属性包括：

策略属性名称	说明
打印机类型	有共享、网络、本地和虚拟打印机四种类型。 如果四种类型都不选择，则认为是所有类型的打印机，即相当于四种打印机全部选中，在保存后，这个属性中的四种类型会全部被选中。
打印机描述	设置打印机名称。可以指定网内某台计算机上的打印机，如：“\\server*”表示\\server 上的所有打印机；“SomePrinter”为名称为 SomePrinter 的打印机。
打印任务	设置打印任务名称，支持通配符。
水印模板	选择打印模板来指定水印信息，水印模板可在“**分类管理->水印模板->打印水印模板**”中进行设置。
应用程序	指定进行打印的应用程序。
授权软件	指定进行打印的授权软件。

注意 只有注册了加密序列号“授权软件”一项才会出现。

6.19 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。

屏幕水印策略的属性包括：

策略属性名称	说明
水印模板	选择打印模板来指定水印信息，水印模板可在“**分类管理->水印模板->屏幕水印模板**”中进行设置。
显示方式	可以选择全屏幕水印或者软件窗口水印，全屏幕水印为整个屏幕显示水印内容，窗口水印则为指定的程序窗口显示水印内容。
应用程序	选择应用程序，当运行指定的应用程序时，则出现屏幕水印。
授权软件	选择授权软件，当运行指定的授权软件时，则出现屏幕水印。
网站	可以设置指定的网站网址，当浏览器在访问指定的网站时出现窗口水印。显示方式需指定为“**软件窗口水印**”。网站的设置可以是完整的网址，也可以包含通配符。

注意 只有注册了加密序列号“授权软件”一项才会出现。

6.20 移动存储授权策略

为了方便管理企业内部使用的移动盘，防止企业内部机密资料通过移动存储设备外泄，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。

设置策略前，管理员需要对企业内用到的移动盘进行合理的分类， 移动存储库的分类可参考后面的“**分类管理->移动存储分类**”的说明文档。

移动存储设备的类型和操作权限包括：

策略属性名称	说明
加密盘类型	默认是“全部”，可以通过下拉列表选择加密盘或非加密盘或安全 U 盘；设置的策略只对所选的加密盘类型有效；

可读	允许任意程序以只读方式读取移动盘的内容，只有勾选此项，下面三项才有效。
自动解密	允许在资源管理器中从移动盘将文档复制到本地或者网络上时自动解密，而其他的应用程序读取移动盘上的文档不会自动解密；
可写	允许任意程序写到移动盘上，当不允许可写时，会禁止文档复制或保存到移动盘上，同时也会禁止删除，改名移动盘上的文档；只有勾选此项，自动加密才有效；
自动加密	禁止除了资源管理器之外的任何程序写数据到移动盘，当资源管理器复制文档到移动盘时，自动对文档加密。
移动存储类别	移动存储默认是<全部>，是指所有的移动存储设备，要设置指定的移动盘，只能到移动存储分类中选择，可以指定一个分类，也可以是具体的一个移动盘。
描述	通过移动存储设备的设备描述来匹配移动盘；

提示 如果企业想执行严格的移动盘控制策略，可以首先在整个网络中设置所有的移动盘都只读，不可写。

然后针对不同的部门和个人，设置其对不同的移动盘分类有不同的权限。比如每个部门都只能对属于自己部门的移动盘能够读写，而且读写时自动加密解密。

这样移动盘在部门内部使用是不受限制的，而且不会被其他部门的人读取数据，而那些外来的移动盘则只能读不能写。

注意 如果同时设置了文档控制策略和移动存储授权策略，则先执行文档控制策略，再执行移动存储授权策略。

例如允许读写移动盘，并且加密；而文档策略有禁止复制 word 文档到移动盘。则最后执行的结果是不允许复制 Word 文档到移动盘，而其他的文档复制到移动盘时会自动加密。

6.21 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，极大的规范员工电脑的软件使用情况。

设置策略前，管理员可以对需要管理的软件安装包和卸载软件进行合理的分类，软件安装包的分类可参考后面的“**分类管理->软件安装包**”的说明文档，卸载软件的分类可参考后面的“**分类管理->软件卸载**”的说明文档。

软件安装管理策略，不支持用户策略。

图标按钮	说明
	修改选中计算机软件安装权限；
	删除选中计算机软件安装权限；
	可以选择导出策略文件、导入策略文件、将当前策略复制到其他客户端。

策略设置项如下：

策略设置项	说明
软件安装控制	对安装的软件进行控制；
禁止全部软件的安装	勾选此项，则会限制所有软件安装包的安装； 可以在下方的“允许以下软件的安装”中，通过在软件安装包库中选择或是手动输入安装包名称的方式设置软件安装包，此处设置的安装包则允许安装；
软件卸载控制	对卸载的软件进行控制；
禁止全部软件的卸载	勾选此项，则会限制所有的软件卸载； 可以在下方的“允许以下软件的卸载”中，通过在软件卸载库中选择或是手动输入软件名的方式设置卸载软件，此处设置的卸载软件则允许卸载；
禁止以下软件的卸载	勾选此项，并通过在软件卸载库中选择或是手动输入软件名的方式设置卸载软件，则会禁止这些软件的卸载，其余软件的卸载不做限制。

注意 手动输入软件安装包名时，会直接根据名称匹配。如设置软件安装控制策略，禁止全部软件安装，手动输入允许“VMware.exe”安装，此时将 QQ 的安装包改名成 VMware.exe 能安装成功。所以建议设置策略时从分类库中选择软件安装包，如此一来即使将非指定安装包改名为允许的安装包名称，策略仍旧会生效。

第七章. 监视

7.1 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，为事后追查责任提供重要依据，及时发现非法的聊天内容，同时避免员工任意聊天而影响正常工作的情况。

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。

即时通讯内容记录

即时通讯记录包含的内容有：

IM 内容字段	说明
聊天工具	记录使用的即时通讯工具；
本地账户	记录本地的即时通讯的账户昵称；
对方账户	记录聊天对方的账户昵称；
开始时间	该聊天记录的开始时间；
结束时间	该聊天记录的结束时间；
聊天类型	该聊天记录的类型，分为多聊和单聊；
聊天语句数	统计聊天内容的语句数量，判断聊天内容的多少；
聊天内容	记录聊天的详细时间以及内容。

其中，聊天内容支持正则表达式查询，输入格式为“R:+正则表示式”。如：查询聊天内容包含身份证，可输入“R:\d{17}[\d|x]|\d{15}”；查找聊天内容含手机号，输入“R:0?(13|14|15|18)[0-9]{9}”。

聊天内容支持查看发送的图片和文件副本。当发送的是文件，会有文件名称的

链接，点击链接会弹出普通下载文件窗；当发送的是图片，无论是直接发图片文件或截图，会显示相应图片的缩略图和对应图片名称的链接，双击图片可以打开显示大图，点击链接会弹出普通下载文件窗进行下载。

当前支持查看图片和文件的 IM 有：QQ、TIM、微信、企业微信。

保存聊天内容

除了直接在控制台上查看聊天内容，管理员也可以将聊天内容保存起来，方便日后查询。

选中一个或多个需要保存的聊天记录，单击右键“**导出聊天记录**”，将所选聊天内容保存为一个 htm 或 xls 文件。

查询聊天内容

即时通讯内容可以按以下条件进行查询：

查询条件	说明
聊天工具	根据聊天工具查询，默认是全部，也可在下拉框中选择其中一种聊天工具进行查询；
聊天类型	根据聊天类型查询，默认是全部，也可以在下拉框中选择单聊或多聊进行查询；
用户 ID 或昵称	根据聊天双方的账户 ID 或昵称进行查询，查询指定账户的聊天记录及内容；
内容	根据聊天内容进行查询，可针对部分关键字进行快速定位，从而找到关心的聊天记录。
聊天语句数	根据聊天语句数进行查询，可指定聊天语句数范围进行查询；
聊天字符数	根据聊天字符数进行查询，可指定聊天字符数的范围进行查询。

7.2 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，及时阻止非法的邮件内容。

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。

邮件记录内容

邮件记录包含的内容有：

属性名称	说明
发送/接收	表示发送的邮件记录， 表示接收的邮件记录；
主题	邮件的主题；
发件人	邮件的发件人的邮箱地址；
收件人	邮件的收件人的邮箱地址，包括抄送和暗送的邮件地址，在邮件记录的属性窗口中查看；
附件	“ ” 表示邮件有附件，邮件记录会自动备份附件文件，点击“ ” 按钮直接查看或保存附件文件；
大小	记录邮件的大小；
正文	选中一条邮件记录，在下面的视图中可以直接查看正文内容。

保存邮件内容

除了直接在控制台上查看邮件记录及内容，管理员也可以将邮件文件导出来保存。

选中一条邮件记录，单击右键“**导出邮件文件**”将该邮件保存为 eml 文件，可以直接通过 outlook 打开并查看该文件。也可同时选择多个邮件同时导出保存。

查询邮件

可以按以下条件对邮件及内容进行查询：

查询条件	说明
邮件类型	根据邮件类型查询，默认是全部，也可在下拉框中选择其中一种邮件类型进行查询；
发送/接收	管理员可以只统计发送或接收的邮件；
发件人	根据发件人邮箱地址查询；

收件人	根据收件人邮箱地址查询； 具体还可以筛选收件人的类型查询，查询类型包括：全部、收件人、暗送、抄送。 可输入多个收件人地址，用“;” “,”作为分隔符；则收件人同时为设置的多个时，才符合该条件；
主题	根据邮件主题查询，查询主题包含指定关键字的邮件记录；
内容	根据邮件内容查询，查询包含指定关键字的邮件，以帮助管理员快速定位关心的邮件内容；
包含附件	不勾选该项，查询到所有邮件记录(包含带附件和不带附件的邮件)，勾选该项，只查询包含附件的邮件；
附件名称	查询包含附件，且附件文件名称中包含指定关键字的邮件记录。
大小	设置邮件的大小范围，查询设置范围内的邮件记录。

7.3 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。

图标按钮	说明
	保存当前帧按钮，将当前屏幕快照保存成图片形式。
	会话按钮，如果某台计算机登录了两个以上用户或某个用户同时登录两台以上计算机，管理员可以通过选择查看其中某一个的屏幕快照。
	适合窗口大小。
	原始大小。
	跟踪按钮，屏幕快照会自动刷新，刷新间隔时间在“**工具->选项->实时信息**”中查看和修改。
	停止跟踪，屏幕快照不会自动刷新。

选择了目标计算机之后，选择右键菜单“**跟踪**”对该计算机进行实时跟踪，图像区会不断地显示选定计算机的屏幕变化。当需要停止时，再选择右键菜单“**跟踪**”会停止跟踪。

7.4 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。

设置监视矩阵的大小，系统自动在一定的时间间隔内更新屏幕快照，同时在到达一定的时间后轮转到下一批待监视的计算机，方便管理员同时监控多台计算机。

用户可以通过功能按钮快速查看最前一页、上一页、下一页和最后一页的计算机的屏幕快照；可以通过按钮“  ”选择需要监控的计算机或计算机组；可以通过按钮“  ”设置屏幕自动轮转；选择某一个被监控的计算机屏幕，通过按钮“  ”，或是双击该计算机的屏幕，可以对其进行全屏监视。

锁定位置

您可以在某一台计算机的屏幕的右键菜单里选中“**锁定位置**”使得在每一个多屏监视画面中都能看到该计算机的屏幕快照。被固定的计算机屏幕的标题是黄底黑字，假如您不想再固定该计算机的屏幕，您只要在该计算机的屏幕的右键菜单里钩选掉“**锁定位置**”恢复。

屏幕信息

鼠标移动到一个屏幕会显示当前客户端机器的屏幕信息，包括：计算机名称、网络地址、用户、状态。

定位到计算机树

您可以在某一台计算机的屏幕的右键菜单里选中“**定位到计算机树**”，从而可快速定位到该计算机在计算机管理树处的位置。

7.5 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，只有设置了屏幕记录策略的客户端机器才能查询到屏幕记录。管理员也可以根据一定的查询条件快速找到需要的屏幕记录进行查看。

查询条件包括：

查询条件	说明
日期范围	设置开始日期和结束日期，查询一个时间段内的所有屏幕历史记录；
计算机名称	查询指定计算机名称的屏幕记录，支持模糊查询，如输入“TEC”，查询到所有计算机名称中包含“TEC”的计算机屏幕记录；
网络地址	输入指定的网络地址，查询该计算机的屏幕记录，可以输入一个 IP 地址，也可以输入一个 IP 地址范围，如：192.168.1.100-192.168.1.200。
范围	选择计算机范围进行查询，可查询一个分组的屏幕记录，其中包含已删除组。

查询到的屏幕记录日志包括：

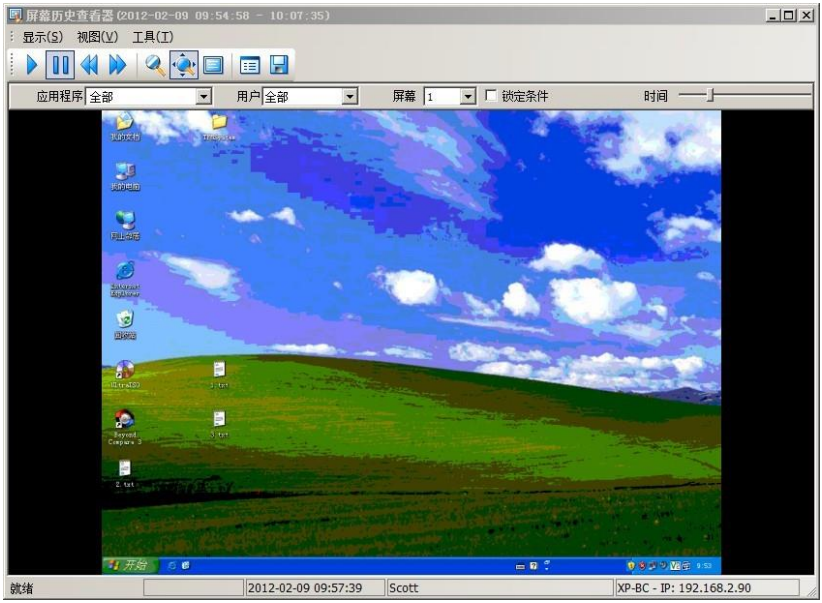
日志属性名称	说明
日期	屏幕记录的日期，屏幕记录以“天”为单位，一天的屏幕数据记录一个文件；
计算机	记录的客户端机器；
会话	会话 ID，如果只登录一个用户，则会话 ID 是 0，登录第二个用户，则会话 ID 是 1，如果登录过多个用户，则有多个屏幕记录，一个会话会记录为一个文件。 Vista 下第一个用户的会话 ID 为 1；
开始时间 结束时间	屏幕记录的开始时间和结束时间；
文件名称	屏幕数据是存放在 SQL 数据库，文件名称为<SQL>

7.6 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。

界面简介

屏幕历史查看器窗口包括：标题栏、菜单栏、工具栏、查询栏、时间刻度尺、图像显示区以及状态栏。



显示

可以通过菜单或工具栏上的按钮选择屏幕帧的位置，也可以直接拖动时间刻度尺上的滑块直接显示某一帧。

视图

管理员可以根据自己的需要在“视图”菜单选择是否显示工具栏、状态栏。同时类似于控制台模块中的图像区的显示方式，也有原始大小、按比例缩放和全屏幕。

播放速度

通过菜单“**视图->速度**”可以调节屏幕播放的速度。分为快、普通和慢三种速度，用户可以根据自己的需要选择播放速度。

查询

通过查询栏，管理员可以快速定位查询到需要的屏幕历史，可以分别根据应用程序、用户、屏幕和时间刻度尺进行查询。

查询项	说明
应用程序	默认播放所有应用程序的屏幕历史，也可从下拉菜单中指定一种或多种应用程序，只播放该程序的屏幕历史；
用户	如果屏幕记录中记录了多个用户的屏幕历史，可以指定其中一个用户只查看该用户的屏幕历史；
屏幕	如果客户端机器有多个显示屏，则可以选择其中一个屏幕查看屏幕数据；
锁定条件	将以上三个查询条件锁定，可查看同时满足这三个查询条件的屏幕数据；
时间刻度尺	显示当前帧对应的时间，拖动滑块到指定的位置，查看当前帧的屏幕，鼠标停在上面时能显示该帧的基本信息。 选择菜单“**工具->窗口标题变化**”可查看每一帧的基本信息，包括：时间、用户、应用程序和标题。

导出为视频文件

管理员可将需要的屏幕历史保存起来，留作以后使用。选择“**工具->另存为视频文件**”，有 4 种保存方式，管理员可以指定其中一种方式保存屏幕历史。

保存方式	说明
按时间保存	保存一段时间内的屏幕数据，拖动时间刻度尺上的滑块，设置开始时间和结束时间；
按应用程序保存	只保存指定的应用程序对应的屏幕历史记录；
按用户保存	只保存指定的一个用户对应的屏幕历史记录；
全部保存	保存所有的屏幕历史。

屏幕历史按帧导出成图片

管理员可以屏幕历史按帧导出成图片。选择“**工具->屏幕历史按帧导出成图片**”，有 4 种导出方式，管理员可以指定其中一种方式导出图片。

导出方式	说明
时间	按帧导出一段时间内的屏幕数据，拖动时间刻度尺上的滑块，设置开始时间和结束时间；

应用程序	只按帧导出指定的应用程序对应的屏幕历史记录；
用户	只按帧导出指定的一个用户对应的屏幕历史记录；
全部	按帧导出所有的屏幕历史。

窗口标题变化信息

管理员可以查看屏幕历史的窗口标题信息。选择“**工具->窗口标题变化信息”,** 可通过右键菜单“打印预览/打印”这些信息。 同时也可以导出，支持 3 种格式的导出文件：Web 文件（*.htm; *.html）、Excel 文件（*.xls）和文本文件（*.csv）。

第八章. 远程维护

IT 人员为 PC 做简单的日常维护工作所花的时间占其总工作量的 70-80%，大大增加计算机网络的综合管理成本。而且如果问题没有得到及时有效的处理，也会极大影响企业的生产力。因此有必要减少 IT 人员的一些无谓操作，大幅度提升他们的工作效率，使得 IT 人员更加关注于管理工作，并将精力集中于能够提升企业管理效率的信息系统中。

IP-guard 能帮助 IT 人员实时查看远程计算机的信息，帮助分析和解决远程计算机的故障。

8.1 远程维护

8.1.1 应用程序列表

选择菜单“**维护->应用程序**”可以实时查看客户端机器的应用程序列表，查看当前启动的所有任务以及状态信息，其中当前激活的应用程序名称用深蓝色粗体字显示。

图标按钮	说明
	会话按钮，如果客户端机器登录多个用户，单击该按钮选择不同的用户查看其应用程序列表；在用户模式下，如果该用户在多个计算机上登录，单击该按钮选择不同的计算机查看应用程序列表。
	跟踪按钮，应用程序列表会自动刷新，时间间隔在“**工具->选项->实时信息**”中设置和查看。

结束任务

管理员可以在控制台上远程结束应用程序任务，选择需要结束的应用程序，单击右键“**结束任务**”确定后关闭指定的应用程序。

8.1.2 进程列表

选择菜单“**维护->进程列表**”可以实时查看客户端机器上的所有当前进程，进程信息包括：文件名称、PID、时间、会话 ID、CPU、CPU 时间、内存、虚拟内存、基本优先级、句柄数、线程数以及路径。

字段名称	说明
时间	该进程的启动时间；
路径	该进程所在客户端机器上的详细路径；
其它	其它各列属性与操作系统任务管理器的进程页中的各属性含义相同。

进程列表的各列属性可以帮助管理员分析是否有非法的进程或病毒并尽快解决问题。

图标按钮	说明
	会话按钮，只在用户模式下有效，选择查看不同的计算机的进程列表；
	跟踪按钮，与应用程序列表中的含义相同。

结束进程

管理员可以在控制台上远程结束指定的进程，选择需要关闭的进程，单击右键“**结束进程**”关闭客户端机器上的进程。

8.1.3 性能

选择菜单“**维护->性能**”可以远程实时查看客户端机器的各种性能，包括：CPU 的使用率、内存的使用率等。其中，总数、物理内存、认可用量、核心内存的值是客户端机器上的【任务管理器】->【性能】中的数据。

图标按钮	说明
	会话按钮，只在用户模式下有效，查看不同计算机的性能列表；
	跟踪按钮，与应用程序列表中的含义相同。

8.1.4 设备管理器

选择菜单“**维护->设备管理器**”可以实时查看客户端机器上的设备列表，包括：处理器、磁盘驱动器、存储卷、键盘、鼠标、网络适配器等各种计算机硬件设备。

图标按钮	说明
	设备列表的查看方式，包括：按类型查看、按连接查看以及是否显示隐藏的设备；
	只在用户模式下有效，选择查看不同计算机的设备。

禁用/启用设备

管理员可以在控制台上远程禁用/启用设备管理器中的硬件设备，选择需要禁用/启用的设备，单击右键“**禁用**”或“**启用**”来远程操作客户端机器的设备。

8.1.5 系统服务

选择菜单“**维护->系统服务**”可以实时查看客户端机器的系统服务列表信息，包括：名称、描述、状态、启动类型、登录身份、路径。

图标按钮	说明
	只在用户模式下有效，选择查看不同计算机的系统服务

远程操作

管理员可以像在本地操作一样设置和更改服务的状态以及启动类型。选择需要设置的服务，单击右键“**启动/停止**”更改服务的状态，右键“**启动类型->自动/手动/禁用**”中选择需要设置的启动类型。

8.1.6 磁盘管理

选择菜单“**维护->磁盘管理**”可以实时查看客户端机器的磁盘分区列表以及使用情况，包括的内容有：卷标、文件系统、容量、空闲空间、%使用。

图标按钮	说明

	只在用户模式下有效，选择查看不同计算机的磁盘管理

8.1.7 共享文件夹

选择菜单“**维护->共享文件夹**”实时查看客户端机器的共享情况，包括：网络共享、会话、打开文件。

图标按钮	说明
	网络共享视图按钮；
	会话视图按钮；
	打开文件视图按钮；
	只在用户模式下有效，选择查看不同计算机的共享信息

网络共享

管理员通过查看网络共享可以知道客户端机器开启了哪些共享文件，并可以根据安全需要实时关闭一些共享，选择需要关闭的共享，单击右键“**停止共享**”关闭该共享文件。

会话

单击“显示”按钮选择“会话”模式可以查看客户端机器上的共享文件是否有远程机器访问，并且访问共享的远程机器的情况，包括：用户、计算机、类型、打开文件、连接时间、空闲时间、是否来宾。

假如管理员发现非法的访问连接，可以实时关闭该连接，选择该会话，单击右键“**关闭会话**”暂时关闭该会话。

打开文件

打开文件列表是远程机器访问客户端机器共享文件的列表，包括：打开文件、访问者、锁定、模式。

管理员也可以通过右键“**将打开的文件关闭**”或“**中断全部打开的文件**”实时关闭一个或所有的打开的文件。

8.1.8 计划任务

选择菜单“**维护->计划任务**”可实时查看客户端机器上的计划任务列表，包括：名称、计划、应用程序、下次运行时间、上次运行时间、状态、上次结果以及编写者。

管理员可直接通过控制台删除非法的计划任务，选择需要删除的计划任务，单击右键“**删除**”实时删除指定的计划任务。

图标按钮	说明
	只在用户模式下有效，选择查看不同计算机的计划任务

8.1.9 用户和组

选择菜单“**维护->用户和组**”可实时查看客户端机器的所有本地用户以及用户组。

本地用户列表包括：用户名称、全名以及描述。

用户组列表包括：组名称以及描述。

图标按钮	说明
	只在用户模式下有效，选择查看不同计算机的用户和用户组。

8.1.10 软件管理

选择菜单“**维护->软件管理**”可以查看客户端机器上已安装的软件列表，管理员可通过右键菜单卸载客户端机器上安装的软件。

卸载软件有两种方式：

卸载方式	说明
默认卸载	此方式实际上调用的是软件自身的静默卸载程序，若软件本身不提供静默卸载功能，则此卸载方式不可选。
高级卸载	通过 IPG 客户端分析出所选软件的相关安装项信息，确定卸载时清除相关文件以达到卸载目的。

8.1.11 启动项

选择菜单“**维护->启动项**”可以查看客户端机器的启动项列表，管理员可通过右键菜单删除客户端上的非法启动项。

8.2 远程控制

8.2.1 远程控制

远程控制是通过控制台远程操作客户端机器，为网络管理提供方便，帮助管理员远程查看机器故障，快速解决系统问题。

选定目标计算机，选择菜单“**维护->远程控制**”，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**”，控制台会弹出确定请求远程用户授权的提示框，点击“是”，目标客户机会弹出对话框询问当前用户是否允许控制台对其远程控制。如果用户允许，则进入控制界面，否则控制结束。

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。

设置了密码的客户端机器，也可以通过用户授权的方式进行远程控制。但是如果策略设置了允许远程控制并且需要强制确认，只能通过用户授权的方式来控制。

证书授权

具有**“通过证书授权方式远程控制”**权限的管理员，选定目标计算机，选择菜单"维护->远程控制"，可直接强制远程控制目标计算机，无需通过用户授权和密码授权。

注意 购买正式产品的客户可向我们申请获取远程控制授权证书，将授权证书置于服务器安装目录下，否则无法使用“证书授权方式远程 ”的权限。

远程控制界面

当进入远程控制的状态时，目标计算机的右上方会显示“**Remote Controlling...**”。

通过工具栏按钮，可以选择屏幕缩放的比例，以及是否全屏幕控制。在全屏幕控制时，如果需要退出全屏显示，可直接按 F12 键。

按钮“  ”可以控制显示色彩在 256 色和真彩色之间转换。

按钮“  ”可以对目标计算机的键盘和鼠标设置锁定和解锁；

按钮“  ”可以控制是否允许在控制台与目标计算机之间进行剪贴板操作；

如果需要向受到远程控制的计算机使用 Ctrl-Alt-Del、Ctrl-Esc 或 F12，您可用鼠标右击 IP-guard 远程控制窗口的标题列或在 Windows 工具列上远程控制窗口的图标，并在弹出的菜单选择 “Send Ctrl-Alt-Del”、“Send Ctrl-ESC”或“Send F12”。

说明 远程控制支持多屏显示器机器。

8.2.2 远程文件传送

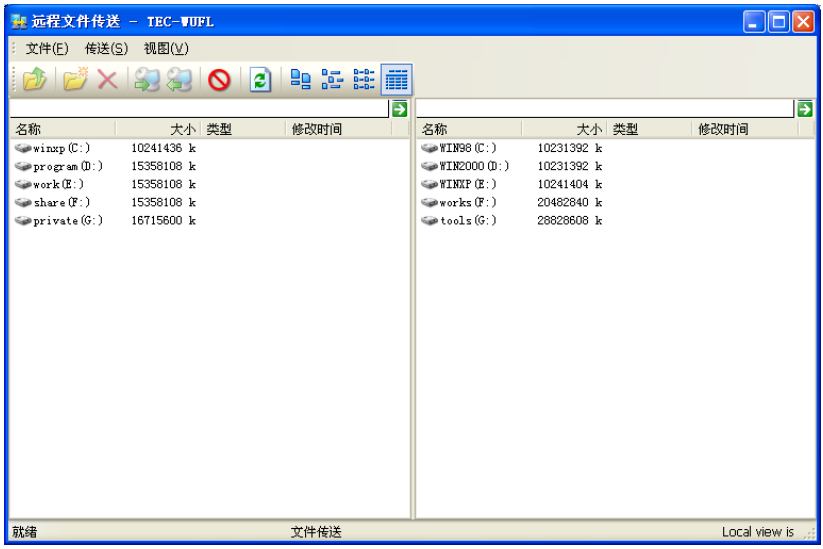
远程文件传送是指在控制台机器和目标客户端机器之间的文件传送，通过远程文件传送功能，管理员可以快速分发文件到目标计算机，提高工作效率。

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。

界面介绍

远程文件传送窗口包括：标题栏、菜单栏、工具栏、本地资源视图、远程资源视图以及状态栏。

其中本地资源视图是控制台机器的资源信息，远程资源视图是远程客户端机器的资源信息。双击文件夹进入下一级目录，也可以直接在地址栏中输入文件的路径来查找文件。



文件操作

管理员可以直接双击进入下一级目录，也可以在地址栏中直接输入路径来查找文件，选择“**文件->向上**”返回上一级目录。同时可以对文件做一些简单操作，包括新建文件夹、重命名、删除，地址栏为空也就是在根目录下无法进行这些文档操作。

远程视图和本地视图操作相同。

文件传送

传送功能	说明
本地到远程	选中本地机器需要传送的文件，选择菜单“**传送->本地到远程**”就可以把选中的文件传送到远程目标计算机；
远程到本地	选择远程机器中需要传送的文件，选择菜单“**传送->远程到本地**”复制远程文件到本地计算机；
终止传送	在文件传送过程中选择菜单“**传送->停止**”可以终止文件传送，状态栏会显示文件传送失败。

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。

获取文件列表

点击远程传送窗口中的  按钮，根据实际需要设置好文件列表设置，点击【**确定**】按钮，即可将远程客户端的文件列表信息传送到本地。

文件列表设置项包括以下：

传送功能	说明
文件列表路径	获取远程客户端指定路径下的文件列表，默认为获取全部磁盘，可以输入指定的路径，如 D:\test；
包含范围	此范围内的文件类型或路径，会获取；默认为空，即全部包含；可手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等；
排除范围	此范围内的文件或路径，不会获取；默认为空，即都不排除；可手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等；
包含系统目录下的文件	默认不获取系统 Windows 目录下的文件列表，勾选此项则会获取；
包含程序目录下的文件	默认不获取系统 Program Files 目录下的文件列表，勾选此项则会获取；
保存文件	选择文件列表信息的存放位置，获取完文件列表信息后会在指定的位置输出结果文件。

显示模式

本地与远程视图均支持大图标，小图标，列表，详细信息等显示模式。单击工具栏上的显示图标选择合适的排列方式。

注意　需要传送文件时，本地视图和远程视图都不能为根目录，否则不能传送文件。

第九章. 安全检测

安全检测功能，可以通过设置各项安全检测条件，使不满足安全检测条件的客户端阻断网络或阻断接入准入网关。

9.1 安全检测条件

管理员可以根据企业管理需要，先设置好安全检测条件，则设置安全检测策略时便可以直接选择安全检测条件类别进行控制。

选择菜单“**安全检测->安全检测条件**”打开安全检测类别窗口，在此处设置安全检测类别。

操作	说明
新建	菜单栏选择“**操作->新建**”，新建安全检测条件，输入不为空的条件名，设置各项检查条件后完成新建操作；
复制	选中一条已有的安全检测条件，右键菜单选择“**复制**”或者菜单栏中选择“**操作->复制**”，可以将选中的安全检测条件复制成一条新的检测条件；
导出	在左侧视图中选中“**安全检测条件类别**”节点，右侧视图将出现所有的安全检测条件，可以选中一个或多个安全检测条件，工具栏中点击导出图标，则会导出选中的安全检测条件，导出的文件格式只支持 xml；
导入	工具栏中点击导入图标，选择此前导出的安全检测条件，可以导入成功。

可以设置的安全检测条件包括：杀毒软件检查、软件安装检查、程序检查、系统服务检查、系统补丁检查以及其他检查。

9.1.1 杀毒软件检查

杀毒软件检查，主要是针对客户端机器的杀毒软件安装情况进行检查。

具体设置项说明如下：

设置项	说明
必须运行杀毒软件	选择此项，则启用杀毒软件检查；该项为选中的情况下，设置项“必须运行以下任一杀毒软件”和“病毒库更新到最新”才可编辑且才能生效；
必须运行以下任一杀毒软件	启用杀毒软件检查的前提下： 不勾选此项，则安装任一杀毒软件均可满足检查要求； 勾选此项，则杀毒软件列表中选中的杀软需安装任意一个方可满足检查要求； 如果杀毒软件列表为空或均未选中，则安装任一杀毒软件均可满足检查要求；
病毒库更新到最新	启用杀毒软件检查的前提下： 不勾选此项，不对病毒库版本做检查； 勾选此项，则需要病毒库更新到最新版本方可满足检查要求；
说明	在此处输入相关说明文字，用于客户端不满足杀毒软件检查条件时的提示。 当设置安全检查策略时勾选了“显示检测结果”时，客户端不满足杀毒软件检查则会收到检查结果，以及此处设置的说明信息。

添加杀毒软件

杀毒软件列表默认为空，需要管理员手动添加。点击**【添加】**按钮，输入杀毒软件名称，杀毒软件名称不能为空，支持通配符；输入备注信息，点击**【确定】**按钮完成添加。

9.1.2 软件安装检查

软件安装检查，主要是针对客户端机器的软件安装情况进行检查。

设置界面中有必须安装的软件列表（上起第一个软件列表）以及禁止安装的软件列表（上起第二个软件列表）。具体设置项说明如下：

设置项	说明
必须安装以下全部软件	选择此项，则必须安装的软件列表中所有选中的软件都必须安装方可满足检查要求； 如果必须安装的软件列表为空或均未选中，则代表对安装软件不做检查；

只须安装以下任一软件	选择此项，则只要安装了必须安装的软件列表中任一软件就可满足检查要求； 如果必须安装的软件列表为空或均未选中，则代表对须安装的软件不做检查；
禁止安装以下软件	所有禁止安装的软件列表中选中的软件都没有安装，方可满足检查条件； 如果禁止安装的软件列表为空或均未选中，则代表对禁止安装的软件不做检查；
说明	在此处输入相关说明文字，用于客户端不满足软件安装检查条件时的提示； 当设置安全检查策略时勾选了“显示检测结果”时，客户端不满足软件安装检查则会收到检查结果，以及此处设置的说明信息。

添加软件列表

必须安装的软件列表和禁止安装的软件列表默认为空，需要管理员手动添加。两个列表的添加方式一致。

点击【**添加**】按钮，在弹出的添加对话框进行添加，添加有两种方式。

数据库中添加

数据库添加的列表中会列出当前服务器收集到的软件信息，直接选定需要的软件，或者通过输入查询条件过滤出需要的软件再选定。

手动添加

当数据库中未包含所需的软件时，可以通过手动添加。 点击添加按钮  ，输入软件的各项检查属性即可。

各属性设置项说明如下：

属性设置	说明
软件名称	输入软件名称，支持通配符；软件名称不能为空；
公司名称	输入软件的公司名称，支持通配符；公司名称可以为空，为空时则不对公司名称做匹配；
操作符	当输入了软件版本后，操作符一项才可以选择，下拉菜单中选择操作符。版本信息为空，操作符也会被清空；
版本	输入软件的版本，会根据前面的操作符一起作为匹配条件，如：==3.58.1204 ，说明需要软件版本等于3.58.1024。

9.1.3 程序检查

程序检查，主要是针对客户端机器的程序运行情况进行检查。

设置界面中有必须启动的程序列表（上起第一个程序列表）以及禁止启动的进程列表（上起第二个进程列表）。具体设置项说明如下：

设置项	说明
必须启动以下全部程序	选择此项，则必须启动的程序列表中所有选中的程序都必须启动方可满足检查要求； 如果必须启动的程序列表为空或均未选中，则代表对必须启动的软件不做检查；
只须启动以下任一程序	选择此项，则只要启动了必须启动的程序列表中任一程序就可满足检查要求； 如果必须启动的程序列表为空或均未选中，则代表对必须启动的程序不做检查；
禁止启动以下程序	所有禁止启动的程序列表中选中的程序均没有启动，方可满足检查条件； 如果禁止启动的程序列表为空或均未选中，则代表对禁止启动的程序不做检查；
说明	在此处输入相关说明文字，用于客户端不满足程序检查条件时的提示； 当设置安全检查策略时勾选了“显示检测结果”时，客户端不满足程序检查条件则会收到检查结果，以及此处设置的说明信息。

添加程序列表

必须启动的进程列表和禁止启动的进程列表默认为空，需要管理员手动添加。两个列表的添加方式一致。

点击【**添加**】按钮，在弹出的添加对话框进行添加，输入程序的各项检查属性即可。

各属性设置项说明如下：

属性设置	说明
程序名	输入程序名称，支持通配符；程序名不能为空；
操作符	当输入了程序版本后，操作符一项才可以选择，下拉菜单中选择操作符。版本信息为空，操作符也会被清空；

程序版本	输入程序的版本，会根据前面的操作符一起作为匹配条件，如：==3.58.1204 ，说明需要程序版本等于3.58.1024；
备注	可根据需要输入一些备注信息，备注信息不作为匹配条件。

9.1.4 系统服务检查

系统服务检查，主要是针对客户端机器的系统服务运行情况进行检查。

设置界面中有必须启动的服务列表（上起第一个服务列表）以及禁止启动的服务列表（上起第二个服务列表）。具体设置项说明如下：

设置项	说明
必须启动以下全部服务	选择此项，则必须启动的服务列表中所有选中的服务都必须启动方可满足检查要求； 如果必须启动的服务列表为空或均未选中，则代表对必须启动的服务不做检查；
只须启动以下任一服务	选择此项，则只要启动了必须启动的服务列表中任一程序就可满足检查要求； 如果必须启动的服务列表为空或均未选中，则代表对必须启动的服务不做检查；
禁止启动以下服务	所有禁止启动的服务列表中选中的服务均没有启动，方可满足检查条件； 如果禁止启动的服务列表为空或均未选中，则代表对禁止启动的服务不做检查；
说明	在此处输入相关说明文字，用于客户端不满足系统服务检查条件时的提示； 当设置安全检查策略时勾选了“显示检测结果”时，客户端不满足系统服务检查条件则会收到检查结果，以及此处设置的说明信息。

添加服务列表

必须启动的服务列表和禁止启动的服务列表默认为空，需要管理员手动添加。两个列表的添加方式一致。

点击【**添加**】按钮，在弹出的添加对话框进行添加，输入系统服务名称，不能为空，支持通配符；输入备注信息，点击【**确定**】按钮完成添加。

注意 添加时输入的是服务名称，不是显示名称。

9.1.5 系统补丁检查

系统补丁检查，主要是针对客户端机器的系统补丁安装情况进行检查。

具体设置项说明如下：

设置项	说明
对以下系统补丁进行检查	所有系统补丁列表中选中的补丁均有安装，方可满足检查条件； 如果系统补丁列表为空或均未选中，则代表对必须安装的补丁不做检查；
说明	在此处输入相关说明文字，用于客户端不满足系统补丁检查条件时的提示； 当设置安全检查策略时勾选了“显示检测结果”时，客户端不满足系统补丁检查条件则会收到检查结果，以及此处设置的说明信息；

添加系统补丁列表

系统补丁列表默认为空，需要管理员手动添加。

点击【**添加**】按钮，在弹出的添加对话框进行添加，添加有两种方式。

数据库中添加

数据库添加的列表中会列出当前服务器收集到的补丁信息，直接选定需要的补丁，或者通过输入查询条件过滤出需要的补丁再选定。

手动添加

当数据库中未包含所需的补丁时，可以通过手动添加。 点击添加按钮  ，输入补丁的各项检查属性即可。

各属性设置项说明如下：

属性设置	说明
补丁 ID	补丁的 ID 号，需要输入正整数；
名称	补丁的名称，可以不填；

备注	可根据需要输入一些备注信息，备注信息不作为匹配条件。

9.1.6 域用户身份检查

域用户身份检查，主要是针对客户端机器的登录用户是否为指定的域用户进行检查。

具体设置项说明如下：

设置项	说明
启用域用户身份检查功能	选择此项，则启用域用户身份检查功能；该项为选中的情况下，设置项“必须登录以下任意域用户”和“禁止登录以下域用户”才可编辑且才能生效；
必须登录以下任意域用户	启用域用户身份检查的前提下： 此项不能设为空，默认值为*，表示任意域的任意用户，则客户端只要登录了任意域用户均可满足检查要求；设置格式为：域名\用户名，用户名支持通配符，则客户端需登录设置项中的任意域用户方可满足检查要求；
禁止登录以下域用户	启用域用户身份检查的前提下： 此项默认值为空，设置格式为：域名\用户名，用户名支持通配符；则客户端登录的域用户不满足此设置项中的任意域用户方可满足检查要求；
说明	在此处输入相关说明文字，用于客户端不满足域用户身份检查条件时的提示。 当设置安全检查策略时勾选了“显示检测结果”时，客户端不满足域用户身份检查则会收到检查结果，以及此处设置的说明信息。

9.1.7 其他检查

其他检查，主要是针对客户端机器的文件、注册表等情况进行检查。

具体设置项说明如下：

设置项	说明

检查条件	所有检查条件列表中选中的条件均满足，方可满足检查条件； 如果检查条件列表为空或均未选中，则代表对其他检查条件不做检查；
说明	在此处相关说明文字，用于客户端不满足其他检查条件时的提示； 当设置安全检查策略时勾选了“显示检测结果”时，客户端不满足其他检查条件则会收到检查结果，以及此处设置的说明信息；

添加其他检查条件列表

其他检查条件列表默认为空，需要管理员手动添加。

点击【**添加**】按钮，在弹出的添加对话框选择类型，运算符，输入具体文件名称、注册表值、内容，点击【**确定**】按钮完成添加。

类型设置说明如下：

设置项	说明
文件	判断某个文件是否存在，需要输入全路径；
文件类型	判断文件以及版本，需要输入全路径
注册表项	判断某个注册表项存在；
注册表值	判断某个注册表项以及注册表值作更详细的定位。

提示 条件的指定文件路径的字符串可以包含预定的宏，如：

"tmp"	temp folder(c:\windows\temp)
"win"	windows directory(c:\windows)
"sys"	system directory(c:\windows\system32)
"pf"	program files(c:\program files)
"sd"	system drive(c:\)
"cf"	common files(c:\program files\common files)

9.2 安全检测设置

选择菜单“**安全检测->安全检测设置**”，可以设置安全检测策略。安全检测策略会对客户端进行指定的安全项检查，不符合检查条件的客户端可以设置阻断

其网络，保障客户端机器的按照管理规定使用。

策略属性说明如下：

策略属性	说明
检测条件	添加策略时会先要求选则安全检测条件，每条策略只能选择一个安全检测条件，选择之后会在此显示当前策略的条件，点击?可查看条件概览；
检测	有“检测”和“不检测”可选； 选择“检测”，则根据所选检测条件内容进行检测； 选择“不检测”，则不会进行安全检测，同时下面的设置将无法设置；
客户端状态	有“全部”、“仅在线”和“仅离线”可选； 选择“全部”，则客户端无论在线还是离线，安全检测策略都会执行； 选择“仅在线”，则只当有客户端在线时，安全检测策略才会执行； 选择“仅离线”，则只有当客户端离线时，安全检测策略才会执行；
警告	勾选此项，则当检测模式为“检测”，检测结果不满足时，会弹出警告信息；
警告信息	对显示哪些警告信息做设置； 警告信息将显示在气泡框 和安全检测结果框中；
显示检测结果	勾选此项，则会显示检测结果；
显示检测明细	勾选此项，则会显示具体的检测明细； 当设置检测条件为通配符时或有多个匹配项时，也会显示多种匹配明细；
警告时间间隔	警告信息会以气泡形式在不符合条件的客户端机器上弹出； 此处设置弹出警告的时间间隔，单位为分钟；
阻断网络	勾选此项，则当检测模式为“检测”，检测结果不满足时，会被阻止访问网络
例外地址	设置例外地址，多个地址可以用逗号“,”隔开。 被阻止访问网络时，可以访问例外地址。
阻断接入	当在 IP-guard 控制台上连入了准入设备，才会出现此设置项；勾选此项，则不满足检测条件时，会被准入设备阻断。

9.3 安全检测日志

选择菜单“**安全检测->安全检测日志**”， 可以查看计算机的安全检测日志信息。

安全检测日志包含的属性有：检测结果、计算机、计算机组、时间、内容。

属性名称	说明
检测结果	安全检测的结果，包含通过和未通过两种结果；
计算机	计算机名称；
计算机组	计算机所在的计算机组名称；
时间	当前检测结果记录时间；
内容	检测结果内容； 检测通过时内容为：全部条件检测通过； 检测不通过时会列出具体不满足的条件，以及动作。

9.4 安全检测状态

控制台安全检测状态

选择菜单“**安全检测->安全检测状态**”，可以查看客户端的安全检测状态。

当选择单个计算机时，包含的内容有：

内容属性	说明
检测状态综述	检测时间：最后一次检测时间； 检测结果：全部检测条件的综合检测结果； 动作：当前客户端采取的动作；
具体检测结果	安全检测策略设置的所有安全检查条件的名称、结果和动作，还有每个条件的每个检查项的检查结果； 检测结果为通过的检查项默认是收缩起来，检查结果为不通过的检查项默认为展开显示具体的检查结果；

当选择整个网络或是某个分组时，可以切换多种视图进行查看。

图标	说明

	点击可选择安全检测条件，会按选定的安全检测条件显示统计结果；
	将所有展开的节点收起，只显示当前选中节点下的第一级节点的当前选择条件的检测结果，该视图为默认视图；
	将所有收起的节点展开，显示当前选中节点下的所有节点的当前选择条件的检测结果，计算机图标颜色表示状态，亮的表示在线，灰的表示离线；
	显示所有计算机或这个组内计算机的视图；
	显示所有的计算机组视图。

客户端安全检测状态

当设置安全检测策略勾选了“警告”，客户端检测不通过时，系统托盘会弹出警告图标，也会有气泡弹出。双击托盘图标，弹出安全检测结果框。

安全检测结果框包含的内容有：检测状态综述，具体检测结果。

内容属性	说明
检测状态综述	检测时间：最后一次获得结果的时间； 检测结果：显示全部条件的综合检测结果； 动作：当前客户端采取的动作；
具体检测结果	安全检测策略设置的所有安全检查条件的名称、结果和动作，还有不通过的检查项的检查结果，和警告信息； 检测结果为通过的检查项则不会显示。

客户端默认五分钟检查一次，如果当前已经符合了条件检查但安全检测结果框中为仍不通过，可能是还没到客户端下一次检查的时间点。此时可以点击安全检测结果框中的“**重新检测**”按钮，则客户端会立即检测得出最新的检测结果。

第十章. 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，使用敏感信息识别扫描任务/工具发现客户端上包含有特定敏感信息的文档，并通过设置敏感信息策略监控这些包含敏感信息的文档的外传、存储情况。

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。

10.1 敏感信息全盘扫描任务

管理员可同时对多台客户端设置敏感信息全盘扫描任务，实现目标客户端的本地磁盘扫描，识别并记录其中匹配敏感内容的文件，同时可指定对扫描得到的匹配敏感内容的文件进行加密。

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。

10.1.1 设置任务

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。

常规设置说明：

设置选项	说明
任务名称	当前任务的任务名。系统会自动填上默认值，可以修改；

设置选项	说明
选择对象	选择执行任务的目标计算机；
敏感内容	选择用于匹配文档的信息分类；
包含文件	此范围内的文件，会被扫描； 可以在给定的预定义文件类型中选择；也可点击 按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等；
搜索压缩包中的文件	勾选此选项，可识别压缩包中包含敏感内容的文档；
排除文件	此范围内的文件，不会被扫描； 可以在给定的预定义文件类型中选择；也可点击 按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。

说明 排除范围的优先级大于包含范围。

高级设置说明：

设置项	说明
任务选项	设置任务执行的内容；
仅扫描	仅扫描客户端上的文档，记录匹配中信息分类的文档；
扫描并加密	扫描客户端上的文档，加密并记录匹配中信息分类的文档；
扫描时段	设置任务开始扫描的时间。在下拉菜单中选择符合要求的时间分类； 此处下拉菜单中选择分类的即为时间类型管理中的各分类。
性能设置	任务进行时的性能设置。
扫描速度任务优先	扫描速度会快，对系统性能会有一定影响；建议在执行任务时间为非工作时间时，选择此项。
系统性能优先	扫描速度会放慢，对计算机的资源消耗不会太高，保证系统性能；执行任务时间为工作时间时，建议选择此项。
仅在空闲时扫描	客户端空闲时才会扫描指定文件，其余时间不扫描；客户端空闲指：控制台上显示该客户端的状态为“正在运行（空闲）”；
文件大小	此大小范围内的文件才会被扫描；

文件安全属性	设置在扫描并加密情况下，匹配中敏感分类的文件被加密后的安全属性，包括设置权限和访问权限，加密后的文档的安全属性和此处设置一致。

说明

1. 若没有购买加密模块，则不会出现“**扫描并加密**”选项；
2. 选定计算机对象、包含文件、敏感内容中任一项为空时，扫描任务不可创建。
3. 管理员创建敏感信息全盘扫描任务，选择扫描并加密时，并设置文档安全属性时，受其本身的安全区域和级别限制。
4. 敏感信息全盘扫描任务创建成功后，则无法修改任务设置，请在创建任务时务必确认好每项设置。

10.1.2 查看任务信息

当前任务信息

在全盘扫描功能界面的上半视图中，可以查看任务的基本信息。

内容项	说明
任务名称	扫描任务的名称；
计算机	客户端的计算机名称；
组	客户端所在分组的名称；
状态	客户端当前的运行状态；
开始时间	当前任务开始执行的时间；
结束时间	当前任务结束执行的时间；
任务状态	当前任务的状态； 1. 当扫描功能为启用时，当前任务会执行，状态为“已启动”； 2. 当扫描功能为禁用时，当前任务会暂停，状态为“暂停”； 3. 在任务启动和暂停的过程中，对应会有“正在启动”/“正在暂停”的状态； 4. 当扫描任务执行完成后，状态为“完成”；
进度	任务的完成进度，会根据当前进度自动更新。

其他任务信息

选中一台客户端，在全盘扫描功能界面下半视图的“**任务信息**”选项卡中，除了可以查看该台客户端任务明细，明细包括创建该加密任务时对应的各项设置内容。

说明 敏感全盘扫描任务仅执行一次，执行完毕后无法重复执行。

10.1.3 查看任务日志

在敏感信息全盘扫描功能界面，选中一台客户端，在下半视图的“**任务日志**”选项卡中，可以查看该客户端执行任务的日志。通过工具栏上的刷新按钮进行刷新。

内容项	说明
时间	该条任务日志产生的时间；
任务名称	当前执行的任务名称；
内容	包括：当前任务完成的百分比，当前扫描的目录，该任务的主要信息（扫描的文档个数、匹配中敏感内容的个数）。

10.1.4 启用/禁用扫描功能

禁用

计算机的扫描功能默认为启用状态。在全盘扫描功能界面，选中一条或多条任务，点击禁用按钮，或是右键菜单中选择“**禁用扫描功能**”，选中任务将暂停执行。

启用

选中一条或多条被暂停的任务，点击启用按钮，或是右键菜单中选择“**启用扫描功能**”，选中的任务将继续执行。

10.1.5 删除任务

选中一条或多条任务，点击删除按钮，或是右键菜单中选择“**删除计算机任务**”，则选中的任务将被删除。

10.1.6 查询计算机任务

查询

点击查询按钮，弹出查询对象选择对话框，选择指定的计算机或者计算机组，点击【**确定**】按钮，则计算机列表中仅会出现符合查询条件的计算机，可进行针对性查看。

模式

点击模式切换按钮，可以选择显示所有的计算机，也可以选择仅显示有任务的计算机。

10.2 敏感信息扫描工具

10.2.1 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。

10.2.2 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。

注意 远程敏感信息扫描仅可对在线客户端执行。

10.3 敏感信息控制策略

管理员可设置敏感信息控制策略，对匹配敏感内容的文档进行管控，放开其他文档的控制。

10.3.1 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	策略名称，系统会自动填上默认值，可以修改。
审计	勾选时，客户端匹配敏感内容的文件触发策略时，会记录下触发策略的文档，不勾选则不会记录；
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	勾选时，记录触发策略时客户端的屏幕，可在“**敏感信息->敏感信息日志**”中找到触发策略的日志记录，“**右键->查看屏幕日志**”。

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；

策略的图标按钮说明

图标按钮	说明
	新建，点击该按钮新增加一条策略；
	上移，将选中的策略上移一个位置；
	下移，将选中的策略下移一个位置；
	删除，点击该按钮删除选中的策略；
	恢复，取消新建或修改策略时点击该按钮；
	保存，设置或修改策略后需保存才会生效。
	表示该策略的模式是“允许”；
	表示该策略的模式是“禁止”；
	表示该策略的模式是“忽略”；
	表示该策略的模式是“不操作”；
	表示该策略设置了报警；
	表示该策略设置了警告；
	表示该策略设置了锁定计算机；
	表示该策略设置了到期时间。

10.3.2 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；设置策略后，通过移动盘、网络盘、邮件、IM、浏览器等途径的外传文件时，客户端将自动对文件进行扫描，若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。

策略属性说明

策略属性	说明

动作	对触发策略的外传操作的控制动作，包括禁止、允许、忽略 禁止：禁止触发策略的外传操作，不继续匹配下面的策略； 允许：允许触发操作的外传操作，不继续匹配下面的策略； 忽略：不控制触发策略的外传操作，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。
敏感内容	选定已有的敏感信息分类(在“**分类管理->敏感信息分类库**”中设置)作为敏感内容；
备份副本	勾选后将备份触发策略的文件，在“**日志->文档操作日志**”中查看；
复制到移动盘	控制文件发送到移动盘；
复制到网络盘	控制文件发送到网络共享路径；默认控制全部网络共享路径，支持自定义；
包含范围	设置网络路径，可设置多个，传送文档到包含范围中的路径时，会扫描文档并控制敏感文档，设置格式为\\server\temp，或\\server\temp*，不能以“\”结尾；
排除范围	设置网络路径，可设置多个，传送文档到排除范围中的网络共享路径时不扫描文档，不进行控制；
IM 传送文档	控制匹配策略的文档通过聊天工具外传，聊天工具默认选择全部 支持的聊天工具包括：QQ、ICQ、MSNMessenger、YAHOO、TM、蓝信、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
发送邮件	
发件人	对发件人的邮箱地址做控制，可选择邮件分类库中邮件地址，也可手动输入；
收件人	对收件人的邮箱地址做控制，可选择邮件分类库中邮件地址，也可手动输入；
仅匹配一个收件人	勾选此项时，只要有一个收件人存在于设置的收件人中，都能匹配策略； 不勾选此项，则需要所有的收件人都存在于设置的收件人中，才能匹配策略；
仅识别邮件正文	勾选此项时，仅扫描邮件正文 不勾选此项，则扫描邮件正文和附件。

上传控制	对通过浏览器、百度网盘客户端、微云客户端上传匹配敏感内容的文档进行控制。 支持的浏览器包括 firefox, 360se, chrome, baidubrowser, iexplore, opera, safari, qqbrowser, liebao, baidubrowser, 360chrome

说明

1. 发送邮件控制功能仅支持扫描邮件客户端发送的邮件，无法扫描网页邮件的正文和附件。如需扫描在网页邮件中上传的附件，可通过上传控制实现，但无法扫描网页邮件中的正文。
2. 敏感信息外传控制策略默认支持穿透压缩包识别压缩包中包含敏感内容的文件，当压缩包中的文件匹配中策略时，则策略控制整个压缩包的外传操作。

10.3.3 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；设置策略后，当本地新建、修改、复制、接受一份文件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。

策略属性说明

策略属性	说明
加密	勾选此项时，非加密的本地文件匹配敏感内容触发策略时，将加密此文件。可设置加密后文件安全属性，包括设置权限和访问权限；
敏感内容	选定已有的敏感信息分类(在“**分类管理->敏感信息分类库**”中设置)作为敏感内容；
文件类型	设置需要监控的本地路径，支持通配符；
包含范围	设置进行扫描的目录范围和文件类型，当本地文档所在目录和类型满足条件时才会进行扫描。支持多条设置，新建设置默认为本地硬盘目录的所有支持识别的文件。
排除范围	设置不进行扫描的目录范围和文件类型，支持多条设置 ；

其中，包含范围和排除范围中的目录设置目前支持本地硬盘，不支持网络盘。

目录必须是一个确定的合法的客户端本地磁盘路径,支持通配符“*”和通用路径{sd}。如：{sd}users*\Documents。注意，“*”在目录中仅能表示一层文件夹。{sd}代表系统盘根目录，如 C:\，必须使用小写字母，{sd}后直接接文件夹名，不能加“\”。

说明 1.若没有购买加密模块，则不会出现“加密”选项；
2.敏感信息落地控制策略默认支持穿透压缩包识别压缩包中包含敏感内容的文件。

10.4 敏感信息日志

敏感信息日志会记录在敏感信息全盘扫描任务、敏感信息外传控制策略、敏感信息落地控制策略中扫描到的匹配敏感内容的文件。管理员通过查看日志记录可以发现用户硬盘中保存的匹配敏感内容文件的情况，以及用户对这些文件的操作情况，为事后追查分类文件泄密提供审计线索。

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，包括类型、加密、禁止、警告、时间、计算机、计算机组、用户、用户组、信息分类、文件名称、路径、文件大小、描述。

属性名称	说明
类型	触发扫描的操作类型；包括复制到移动盘、复制到网络盘、IM 传送文件、发送邮件、新建、修改、扫描、上传文档。
加密	策略/任务对文件进行了加密操作；
禁止	策略阻止了文件的外传操作；
警告	触发策略后，控制台提示警告信息；
信息分类	文件匹配的策略中所有已选择的信息分类；
文件名称	文件的名称；
路径	文件所在路径；
文件大小	文件的大小；
描述	记录操作的一些详细信息，如使用 IM 外传使用的工具和发送邮件外传时邮件的详细。

敏感信息日志除了可以按通用的时间、时间类型 、范围查询外，还可以按以下

条件进行查询：

查询条件	说明
操作类型	默认是全部操作类型，也可通过下拉框选择其中一种或多种操作类型进行查询，比如，新建和修改的文档；
信息分类	默认是全部信息分类，也可看下拉框选择其中一个或多个信息分类查询，当选择多个信息分类查询时，匹配任一信息分类的日志均会显示在查询结果中；
路径	文件所在路径；
大小	文件的大小范围；
文档名称	操作文档的名称； 通过类型查找时，可在给出的默认类型中选择，也可以手动添加类型名称；
加密	勾选时被加密的日志，不勾选时查询全部的日志
禁止	勾选时仅查询被禁止的文件日志，不勾选时查询全部的日志
警告	勾选时仅查询有警告弹出的日志，不勾选时查询全部的日志；

说明 当扫描、触发策略的文件在压缩包中时，以每个匹配敏感内容的文件记录一条日志。

选中日志右键，可进行打印、打印预览、导出日志、删除日志、查询屏幕历史等操作。

第十一章. 资产管理

11.1 资产管理

资产管理功能搜集了所有客户端机器的软、硬件资产信息，方便管理员对企业内部的软硬件资产的维护和查看，并提供了各种查询条件，更方便了对各种资产的统计。

选择菜单“**资产管理->资产管理**”进入资产管理主窗口。资产管理窗口包括：标题栏、菜单栏、工具栏、任务导航栏、数据显示区、状态栏。

11.1.1 资产类别及资产属性说明

资产类别

资产的类别包括：

类别	说明
计算机类	是对客户端所在计算机的一些概要性的描述，如登录用户、域、机器名称等。
硬件类	是客户端机器的所有硬件设备，包括 CPU、内存、硬盘、主板、网卡等。
软件类	是客户端机器的软件类别，包括：操作系统、应用软件、杀毒程序、Windows 系统软件、微软产品补丁。
自定义类别	由客户自定义的无法自动获取的资产（如交换机，路由器，办公桌等）

资产属性

对于每一种资产，我们可能会有多个属性来描述它。比如对于内存有名称、插槽、容量、最大容量、内存条类型（如 DDR、SDRAM 等）；而对于硬盘我们会有名称、序号、容量等。

属性包括类别属性和实例属性

属性类型	说明
类别属性	是资产的统计属性，属于这个类，比如针对内存，会有其类别属性如内存总容量、最大容量和内存条数量等。
实例属性	是指这个资产类的一个实例的属性，比如内存是一个资产类，内存可以有多个，而针对每一个内存有其实例属性，如插槽、容量、类型等。

计算机类只会有类别属性(因为计算机始终只有一个)。
硬件和软件资产包含有类别属性和实例属性。
自定义类别只会有实例属性(因为这些都是用户自己定义的)。

11.1.2 资产类别管理

资产类别管理中会列出所有的资产类别及其各种属性，管理员可以通过资产类别管理查看某一种资产的所有属性，也可以手工添加资产属性。

选择菜单“**资产管理->资产类别管理**”打开资产类别管理窗口，左边视图是所有资产的树形结构，显示类别树，而右边视图是该资产的属性列表。在属性列表中，黑色字体的属性为类别属性，蓝色字体的属性为实例属性。

属性的值类型

属性有 5 种类型，用不同的图标表示。

图标	类型
	文字
	整数
	小数
	日期
	是/否

自定义属性

除了系统为各种资产定义的属性，管理员可以手工自定义属性。

假如需要新增一个 CPU 的实例属性“保修期”，在 CPU 右边的属性列表区域，选择菜单“**操作->新建属性**”打开资产属性编辑框，选择属性类型为“实例属性”，输入资产属性名称“保修期”，指定值类型为“日期”，单击【确定】按钮。

自定义的资产属性名称后加星号“*”标识。自定义的属性可以选择菜单“**操作->重命名**”或“**操作->删除**”来修改，但是系统默认的资产属性不能重命名和删除。

自定义资产

管理员可以自定义资产，将企业内的其它资产记录起来，方便随时查看和统计。

例如，企业内有 3 台打印机，管理员可以自定义资产“打印机”并且添加其属性值。选择菜单“**操作->新建资产**”输入资产名称为“打印机”，为打印机添加实例属性：型号、部门、购买日期、价格等。

对于自定义的资产，需要管理员手工添加这些属性值，属性值在菜单“**资产管理->其它资产**”中添加。

11.1.3 硬件资产查询

选择菜单“**资产管理->硬件资产**”可以查看客户端机器的所有硬件资产，也可以根据需要查询统计各类资产。

查看资产信息

系统默认统计所有客户端机器的 CPU、内存、硬盘驱动器和网卡概述信息，选择需要查看的计算机，单击右键“**属性**”或直接双击查看单个计算机的硬件资产信息。

资产信息窗口会默认显示计算机类和硬件类的资产信息，类似资源管理器，左边树形结构，显示类别树，右边是列表结构，显示属性内容。选择菜单“**显示->所有类别信息**”或“**显示->软件类别信息**”也可查看其它资产信息。

在资产实例属性中，有个默认属性【摘要】是对该资产实例的摘要信息，也是显示在资产类别树中的名称；在所有的类别属性中，有个默认属性【概述】是对所有实例的摘要的汇总。

提示 查看资产信息时，可以直接为自定义资产属性添加值。找到自定义的属性，选择菜单“**操作->属性**”打开资产属性编辑框，输入内容添加属性值。

查询资产

管理员可以设置一个或多个查询条件来统计需要查看的结果，单击资产结果列表右上方的查询按钮“  ”打开查询条件设置框，设置查询条件：

查询条件	说明
范围	默认是{整个网络}内所有的客户端机器，单击右边的“...”按钮只选择其中一个计算机组
	添加按钮，单击该按钮打开条件设置对话框，每个条件包括：资产属性、运算符和内容，如：内存-数量 == 2 是一个查询条件，CPU-名称 包含 “AMD”也是一个查询条件
	删除设置的查询条件
	查看并修改查询条件
满足任何一条即可	选中该项，则满足任何一个查询条件即可；不选中该项，则需要同时满足所有的查询条件

注意 设置查询条件时，如果一个条件中包含了某一个资产 A 的实例属性，再添加条件时就不可以再包含另一个资产 B 的实例属性，只能再添加类别属性的条件。

设置了查询条件后，添加结果列表，选择需要显示的资产属性。

图标按钮	说明
=>	在左边的资产类别树中选择需要显示的属性直接双击或单击该按钮移动到结果列表中
<=	将资产属性从结果列表中移出，可同时选择多个移出

注意 结果列表和查询条件一样，如果已经包含一个资产 A 的实例属性，无法再添加另一个资产 B 的实例属性。

设置好查询条件以及结果列表后，为了方便日后查询，可以将当前的设置保存或设置为默认，也可以删除不要的查询设置。

操作	说明
保存	输入保存的名称，单击【保存】按钮，下次需要使用时，直接从名称下拉框中找到输入的名称调出之前的设置；
删除	单击【保存】按钮，删除已经保存的查询设置。

设为默认	管理员可以更改查询设置并将其设为默认查询，单击【设为默认】按钮，则以后重新打开资产管理窗口，都显示的是默认查询结果

编辑自定义属性内容

以前面提到的自定义属性“CPU-保修期”为例，设置查询条件：“CPU-保修期”为“不存在”，结果列表：“计算机-概述”，“CPU-摘要”，“CPU-保修期”，查询结果可以看到“CPU-保修期*”列的内容都为空，选中一行记录，点击该列的区域，鼠标成可编辑状态，输入属性内容，该属性内容会保存到数据库。可依次添加其他的该属性值。

注意 结果列表中必须包含“CPU-保修期”，除此之外，由于“CPU-保修期”是自定义实例属性，所以结果列表中还必须包含 CPU 的其它任意一个实例属性，否则无法编辑属性值。

11.1.4 硬件资产变更

硬件资产变更记录了所有客户端机器的硬件资产的变化情况，包括增加、删除和变化。选择菜单“**资产变更->硬件资产变更**”查看所有硬件资产变更记录。

查看资产变更内容

硬件资产变更记录包含的内容有：变更类型、时间、计算机、计算机组、网络地址、资产类别、描述。

字段名称	说明
变更类型	资产的变化类型，包括增加、删除、变化；
资产类别	发生变化的资产类别；
描述	发生变化的描述信息，右键单击变更记录**“属性”**中可以查看详细信息，包含了资产的各属性内容的变更。

查询资产变更

选择菜单“**文件->新建查询**”打开硬件资产的查询栏，管理员可以设置各种查询条件来有针对性地查询：

查询条件	说明
时间和范围	通用查询条件；

类型	硬件资产类别，默认是全部，也可以在下拉框中指定其中一种资产进行查询；
内容	根据描述信息查询，支持模糊查询。

11.1.5 软件资产查询

选择菜单“**资产管理->软件资产**”切换到软件资产查询，默认查询计算机以及操作系统，管理员可以设置其它查询条件查询需要的结果。

软件资产查询类似与硬件资产查询，请参考硬件资产查询的说明。

11.1.6 软件资产变更

软件资产变更记录了所有客户端机器的软件变化情况，包括：增加、删除和变化。选择菜单“**资产管理->软件资产变更**”查看所有软件资产变更记录。

软件资产变更记录的内容与硬件资产变更记录类似，查询条件包括：

查询条件	说明
时间和范围	通用查询条件；
类型	软件资产的类别，包括：操作系统、应用软件、杀毒软件、Windows 系统软件、微软产品补丁；
内容	根据描述信息查询，支持模糊查询。

11.1.7 其它资产

管理员在资产类别管理中定义了资产类别以及资产属性后，需要在“**资产管理->其它资产**”中添加资产属性内容。

添加自定义资产

以前面定义的“打印机”为例，选择菜单“**文件->新建查询**”打开查询条件框，查询条件为空，结果列表为：打印机-型号、打印机-部门、打印机-购买日期、打印机-价格，查询出打印机的所有属性。

单击查询结果列表右上方的添加按钮“  ”输入第一台打印机的各种属性值，再依次添加记录，输入第二台和第三台打印机的属性值。打印机的属性记录会

保存起来，方便日后查询。

查询自定义资产

添加保存自定义资产的属性值后，也可以建立查询条件，选择菜单“**文件->新建查询**”设置查询条件，如：“打印机-价格” >= 1000，结果列表：打印机-型号、打印机-部门、打印机-购买日期、打印机-价格，则只查询出价格在 1000 元以上的打印机。

11.2 软件版本管理

如果企业购买了一些软件，并且这些软件具有安装数量的限制。软件版本管理可以帮助企业管理这些软件的安装授权情况。

11.2.1 软件类别管理

选择菜单“**软件版权管理->软件类别管理**”打开软件类别管理窗口，左边视图是所有软件的类别，而右边视图是该类别的软件列表。软件类别收集的信息包括软件信息，以及操作系统信息。

管理员根据企业购买的软件来分类，每款软件需要建一个类别。对于软件类别的操作包括：

操作	说明
新建分类	在应用程序类别根目录，选择“**操作->新建**”或单击右键“**新建**”增加一个新类别并输入类别名称；
移动应用程序	增加了分类，需要将相关的程序都移动到该分类，找到相关程序，右键“**移动到**”指定目标分类进行转移，或按住鼠标左键拖拽到指定分类； 可同时选中多个应用程序进行转移，按住 Ctrl 键或 Shift 键进行多选；

查找	选择“**文件->查找**”可以查找指定的应用程序及所在分类。 查找功能也可用于快速分类，比如需要将所有 QQ 程序移动到 QQ 分类，可以在查找中输入内容“qq”，则会查询所有的 qq 程序，然后将查询的结果一起拖拽到 QQ 分类，这样大大方便了管理员的分类工作。

11.2.2 版权采购情况

选择菜单“**软件版权管理->版权采购情况**”可以查看企业采购的所有软件信息，也可以根据需要查询各类软件信息。

新增软件采购信息

企业每购买一款软件，都可以在版权采购情况中新增一项采购信息。

点击右上角的新建按钮“”，填写采购的软件信息，可填写信息有：

策略属性	说明
采购日期	软件采购的日期；
软件类别	选择已定义的软件类别，必填项；
名称	对本次采购自定义一个描述，必填项；
数量	软件的 license 数量，此软件能安装在多少台计算机上，必填项；
到期日期	软件的有效期；
状态	此软件当前的状态，有效还是无效；
版本	软件的版本号；
制造商	软件的制造商；
合同编号	本次采购的合同编号；
合同金额	采购此软件的合同金额；
联系人	采购此软件的联系人；
联系方式	联系人的联系方式；
序列号	软件的序列号；
备注	其他需要记录的信息。

11.2.3 软件类别查询

选择菜单“**软件版权管理->软件类别查询**”可以查看客户端机器的所有软件信息，也可以根据需要查询各类软件信息。

使用右键菜单可以设置客户端上各软件的授权情况，如合法、非法、试用、免费。如企业够买了 10 套 Office 软件，在某客户端上安装了一套，则找到此客户端机器上的 Office 软件，设为合法。

11.2.4 软件类别统计

选择菜单“**软件版权管理->软件类别统计**”可以统计企业内指定软件类别的授权情况。

例如，可以查询统计企业内安装 Office 软件的数量；可以查询统计企业内已经设为合法或非法的 Office 软件的数量。

11.2.5 软件版权统计

选择菜单“**软件版权管理->软件版权统计**”可以统计企业内指定采购的软件的授权情况。

例如，可以查询统计企业内 Office 软件的购买数量、已授权的数量、剩余可授权数量、非法安装的数量、试用的数量等。

11.3 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，并且根据需要为客户端机器自动安装补丁，增强系统安全性，也节约企业下载成本，提高网络管理员的工作效率。

补丁的扫描、下载和安装

在安装服务器的机器上同时运行着补丁下载器，它会自动下载并更新补丁检测文件(wsusscan.cab)。客户端第一次安装后会自动从服务器下载补丁检测文件，一般在客户端启动半小时后自动检测补丁的安装情况。

如果对补丁安装没有特别要求，需要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**”。如果在客户端的补丁扫描已经完成再设置这 2 个选项，则只对以后扫描到的补丁和新加入的客户端生效。

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。

如果没有在“**工具->选项->补丁选项**”中设置“自动下载”和“自动安装”，则需要管理员为补丁设置下载策略来下载补丁到服务器，同时设置需要安装补丁的计算机，客户端机器会根据设置从服务器中获取补丁安装文件并且自动安装。

提示 设置下载策略和安装策略时可结合 CTRL 和 SHIFT 键，同时对多个补丁或计算机设置策略。

控制功能

管理员可以在控制台上直接下达扫描或下载补丁的命令，在列表视图的右上方有一个命令按钮“”和范围按钮“”。点命令按钮，可以选择下载检测文件，刷新补丁下载状态和检测整个网络系统补丁。

控制功能	说明
下载检测文件	选择“**下载检测文件**”，服务器会立即下载最新版本的补丁检测文件；
刷新补丁下载状态	选择“**刷新补丁下载状态**”，服务器会立即下载设置了下载策略的补丁；
检测整个网络系统补丁	选择“**检测整个网络系统补丁**”，所有的客户端机器会立即扫描一次补丁；
检测系统补丁	假如只需要立即扫描一台机器的补丁，右键单击计算机信息，选择菜单“**检测系统补丁**”，则只会立即扫描指定的客户端机器的补丁；
选择计算机范围	点击范围按钮可选择查看一个计算机组或单个计算机的补丁安装情况。

11.3.1 按补丁模式查看

补丁日志内容

按补丁模式查看可以查看由客户端机器上扫描出来的所有补丁列表，补丁记录包括：

属性名称	说明
严重级别	补丁本身的级别，包括：低、中等、重要、严重和未知。
公告号	微软发布的补丁的公告号。
补丁 ID	补丁 ID。
发布时间	补丁的发布时间。
名称	补丁的名称，一般也包含了补丁 ID。
下载策略	管理员设置的该补丁的下载策略：下载/不下载，不下载该列为空，服务器不会自动下载这个补丁。选择该补丁，右键可以设置下载策略。
下载状态	补丁的下载状态，包括：未下载、下载中、已下载，鼠标移动到一个补丁，会自动显示该补丁的下载进度，下载完成为 100%。
未安装数量	需要安装该补丁但是没有安装的客户端机器的数量，选择该补丁，在下面的计算机列表中可以查看已安装和未安装的计算机；
已安装数量	需要安装该补丁且已经安装的客户端机器的数量；
计算机总量	系统检测出需要安装该补丁的客户端机器总数，即未安装数量和已安装数量的总和；
安装成功率	该补丁的安装成功率，即已安装数量和计算机总量的比值；
详细信息	双击或右键单击一个补丁“详细信息”可以查看补丁的其它信息，包括：下载路径、补丁大小以及补丁的描述信息。

补丁下载设置

在补丁模式下查看到所有客户端机器的补丁列表。如果之前没有设置“新出现的补丁默认自动下载”，则管理员需要手工设置。

右键单击补丁信息，设置“下载/不下载”，设置了“下载”的补丁服务器会自动下载，下载策略中用“✔”表示；设置了“不下载”的补丁服务器不会自动下载，下载策略中内容为空。

对于以后出现的补丁，也可以设置是否自动下载。在控制台主菜单“**工具->选项->服务器设置->补丁选项**”中可以设置【新发现的补丁默认自动下载】。

补丁查询

在补丁模式下，点击列表视图的右上方的查询按钮，可根据条件查询具体的补丁，查询条件包括严重级别、公告号、补丁 ID 和名称。其中严重级别有：全部、未知、低、中等、重要、严重。公告号、补丁 ID 和名称支持通配符、部分匹配。

11.3.2 按计算机模式查看

计算机日志内容

按计算机模式查看可以查看所有客户端机器的信息以及补丁安装情况，计算机信息包括：

属性名称	说明
计算机	客户端机器的分组和计算机名称；
网络地址	计算机的 IP 地址；
操作系统	计算机的操作系统；
最后扫描时间	计算机的补丁扫描的最后时间；
安装策略	是否自动安装补丁。
未安装数量	该计算机需要安装但尚未安装的补丁数量，选择该计算机，在下面的补丁列表中可以查看已安装和未安装的补丁；
已安装数量	该计算机需要安装且已经安装的补丁数量；
补丁总量	该计算机需要安装的补丁总数，即未安装数量和已安装数量的总和。

计算机补丁安装设置

在“**补丁管理->计算机模式**”下显示了客户端机器列表以及补丁安装明细。如果之前没有设置“新出现的客户端默认自动安装”，则管理员需要手工设置。

右键单击计算机信息，设置“**安装/不安装**”，设置了安装的计算机会自动安装下载了的补丁；设置不安装的计算机不会自动安装补丁。

管理员也可以针对单个计算机的部分补丁单独设置安装策略，在指定计算机的

补丁明细列表中选择补丁记录，右键设置“安装/不安装”。

在控制台主菜单“**工具->选项->服务器设置->补丁选项**”中可以设置【新发现的客户端默认自动安装】。

11.4 漏洞检查

漏洞检查功能自动扫描网络内的计算机的漏洞并进行统计，方便网络管理员查看及统计计算机漏洞，并针对这些漏洞及时采取应对措施，修复计算机漏洞，增强计算机的安全性。

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。

11.4.1 按漏洞模式查看

在“**漏洞检查->漏洞模式**”下可以查看漏洞列表以及哪些计算机有漏洞，漏洞列表包含的内容有：

属性名称	说明
严重级别	漏洞的级别，包括：信息、一般和严重；
名称	漏洞的名称摘要；
有漏洞数量	存在该漏洞的客户端机器的数量；
无漏洞数量	没有该漏洞的客户端机器的数量；
其它详细信息	右键单击一个漏洞信息“详细信息”中可以查看该漏洞的详细描述信息以及解决方法，管理员可以根据解决方案手工修复漏洞。

11.4.2 按计算机模式查看

在“**漏洞检查->计算机模式**”下查看计算机信息以及漏洞明细。
计算机信息包括：计算机、计算机组、网络地址以及操作系统；
漏洞明细包括：严重级别、名称、有无漏洞。

双击某个漏洞，可查看漏洞的详细信息及解决方法。

11.5 软件分发

通过 IP-guard 控制台，管理员可以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，透过使用软件分发功能，管理员能迅速地对整个网络的软件使用和业务应用做统一的部署，大大减轻了管理员的负担。

选择菜单“**资产管理->软件分发**”管理员可以建立分发任务。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。

11.5.1 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。

设置常规信息

首先设置常规信息，包括：

字段名称	说明
程序包名称	程序包名称默认为“新程序包”，管理员可以修改名称，但是不能为空；
创建时间 修改时间	这两项都是系统自动生成的，不能编辑，新建时为空，创建完成再查看或者编辑时就可以看到创建时间和管理员名称；如果修改了该程序包，修改时间也会跟着变化；
操作系统	选择该程序包有效的操作系统，可以选择多个，默认全选；
系统语言	选择一种该程序包有效的系统语言，默认选择“全部”。

设置文件信息

在左边视图中切换到“文件信息”设置文件信息，包括：

字段名称	说明
常规	包括程序包大小、所在计算机、原始路径。
程序包大小	程序包创建后的大小（只读）；
所在计算机	创建该分发程序包时控制台所在的计算机名称（只读）；
原始路径	该分发程序包文件的原始路径（只读）；
分发模式	包括安装软件，执行程序和派发文件三种方式。
安装软件	派发应用软件安装程序到客户端机器并且安装；
执行程序	在客户端机器执行且仅执行一次指定的程序；
派发文件	派发指定的文件到客户端机器上；
命令行	当分发模式是“安装软件”或“执行程序”时，需要设置命令行参数。 安装软件模式的命令行一般为核心安装文件的名称，执行程序模式的命令行为执行程序的文件名称。 可以手工输入命令行，也可以在下面的文件列表中选择要执行的安装文件或程序，右键提取文件名为命令行。
目标路径	当分发模式是“派发文件”时，需要设置文件包的目标路径，即文件被派发到目标计算机的详细路径。目标路径默认为“{desktop}\deploy files”，即系统桌面的“deploy files”目录。
运行模式	“以当前登录用户身份运行”是指以当前客户端机器登录的用户权限来安装程序。不选中“以当前登录用户身份运行”则是以系统 system 用户的权限来安装程序。
文件列表	显示程序包中的各个文件和目录。文件列表信息包括：文件名称、文件大小、修改时间以及版本信息。 点击列表右上方的新增按钮“”，选择需要分发的文件(文件夹)，可同时添加多个文件和文件夹，但是这些文件和文件夹必须在同一个父文件夹内。 每次点击新增按钮选择文件时都是重新创建一个新文件列表，会自动覆盖掉之前选择的文件列表。

设置检测条件和必要条件

检测条件是检查软件是否成功安装的标准，客户端会自动检测此条件，如果满足条件则认为软件安装成功，否则会继续尝试安装。“安装软件”模式必须设置检测条件，其它分发模式不需要设置。

必要条件是执行本程序包所必须具备的条件，在派发程序包之前检测该条件，

条件满足才派发，否则不派发，此条件是可选配置。

针对不同的系统软件环境的判断，检测条件或必要条件的设置有 5 种类型：

检测条件	说明
文件	判断某个文件是否存在，需要输入全路径；
文件版本	判断文件以及版本，需要输入全路径；
注册表项	判断某个注册表项存在；
注册表值	判断某个注册表项以及注册表值作更详细的定位；
安装的软件	一般是指在“**控制面板->添加/删除程序**”中的程序名称。

检测条件实例：

下面是制作安装 Microsoft Office 2003 程序包的检测条件

条件类型	逻辑	内容
文件	存在	{pf}\Microsoft Office\OFFICE11\EXCEL.EXE
文件版本	>= 11.0.5612.0	{pf}\Microsoft Office\OFFICE11\EXCEL.EXE
注册表项	存在	SOFTWARE\Microsoft\Office\11.0\Access\InstallRoot
注册表值	存在	SOFTWARE\Microsoft\Office\11.0\Access\InstallRoot – Path
安装的软件	包含	Microsoft Office Professional Edition 2003

提示 条件的指定文件路径的字符串可以包含预定的宏，如：

"tmp" temp folder(c:\windows\temp)

"win" windows directory(c:\windows)

"sys" system directory(c:\windows\system32)

"sys32" system directory(32 位系统 c:\windows\system32；64 位系统 C:\Windows\Syswow64)

"pf" program files(c:\program files)

"pf32" program files(32 位系统 c:\program files;64 位系统 C:\Program Files (x86))

"sd" system drive(c:\)

"cf" common files(c:\program files\common files)

"cf32" common files(32 位系统 c:\program files\common files; 64 位系统 C:\Program Files (x86)\common files)

程序包的删除和修改

删除操作是将程序包删除，编辑操作是修改程序包的参数，条件等信息。只有当程序包的状态为“准备就绪”时才可以对程序包进行删除和修改；当没有使用该程序包的分发任务时，该程序包处于“准备就绪”状态。

11.5.2 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。

分发任务的设置包括：

字段名称	说明
任务名称	默认名称是“新任务”，管理员可以修改，名称不能为空。
程序包名称	点击“…”按钮选择需要使用的分发程序包。
最多重试次数	分发任务失败后会尝试重试，重试次数默认是“10”，也可以修改为其它整数（输入 0，则分发任务除非中止，否则如果失败会一直重试下去，直到分发能够成功）。
状态	显示该任务的状态。可点击【设置】按钮设置执行模式以及执行周期。
执行模式	选择“持续执行”，则任务会进行根据执行周期持续执行。 持续执行的情况下，勾选“分发成功后停止执行”，则分发任务成功后，客户端将不会在继续执行分发。 选择“只执行一次”，则任务仅执行一次，无论成功与否，完成后不会再执行。
执行周期	选择“立即执行”，则分发任务创建后马上执行（如果客户端不在线，则在下次启动时执行）。 选择“计算机启动时”，则计算机启动时才执行分发任务（如果客户端在线需要重启才会执行）。 选择“指定时间”并设置好时间，则到了指定的时间才会执行分发任务。

目标计算机	点击“  ”按钮选择分发任务的目标客户端计算机。

任务属性设置好后点击【确定】，分发任务立即启动，在任务列表中可以查看任务分发情况。

可查看到的信息包括：

属性名称	说明
任务名称	创建时设置的任务名称；
程序包名称	创建时选定的程序包名称；
任务状态	任务的当前状态；
成功数量	该任务成功分发到的目标计算机数量；
失败数量	该任务分发失败的目标计算机数量；
进行中数量	该任务还在分发中的目标计算机数量；
其他数量	其他状态的任务数，该数值由任务总数减去成功数量、失败数量以及进行中数量三者之和得到；
计划安装数量	该任务计划要安装的数量，即创建时选定的目标计算机数量；
任务数	任务总数，每台选定的目标客户端计算机拥有一个任务，即也可认为是选定的目标客户端计算机总数；
安装成功率	任务分发的成功概率，即成功数量和计划安装数量的比值。

分发任务也有删除和编辑操作。在任务分发过程中，不能删除和编辑，必须先停止该任务的分发（可以单击某个分发任务，右键选择“停止”），然后再进行删除和编辑。

复制分发任务

在分发任务信息栏中，选中任务右键，选择"**复制该分发任务**"选项，弹出新建对话框，可复制此任务信息新建任务。在新建的对话框中，程序包名称为空，其他选项设置如原任务。

注意 如果分发任务在进行列表中使用的程序包的状态为“程序包正在使用中”，不能删除和修改，只有将分发任务删除，对应的分发程序包的状态才会变为“准备就绪”。

11.6 软件卸载

通过 IP-guard 控制台，管理员可以向客户端设置软件卸载任务，达到快速批量卸载软件的目的。同时可以监控客户端的软件安装情况，防止再次安装指定软件。

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。

两种模式下设置任务时，均需要对任务的模式以及执行时段进行设置，说明如下：

字段名称	说明
任务模式	任务执行时的模式选择。
持续执行	持续执行：会持续监控该软件，一发现有安装，则在指定的执行时段卸载该软件。
仅执行一次	仅执行一次：卸载任务执行一次后，无论成功或失败，不会继续卸载。
执行任务时段	任务的执行时段选择。
立即执行	发现该软件已安装，立即卸载。
空闲时执行	发现该软件已安装，客户端超过 3 分钟不动鼠标和键盘，控制台上客户端状态是（空闲）时，开始卸载。
指定时间执行	发现该软件已安装，在设置的指定时间执行卸载，设定的时间指的是每天的某个时间。

11.6.1 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。

安装软件列表

在“**软件卸载->软件模式**”下可以查看由所有客户端机器上扫描出来的所有安装软件列表，列表包含的内容有：

属性名称	说明

软件名称	软件的名称；
公司名称	软件的公司名称；
安装数量	安装该软件的客户端机器的数量；
任务数	接受卸载该软件任务的客户端机器的数量；

选择一个软件，可以查看具体安装了该软件的客户端机器信息，同时也可以查看执行卸载该软件的客户端机器信息。

安装的计算机以及执行卸载任务的计算机，都包含以下信息：

字段名称	说明
计算机	客户端机器的计算机名称。
计算机组	客户端机器所在的分组。
用户	客户端机器当前登录用户。
网络地址	客户端机器的网络地址。
操作系统	客户端机器的操作系统信息。
状态	客户端的运行状态，和基本信息中的客户端状态一致，包括：正在运行、离线、客户端已被卸载；
软件版本	安装/卸载 选定的软件时，该客户端上该软件的版本号。
软件状态	软件状态分为：使用中/卸载中； 未设置卸载任务，则该软件的状态为“使用中”； 设置了卸载任务，即使受执行时段等的影响任务，并未能马上执行，该软件的状态会变为“卸载中”。
大小	该软件的安装大小。
安装时间	客户端安装该软件的时间。
安装路径	该软件在客户端上的安装路径。
任务模式	持续执行，或仅执行一次。 仅在执行卸载任务计算机列表中显示此列。

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。

11.6.2 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。

客户端机器列表

在“**软件卸载->计算机模式**”下查看计算机信息以及软件安装、卸载的明细。

在客户端机器列表中，选择一台客户端，可以查看该台客户端机器下，所有安装软件的信息，内容包括：软件名称、公司名称、软件版本、大小、安装路径。

同时也可以查看对该台客户端设置的所有软件卸载任务信息。

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。

11.6.3 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：

字段名称	说明
卸载任务	需卸载的软件名称。
任务模式	任务设置时选定的任务模式。
上一次结束时间	客户端上一次结束该任务的时间。 对于仅执行一次的任务，上一次结束时间为该任务执行一次结束时的时间，不会变化； 对于持续执行的任务，上一次结束任务时间为每一次执行任务结束的时间，会变化
任务状态	任务状态分为：未启动/进行中/成功/失败； 对于持续执行的任务，每一次完成后任务状态都会变为未启动，后面跟着上一次执行的结果（成功/失败）

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。

说明

1. 对于“仅执行一次” 且已完成的任务，执行删除操作后，列表中删除此任务。
2. 对于“仅执行一次”且还未执行(没到指定时间)的任务，执行操作操作后，列表中删除此任务，到了指定时间也不会进行。
3. 对于“持续执行”的任务，右键菜单点“删除任务”，列表中删除此任务，以后再安装上指定程序也不会执行。

卸载任务总览

点击软件卸载界面的图标后，会弹出卸载任务对话框，可设置查询条件搜索指定的卸载任务总览信息。查询结果可通过右键菜单打印或导出。

查询条件	说明
范围	客户端机器范围，可选择某个分组；
卸载软件名称	卸载的软件名称，支持模糊查询；
卸载任务模式	卸载任务的模式：全部/仅执行一次/持续执行；
卸载任务状态	卸载任务的状态：全部/未启动/进行中/成功/失败。

第十二章. 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。

12.1 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，为了避免严重问题，将这些系统程序分离开来，单独放在该分类，管理员也可以根据需要移动其它的程序到该分类。

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。

应用程序也可通过“应用程序识别规则”来分类。应用程序识别规则相当于一个标签，能够匹配上这个标签的应用程序记录，就会去到该识别规则所处的分类下。

管理员根据企业管理的需求将类型相同的应用程序放在一个类别，对于分类的操作包括：

操作	说明
新建类别	在应用程序类别根目录，选择“**操作->新建**”或单击右键“**新建**”增加一个新类别并输入类别名称；在一个类别中也可增加子分类，选择该分类，单击右键“**新建**”则在该分类中新建一个子分类；

移动应用程序

增加了分类，需要将相关的程序都移动到该分类，找到相关程序，右键“**设置程序类别**”或选择“**操作->移动到**”指定目标分类进行转移，或按住鼠标左键拖拽到指定分类；弹出设置识别规则窗口，可指定应用程序目标类别和设置识别规则的类型，进行转移；可同时选中多个应用程序进行转移，按住 Ctrl 键或 Shift 键进行多选；

查找

点击工具栏上的“  ”图标或选择“**操作->查找**”，显示查找窗口，可以查找指定的应用程序及所在分类或应用程序识别规则。

应用程序库的查找分为“识别规则查找”和“应用程序记录查找”。

1.当应用程序库界面上显示“应用程序识别规则”栏，则查找框属性是“识别规则查找”，输入条件，点击查询即可查找到对应的识别规则；

2.当应用程序库界面上不显示“应用程序识别规则”栏，则查找框属性是“应用程序记录查找”，输入条件，点击查询即可查找到对应的应用程序记录；

查找功能也可用于快速分类，比如需要将所有 QQ 程序移动到 QQ 分类，可以在查找中输入内容“qq”，则会查询所有的 qq 程序，然后将查询的结果一起拖拽到 QQ 分类，这样大大方便了管理员的分类工作。

导出应用程序

选中一条应用程序或一个应用程序类别，选择“**操作->导出**”或右键“**导出**”，即可导出选中的应用程序；

显示识别规则

点击工具栏上的显示识别规则图标“  ”，可显示或隐藏应用程序识别规则栏；若显示识别规则，则应用程序分类视图会变成上、下视图，识别规则显示在上视图，应用程序显示在下视图。

新建识别规则

点击工具栏上的新建识别规则图标“  ”或选择“**操作->新建识别规则**”，或者通过应用程序记录创建；打开设置识别规则窗口，可按名称、文件名称、公司名称、图标和应用程序类别来设置新的识别规则；选中识别规则，在应用程序栏看见能够匹配上的应用程序；

导入识别规则库

选择“**操作->导入识别规则库**”，可导入识别规则库文件，文件类型为.csv 文件；

导出识别规则库

选择“**操作->导出识别规则库**”，可将应用程序库上的识别规则导出到本地，保存为.csv 文件类型；

删除识别规则	选中一条识别规则，“**右键->删除**”，能删除掉识别规则；但跟随此识别规则的应用程序记录不会被删除，该应用程序记录会寻找其它能匹配上的识别规则，若寻找匹配失败，则会自动回到未分组中。

注意 未分类和系统应用程序类别都不能删除，也不能创建子类别。

新建识别规则

目前支持的识别规则如下：

识别规则	说明
文件名称识别	仅根据文件名识别，文件名称相同的程序识别为同一类；
文件名称+公司名称识别	根据文件名称和公司名称识别，两者均匹配的程序识别为同一类；
这类应用程序的特征识别	根据应用程序内部 hash 值识别，此 hash 值为程序自定义的算法得出，可最大程度的使出自一间公司的同一款软件，不同版本的程序被识别为同一类（如搜狐新闻 1.6.0 和搜狐新闻 1.7.3），也可避免因修改应用程序名称而规避掉前面两种识别规则；
这个应用程序的特征识别	根据应用程序唯一标志识别，匹配上此标志的程序识别为同一类，仅针对所选程序可匹配成功，其他程序不会匹配成功。

说明 应用程序匹配识别规则的优先级为：这个应用程序的特征识别>文件名称+公司名称识别>文件名称识别>这类应用程序的特征识别。

识别规则的创建方式有两种：手动创建和通过应用程序记录创建。

手动创建识别规则的步骤如下：

1）点击工具栏上的显示识别规则图标“  ”，显示出应用程序识别规则栏；

2）选中一个应用程序分类组，点击工具栏上的新建识别规则图标“  ”或选择“**操作->新建识别规则**”，弹出识别规则设置窗口；

3）在识别规则设置窗口中输入名称+文件名称，可以选择是否勾选公司名称，选择类别，填写备注信息，点击“**确定**”；

4）在该应用程序分类组下显示出新建成功的识别规则，选中此识别规则，可以在应用程序栏看见能够匹配上的应用程序。

注意 1.通过手动创建识别规则的方法只能创建出“以文件名称识别的规则”和“以文件名称+公司名称识别的规则”。

2.在创建时勾选公司名称的识别规则即为“以文件名称+公司名称识别的规则”。

3.创建时不勾选公司名称的识别规则即为“以文件名称识别的规则”。

通过应用程序记录创建识别规则的步骤如下：

1）在应用程序栏，选中一个应用程序记录，“***右键->设置程序类别***”或者直接拖拽一个应用程序记录至左侧分类树中的某个分组，弹出“设置识别规则”窗口；

2）在设置识别规则窗口点击…按钮，选择应用程序分组类别；若是拖拽方式，分组会默认为应用程序记录拖拽至的分组；

3）选则需要创建的识别规则类型，包括有：文件名称识别、文件名称+公司名称识别、这类应用程序的特征识别、这个应用程序的特征识别；

4）点击“***确定***”按钮，即可在对应分组下找到新建的识别规则，选中此识别规则，可以在应用程序栏看见能够匹配上的应用程序。

注意 通过应用程序记录创建识别规则不需要手动输入名称等信息，识别规则上的信息均是从应用程序记录中自动获取的。

12.2 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。

操作	说明

新建分类	在左侧的网站类别视图选择“**操作->新建->网站类别**”新建网站类别并命名；也可在一个分类下面新建一个子分类；
新建网站标识	建好分类后，在右侧的网站视图单击右键“**新建->网站标识**”增加一个网站识别并输入名称和网址，网址的输入可以是完整的网址，也可以支持通配符“*”“？”等，如：*sina*，*game*等；
导入网站标识	选中某个分类，在右侧的网站视图单击右键“**导入网站标识**”，可批量导入网站标识；
查找	选择“**操作->查找**”或单击工具栏上的查找按钮  可以查找指定的网站属于哪个分类或是否存在，查找支持模糊查询。
导出网站库	在左侧的网站类别视图选择“**操作->导出网站库**”，或者右键菜单中选择“**导出网站库**”，可以导出整个网站库，包含所有的层级结构和网站标识；
导入网站库	在左侧的网站类别视图选择“**操作->导入网站库**”，或者右键菜单中选择“**导入网站库**”，可以将事先导出的网站库导入到“**网站类别**”节点下。

此外，可以在网页浏览日志和上网浏览统计中，选中一条记录，单击右键“**添加到网站类别**”， 将该记录的网址添加到指定的已存在分类库中。

12.3 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。

操作	说明
添加时间类型	单击该增加按钮“  ”增加一个新类别并且输入类别名称，时间范围默认是全天，需要手工编辑修改时间段。
删除时间类型	选择需要删除的时间类别，单击删除按钮“  ”删除时间类型，系统默认的四个时间类型不能删除。

12.4 移动存储分类

为了方便管理企业内部移动存储盘的使用，我们需要在移动存储库中首先对企业内部所有使用的移动存储盘进行分类。管理员可以把属于一个部门或者个人使用的移动存储盘放在一个分类，然后对这些分类的存储盘授予不同的权限，以防止资料的泄露。

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。

移动存储盘可进行注册管理。选择“*分类管理->移动存储*”打开移动存储窗口，系统默认有 “已注册”类别和“未注册”类别。所有新获取到的移动存储盘都会存储在“未注册”类别中，注册了的移动存储盘将会移至“已注册”类别下。管理员可以手工在“已注册”类别中添加新类别，“未注册“类别下不可再建类别。

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。

本地移动存储信息各项操作说明：

图标按钮	说明
	手工刷新本地移动存储列表；
	设置移动存储分类，，第一次插入的盘默认放在“未分类”，单击该按钮，可以选择其它分类进行存放；
	安全退出本地插入的加密盘.
	修改移动本地移动存储设备的卷序列号；
	保存按钮，将移动存储信息保存到分类库；

	点击出现的菜单，可对移动设备进行相关操作；
设置移动存储分类	第一次插入的盘默认放在“未分类”，单击该按钮，可以选择其它分类进行存放；
格式化成非加密盘	将一个加密盘格式化为非加密盘；
格式化成加密盘	将一个非加密盘格式化为加密盘；
初始化安全 U 盘	初始化安全 U 盘交互区，会要求重新设置交互区的密码，初始化后交互区原有的所有文件将会被清空；
安全退出	安全退出本地插入的加密盘；
设置卷序列号	修改移动本地移动存储设备的卷序列号；
查看交互区日志	查看安全 U 盘中还未上传的交互区日志；
	移动存储注册管控的相关操作；
注册	注册移动盘；
注销	注销已注册的移动盘；
取消挂失	对已挂失的移动盘取消挂失；
修改注册信息	修改移动盘的注册信息。

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，可设置包含范围和排除范围，以及是否弹出警告信息。

启用注册管控后，在设置范围内的客户端上，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。

图标按钮“  ”的其余操作说明：

操作名称	说明
注销	已注册，但不再使用的移动存储，可以选择注销操作； 注销后的移动存储盘将不能在客户端上再使用，信息会自动移动到“未注册”类别；
挂失	已注册，但遗失了的移动存储，可以选择挂失操作； 挂失后的移动存储盘将不能在客户端上再使用，信息仍然保留在原分组。
取消挂失	执行了挂失的移动存储盘找回来了，若想继续使用此盘，可以选择取消挂失操作； 取消挂失后的移动存储盘将能正常在客户端上使用；
修改注册信息	此操作可修改注册时填写的设备名称、设备编号等信息；

移动存储的属性说明

移动存储设备包括 U 盘、移动硬盘、记忆棒、智能卡等可移动设备。移动存储的属性内容包括：

属性名称	说明
UDiskID	每一个可移动设备都有一个 UDiskID，UDiskID 是一个移动存储设备的唯一标识信息，格式化也不会发生改变；
卷序列号	每一个可移动设备都有一个序列号，格式化后卷序列号可能发生改变。
设备描述	对这个移动存储的描述信息。

备注信息	为了方便查看和区分移动盘，可以添加一些注释信息，默认为空，单击右键“**修改备注**”输入备注信息，比如：使用者，资产编号等。
卷容量	该移动存储盘的容量大小。
分区格式	该移动存储盘的分区格式，一般为：FAT，FAT32，NTFS。
类型	是否为加密盘，类型为空表示为普通盘（非加密盘）
卷标	移动存储盘的卷标。
首次注册时间	该移动存储盘首次注册的时间；
过期时间	该移动存储盘注册时设置的过期时间；
状态	该移动存储盘的注册状态，分为以下 5 种： 1.正常：已注册的移动存储盘； 2.注销：执行了注销操作的移动存储盘； 3.挂失：执行了挂失操作的移动存储盘； 4.过期：注册时设置了有效期，过了有效期的移动存储盘； 5.未注册：没有注册过的移动存储盘；
上次操作时间	上一次该移动存储盘使用（插入或拔出）的时间；
上次操作的计算机	上一次使用该移动存储盘的客户端计算机；
数量	该移动存储盘的识别信息数量，即有多少条移动存储信息在当前识别规则下识别为该移动存储盘； 选中该移动存储盘，右键属性，可以查看具体的识别信息；
设备名称	移动存储设备的名称信息；
设备编号	移动存储设备的编号信息；
部门	移动存储设备所属部门信息；
设备使用人	移动存储设备的使用人名称；
职位信息	移动存储设备的使用人的职位信息；
联系方式	移动存储设备的使用人的联系方式信息；
工号	移动存储设备的使用人的工号信息；
最后修改时间	该移动存储盘注册信息的最后修改时间；
查看使用情况	双击移动存储信息可以查看其详细属性，点击【查看使用情况】按钮可以查看该盘的使用情况，确定该存储盘的使用范围。或直接右键单击一条存储信息选择“**查看使用情况**”查看该存储盘的使用情况。

识别规则

选择“**分类管理->移动存储**”打开移动存储库，选择菜单“**操作->识别规则**”设置移动存储识别规则。目前支持 UDisk ID 和卷序列号两种识别方式。

默认使用 UDiskID 作为匹配规则。如果多个移动设备的 UDiskID 相同，则需要在识别规则中可添加此 UDiskID 为非法 UDiskID，非法 UDiskID 的移动存储设备则使用卷序列号作为匹配规则。

可以设置特定的一个或多个 UDiskID 为非法 UDiskID，输入完整的 UDiskID 内容，支持“;” “,”作为分隔符。也可以设置任意的 UDiskID 为非法 UDiskID，即所有移动存储设备都使用卷序列号为匹配规则。

查找

移动存储库提供了多种查询条件以方便管理员查找需要的移动存储信息，选择“**文件->查找**”或直接点击工具栏上的【查找】按钮“🔍”打开查询框：

查找条件	说明
UDiskID	按 UDiskID 进行查询，输入指定的 UDiskID，支持模糊查询；
卷序列号	按卷序列号进行查询，输入指定的卷序列号，这里不支持模糊查询，需要输入完整的序列号；
类别	默认是全部分类，也可以指定其中部分类别进行查询；
描述	按移动盘的描述信息进行查询，支持模糊查询，比如输入 usb，则查询出的结果中设备描述包含 usb；
卷标	不输入任何任务代表全部，输入卷标如 h 进行查询；
加密盘类型	默认是所有类型，也可以指定加密盘或非加密盘进行查询；
分区格式	按照分区格式进行查询，如输入 NTFS 查询分区格式为 NTFS 的所有移动盘信息；
备注	根据备注信息进行查询，支持模糊查询；
卷容量	设置一个卷容量的范围，按移动盘的卷容量进行查询；
最后使用时间	设置一个时间范围，按移动盘的最后使用时间进行查询；
注册有效期	设置一个时间范围，按移动盘的注册有效期进行查询；
注册状态	默认全部状态，也可以指定状态进行查询；
关键字	设置关键字，在注册信息和备注里查找，支持模糊匹配。

管理员可设置多个查询条件，进行更精确的查询，查询的结果中包含了移动盘

所属的类别信息，管理员可以拖动移动盘信息到指定的类别。

状态统计

在移动存储分类库选择“**操作->状态统计**”，可查看移动存储库中 U 盘的注册和使用情况。

导入导出移动存储库

在移动存储分类库选择“**操作->导出移动存储库**”，可将当前整个移动存储分类库导出。“**操作->导出移动存储库**”则可将事先导出备份的移动存储分类库整个导入。

注意 1.导出时，识别规则中的非法 UDiskID 信息和所有已注册信息，不导出未注册信息；
2.当识别规则中包含“仅使用卷序列号识别”时，无法进行导入导出操作。

12.5 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。

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。

12.6 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。

12.7 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。

操作	说明
新建分类	在左侧的软件安装包类别视图选择“**操作->新建**”新建软件安装包类别并命名；也可在一个分类下面新建一个子分类；

新增软件安装包	建好分类后，在右侧的软件安装包视图单击右键“**新增**”，此时会弹出新增设置对话框， 在软件安装包列表视图： 单击工具栏上的添加文件按钮，可以选择软件安装包添加； 也可以单击工具栏上的添加文件夹按钮，选择某个文件夹添加，此时选定文件夹里的软件安装包将会被添加； 不支持手动输入添加； 在分类视图： 选择需要添加到的分类； 选择新增重复时的新增方式： 允许新增到不同分类：当新增的软件安装包已存在分类库的其他分类时，允许新增的安装包到不同的分类； 仅新增新的安装包，忽略已存在的安装包：忽略已存在分类库中的安装包，只增加新的安装包 把安装包从原来的分类移动到新分类：当新增的软件安装包已存在分类库的其他分类时，会把安装包从原来的分类移动到新分类
查找	选择“**操作->查找**”或单击工具栏上的查找按钮可以查找指定的软件安装包，支持模糊查询。
属性	在右边的列表视图选中一个软件安装包，选择“**操作->属性**”或单击工具栏上的属性按钮，可以查看该软件安装包的相关属性信息；
复制到	在右边的列表视图选中一个或多个软件安装包，右键菜单“**复制到**”，会将选中的记录复制到其他分组，一个软件安装包可以同时存在于不同分组。通过手动拖拽的效果与复制到一致。
移动到	在右边的列表视图选中一个或多个软件安装包，右键菜单“**移动到**”，会将选中的软件安装包剪切到其他分组，原来的分组不再有此安装包。

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。

12.8 软件卸载分类

管理员可以根据企业需要，将软件进行分类，方便管理员按照类别控制员工卸

载情况。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。

软件卸载库的新建分类、查找、查看属性、复制到、移动到操作类同于软件安装库，新增卸载软件操作则有不同。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。

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

12.9 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。

操作	说明
新建分类	在左侧的邮箱类别视图选择“**操作->新建->邮箱类别**”新建邮箱类别并命名；也可在一个分类下面新建一个子分类；
新建邮箱标识	建好分类后，在右侧的视图单击右键“**新建->邮箱标识**”增加一个邮箱识别并输入名称、邮箱、组织机构、备注信息； 其中，邮箱为必填项，支持通配符。可以输入完整的邮箱地址，如“123@qq.com” ，可以使用通配符输入一类邮箱地址，如“*@126.com”；
导入邮箱标识	选中某个分类，在右侧的视图单击右键“**导入邮箱标识**”，可批量导入邮箱标识；
查找	选择“**操作->查找**”或单击工具栏上的查找按钮可以查找指定的邮箱属于哪个分类或是否存在，查找支持模糊查询。
导出邮箱类别	在左侧的邮箱类别视图选择“**操作->导出邮箱类别**”，或者右键菜单中选择“**导出邮箱类别**”，可以导出整个邮箱类别，包含所有的层级结构和邮箱标识；

导入邮箱类别	在左侧的邮箱类别视图选择“**操作->导入邮箱类别**”，或者右键菜单中选择“**导入邮箱类别**”，可以将事先导出的邮箱类别导入到“**邮箱类别**”节点下。

12.10 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。结合管理员对不同类别的文档设置不同的操作权限，程序可控制、记录不同分类的文档的外传和使用情况。

管理员设置用于识别文档的文字规则时，需要设置的分类包括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。

选择“**分类管理->敏感信息分类库**”打开敏感信息分类库窗口：

操作	说明
新建	选中信息分类/特征规则总节点，选择“**操作->新建**”或单击工具栏上的新建按钮，新建信息分类/特征规则；
查找	选择“**操作->查找**”或单击工具栏上的查找按钮  可以查找指定的特征规则和信息分类，查找支持模糊查询；
显示隐藏特征规则	使用关键字提取工具生成的特征规则导入到分类库后默认隐藏，选择“**操作->显示隐藏特征规则**”，可查看这些特征规则；
导入	选择“**操作->导入**”，选择信息分类库文件，可导入事先导出信息分类/特征规则分类库；
导出	选择“**操作->导出**”，可将指定的信息分类/特征规则，导出时可选择：导出全部、导出信息分类、导出特征规则； 导出全部：导出整个信息分类库和特征规则库； 导出信息分类：导出指定的信息分类和应用到这些信息分类的特征规则，未应用到这些信息分类的特征规则将不导出； 导出特征规则：仅导出指定的特征规则。

特征规则相关设置项说明

操作	说明
特征规则名称	管理员自定义特征规则名称，不可以@开头，不可重名；
类型	指定包含内容、排除内容中设置信息的类型，可选择关键字和特征规则 关键字：包含内容、排除内容中为具体的文字 正则表达式：包含内容、排除内容中为正则表达式；
去重	勾选此项时，则在使用此特征规则匹配文档时，匹配中包含内容的同一文字多次出现时，出现次数仅计为一次； 不勾选此项，出现次数按实际出现次数计算；
区分大小写	勾选此选项，使用包含内容匹配文档时，英文内容区分大小写匹配；
命中次数	文档中匹配包含内容的文字出现次数和的最小值，值为 1-10000 整数，当文档中匹配包含内容的文字的出现次数之和大于或等于此值时，文档才匹配上此规则；
包含内容	设置用于匹配文档的文字或正则表达式，支持设置多个，关键字可用英文分号和逗号隔开，正则表达式仅支持用英文分号隔开；
排除内容	设置不进行匹配的文字或正则表达式，设置规则如包含内容，优先级大于包含内容。

信息分类相关设置

操作	说明
信息分类名称	管理员自定义信息分类名称，不可重名；
备注	该信息分类的备注信息；
规则组	信息分类包含的特征规则，可选择多个；
规则权重	默认权重值为 100，管理员可根据需要修改为 0~100 的整数，当文档匹配中的特征规则的权重之和大于等于 100 时，文档才匹配中此信息分类；

12.11 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。

功能按钮说明

图标按钮	说明
	增加模板，当选中“**打印水印模板**”总节点时，则增加的是打印水印模板，当选中“**屏幕水印模板**”总节点时，则增加的是屏幕水印模板。
	修改选中的水印模板；
	删除选中的水印模板；
	查找名称中含有指定内容的水印模板。

12.11.1 创建水印模板

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；

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。

12.11.2 水印对象说明

水印对象的设置包括水印样式和水印类型，

水印对象属性	说明
水印样式	
平铺	水印在整个显示界面中以设置好的水平/垂直间距重复排列而成；
指定位置	水印根据设置的具体位置呈现，不会重复排开；
水印类型	
文字水印	水印内容为文字；
图片水印	水印内容为图片水印；
二维码水印	水印内容为二维码。

每种水印样式下都可分别选择不同的水印类型，且每种水印样式下可以有多个同样的水印类型，它们共同组成一组水印设置。点阵可看做是与一组水印设置对等且独立的水印设置，点阵和一组水印设置组成一个水印模板。

12.11.3 水印对象设置

选中一个水印对象时，在右边的视图可以设置属性，包括以下：

属性名称	说明
对象名称	该水印对象的名称；
水印内容	具体的水印内容，不同的水印类型对应的水印内容不同，之后会详细说明；
参数设置	具体水印的参数设置，不同的水印类型对应可设置的参数不同，之后会详细说明；

水印位置/水印间距	如果是水印样式为“**指定位置**”的水印对象，则需要设置水印位置，具体在指定位置通用属性说明中详述； 如果是水印样式为“**平铺**”的水印对象，则需要设置水印间距，具体在平铺通用属性说明中详述。

指定位置通用属性

指定位置的通用属性为水印位置。

属性名称	说明
水印位置	
位置	水印显示在页面的位置（包括：顶部、底部、左侧、右侧、居中、左上角、右上角、左下角和右下角）；
水平距离	水印基于指定水印位置的水平偏移距离，正数向右，负数向左；
垂直距离	水印基于指定位置的垂直偏移距离，正数向上，负数向下。

平铺通用属性

选择“**平铺**”节点时，可以对所有平铺水印设置通用属性。

参数名称	说明
倾斜度	可以调整平铺水印对象的倾斜度，包含左倾斜、居中和右倾斜，可指定倾斜的度数；
页边距	平铺水印在界面的填充范围，可分别设置左/右/上/下的间距；

说明 倾斜度仅对文字水印生效。

平铺样式的各类型水印，也有通用的属性。

属性名称	说明
水印间距	
与上个对象水平距离	与上一个同一类型水印对象（文字水印/图形水印）的水平距离；
与上个对象垂直距离	在平铺水印中，与上一个同一类型水印对象（文字水印/图形水印）的水平距离；

与上个对象同一行	勾选此项，则在平铺水印中，与上一个同一类型水印对象（文字水印/图形水印）为同一行，不勾选此项，则不为同一行； 默认不勾选。

文字水印设置

文字水印的水印内容和参数设置说明如下：

属性名称	说明
水印内容	可以选择显示 IP 地址、网卡地址、计算机地址、计算机别名、计算机组、用户、用户别名、完整用户、用户组、日期、时间、编号、打印任务名称等，也可以添加自定义内容；
参数设置	
字体	文字水印显示内容的字体；
大小	文字水印显示内容的字体大小；
颜色	文字水印显示内容的字体颜色；
倾斜度	指定文字水印显示内容的倾斜度

图片水印设置

图片水印的水印内容和参数设置说明如下：

属性名称	说明
水印内容	
图片内容	选择作为水印内容的图片，目前只支持.jpg 和.bmp 格式的图片；
参数设置	
图片高度	调整导入的图片的高度；
倾斜度	调整导入的图片的宽度。

二维码水印设置

二维码水印的水印内容和参数设置说明如下：

属性名称	说明
水印内容	可以选择显示 IP 地址、网卡地址、计算机地址、计算机别名、计算机组、用户、用户别名、完整用户、用户组、日期、时间、编号、打印任务名称等，也可以添加自定义内容； 选定内容会显示为二维码水印的扫描结果内容；

参数设置	
大小	二维码水印的显示大小。

点阵水印设置

属性名称	说明
参数设置	
圆点直径	点阵圆点的大小；
圆点颜色	点阵圆点的颜色；
透明度	点阵水印的透明度；
水印间距	
点阵边长	一个点阵图案的边长；
点阵间距	两个相邻点阵图案之间的距离
图形块间距	两组点阵图块之间的距离（一组点阵由 9 个点阵图案组成）

12.11.4 效果预览

设置好水印对象的属性后，可以在最右端的预览水印效果。

图标按钮	说明
	打开一个新窗口，全屏幕显示相应水印的原始大小，按下 ESC 键返回；
	在预览窗中，显示相应水印的原始大小
	在预览窗中，以适合窗口的大小显示相应水印
	预览窗口的纸张方向变为横向，水印随之变化，仅打印水印可以选择；
尺寸	水印效果的尺寸。

第十三章. 申请管理

基于管理需要，企业内部常会设置设备控制、打印控制等桌面申请管理策略限制并规范员工对企业资源的使用。被策略限制的员工因工作原因需临时解除限制时，可以提交申请说明理由，管理员审批通过后即可在指定的条件下临时解除相应桌面申请管理策略的限制。

13.1 桌面申请管理

13.1.1 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。

审批状态为审批中的申请可以否决，审批状态为已批准但未开始执行的申请也可以否决。

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。在桌面申请管理视图中，选择一条或多条申请，根据需要选择一种删除模式：删除选中的记录、删除本页记录、删除所有满足条件的记录。

说明 任何状态的申请均可以删除，已审批但未分发的申请被删除后，审批结果不会继续分发到客户端。

13.1.2 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。

图标按钮	说明
	一个管理员既可以是委托者，也可以是受托者；可切换查看委托的情况以及受托的情况。系统管理员还可以切换查看所有管理员的委托情况。
	进行审批权限委托设置；
	删除委托的权限，即收回委托的权限。

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。

注意 受委托的权限，不能被委托或代委托给其他管理员。

13.1.3 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。

功能按钮说明

图标按钮	说明
	查找，点击该按钮可按条件查询对应的审批流程；
	新建，点击该按钮新增加一条流程；
	编辑，点击该按钮编辑选中的流程；
	删除，点击该按钮删除选中的流程；
	复制，点击该按钮复制选中的流程
	上移，将选中的流程上移一个位置；
	下移，将选中的流程下移一个位置；
	替换，选中具体的流程后点击该按钮，可设置替换新的

	审批人；
	恢复，取消新建或修改流程时点击该按钮；
	保存，设置或修改流程后需保存才会生效。

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。

基本设置包括以下：

字段名称	说明
流程名称	新建的流程的名称，不能输入已存在的流程名。不输入时，则默认为“审批流程”，其后新建的流程默认名称为“审批流程_1”、“审批流程_2”，以此类推；
申请类型	能匹配此流程的申请类型，可勾选全部也可选择其中某一类或几类；
申请对象	能匹配此流程的申请对象，可以选择计算机、用户，也可以选择角色；

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。流程环节设置包括以下：

字段名称	说明
环节名称	新增的环节名称，格式不限，必填，不能与已有的重复；
审批人员	此环节的所有审批人员，可选择多个审批人，必选；
审批通过条件	此环节通过的条件，可选择“必须由全体审批人员批准通过”，或者“必须由指定人数的审批人批准通过”。指定的人数不能大于全部审批人员的人数。任意一人拒绝申请此环节不能通过。
处于该环节时审批员可以修改申请内容	勾选此项，则此环节的审批员可根据需求调整修改申请的内容，修改过的申请审批通过后，以修改后的内容执行

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。

说明 原审批人只能在选中的流程中包含的审批人中选择，新审批人可以在所有用户中选择。替换审批人后，原先属于此流程的未完成的申请都会失效。

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。

13.1.4 自动审批设置

管理员可以根据需要赋予对应的审批员自动审批的权限，开启功能后提交给对应审批员的申请会自动批准。

审批员需要有“**允许设置自动审批**”的权限才能开启自动审批，管理员可在控制台“**工具->账户管理->功能权限->桌面申请管理**”中，勾选“**允许设置自动审批**”，赋予审批员自动审批的权限。

开启自动审批

审批员登录控制台“**桌面申请管理->自动审批设置**”，点击编辑按钮，勾选“**启用自动审批功能**”选项，并点击确定，开启自动审批功能。客户端提交给对应审批原的申请会自动批准。

查看申请明细

当申请是自动审批通过时，控制台“**桌面申请管理->申请管理**”中查看申请明细以及客户端的“**查看桌面申请情况->查看申请信息**”中，申请明细显示的审批动作为：批准申请（自动）。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。

高级设置内容如下：

使用设备

高级设置	说明
设备类型	勾选允许客户端申请的设备类型，默认勾选全部；
设备描述	填写允许客户端申请的设备描述，支持通配符，默认不限制。

使用移动存储

高级设置	说明
读写权限	勾选允许客户端申请的移动存储设备的读写权限，默认只读。

打印\打印不带水印

高级设置	说明
打印任务名称	可以设置允许客户端申请的打印任务名称，支持通配符，默认不限制。
打印机类型	勾选允许客户端申请的打印机类型，可选本地打印机、共享打印机、网络打印机、虚拟打印机，支持多选，默认选择全部；
打印机描述	可以填写允许客户端申请的设备描述，支持通配符，默认不限制；
应用程序	可以添加允许客户端申请的应用程序名，默认为全部；
备份文件	勾选此项可以备份申请打印\打印不带水印的文件，备份文件在文档打印日志中查看。

发送邮件

高级设置	说明
收件人	填写允许客户端申请的收件人邮箱地址，支持通配符；
文件名称	设置允许客户端申请的文件类型，排除范围优先于包含范围，默认为所有文件。

聊天工具传送文件

高级设置	说明

文件名称	设置允许客户端申请的文件类型，排除范围优先于包含范围，默认为所有文件；
聊天工具	设置允许客户端申请的聊天工具，支持多选，默认选择全部；
备份文件	勾选此项可以备份申请通过聊天工具传送的文件，备份文件在文档操作日志中查看。

上传文件和数据

高级设置	说明
网站或网络地址	填写允许客户端申请的网站或网络地址，支持通配符，多个网站或者网络地址用“;”隔开；
端口范围	填写允许客户端申请的端口范围，多个端口用“;”隔开。

复制到移动盘\复制到网络盘\刻录光盘

高级设置	说明
文件名称	设置允许客户端申请的文件类型，排除范围优先于包含范围，默认选择所有文件；
备份文件	勾选此项可以备份申请复制到移动盘\复制到网络盘\刻录光盘的文件，备份文件在文档操作日志中查看。

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。

13.2 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。

13.3 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。

13.4 权限查看

13.4.1 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。

13.4.2 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。

13.5 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。

申请通用设置说明

申请时的时间设置，在任意一种申请中其含义都是相同的。

设置名称	说明
有效时间段	在设置的时间段内控制解除；
审批通过后的有效时间	从审批通过后开始计时，指定时间内控制解除；
在有效时间内可启用时间	对有效时间范围的一个限制，可点击“？”查看具体解释；

13.5.1 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。

13.5.2 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。

13.5.3 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。

13.5.4 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。

13.5.5 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。

13.5.6 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。

13.5.7 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。

13.5.8 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。

13.5.9 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。

文字按钮	说明
启用	申请通过审批之后，点击启用可令申请中指定的限制解除。
重新申请	针对被拒绝、被否决、已取消、已失效、已完成、已过期、被删除的申请，可重新发送申请。
删除	删除申请，可删除已取消、失效、已完成、被删除、被拒绝、被否决的申请，不可删除等待审批、已批准、执行中的申请
查看	查看申请的详细信息。
导入审批	离线时，导入控制台提供的审批文件，以获取审批结果。
离线申请	生成离线申请文件，发给控制台进行审批。
取消申请	取消申请。

13.6 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。

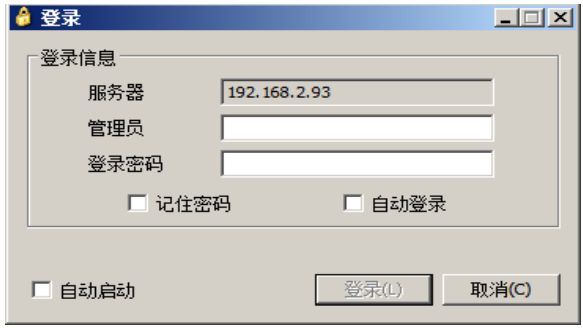
客户端自我备案操作可参考客户端申请的操作，通过右键客户端托盘图标选择“**桌管申请**”，弹出申请向导，选择对应申请类型进行申请，最后在申请向导界面中点击“**自我备案**”按钮进行自我备案，完成后即可直接执行对应申请的操作。

13.7 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。

13.7.1 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**”。

若同时勾选“**自动启动**”和“**自动登录**”，并输入正确的管理员帐户和密码后，则下次客户端启动并且连上服务器后，代理控制台能在后台自动登录启动，但不会弹出代理控制台主界面，用户可以在客户端托盘图标菜单中调出。

13.7.2 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。

13.7.3 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**”。

第十四章. 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，有效保护网络内的机密文件，防止外来计算机接入网络窃取资料，同时也可以减少病毒的入侵，增强企业内计算机的安全性。

选择菜单“**工具->网络接入检测**”打开网络接入检测窗口。

14.1 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。

如果启动接入检测的同时设置了“检测 IP 地址范围”，则只会扫描 IP 地址属于设置的 IP 地址范围内的网络设备，前提是这个 IP 地址范围内有安装了客户端模块的机器。

勾选“按 Mac 管理模式报警新机器接入网络”，新扫描到计算机的 Mac 地址不在已有的计算机列表中，控制台上会有报警信息，提示检测到新的计算机。不勾选此项，则使用 IP+Mac 组合管理模式，当扫描到计算机的 IP 和 Mac 的组合存在于已有计算机列表中则不报警，若 IP 存在但 Mac 不存在，或者 Mac 存在但 IP 不存在，都会把它识别为新的计算机并报警。

计算机列表

扫描出来的计算机分为客户端和非客户端，显示在计算机列表的客户端项。

客户端类型	说明
客户端	表示安装了客户端模块的计算机。

未知	表示没有安装客户端模块的计算机。当“系统->设置”中勾选了“**阻断所有未安装客户端的计算机接入网络**”时会对其进行阻断，禁止它与保护的计算机之间的通讯。

查看计算机列表可以选择 IPMAC 模式和 MAC 模式。

查看模式	说明
IPMAC 模式	IP 和 MAC 唯一决定一个计算机。
MAC 模式	仅由 MAC 决定一个计算机。

如果计算机的 IP 地址使用动态分配，会经常变化，使用 IPMAC 模式查看则会看到多台 MAC 相同但 IP 地址不同的同名计算机。这种情况使用 MAC 模式查看，则会把多台 MAC 相同但 IP 地址不同的计算机合并成一台计算机，IP 为最近一次的 IP。

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。

规则类型	说明
IP/MAC 规则	对指定 IP 地址和 MAC 地址设置规则，IP 和 MAC 唯一决定一个计算机，如果以后这个计算机被检测到，则使用此规则。
IP 规则	只根据 IP 地址设置规则，如果计算机记录包含该 IP 地址，并且没有设置规则，则会自动更新为该 IP 地址的类型。 假如设置 IP 地址 192.168.1.1 为授权，以后扫描到的计算机中，只要 IP 地址为 192.168.1.1，MAC 地址任意，则其规则自动为：IP 授权。
MAC 规则	只根据 MAC 地址设置规则，如果计算机记录包含该 MAC 地址，并且没有设置规则，则会自动更新为该 MAC 地址的类型。 假如设置 MAC 地址 6C-F0-49-64-FA-00 为授权，以后扫描到的计算机中，只要 MAC 地址为 6C-F0-49-64-FA-00，MAC 地址任意，则其规则自动为：MAC 授权。

规则类型	说明
授权	设置为授权的计算机不会被阻断，可将网络内管理者的计算机或关键网络设备设为授权，防止因为没有安装客户端被阻断。
保护	一般是将网络内重要的计算机设置为保护，以阻断非法计算机访问并窃取机密资料。

阻断	设置为阻断的计算机，当设置了启动接入控制功能后，会对其进行阻断，禁止它与保护的计算机之间的通讯。
常规	设置为常规即没有设置接入规则，用于清除授权、保护、阻断的规则。

提示　设置 IP 规则或者 MAC 规则，会增加自定义记录，对于不限制的 MAC 或者 IP 显示为<任意>。设置计算机类型时，可同时选择多个计算机进行同时设置。

14.2 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。

14.3 其它设置功能

设置检测代理

有小红旗标志“”的计算机是检测代理，检测代理负责扫描本网段内所有在线的计算机，并且执行控制功能，阻断非法的计算机。

为了方便管理网络内的计算机，管理员可以指定一台或几台稳定的客户端机器（例如没有安装个人防火墙且不经常关机的机器）优先成为检测代理。这样，只要这些机器正常运行，它们其中的一台就能成为检测代理。

选择一台计算机，右键菜单“**代理级别->优先**”，该计算机会有蓝色小旗“”标志。只有类型为“正常”的机器才可以设置为代理级别，设置之后优先成为检测代理。

选择右键菜单“**代理级别->禁止**”，管理员可以指定部分计算机不能成为代理。

预定义计算机类型

除了检测代理扫描出来的计算机，管理员可以手工添加计算机，并为其指定类型，方便提前控制。选择“**控制->添加**”增加计算机，管理员可以设置 IP-MAC 的类型，也可以只设置 IP 或 MAC 的类型，并设置规则。

设置类型	说明
IP-MAC	指定 IP 地址和 MAC 地址并设置类型，IP 和 MAC 唯一决定一个计算机，如果以后这个计算机被检测到，它的类型会自动更新为预先指定的类型；
IP	只根据 IP 地址指定类型，如果计算机记录包含该 IP 地址且没有指定类型，则会自动更新为该 IP 地址的类型； 假如设置 IP 地址 192.168.1.1 为授权，以后扫描到的计算机中，只要 IP 地址为 192.168.1.1，MAC 地址任意，则其类型自动为：IP 授权。
MAC	只根据 MAC 地址指定类型，如果计算机记录包含该 MAC 地址且没有指定类型，则会自动更新为该 MAC 地址的类型。 假如设置 MAC 地址 00-F0-4C-8C-DE-6A 为非法，则以后扫描到的计算机中，只要包含了这个 MAC 地址，其类型会自动更新为：MAC 非法
规则	管理员可以指定为授权、非法、保护或正常

添加成功后，则以后符合条件的计算机出现时，其类型会自动更新为预先设置

的类型，检测代理会根据类型控制这些计算机的访问权限。

查找、修改和删除计算机

计算机记录太多，不方便查看时，管理员可以通过查询栏来查找自己要查看的计算机列表，可根据最后在线时间、IP 地址范围、名称、接入规则、是否客户端来查询。。

在计算机列表中双击任意记录，或者选择“**控制->属性**”，可以打开属性对话框。在属性对话框中显示了计算机识别的所有信息，同时在这里也可以修改名称、规则、代理级别。

对于长久未使用的计算机，可以删除，如果该计算机再次出现，则列表中仍会再显示该计算机。

第十五章. 数据备份

15.1 使用数据库备份

主数据库备份

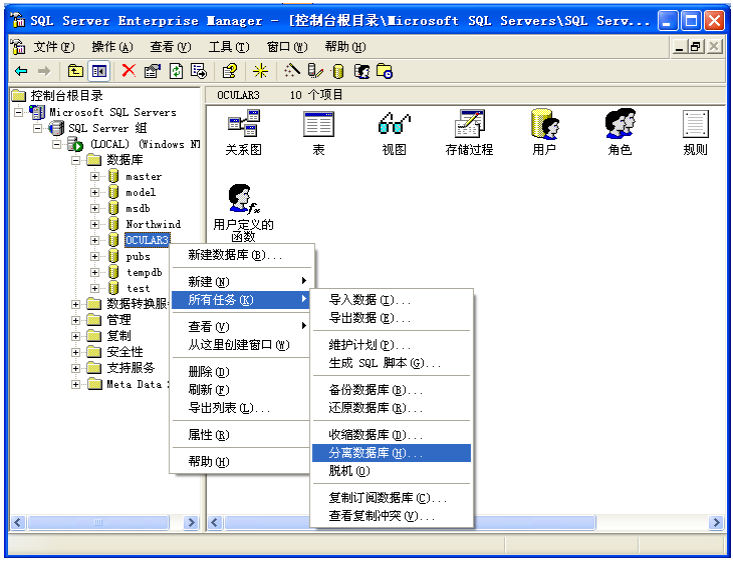
为了防止数据库文件破坏或其它意外情况造成服务器不能正常启动，建议管理员做好各种分类和策略后备份一下数据库文件。

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。

15.2 控制台备份管理

15.2.1 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。

 说明　　关于将备份数据存储到网络路径，有几点注意事项：

1.服务器和数据库不在同一台机器上时，不支持将备份数据保存到网络路径；

2.测试连接时，确保服务器和控制台所在机器没有使用非填入的用户名连接该网络路径，否则可能导致测试连接不成功；

3.加载备份时,无法加载网络路径的数据,需要先将数据从网络路径复制到服务器所在机器后进行加载。

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。

备份计划列表

备份计划列表显示了备份任务的基本属性，包括：创建时间、下次执行时间、数据范围、删除原数据、备份路径。可以编辑、删除备份任务。

字段名称	说明
创建时间	备份任务的创建时间；
下次执行时间	任务下一次开始执行的时间，如果该任务从未执行过，则为首次执行时间。
数据范围	任务备份的数据类型范围；
删除原数据	是否在备份后删除数据库中已备份的数据；

备份任务列表

备份任务列表显示了备份任务的基本属性，包括：起始日期、终止日期、备份路径、是否删除原数据、备份时间和状态。备份任务明细列表显示备份任务的详细信息，包括在什么时间备份了哪个数据库。

字段名称	说明
起始日期 终止日期	在此日期范围内的数据进行备份；
备份至	备份的数据文件所在的目录；
删除原数据	是否在备份后删除数据库中已备份的数据；
开始时间 结束时间	备份任务的启动时间和备份完成的时间，由此可以得出备份任务完成所需要的时间；
状态	正在备份中的任务状态是实时变化的，可以查看当前备份到了哪个数据库，状态还包括：任务被取消、任务成功完成、任务失败等。

在备份任务列表里，右键菜单还可以做以下的操作：

菜单项	操作
取消任务	停止备份当前选中的任务；
删除日志	删除选中的任务日志。未完成的任务不可删除。
属性	查看备份任务条件，查看当前备份任务的详细设置；
刷新	刷新备份任务列表

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。

15.2.2 加载和卸载备份数据

管理员可以把 3.0 和 3.1 的备份数据加载到数据库中查看。加载备份数据只是将备份的数据还原到服务器中，但并不破坏服务器现有的数据。

选择菜单“**工具->服务器管理->数据库备份管理**”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。

支持加载本地目录和网络盘目录上的数据。加载网路盘目录数据时，需要点击窗口下方的【浏览网络位置】按钮，输入具体的网络路径，如：

\\192.168.1.1\backupdata，支持域名，点击【确定】完成网络盘路径的指定。

备份数据列表中显示了备份数据日期、文件路径和文件大小，对于同一天的备份数据，最多可以同时加载 10 个。

加载了的备份数据可以直接通过控制台查看以及查询，不会影响服务器中本身数据的查看。

 说明

关于加载网络路径的数据，有几点注意事项：

1. 数据库需要 SQL Server 2012 及以上版本；
2. SQL 数据库所在机器，以及指定的网络路径，需加入到同一个域环境中，且 SQL Server 服务的登录身份需为域账户并对指定的网络路径有完全控制权限。

卸载备份数据

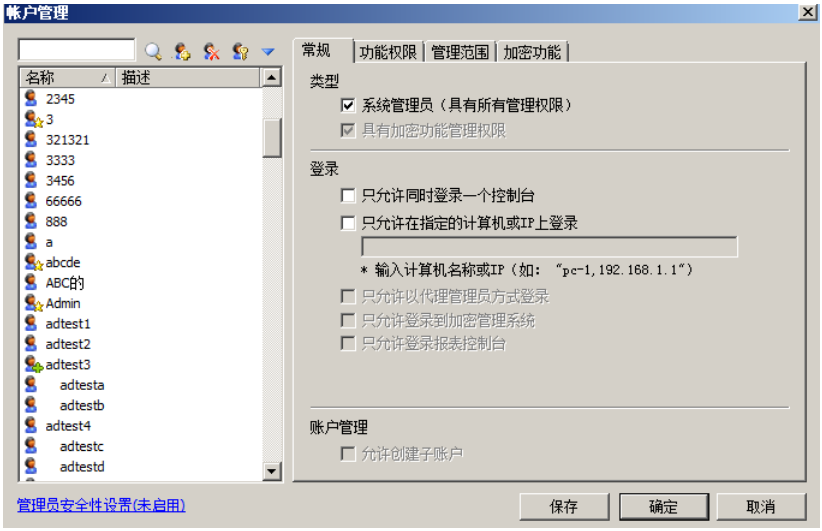
假如不需要查看某个备份数据，也可以将备份数据从服务器中卸载。选择需要卸载一个或者多个的备份数据，单击【卸载备份】按钮“  ”，可以查看待卸载的备份列表，再单击【确定】，对应的备份数据列表将被删除，在控制台上也不能再查看到这些备份数据。

第十六章. 工具

16.1 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。新建管理员账号时点击“**保存**”按钮后，可以继续在账户页面进行添加密码、添加账户操作。



图标按钮	操作
	添加管理员帐号，也可输入描述信息；
	删除管理员帐号，系统管理员“Admin”无法删除；
	修改管理员账号的登录密码，密码默认为空；
	点击展开其他功能菜单；

启用	启用已禁用的管理员账号；
禁用	禁用管理员帐号，系统管理员“Admin”无法禁用；
移动到	移动管理员，可分为以下 3 种操作： 1.普通管理员 A 无子管理员，将管理员 A 移动到管理员 B，则管理员 A 将变为管理员 B 的子管理员； 2.管理员 A 有子管理员 C，将子管理员 C 移动到管理员 B，则 C 将不再是管理员 A 的子管理员，而变成管理员 B 的子管理员； 3. 普通管理员 A 有子管理员 C，将子管理员 C 移动到整个网络，则 C 将变成一个普通管理员，不再是管理员 A 的子管理员；
导入加密审批人员账号	导入加密审批人员的账号信息文件，导入文件只支持 csv 和 txt 格式。账号文件中每行为一个账号，以逗号“,”分隔账户名和账户描述。已存在的账号不会导入。导入的账号自动勾选上“**具有加密功能管理权限**”和“**只允许以代理管理员方式登录**”
复制权限到	选择一个管理员 A，将其权限复制给另一个管理员 B，则管理员 B 将具有自身权限和管理员 A 权限的叠加
导出账户功能权限	可将当前所有管理员的权限导出查看，导出结果中，拥有该项权限则对应单元格内容为“√”，无此选项则对应的单元格内容为“×”。

说明

关于复制权限到，有几点说明：

1. 无法将系统管理员的权限，复制给一个已创建子管理员的非系统管理员，也不可复制给子管理员；

2.要将非系统管理员 A 的权限复制给一个子管理员（父管理员为 B），分以下两种情况：

a. 管理员 A 的权限在管理员 B 权限范围内，需要管理员 A 本身无子管理员方可复制成功，若管理员 A 有子管理员，则无法复制成功；

b. 管理员 A 的权限超出管理员 B 的权限范围，则无法复制成功。

16.1.1 管理员密码安全性验证

管理员密码安全验证，包括对密码复杂度和密码错误次数的限制，主要是为了加强对管理员密码的保护，防止恶意程序破解管理员密码。管理员密码安全性默认为不开启，系统管理员可以在账户管理界面的左下角点击“管理员密码安全性验证”，进行设置。

设置	内容
启用管理员密码安全性验证	勾选此项，则开启管理员密码验证功能，下面的设置才会生效。
密码复杂度	管理员密码复杂度的相关设置。
密码不能为空	勾选该项，如管理员账号登陆控制台时密码为空，则会强制要求其更改为非空密码，否则该管理员账号不能登录。
密码最小长度	勾选该项，并设置最小长度值，如果管理员的密码长度小于该设置长度，会强制要求更改为符合最小长度要求的密码，否则该管理员账号不能登录控制台。
密码复杂性验证	勾选该项，如管理员账号登陆控制台时密码不符合复杂度，会强制要求更改为满足复杂度要求的密码，否则该管理员账号不能登录控制台。 点击?可以查看密码复杂度的要求。
密码错误次数验证	管理员密码错误次数的相关设置。
启用密码错误次数验证	勾选此项，并设置在限定时间、密码错误次数、锁定管理员账号的时间。则管理员账号登陆控制台时，在限定的时间内密码输入错误次数达到指定次数，该管理员账号会被锁定，指定时间内都不能在登陆控制台，即使密码正确。
超时锁定	管理员登录控制台超时锁定的相关设置。
空闲超过一定时间，锁定控制台	勾选此项，并设置限定时长。则管理员登录控制台后，控制台的空闲时间达到设定值时，控制台自动锁定，需要重新输入管理员密码才能登录。 此设置在管理员登录代理控制台时同样生效。控制台上的超时锁定设置，优先于代理控制台上的锁定设置。

账户密码错误达到指定的次数被锁定时，生成一条审计日志，可登陆审计控制

台查看。

说明 1. “管理员密码安全性验证“设置对所有管理员生效。
2. 为了防止恶意锁定 Admin/Audit 账号，Admin/Audit 账号在服务器所在的计算机上登陆控制台时，错误次数不受限制。

16.1.2 管理员权限

管理员管理权限拥有四大模块。包括：常规，权限，管理范围和加密功能。

管理权限	内容
常规	指定管理员的类型，管理员登录的模式等。
功能权限	指定管理员拥有的常规功能权限。包括管理客户端的日志，设定各种策略，客户端远程维护及补丁管理等。
管理范围	指定非系统管理员所能管理的范围，可以选择全部的计算机和用户，也可以在计算机和用户之间选择一个进行管理。
加密功能	指定非系统管理员帐户拥有的加密功能的权限。包括管理权限和安全区域。

常规：

常规权限	说明
类型	
系统管理员	只有系统管理员能查看和管理授权软件和安全区域。系统管理员图标带有五角星，非系统管理员图标不带五角星。
具有加密功能管理权限	选择此项才能对加密系统进行管理。
登录	
只允许同时登录一个控制台	不能同时登录多个控制台。
只允许在指定的计算机或 IP 上登录	只能在指定的计算机名称或指定 IP 的计算机上登录。

常规权限	说明
只允许以代理管理员方式登录	只能在加密客户端上登录代理管理员进行管理，不能在控制台上登录。
只允许登录到加密管理系统	能从控制台上登录，登录后直接显示加密管理系统界面，不能使用 IP-guard 控制台上除加密以外的功能。
通过证书授权方式远程控制	此项需要服务器安装目录存在远程控制授权证书，并且是使用 Admin 账号登录控制台才会显示出来。 勾选此项，则管理则可以直接强制远程连接客户端，不需要用户授权以及密码授权。
账户管理	
允许创建子账户	勾选此项，则管理员具有创建子管理员的权限； 拥有此权限的管理员，登录控制台，选择菜单“**工具->账户**”，可以创建子管理员，子管理员的权限小于等于父管理员的权限。 只有普通管理员可以创建管理员，系统管理员和 Admin、Audit 此项无法勾选。

说明 “允许创建子账户”仅针对非系统管理员可选，即只有非系统管理员可以创建子管理员，系统管理员和 Admin、Audit 此项无法勾选。

管理员的功能权限

功能权限	说明
文件	主要是对计算机树与用户树的操作的权限，如：新建组，移动，重命名，删除等。同时也包括导出数据与打印。
控制	主要是对客户端控制的权限。 包括：锁定/解锁，发送通知消息， 注销计算机帐户，开机/关机，远程唤醒，卸载客户端。
统计	主要是对统计记录查询的权限。 包括：应用程序统计，上网浏览统计，网络流量统计等。
日志	主要是对日志记录查询的权限。 包括：基本日志，应用程序日志，上网浏览日志，文档操作日志，共享文档日志，文档打印日志，资产变更日志，策略日志，系统日志，备份文档，移动存储日志。

功能权限	说明
策略	主要是对策略查询与修改的权限。 包括：查看/设置基本策略，查看/设置应用程序策略，查看/设置上网控制策略，查看/设置设备控制策略，查看/设置打印控制策略，查看/设置屏幕记录策略，查看/设置日志记录策略，查看/设置远程控制策略，查看/设置流量控制策略，查看/设置端口控制策略，查看/设置邮件控制策略，查看/设置 IM 文件控制策略，查看/设置上传下载控制策略，查看/设置文档控制策略，查看/设置系统报警策略，查看/设置移动存储授权策略，查看/设置客户端配置策略，查看/设置软件安装管理策略。
监控	主要是对屏幕，邮件，即时通讯等记录进行查询与导出等操作的权限。 包括：查看实时屏幕，查看邮件记录，查看即时通讯记录，查看屏幕历史，导出屏幕历史等。
维护	主要是对远程计算机进行维护操作的权限。 包括：查看远程信息，控制远程信息，远程控制，远程文件传送等。
资产管理	主要是对资产进行管理的权限。 包括：查看资产信息，设置资产类别属性，修改自定义类别与属性等。
补丁管理	主要是对系统补丁进行管理的权限。 包括：查询补丁信息，设置补丁参数，执行补丁安装。
漏洞管理	主要是对系统漏洞进行管理的权限。 包括：查询漏洞检查情况，设置漏洞检查参数等。
软件分发	有两部分，对分发包操作的权限。 包括：查询分发包，设置分发包等；对分发任务操作的权限。包括：查询分发任务及安装情况，设置分发任务，执行分发任务等。
软件卸载管理	主要是对软件卸载功能进行管理的权限。 包括：查询软件卸载任务，设置软件卸载任务
网络接入检测	主要是接入检测功能的权限。 包括：查看接入检测、设置接入检测和设置策略。

功能权限	说明
所有分类管理	主要是能管理的类别的权限。 包括：应用程序类别，网站类别，时间类别，网络地址类别，网络端口类别，移动存储，软件安装包分类库，软件卸载分类库，邮箱类别，水印模板库，敏感信息分类库。 其中移动存储库又细分出：移动存储库，管理加密盘，格式化加密盘，初始化安全 U 盘，专用盘安全 U 盘交互日志，注册管控。 水印模板库又细分出：查看水印模板库、设置水印模板库。 敏感信息分类库又细分出：查看敏感信息分类库、设置敏感信息分类库。
桌面安全管理	主要是桌面安全管理功能的权限。 包括：查看普通申请和审批申请，删除申请，审批否决权限，审批权限委托，查看普通模块审批流程，设置普通模块审批流程，查看申请权限，设置申请权限。
删除	主要是指定能删除哪些记录的权限。 包括：统计，日志，邮件，即时通讯的删除。
备份数据	主要是备份数据与查看数据的权限。 包括：备份日志，查看数据 。
参数设置	主要是设置服务器和邮件报告服务器。 包括：服务器设置、邮件报告服务器设置。
安全检测	主要是安全检测功能的权限。 包括：安全检测条件，安全检测设置，安全检测日志，安全检测状态。
中继服务器管理	主要是管理中继服务器功能的权限 包括：查看中继服务器、设置中继服务器。
角色	主要是策略角色功能的权限 包括：查看角色、设置角色、分配角色。
文档云备份服务器	主要是文档云备份服务器功能的权限 包括：管理文档权限、设置配置权限、查看扫描任务和日志、设置扫描任务。
敏感信息	对策略、日志的查询与修改的权限。 包括：查看敏感信息全盘扫描任务和日志、设置敏感信息全盘扫描任务、查看/设置敏感信息外传控制策略、查看/设置敏感信息落地控制策略、查看/删除敏感信息日志。
生成客户端确认码	是指生成客户端确认码的权限。

功能权限	说明
生成客户端离线辅助工具	生成客户端离线辅助工具的权限。
生成客户端离线数据收集工具	生成客户端离线数据收集工具的权限。
管理加密盘	主要包括：设置分类，设置策略等。
格式化为加密盘	如果选择了该项，则管理加密盘的权限会自动勾选，对加密盘有完全的控制权限。
邮件报告	主要是设置邮件报告的权限。
产品维保升级管理	升级管理权限，可以更新维保码、检查和下载新版本，有维保服务期到期提醒。
客户端升级管理	客户端升级管理的权限，需要管理员的管理范围是全部计算机，选择了此项权限才能生效 。
域组织结构管理	使用组织架构同步功能的权限。
计算机管理	计算机管理的权限，需要管理员的管理范围是全部计算机，选择了此项权限才能生效。
报表系统登录权限	登录报表系统的权限。
准入网关管理	主要是 IP-guard 服务器连接准入服务器的相关权限。 包括：查看准入设备，设置准入设备。

加密功能：

管理权限	说明
文档加密和外发	对文档加解密和外发的权限。 包括：启用/禁用加密功能，远程管理加密文档，文档加密/解密，文档外发，文档加密算法设置。
授权软件	管理授权软件库的权限。
安全区域	增加、修改、删除安全区域的权限。
外发对象	设置外发对象和外发计算机的权限。
权限设置	对客户端设置加密策略的权限。 包括：查看加密权限，设置加密权限，加密系统登录注销管理，查看加密参数设置，设置加密参数，查看文档备份策略，设置文档备份策略，查看长期离线授权，设置长期离线授权。

管理权限	说明
加密文档操作日志	对加密文档操作日志的操作权限。 包括：查看加密文档操作日志，查看备份的加密文档，删除加密文档操作日志。
任务管理	对全盘扫描功能的操作权限。 包括：查看全盘扫描任务和日志，设置加密任务，设置解密任务。
流程管理	对各种申请的管理权限。 包括：查看解密申请和审批情况，删除解密申请，解密审批权限，查看外发申请和审批情况，删除外发申请，外发审批权限，查看临时离线申请和审批情况，删除临时离线申请，临时离线申请审批权限，查看安全属性变更申请和审批情况，删除安全属性变更申请，安全属性变更审批权限，审批权限委托，查看加密审批流程，设置加密审批流程
备用服务器	对备用服务器的操作权限。 包括：查看备用服务器，设置备用服务器。
文档备份服务器	对文档备份服务器的操作权限。 包括：查看文档备份服务器，设置文档备份服务器
USBKey 管理	对 USBKey 功能的操作权限。 包括：新增/删除 USBKey 信息，修改 USBKey 信息，查看 USBKey 日志，删除 USBKey 日志
智能终端管理	使用智能终端管理功能的权限。 包括：查看智能终端；修改智能终端；授权智能终端

安全区域	说明
全部安全区域和级别	能管理所有安全区域和级别的文档。
全部安全区域的指定级别	能管理所有安全区域的指定级别以下的文档。安全级别共有五个等级：普通、内部、秘密、机密和绝密。如指定级别为秘密，则能管理普通、内部和秘密级别的文档。
指定安全区域与相应的级别	能管理指定的安全区域与相应级别以下的文档。

管理员在设置安全权限的时候根据实际需要出发，不要赋予不应该的权限。

16.2 计算机管理

为了便于管理员对整个网段安装了客户端模块的计算机进行管理，也方便用户可以查询 license 的使用情况，比如查询现在使用了多少个 license，是否超出了 license 范围等，我们可以通过计算机管理来查看这些情况。

另外，当企业环境中存在大量的计算机，且在计算机的硬件维护过程中需要更换硬盘或网卡时，可能会需要重新指定客户端 ID，使更换硬盘或网卡后的计算机仍然被识别为原有的客户端。客户端 ID 的重新指定操作，也可以在计算机管理窗口中完成。

16.2.1 计算机管理窗口简介

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，计算机窗口中包含查询栏、计算机授权信息列表以及计算机识别信息列表。

计算机授权信息列表中包含的内容有：

属性名称	说明
	该图标表示计算机在 license 范围内，属于授权的计算机，没有这个标志的计算机超出了 license 范围，请通过“**授权信息**”查看购买的 license 和当前使用的 license 数量。
名称	客户端计算机在控制台上显示的名称；
ID	服务器为客户端分配的 ID，唯一标志该计算机；
网络地址	客户端使用的 IP 地址；
网卡地址	客户端的网卡地址和 IP 地址；
所属分组	客户端所属的计算机分组；
状态	客户端当前的运行状态，包括：正在运行、离线；
冲突	客户端是否冲突，内容为空代表不冲突，内容为“是”代表冲突；
最后出现时间	客户端最后一次出现的时间；
安装时间	客户端的安装时间；
版本	客户端的版本信息；
离线天数	客户端的离线天数。

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。

计算机识别信息列表中包含的内容有：

属性名称	说明
	该图标上有红色小勾，表示客户端当前正在使用该条识别信息。
操作系统	客户端当前的操作系统信息
硬盘 ID	客户端的硬盘 ID 信息
网卡地址	客户端的网卡地址；
计算机	客户端的计算机名；
首次出现时间	客户端第一次连接上服务器的时间

管理员可以根据查询条件快速查找需要查看的计算机信息，查询条件包括：

查询条件	说明
全部	默认查询所有安装了客户端模块的计算机；
按 IP 地址	设置 IP 地址范围，查询指定范围内的客户端机器；
按最后出现日期	设置日期范围，查询最后出现日期包含在该范围内的客户端，方便查找已经一段时间没有出现的客户端；
按客户端 ID	根据客户端 ID 查询指定的一个客户端信息；
按名称	按客户端在控制台上显示的名称查询，支持模糊查询。
离线天数	设置离线天数，查询离线天数在指定时间内的客户端机器；
状态	按客户端在控制台基本信息上显示的状态查询；
网卡地址	按客户端在控制台基本信息上显示的网卡地址查询；
硬盘 ID	按客户端在计算机管理—识别信息中显示的硬盘 ID 查询。

在计算机授权信息数据框中，还有一些辅助功能按钮，说明如下：

操作	说明
	导出计算机授权列表信息为 HTML 文件、xls 文件、csv 文件保存；
	打印计算机授权信息列表
	打印预览计算机授权信息列表

	删除，管理员可以删除不需要的客户端来释放 license 数量，删除会在卸载客户端的同时减少 license 数量；
	卸载，卸载客户端不会减少 license 数量。
	启用透明加密授权。
	启用只读加密授权。
	取消计算机的加密授权。

执行了删除或卸载的操作后，管理员必须单击【确定】按钮对改动进行确认，否则所做的操作将不生效。这样做的目的也是为了减少失误。

16.2.2 重新指定客户端 ID

一般来说，在两种情况下是需要重新指定客户端 ID 的：

1.为解决冲突状况而重新指定客户端 ID。企业内的两台机器互换硬盘后同时上线，可能会被识别为同一个客户端，此时控制台会弹出冲突提示，在计算机管理窗口中，可看到在计算机授权信息列表中，该客户端的信息显示为红色；点击该条授权信息，可查看到有两条或多条识别信息。

2.企业内的机器硬盘或网卡损坏需要更换，更换硬件后的机器可能会被识别为新的客户端，需要将新识别出来的客户端指定为原有的客户端 ID。

步骤：

1）在计算机授权信息列表中点击需要重新指定的客户端，单击其识别信息；

2）点击列表右上角的  按钮，进行计算机识别设置，具体有两种设置方式：

A.为计算机识别重新分配新的客户端。重新为识别信息分配 ID，可自定义名称。重新分配的客户端名称会显示在控制台计算机树的未分组中。

B.移动计算机识别信息到指定的客户端。可手动输入已有的客户端 ID，也可以通过  按钮选择已有的客户端。如将 B 的识别信息指定为已有的客户端 A，则控制台上 A 的名称将会自动被更改成 B。

16.2.3 查看客户端识别跟踪日志

由于操作系统、硬盘、网卡更换等原因，客户端的识别信息可能会发生改变，通过客户端识别跟踪日志，可以查看客户端识别信息的改变情况。

步骤：

1）在计算机授权信息列表中点击需要查看识别跟踪日志的客户端，单击其识别信息；

2）点击列表右上角的  按钮，进行客户端识别跟踪日志查询。信息包括以下：

属性名称	说明
时间	客户端登录上线时的时间；
识别方式	客户端使用的识别方式；
匹配结果	客户端识别后的匹配结果；
ID	客户端的 ID；
名称	客户端的名称；
操作系统	客户端当前操作系统；
操作系统目录	客户端当前操作系统目录；
网络地址	客户端的网络地址信息；
网卡地址	客户端的网卡地址信息；
硬盘 ID	客户端的硬盘 ID 信息。

识别信息发生改变，则会有相应的记录内容，前后不同的记录会标红。

16.3 U 盘加密客户端管理

点击“**工具->客户端管理->U 盘加密客户端管理**”，可以统一管理 U 盘加密客户端，仅有授权的 U 盘加密客户端会出现在此窗口列表中。

U 盘加密客户端列表信息各项属性说明：

属性名称	说明
UDiskID	制作成 U 盘加密客户端的 U 盘的 UDiskID，UDiskID 是一个移动存储设备的唯一标识信息，格式化也不会发生改变；
名称	该 U 盘加密客户端授权时设置的名称；
所属分组	该 U 盘加密客户端在计算机树上所属的分组；
授权状态	该 U 盘加密客户端的授权状态，分为：已授权、未授权；
版本	该 U 盘加密客户端的版本；

过期时间	该 U 盘加密客户端授权时设置的过期时间；
安装时间	该 U 盘被制作成加密客户端的时间；
最后在线时间	该 U 盘加密客户端最后连接服务器的时间；
认证间隔	该 U 盘加密客户端的认证设置时间。

U 盘加密客户端各项操作说明：

操作	说明
	添加 U 盘加密客户端授权；已授权的 U 盘加密客户端，会带有图标  ；
	删除 U 盘加密客户端，需要将 U 盘插入运行控制台的机器上时方可进行删除，删除后若想使用该 U 盘再作为 U 盘加密客户端，需要重新制作；
	修改该 U 盘加密客户端的授权设置，分为全局设置和自定义设置。 自定义设置优先于全局设置，设置了密码自定义设置的 U 盘加密客户端，在其 UDiskID 前会出现“*”；
	导出当前 U 盘加密客户端的策略文件；
	将被禁用的 U 盘加密客户端启用；
	禁用 U 盘加密客户端，禁用后无法使用加密功能；
	设置密码复杂度，分为全局设置和自定义设置。 自定义设置优先于全局设置，设置了密码自定义设置的 U 盘加密客户端，在其 UDiskID 前会出现“#”；

添加 U 盘加密客户端授权时，设置项如下：

名称	说明
导入可移动盘信息	导入授权所需文件；
文件路径	选择导出的 U 盘信息文件.uea；
可移动盘授权信息	设置该 U 盘授权的相关信息；
UdiskID	该 U 盘的 UdiskID，由系统自动生成，不可更改；

可移动盘名称	设置可移动盘的名称，设置的名称将在控制台计算机树上显示；
所属分组	设置该 U 盘客户端所属分组；
有效期至	设置该 U 盘客户端授权的有效时间，超过设置的时间后该 U 盘客户端即为过期，无法使用加密功能。若不勾选有效期则可一直使用；
认证间隔	勾选此项并设置指定天数，则客户端在此天数内必须要连接服务器至少一次，否则将视为过期，无法使用加密功能。

U 盘加密客户端密码设置项如下：

设置	内容
首次登录必须修改密码	勾选此项，则该 U 盘客户端首次登录时，会提示密码，不修改无法使用；
密码复杂度	U 盘加密客户端登录密码的复杂度相关设置；
密码不能为空	勾选该项，如 U 盘加密客户端登录时密码为空，则会强制要求其更改为非空密码，否则该 U 盘加密客户端不能登录；
密码最小长度	勾选该项，并设置最小长度值，如果 U 盘加密客户端的登录密码长度小于该设置长度，会强制要求更改为符合最小长度要求的密码，否则该 U 盘加密客户端不能登录；
密码复杂性验证	勾选该项，如 U 盘加密客户端登录时密码不符合复杂度，会强制要求更改为满足复杂度要求的密码，否则该 U 盘加密客户端不能登录； 点击?可以查看密码复杂度的要求；
密码错误次数验证	U 盘加密客户端密码错误次数的相关设置；
启用密码错误次数验证	勾选此项，并设置最大错误次数，当密码错误达到指定次数，该 U 盘加密客户端会被锁定，可以设置锁定指定的时间，也可以设置一直锁定。

注意 如果一个 U 盘加密客户端被一直锁定了，可通过重置密码解除锁定。

16.4 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。

1.策略触发报警信息

针对所有的 IP-guard 策略，只要设置策略时勾选了“报警”，则触发策略时会在控制台机器上弹出报警气泡进行通知，并记录在“**工具->警报**”中。

2.服务器报警信息

IP-guard 服务器自身机制定义的报警，出现相应的情况都会在控制台弹出气泡报警信息。主要的服务器报警信息如下：

报警名称	说明
客户端登录冲突	两台客户端被识别为同一台客户端时，会认为客户端登录冲突，会报警；
ZTEMP 目录所在磁盘分区的空间不足	缓存目录所在磁盘分区的空间低于 512M，会报警；
DATA 目录所在磁盘分区的空间不足	数据目录所在磁盘分区的空间低于 512M，会报警；
检测到新的计算机	网络中出现新的计算机，会报警；
发现长时间离线客户端	发现离线时间超过指定时长的计算机，会报警； 在控制台“**工具->选项->控制台设置->实时警报**”启动客户端离线报警功能并设定指定天数；
明文备份服务器空间不足	明文备份路径所在盘的剩余空间低于指定值时，会报警； 加密文档备份服务器的运行图标上点击右键，右键菜单“**工具->选项**”，“**空间管理设置**”中的“**空间报警限制**”处设置指定值；

明文备份服务器停止收集	明文备份路径所在盘的剩余空间低于指定值时停止备份，会报警； 加密文档备份服务器的运行图标上点击右键，右键菜单“**工具->选项**”，“**空间管理设置**”中的“**停止备份限制**”处设置指定值；
访问数据库时出错	执行备份任务时，若访问数据库出错，会报警，报警信息中有出错描述；
服务器所在计算机时间是否信任	服务器上一次记录下的时间，和当前的系统时间不一致，会报警，报警信息中提示是否信任当前系统时间；

3.客户端异常报警信息控制台“**工具->选项->控制台设置->实时警报**”中，启动了客户端异常报警，则发现有异常客户端时，会报警，报警信息中显示异常客户端列表。

实时报警默认最多能显示 500 条记录，管理员可以通过“**工具->选项->实时报警->报警窗口**”来调整实时报警窗口能够显示报警记录的最大数量。

警报信息记录的是实时报警，关闭控制台或重新登录控制台报警记录会自动清空。如果管理员需要查询，策略触发报警信息请到“**日志->策略日志**”中查询；服务器报警信息请到“**日志->系统事件**”中通过输入关键字进行查询；客户端异常报警信息目前无法查询，可在“**工具->网络接入检测**”中查看当前的异常客户端

16.5 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。

图标按钮	操作
	添加邮件配置。
	删除邮件配置。

报警信息邮件需要设置以下参数：

参数	说明
名称	用户自己定义的一种对该邮件配置的描述。当添加配置时，控制台会默认添加名称，管理员也可以自定义名称。
邮件标题	设定发送的邮件报告标题。
最大报警个数	每封邮件最多包含报警信息的个数。超过此个数则在下一封邮件中发送。默认值为 100。
最低报警级别	默认是全部，发送所有报警级别的报警信息，如果选择低，则发送低、重要、严重的报警信息；选择重要，则发送重要和严重的报警信息。
发送时间间隔	指定邮件发送的时间间隔。默认值为 30。单位：分。
收件人地址	接收报警信息的邮箱地址。
发送邮件测试	测试能否发送到收件人邮箱。
以附件发送	勾选则报警信息以附件形式发送。默认不勾选，以正文形式发送。
附件解压密码	以附件形式发送会发送一个压缩文件，此压缩文件可设置密码。
报警类型	**指定需要发送报警邮件的策略类型，如：应用程序控制策略、网页浏览控制策略、系统报警策略等。**
计算机范围	指定邮件报告中所管理的计算机范围。
用户范围	指定邮件报告中所管理的用户范围

注意 **计算机范围和用户范围是“或”的关系，只要在其中一个范围内，就会发送邮件。**

所有管理员均可以查看到、修改、删除自己添加的邮件报告，系统管理员 admin 还可以查看和删除其他管理员添加的邮件报告设置，但不能编辑。

邮件发送情况，如发送时间、发送邮箱、是否成功等信息，可以在“**日志->系统事件**”中查看。

16.6 准入网关管理

基于准入设备的网络准入控制功能，使用时需要服务器和准入设备相连接。点

击“**工具->准入网关管理**”，可以对准入设备进行添加/删除/修改等管理。

图标按钮	说明
	添加准入设备；
	修改准入设备信息，可以修改显示名称和准入设备 IP；
	删除准入设备；删除准入设备之后，服务器和准入设备的连接会断开，但准入设备上的容灾设置仍生效。需登录准入设备管理界面，在服务器管理中删除该对应的服务器，容灾设置才会连同删除。

一台服务器可连接多台准入设备。在准入设备列表中，可以查看准入设备相关信息，包括：控制器 IP，连接状态，最后连接时间。

属性名称	说明
控制器 IP	准入设备的 IP；
连接状态	当前准入设备和服务器的连接状态，主要有： 已连接：准入设备和服务器正常连接； 未连接：准入设备和服务器未能连接； 禁用：在准入设备的网页管理界面上禁用了该服务器； 拒绝：在准入设备的网页管理界面上删除了该服务器；
最后连接时间	准入设备和服务器的最后通讯时间。

16.7 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。

16.8 水印编码查询

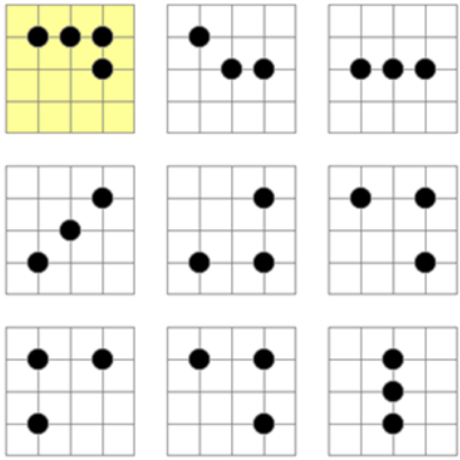
点击“**工具->水印编码查询**”，可根据获取到的点阵水印信息，查询到对应的计算机信息。

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。

屏幕和打印水印都可以设置显示点阵，其中屏幕点阵包含计算机名称、用户名称、IP、日期，打印点阵包含计算机名称、用户名称、IP、日期、打印任务、打印机描述、打印页数、应用程序。

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；

2.打印水印中的点阵水印，每一次不同的打印任务都会产生一种新的点阵；

3.屏幕水印中的点阵水印是根据计算机的信息（计算机名称、IP、日期）而发生变化的，这些信息没变的情况下（周期为天），如果设置了软件窗口水印，则所有软件窗口上的点阵水印图案

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。

16.9 客户端工具

确认码计算器

当安装了客户端的计算机无法连接服务器，例如禁用网卡或出差时，而又临时需要解除策略或者卸载客户端，这时是无法通过控制台去设置相应的策略的。

用户可以直接在客户端机器上调用客户端工具，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“清除所有策略”，点击【生成操作码】按钮；

3) 会弹出一个“检验操作码”对话框,用户需要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【生成确认码】;

6) 管理员将确认码告诉客户端，输入正确的确认码继续执行指定的操作。

使用客户端工具卸载客户端的详细说明请参考前面“安装和部署章节说明”。

客户端离线辅助工具

临时解除策略或者卸载客户端，还可以通过客户端离线辅助工具实现。具体操作步骤：

1) 管理员在控制台“**工具-客户端工具-客户端离线辅助工具**”，调出客户端离线辅助工具，可选择临时清除客户端策略，也可选择永久卸载客户端。

2) 选好需要的操作后，点击【**下一步**】按钮，可以设置工具的有效执行次数、有效时间，以及运行工具时需要输入的密码，密码可以为空。

3) 设置好之后，选择导出路径之后，便可将生成的临时清除策略工具导出。

导出的工具为 EXE 格式的可执行程序，将工具复制到离线客户端上运行即可。

客户端离线数据收集工具

有些客户端可能长期处于离线状态，管理者依然需要定期掌握这些离线客户端的使用情况。可以通过客户端离线数据收集工具进行离线客户端数据的收集和上传。具体操作步骤：

1) 管理员在控制台"**工具-客户端工具-客户端离线数据收集工具**"，调出客户端离线数据收集工具；

2) 选择收集工具要存放的路径，也可以设置使用工具的密码和有效时间；点击【创建】，即可生成的客户端离线数据收集工具。

3) 将生成的离线数据收集工具发给离线客户端，离线在客户端上运行。在工具"**数据收集**"选项卡页面，选择时间区间和数据类型，点击【**备份**】按钮；备份完成后，在工具的同目录下会出现一个"odtb"文件夹；

4) 将离线数据收集工具，以及"odtb"文件夹发给一台在线客户端，在在线客户端上运行。在"**数据管理**"选项卡页面，选择已收集的客户端的离线数据，点击【**上传**】按钮，并等待上传完成。

注意 1.使用正式序列号并且已注册的服务器，才能使用离线客户端数据收集功能

2.对于从未上线的离线客户端，首次上传离线数据后会在计算机结构树的未分组中生成该客户端的节点。

16.10 服务器时间

如果服务器时间不正常，如服务器所在机器的系统时间被人为的调整为数天前或数天后，这会严重的影响到产品的稳定性和安全性，因为许多功能，如：策略的有效时间，数据的生成时间，自动清除等，都依赖于服务器时间的正确性。

当服务器时间出现异常，管理员登陆控制台，会弹出气泡报警提醒，并且定时反复提醒。此时需要管理员修改服务器的操作系统时间，并在控制台上重新设置信任。

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。

16.11 中继服务器管理

部署中继器架构体系时，服务器可以连接多台中继器。选择“**工具->服务器管理->中继服务器管理**”，可以对连接到服务器的中继器进行的管理。

授权

设置完中继器的连接参数之后，需要在连接到相应服务器的控制台上对其进行授权。

控制台“**工具->服务器管理->中继服务器管理**”，在窗口左边的中继器结构树中选中对应的中继器，右键菜单选择“**授权**”。成功之后，在右边的显示视图中查看，中继器的状态会相应的变为“**已授权**”。选中一台已授权的中继器，右键菜单选择“**取消授权**”，该中继器会变回“**未授权**”状态。

查看基本信息

选择“**基本信息**”，可以查看选中的中继器的基本信息，包括：

属性名称	说明
状态信息	中继器状态相关信息
名称	控制台“**工具->服务器管理->中继服务器管理**”中显示的中继器名称，默认为中继器所在机器的计算机名。可在控制台上进行重命名；
计算机	中继器所在机器的计算机名称；
申请者	中继器设置连接参数时所设置的申请者；
网络地址	中继器所在计算机的 IP 地址；
运行状态	包括：“未授权，与主服务器断开连接”、“连接成功，未获得授权”、“连接成功，已获得授权”
启动时间	中继器启动的时间；
运行时间	中继器从启动后运行的时间；
连接状态	中继器与主服务器的连接状态。若是能正常连接，则显示“连接成功”，若连接异常，则显示“连接失败”
最后连接时间	中继器与主服务器最后连接的时间
授权状态	主服务器是否对其进行授权，包括：“已授权”、“未授权”；

授权更新时间	主服务器最新一次更新授权的时间；
客户端连接数	连接上该中继器的在线客户端数量；
范围设置	中继器的范围设置信息；
管理范围	中继器的管理范围；
排除范围	中继器的排除范围。

范围设置

选择“**范围设置**”，可以设置中继器的管理范围、排除范围等。

设置项	说明
管理范围	设置中继器能够管理的客户端 IP 地址范围； 设置格式支持 IP 段和子网掩码格式：IP 段格式如：192.168.0.1-192.168.0.100； 子网掩码格式如：192.168.2.1/24； 默认为空，即为管理全部；如设置管理范围为：192.168.0.1-192.168.0.100，则只有在该 IP 地址段内的客户端将连接到该中继器受其管理；
排除范围	设置中继器管理的排除的客户端 IP 地址范围； 默认为空，即不排除任何 IP 地址的客户端；如设置排除范围为：192.168.0.1-192.168.0.100，则在该 IP 地址段内的客户端不会连接到该中继器受其管理；
主动轮询	勾选此项，则中继服务器会按照处于管理范围内的客户端列表主动连接客户端的 8235 端口，不勾选此项，服务器不会主动去连接客户端； 该项默认不勾选。

前置流量

前置流量设置，通过流量策略，对主服务器与中继器之间的通讯流量进行限制。

可以对策略进行各种管理操作：

图标按钮	说明
	新建，点击该按钮新建一条新策略
	修改，点击该按钮修改加一条策略；
	删除，点击该按钮删除选中的策略；

	上移，将选中的策略上移一个位置；
	下移，将选中的策略下移一个位置；

点击新建按钮  ，设置流量设置、数据类型，会生成一条新的流量策略。可建立多条流量策略。设置或修改策略后，需要点击  按钮保存。

新建前置流量策略时各参数说明如下：

参数	说明
流量设置	
限制时间	策略生效的时间，包括：全天、工作时间、休息时间、周末时间、自定义时间，同样的也可以在时间分类管理中进行预先设定。
限制中继器向主服务器发送流量	可限制中继器向主服务器发送的流量，单位为 KB/s，设置的值为整数，若不勾选此项则表示不限制；
限制中继器接收主服务器流量	可限制中继器接收主服务器的流量，单位为 KB/s，设置的值为整数，若不勾选此项则表示不限制；
限制发送和接收流量总和	可限制中继器和主服务器之间发送和接收的流量总和，单位为 KB/s，设置的值为整数，若不勾选此项则表示不限制；
数据类型	
禁止的数据类型	勾选此项，并选择指定的数据类型，则在限制时间，选定的数据类型将禁止发送和接收；不勾选此项，则不对数据类型做限制。

策略匹配原则

策略匹配自上而下匹配，匹配到一条有效的策略后则单条策略生效，不会再往下匹配。

说明　　策略为勾选状态即为有效。

后置流量

后置流量设置，通过流量策略，对中继器与其所连接的客户端之间的通讯流量进行限制。

图标按钮	说明
	新建，点击该按钮新建一条新策略
	修改，点击该按钮修改加一条策略；
	删除，点击该按钮删除选中的策略；
	上移，将选中的策略上移一个位置；
	下移，将选中的策略下移一个位置；

点击新建按钮  ，设置网络地址、限制时间、流量设置，会生成一条新的流量策略。可建立多条流量策略。设置或修改策略后，需要点击  按钮保存。

新建策略时各参数说明如下：

参数	说明
网络地址	策略生效的网络地址范围，可选全部、局域网、外网、企业网、互联网，也可以在分类管理中进行自定义。
限制时间	策略生效的时间，包括：全天、工作时间、休息时间、周末时间、自定义时间，同样的也可以在时间分类管理中进行预先设定。
流量设置	
合计流量	限制网络地址范围内所有 IP 的总流量。 可限制中继器向客户端发送的流量、限制中继器接收客户端的流量、限制发送和接收的流量总和。每项设置的值为整数，也可以不设置，不设置表示不限制。
单计流量	限制网络地址范围内每个 IP 的流量。 可限制中继器向客户端发送的流量、限制中继器接收客户端的流量、限制发送和接收的流量总和。每项设置的值为整数，也可以不设置，不设置表示不限制。

策略匹配原则

策略匹配自上而下匹配，一个 IP 仅会匹配一个单计流量限制和一个合计流量限制

1、策略按照优先匹配的方式匹配

2、每条策略都可以包含合计流量和单计流量的限制，匹配该条策略时，要同时检查单计和合计的流量。

高级设置

高级设置，可以对中继器负载均衡、最大连接数，是否设为备用等进行设置。

属性名称	说明
启用负载均衡	勾选此项则开启负载均衡功能。 负载均衡功能主要实现：部署多台中继器时，连接到这些中继器的客户端，进行均衡分配，让每台中继器都能合理均衡利用资源；
额定连接数	默认为 1000，可以设置为其他数值； 中继器机器性能相对比较高时，可以适当调大额定连接数，反之可调小；
指定负载率	默认为 0，可以设置为其他数值； 指定负载率为 0 时，该中继器的负载率（当前连接数/额定连接数）高于其他中继器，则该中继器上连接的客户端将依照均衡算法被迁出部分，直至整体平衡； 指定负载率为其他数值时，该中继器的负载率（当前连接数/额定连接数）要高于指定负载率时才会有客户端迁出，若负载率低于指定负载率，则不会有客户端迁出；
最大连接数	该中继器的最大连接数，即最多可有多少台客户端连接该中继器； 此项默认不勾选，勾选后默认最大连接数为 3000，也可设置为其他数值；
设为备用中继	勾选此项，则该中继器被设置为备用中继器，只有当客户端与所有可连接的普通中继器无法通讯时，才会连接备用中继器，当备用中继器也无法连接时，客户端则会去连接主服务器。不勾选此项，则该中继器即为普通中继器。 默认为不勾选。

说明

1.客户端仅会在连接优先级同级别的中继器之间进行负载均衡。

2.系统规定，负载率=当前连接数/额定连接数。

负载均衡说明示例 1

公司内部部署了中继器 A 和中继器 B，均可接管整个公司的 1500 台客户端。未启用负载均衡时，中继器 A 连接 1000 台客户端，中继器 B 连接 500 台客户

端

情景一：中继器 A 和中继器 B 性能相当

此时可以设置负载均衡策略：

对中继器 A 启用负载均衡，额定连接数为 1000，指定负载率为 0；

对中继器 B 启用负载均衡，额定连接数为 1000，指定负载率为 0；

效果说明：

此时对于中继器 A，负载率为 1000/1000=100%，对于中继器 B，负载率为 500/1000=50%，由于中继器 A 的指定负载率为 0 且中继器 A 的负载率大于 B 的负载率，故中继器 A 的客户端会部分迁移到中继器 B 上，直至负载平衡。

情况二：中继器 A 的性能优于中继器 B

此时可以考虑更多的客户端连接着中继器 A。

策略 1：

对中继器 A 启用负载均衡，额定连接数为 2000，指定负载率为 0；

对中继器 B 启用负载均衡，额定连接数为 1000，指定负载率为 0；

效果说明：

此时对于中继器 A，负载率为 1000/2000=50%，对于中继器 B，负载率为 500/1000=50%，此时两台中继器负载率一样，客户端不会切换连接到其他中继器。性能好的中继器 A 将比性能稍差的中继器 B 带多一些客户端。

如果不调整额定连接数，也可以通过调整指定负载率，让中继器 A 较中继器 B 能带多一些客户端。

策略 2：

对中继器 A 启用负载均衡，额定连接数为 1000，指定负载率为 120；

对中继器 B 启用负载均衡，额定连接数为 1000，指定负载率为 0；

效果说明：

此时对于中继器 A，负载率为 1000/1000=100%，对于中继器 B，负载率为 500/1000=50%，此时虽然中继器 A 的负载率高于中继器 B，但由于中继器 A

的负载率并未高过其指定负载率 120%，所以中继器 A 的客户端不会迁出。

16.12 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。

当客户端计算机同步类库的时间早于当前类库变更的时间，该同步时间的文字颜色显示为灰色，表示此计算机未同步到最新类库。

图标按钮	说明
	查询计算机，快速定位到指定机器进行查看
	查看类库的最后修改时间

16.13 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。

16.13.1 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。

图标按钮说明

图标按钮	说明
	添加一条同步配置；

	修改选中的同步配置；
	删除选中的同步配置；
	立即执行选中的同步配置；
	查看选中的同步配置，可以看到该同步配置执行后实际的效果，没有选中任何配置，则显示所有同步配置执行后的效果。

 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；

如果该配置的目标设置是到计算机，则执行完配置后，还没有任何计算机接入服务器，在查看同步配置中只能看到同步的计算机分组结构，看不到任何计算机。计算机安装客户端接入服务器后才会在对应的分组中出现。

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。

参数	内容
连接设置	输入 AD 域服务器或 LDAP 服务器相关信息以便服务器可以与 AD 域连接获取其组织架构；
配置名称	配置名称，如不填，则默认使用输入的域名作为名称；
服务器类型	选择服务器类型，包括域服务器、LDAP 服务器；
域名	同步的服务器的域名；
域服务器地址	同步的服务器的 IP 地址； 如果选择的是 LDAP 服务器，可点击“**高级**”，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；
登录账号	如果选择的是域服务器，则需要填写具有获取该 AD 域架构权限的域用户账号；
密码	AD 域登录账号的密码；

启用自动同步	默认为不勾选。勾选此项，并设置同步间隔时间，则系统会根据所设置的同步间隔时间进行自动同步；
对象设置	设置域中的对象（包括域计算机和域用户）同步到服务器的指定位置。一条同步配置可以有多条对象设置，即可设置多组同步关系； 对象设置右上角有对应的图标，可以进行增加、修改、删除以及预览效果的操作。点击➕图标添加一条对象设置，具体参数说明见下；
来源设置	设置域同步关系中的来源，即选择对域中的哪些组织单元进行同步； 设置完连接设置后，需要点击“**测试连接**”按钮，测试连接成功后，来源设置方可正常选择。
来源选择	点击…按钮，选择想要同步的分组。支持多选，但不支持跨级别选择；
排除列表	点击…按钮，选择想要排除的对象。设为排除的对象将不会进行同步，可选择一个或多个计算机、用户或组织单元，可跨级别选；
目标设置	设置选定的域组织结构同步到控制台上哪个位置，支持同步到计算机组和用户组。
计算机组	点击…按钮，选择想要同步到控制台的计算机组目标位置。同步后，选定的来源架构会同步到该目标位置，当有域计算机安装客户端后会自动分配到对应的分组下。 设置计算机组时，需要选择同步模式，详情见同步模式说明。
用户组	点击…按钮，选择想要同步到控制台的用户组目标位置。同步后，选定的来源用户架构中所有的用户，会同步到该目标位置；
其他设置	其他相关设置
不导入无对象 OU	勾选此项，则来源中没有任何对象的 OU 将不会被导入；不勾选此项，则来源中选中 OU 都将被导入。默认此项勾选；
同步禁用对象	勾选此项，来源中禁用的对象将会被同步；不勾选此项，不会同步来源中禁用对象。默认此项不勾选。

同步模式说明如下：

模式名称	说明
仅同步来源中的计算机	仅根据来源域组织单元中的计算机，将客户端机器同步到控制台的计算机组；
仅同步来源中的用户	仅根据来源域组织单元中的用户，将客户端机器同步到控制台的计算机组； 当计算机安装客户端接入服务器后，用登录该客户端的用户去匹配来源中的用户，如果匹配上了用户，则该客户端同步到来源中该用户所在的分组，如果匹配不到用户，则该客户端同步到未分组；
同步来源中的计算机和用户（勾选用户优先计算机）	根据来源域组织单元中的计算机和用户，将客户端机器同步到控制台的计算机组； 当计算机安装客户端接入服务器后，先用登录该客户端的用户去匹配来源中的用户，如果匹配上了用户，则该客户端同步到来源中该用户所在的分组；如果没有匹配上用户，则用该客户端计算机去匹配来源中的计算机，如果匹配上了计算机，则该客户端同步到来源中该计算机所在的分组； 当用户和计算机均没有匹配成功时，则该客户端机器将被分配到未分组。
同步来源中的计算机和用户（不勾选用户优先计算机）	根据来源域组织单元中的计算机和用户，将客户端机器同步到控制台的计算机组； 当计算机安装客户端接入服务器后，先用该客户端计算机去匹配来源中的计算机，如果匹配上了计算机，则该客户端同步到来源中该计算机所在的分组；如果没有匹配上计算机，则用登录该客户端的用户去匹配来源中的用户。如果匹配上了用户，则该客户端同步到来源中该用户所在的分组。 当计算机和用户均没有匹配成功时，则该客户端机器将被分配到未分组。

16.13.2 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。

同步日志包括的内容共有：

属性名称	说明
操作类型	包括：增加、移动、重命名、失败。

对象类型	同步对象类型，包括计算机、计算机组，用户、用户组；
对象名称	同步对象名称；
描述	对应类型事件的现象描述；

注意 当组织架构同步不正常时，可查看同步日志，以便发现错误原因。

同步日志可以按以下条件进行查询：

查询条件	说明
时间	通用查询条件；
操作类型	默认是全部，也可在下拉框中选择其中一种操作类型；
对象类型	根据对象类型进行查询，方便查看指定的对象类型的同步日志；
对象名称	根据对象名称进行查询，可查询指定对象名称的同步日志，支持模糊查询；
描述	根据描述进行查询，支持模糊查询；

16.13.3 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。当域组织架构已同步至服务器，手动在控制台结构树上移动同步范围内的计算机或者用户，会弹出提示框确认是否要移动选中对象，确认移动则这些对象也同时被设置为例外对象。

16.14 客户端升级管理

服务器升级后，会更新客户端的升级包。服务器把客户端和升级包分发给客户端后，客户端会自动安装，重启后就升级成功。

客户端默认不会自动升级，即服务器默认不会将升级包分发给客户端。需要通过客户端升级管理进行设置。

选择“**工具->服务器管理->客户端升级管理**”，可以查看当前服务器上客户端

的升级包版本，通过升级设置，可让客户端自动升级或降级到与服务器一致的版本。

参数	说明
升级设置	
升级包版本	会显示当期升级包的版本信息，右边下拉菜单中可以选择升级设置；
不升级	选择此项，则所有的客户端都不会升级；
自动升级	选择此项，则所有的客户端都会自动升级到最新版本；
仅升级到 XX 版本	此项为锁定升级版本的选项，会根据当前服务器上的升级包版本实际显示具体版本号。选择了具体的锁定版本后，则客户端只会升级到此版本； 当服务器上的升级包和当前锁定的版本为同一个版本时，如同为 3.59.127.0 的版本，则下拉菜单中会显示“**仅升级到 3.59.127.0 版本**”一项； 当服务器上的升级包和当前锁定的版本为不同版本时，如服务器上的升级包版本为 3.59.228.0 的版本，此前绑定的版本是 3.59.127.0，则下拉菜单中会显示“**仅升级到 3.59.127.0 版本**”和“**仅升级到 3.59.228.0 版本**”两项。此时如果选择“**仅升级到 3.59.228.0 版本**”，下一次登录控制台打开此下拉菜单，则只会出现“**仅升级到 3.59.228.0 版本**”一项（因为此时服务器上的升级包版本和当前锁定的版本为同一个）；
分发时间段	只在该时间段内才会向客户端机器分发升级文件；
允许客户端降级到较低版本	如客户端机器上的版本高于当前服务器上客户端升级文件版本，勾选此项，则客户端机器上的客户端会降级；不勾选此项，则客户端机器上的客户端版本保持不变；
查找	查询栏中可输入：名称、计算机、IP 和最后登陆用户进行客户端查找，支持关键字模糊查询，不支持通配符。
范围	只对该范围内的客户端机器分发升级文件；
状态	选定范围内计算机的状态信息，包括计算机名称、网络地址、当前客户端版本、升级状态等。

16.15 选项

选择“**工具->选项**”，管理员可以查看并修改当前控制台和服务器的缺省值。

16.15.1 控制台参数设置

控制台参数里可以设置日志查看，实时信息和实时报警的参数：

参数	说明
基本设置	
登录设置	登陆控制台时的操作，可选择是否记住密码，是否自动登陆，使用密码为空的管理员账号登陆控制台时是否提示；
关闭设置	关闭控制台时的操作，可选择最小化到系统托盘或是退出程序，可选择是否弹出提示，系统默认为关闭时弹出提示框；
升级维护	
未取得产品维保期时	在线升级功能，产品在未取得维保期时的提醒设置 在下次登录后提醒：每次登录控制台都会提示无维保码并弹出更新维保码窗口； 在指定日期以后登录时提醒：设定指定日期，则在指定日期之后每次登录控制台都会提示无维保码并弹出更新维保码窗口； 不会提醒：每次登录控制台不会提示无维保码提示，不会弹出更新维保码窗口
自动检查产品升级	在线升级功能，自动检查产品升级的方式设置 每次登录后自动检查：则每次登录控制台都会检查是否有新版本，如果有新版本，则弹出新版本提示，没有新版本，不弹出提示。 在指定日期以后登录时检查：设置指定日期：则指定日期之前不自动检查新版本，指定日志之后，每次登录后自动检查是否有新版本 不进行自动检查：设置该选项后，不自动检查是否有新版本。
声音设置	
启用声音	勾选此项，则控制台弹出报警信息以及申请通知时，会给出声音提示；
声音类型	有“报警”和“通知”两项可供选择；
文件路径	指定的声音文件路劲，可通过浏览查找，仅支持 wav 文件；

日志查看

日志查询	查询每页显示的最大数量，系统默认为每页 20 条；

实时信息

屏幕监视	实时屏幕跟踪时间间隔，系统默认为 2 秒； 自动轮转时间间隔，系统默认为 2 秒； 默认选择显示所有屏幕，可选择仅显示可视屏幕；
实时维护	应用程序列表跟踪时间间隔，系统默认为 2 秒； 进程列表跟踪时间间隔，系统默认为 2 秒； 性能列表跟踪时间间隔，系统默认为 2 秒；
远程控制	远程控制时的默认操作，可选择默认锁定远端计算机的鼠标和键盘，和仅查看操作计算机；

实时报警

报警窗口	报警窗口显示记录的数量，系统默认为 500 条；
气泡设置	弹出报警气泡：勾选后在此控制台的机器上会弹出因策略触发的实时报警。 弹出气泡的最低警报级别：低，重要，严重
客户端离线报警	启动客户端离线报警功能并设定指定天数，如 10 天，则此控制台在下一次登录时，弹出报警信息，显示离线时间大于或等于 10 天的客户端列表
客户端异常报警	启动客户端异常报警，则出现异常客户端时，弹出报警信息，显示异常客户端列表

加密功能

加密序列号警告	启动加密序列号未注册时提醒，则未注册加密序列号时，弹出报警信息； 启动加密序列号过期时提醒，则加密序列号过期时，弹出报警信息；
加密审批流程提醒	启动保存修改流程时提醒，则修改审批流程并保存时，会提醒“如果当前有申请在审批中，修改流程可能导致申请失效，需要重新申请”，不启用则不会提示；
加密申请通知提醒	启动弹出申请气泡，则有加密、外发、变更安全属性、临时离线等申请提交，会弹出气泡提示，不启用则不会弹出提示。

16.15.2 服务器参数设置

服务器参数里可以设置多个系统参数：

参数	说明
补丁选项	
新出现的客户端默认自动安装	勾选此项，新安装客户端的计算机会自动安装已经下载的补丁，否则新客户端机器不会自动安装补丁。如果需要客户端自动安装补丁，管理员可以在第一次登录控制台时设置该项；
新发现的补丁默认自动下载	勾选此项后新扫描到的补丁会自动下载，否则新扫描到的补丁不会自动下载。如果需要所有扫描出来的补丁自动下载，管理员可以在第一次登录控制台时设置该项；
数据清除	默认为不清除数据，勾选“启用此功能”启动数据清除功能
全局设置	默认为保留全部数据，服务器不会删除任何数据； 可以选择保留指定天数内的数据，指定天数默认为 30 天，服务器会删除 30 天前的数据；
自定义设置	可以分别设置各种日志数据的保留天数； 默认保留天数为“全局设置”，则根据全局设置进行删留数据； 可以选择自定义并设置自定义天数，也可以选择全部保留；
管理范围	
搜索范围	可以添加服务器搜索客户端机器的 IP 地址范围，一般用于客户端无法主动连接正确的服务器，服务器应开启主动轮询功能；
仅允许搜索范围内的计算机连接服务器	勾选此项，则不在搜索范围内的计算机将不会连接上服务器；
排除范围	可以添加服务器的排除客户端机器的地址范围。在排除范围内的客户端不能与该服务器连接；
流量设置	通过设置流量策略，对指定网络范围的客户端依据实际情况进行流量限制，避免服务器和客户端之间的通讯造成带宽占用，影响一些常用通讯。 点击新建按钮，设置网络地址、限制时间、流量设置，会生成一条新的流量策略。可建立多条流量策略。
连接设置	

服务器和客户端之间的带宽设置	带宽设置范围是 1-102400 KB/s，在局域网内一般不用限制带宽，对于 VPN 网络可能会用到；
主动轮询	服务器会按照处于 license 范围内的客户端列表主动连接客户端的 8235 端口，默认开启。不勾选此项，服务器不会主动去连接客户端；
目录设置	
数据目录	管理员可以更改一些数据文件的存放路径，包括：数据目录、缓存目录、软件分发、备份邮件、屏幕历史、备份文档、微软产品补丁。 默认的保存目录是 IP-guard 安装目录；管理员可以修改这个目录，但是之前的数据不会自动移动到新的目录中，需要停止服务器然后手动移动数据到新目录。新目录设置后必须重启服务器才生效。
设置目录	点击设置按钮“  ”打开服务器计算机的目录树，选择新的数据存放目录，直到重启服务器后，保存目录才会更新为新目录；
恢复初始目录	点击恢复按钮“  ”，将指定数据对象的保存目录恢复到初始的目录，初始的目录是服务器模块的安装目录；
剩余空间管理	
存储空间最低剩余值	当存储空间（包括数据目录和缓存目录）小于该值时，会停止收集数据并弹出报警气泡；
剩余存储空间报警值	当存储空间（包括数据目录和缓存目录）小于该值时，会弹出报警气泡，但不停止收集数据；
性能设置	
固定模式	固定模式是设置服务器能并发处理客户端的最大数量，设置的范围是[0-100]；
动态模式	动态模式是服务器自动根据负载调整并发处理客户端得数量。负载级别“标准”表示服务器模块对于数据库进程的平均占用率是 30%；如果是“高”，这个上限值是 50%，如果是“低”，这个上限值是 10%。； 服务器默认是在动态模式下运行，处理模式是“标准”； 一般来说，在动态模式下，服务器的性能越好，并发处理的客户端数量会越多。 对于实时性的操作，如控制台查看实时屏幕，或者进行远程维护等，不受这个选项的影响，会实时处理。
报错设置	

记录验证客户端过程中的报错信息	勾选该项才会记录报错信息，服务器的报错信息可在“**日志->系统事件**”里查看；
记录报错信息的最低别	级别是指报错信息的严重度： 全部 报告全部的错误； 低　通讯中客户端的回应并不是预期的结果； 中等 超过 license 授权； 重要 序列号或者检验码错误； 严重 因为处于服务器排除范围内而无法通过服务器校验
客户端自动删除	
自动删除长期未上线的客户端	勾选该项并设定未上线天数，默认为 30 天。则控制台下一次登录时，自动删除未上线时间大于或等于 30 天的客户端。

流量设置

服务器参数中的流量设置，通过流量策略进行限制。

可以对策略进行各种管理操作：

图标按钮	说明
	新建，点击该按钮新建一条新策略
	修改，点击该按钮修改加一条策略；
	删除，点击该按钮删除选中的策略；
	上移，将选中的策略上移一个位置；
	下移，将选中的策略下移一个位置；

点击新建按钮  ，设置网络地址、限制时间、流量设置，会生成一条新的流量策略。可建立多条流量策略。

新建策略时各参数说明如下：

参数	说明
网络地址	策略生效的网络地址范围，可选全部、局域网、外网、企业网、互联网、也可以在分类管理中进行自定义。

限制时间	策略生效的时间，包括：全天、工作时间、休息时间、周末时间、自定义时间、同样的也可以在分类管理中进行预先设定。
流量设置	
合计流量	网络地址范围内所有 IP 的限制流量。 可限制服务器向客户端发送的流量、限制服务器接收客户端的流量、限制发送和接收的流量总和。每项设置的值为整数，也可以不设置，不设置表示不限制。
单计流量	网络地址范围内每个 IP 的限制流量。 可限制服务器向客户端发送的流量、限制服务器接收客户端的流量、限制发送和接收的流量总和。每项设置的值为整数，也可以不设置，不设置表示不限制。

策略匹配原则

策略匹配自上而下匹配，一个 IP 仅会匹配一个单计流量限制和一个合计流量限制

1、策略按照优先匹配的方式匹配

2、每条策略都可以包含合计流量和单独流量的限制，匹配该条策略时，要同时检查单计和合计的流量。（有单计和合计的目的一是为了特殊 IP 开放，二是为了不超过某条外线自己本身的带宽。）

策略示例 1

如果单独的希望某一 IP 段（192.168.2.50-192.168.2.100）内，每台客户端与服务器之间的流量不超过 200k

那么可设置策略：网络地址为 192.168.2.50-192.168.2.100，单计流量“限制发送和接收流量总和为”200KB/S

策略示例 2

如果希望某一 IP 段（192.168.2.50-192.168.2.100）内所有客户端与服务器之间的总流量不超过 2M

那么可设置策略：网络地址为 192.168.2.50-192.168.2.100，合计流量“限制发送和接收流量总和为”2M/S

策略示例 3

存在以下情况：

1.公司外部的客户端计算机通过 VPN 连入公司网络（划给这部分机器的网段为 192.168.10.1-192.168.10.254），每台机器的带宽为 1M，但管理上需要和 IP-guard 服务器的通讯流量不超过 500K。

2.公司内部的带宽也有限制，总共 10M 的带宽，管理上需要 IP-guard 使用的带宽不要超过 5M。公司内部网段为 192.168. 9.1-192.168.9.254。

3. 某重要办事处的监控计算机（192.168.10.10）需要优先控制，它的限制带宽为 2MB/s

设置策略时和依照以下步骤：

1、添加网络地址分类：名称为“VPN 接入网段”，内容为

192.168.10.1-192.168.10.254；

2、添加网络地址分类：名称为“企业内网”，内容为 192.168. 9.1-192.168.9.254；

3、先设置一条流量策略：网络地址选择“VPN 接入网段”和“企业内网”分类，合计流量“限制发送和接收流量总和为”5MB/s，单计流量“限制发送和接收流量总和为”500KB/s

4、再设置一条流量策略：网络地址设为 192.168.10.10，单计流量“限制发送和接收流量总和为”2MB/s

16.15.3 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。

参数	说明
设置列表	增加、修改、删除邮件报告服务器设置

邮件报告服务器设置列表的按钮含义：

图标按钮	操作
	新建邮件报告服务器设置，点击该按钮进入邮件服务器设置界面。
	删除当前所选的邮件报告服务器设置。
	重新编辑当前所选的邮件报告服务器设置。
	向上排序，将当前所选的邮件报告服务器设置上移一位，已设为默认的设置不参与排序，保持在最底端。

	向下排序，将当前所选的邮件报告服务器设置下移一位，已设为默认的设置不参与排序，保持在最底端。
	设置当前所选的邮件报告服务器为默认服务器。
	取消当前所选的邮件报告服务器为默认服务器。

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。

新增或修改邮件报警服务器需要对以下项目作设置：

参数	说明
名称	用户自己定义的一种对该服务器的描述。当添加一个邮件服务器时，控制台会默认添加名称，管理员也可以自定义名称。
邮件服务器地址	邮件服务器地址，可以是 IP，也可以是域名。
端口	SMTP 端口，默认是 25。
SMTP 帐号	SMTP 帐号。
密码	SMTP 帐号所对应的密码。
要求安全连接（SSL）	勾选此项，则设定的邮件发送服务器使用安全连接（SSL）来发送邮件。
发送邮件地址	用来发送报警邮件的邮箱地址。
昵称	发送邮件的发件人昵称。
邮箱集合	用来接收报警邮件的邮箱后缀的集合，用“;”分隔，如@163.com;@126.com。

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。

16.16 远程获取文件任务

通过远程获取文件任务功能，管理员可以获取客户端上指定目录下的文件，也可获取客户端和插入客户端的 U 盘上的存放文件的列表，以便检查有异常行为的客户端上的可疑文件。

注册序列号为包含远程维护模块的正式序列号且服务器的安装目录下存在远程维护授权证书 RC.Cert，才可使用功能。

拥有“**远程文件传送**”权限（控制台“**工具->账户管理->功能权限->维护**”中设置），和“**通过证书授权方式远程控制**”权限（控制台“**工具->账户管理->常规**”中设置）的管理员，登录控制台，“**工具->远程获取文件任务**”中可打开远程获取文件任务界面。

图标按钮说明：

图标按钮	说明
	创建一个新的任务；
	选中一条正在执行的任务，可暂停此任务；
	选中一条暂停的任务，可启动此任务；
	删除选中的任务；
	查看上一页的任务记录；
	查看下一页的任务记录；

16.16.1 创建任务

创建获取磁盘文件列表任务

在远程获取文件任务界面中，点击  按钮，选择“**创建获取磁盘文件列表任务**”，弹出任务设置界面，添加任务，可获取多台客户端指定路径下文件的列表。

任务设置条件如下：

参数	内容
任务名称	任务名称为必填项，默认为：扫描任务+年月日；
选择任务对象	选择任务作用的对象，为必填项；

扫描路径	包含文件指定扫描的路径，默认情况下显示为全部硬盘；可支持设置本地硬盘、移动盘，设置多个路径使用逗号或分号隔开，不支持通配符；
包含文件	任务扫描包含的文件类型，为必填项，默认为空，点击  按钮弹出设置界面，可选择预定义的文件类型；
排除文件	任务扫描排除的文件类型，默认为空，点击  按钮弹出设置界面，可选择预定义的文件类型；排除文件优先于包含文件。

创建获取移动盘文件列表任务

在远程获取文件任务界面中，点击  按钮，选择“**创建获取移动盘文件列表任务**”，弹出任务设置界面，添加任务，可获取多台客户端上所连接的 U 盘中文件的列表。

创建任务时，如果客户端上已存在获取移动盘文件列表任务，新建或启动同类型任务会将旧的任务暂停。

任务设置条件如下：

参数	内容
任务名称	任务名称为必填项，默认为：扫描任务+年月日；
选择任务对象	选择任务作用的对象，为必填项；
扫描路径	包含文件指定扫描的路径；默认为全部移动盘，不能修改。
包含文件	任务扫描包含的文件类型，为必填项，默认为空，点击  按钮弹出设置界面，可选择预定义的文件类型；
排除文件	任务扫描排除的文件类型，默认为空，点击  按钮弹出设置界面，可选择预定义的文件类型；排除文件优先于包含文件。

 **说明**

获取移动盘文件列表为持续任务，即对客户端设置此任务后，当客户端上新连接一个移动盘时，均会触发客户端获取移动盘文件列表上传到服务器。

2.在距离上次扫描 30 分钟内，用户多次插拔客户端上的移动

盘，均不会再次扫描客户端，扫描 30 分钟后插拔移动盘才会触发客户端进行扫描。当客户端上的移动盘一直连接着客户端，每间隔 8 小时客户端会自动扫描一次移动盘。

创建获取文件任务

在远程获取文件任务界面中，点击  按钮，选择“**创建获取文件任务**”，弹出任务设置界面，添加任务，获取多台客户端指定目录下的文件。

任务设置条件如下：

参数	内容
任务名称	任务名称为必填项，默认为：扫描任务+年月日；
选择任务对象	选择任务作用的对象，为必填项；
选择文件	默认为空，需要填写文件路径和文件名称，设置多个路径使用逗号或分号隔开。

 **说明**

1. 选择文件名称支持通配符，若文件名称填写了通配符，对应目录下仅支持扫描 100 个大小 100MB 内的文件；目录下超过 100 个的文件不会再扫描备份。
2. 选择文件必须填写全路径，路径中不支持通配符；且不支持扫描子目录下的文件。

16.16.2 查看任务信息

对客户端可以设置多个获取磁盘文件列表任务和获取文件任务，任务按照创建顺序依次执行，已启动的任务为当前任务，正在启动的任务为后续任务，当前任务执行完后，后续任务自动变为当前任务。

其中获取移动盘文件列表任务为持续任务，如果客户端上已存在获取移动盘文件列表任务，新建或启动新的获取移动盘文件列表任务时，会将旧的任务暂停，只启动新的任务。

任务信息

在远程获取文件任务功能界面的上半视图中，可以查看每台客户端执行任务的基本信息。

内容项	说明
计算机	客户端的计算机名称。
计算机组	客户端所在分组的名称。
任务名称	对客户端创建的远程获取文件任务名称。
任务类型	对客户端创建的远程获取文件任务的类型。
开始时间	客户端对应任务开始执行的时间。
结束时间	客户端对应任务执行结束的时间。
任务状态	客户端执行远程获取文件的任务状态； 1. 当扫描功能为启用时，任务会执行，状态为“已启动”； 2. 当扫描功能为禁用时，任务会暂停，状态为“暂停”； 3. 在任务启动和暂停的过程中，对应会有“正在启动”/“正在暂停”的状态； 4. 当任务执行完成后，状态为“完成”。
文件数量	执行任务扫描到的文件数量。
文件大小	执行任务扫描到的文件总大小。
进度	客户端当前执行任务的完成进度，会根据当前进度自动更新。

其他任务信息

选中一条任务，在远程获取文件任务功能界面下半视图的“**任务信息**”选项卡中，查看任务的详细设置内容，内容包括扫描路径、包含文件、排除文件。

说明 获取移动盘文件列表任务为持续任务，当完成当前插入移动盘的文件列表获取后，任务状态为变为“暂停”，当有新的移动盘插入时则自动会启动任务。

16.16.3 查看任务日志

在远程获取文件任务功能界面，选中一条任务，在下半视图的“**任务日志**”选项卡中，可以查看该任务执行的日志。通过工具栏上的刷新按钮进行刷新。

内容项	说明
时间	该条任务日志产生的时间。
任务名称	当前执行的任务名称。
内容	当前任务执行的操作描述。

当任务执行完成后，在控制台“**日志->远程获取文件任务日志**”中会显示出远程获取客户端文件的任务日志记录，获取到的文件列表或文件保存在日志记录的副本中，选中一条日志记录双击打开属性窗口，可下载或预览副本文件内容。

记录包括：

属性名称	说明
类型	远程获取文件任务的类型；
任务名称	获取文件任务的名称；
文件名称	获取到的文件名称或文件列表名称；
文件大小	获取到的文件大小；
路径	获取到的文件路径；
描述	任务状态描述；

远程获取文件任务日志可以按以下条件进行查询：

查询条件	说明
任务类型	远程获取文件任务的类型，包括：获取文件、获取磁盘文件列表、获取移动盘文件列表；
任务名称	远程获取文件任务的名称，支持通配符查询；
文件名称	任务获取的文件名称，支持通配符，或选择预定义好的文件类型查询。
文件大小	任务获取的文件大小范围。

第十七章. 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。

17.1 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。

图标按钮说明

图标按钮	说明
	添加一条服务器配置；
	将选中的服务器配置上移一个位置，调整优先级顺序；
	将选中的服务器配置下移一个位置，调整优先级顺序；
	编辑选中的服务器配置；
	删除选中的服务器配置。

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。

17.2 登录验证

17.2.1 控制台设置策略

选择“**工具->服务器管理->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。

17.2.2 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。

17.3 关联验证

17.3.1 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；

17.3.2 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。

17.4 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。

关联信息包括：

属性名称	说明
计算机	有关联用户的计算机名称；
计算机组	计算机所在的分组名称；
计算机关联用户	计算机所关联的用户名称；
关联用户状态	计算机所关联的用户在域服务器上的状态；
最后登录用户	计算机最后登录的用户名称；
关联时间	计算机关联用户的时间；

图标按钮说明

图标按钮	说明
	查询计算机关联用户，快速定位到指定关联信息进行查看；
	显示模式，关联信息列表会根据所选择的显示模式列出符合条件的计算机信息。
	清除关联信息。选中一台计算机执行此操作后，计算机会按照最后登录的用户来进行同步，“计算机关联用户”会变为最后登录的用户；
	重新关联信息。选中一台计算机执行此操作，选择要同步的用户，则该计算机会按照所选用户进行同步，“计算机关联用户”会变为所选用户；
	不关联任何用户。选中一台计算机执行此操作后，则该计算机仅根据计算机来进行同步，不根据用户进行同步。不关联任何用户的计算机，计算机名前显示 “*”标志。
	编辑备注信息。选中一台计算机执行此操作后，会更新列表中该计算机的备注信息。

第十八章. 审计控制台

审计控制台主要是对管理员操作控制台的一种日志记录，方便查询管理员在控制台上做过什么操作。

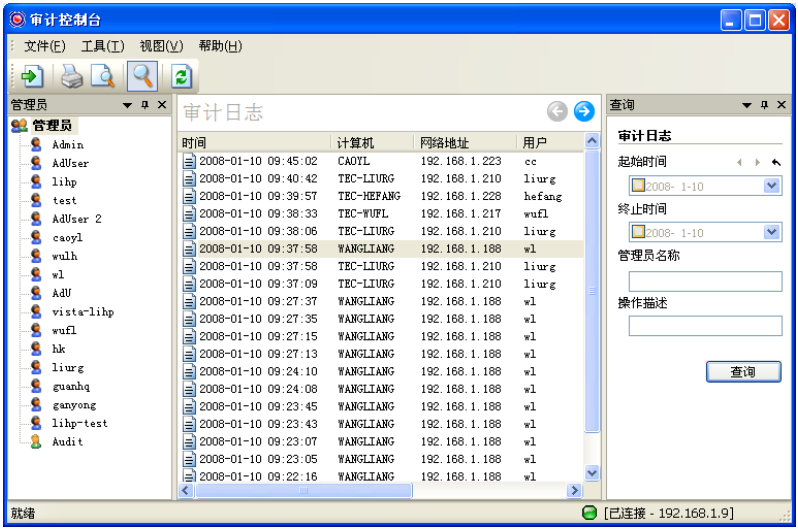
18.1 登录审计控制台

单击安装目录下的 OConsole3.exe 或者“**开始->所有程序->IP-guard V4->IP-guard V4 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。

18.2 审计界面简介

审计控制台包括：标题栏、菜单栏、工具栏、管理员栏、数据视图、查询栏和状态栏。



管理员栏显示的是所有管理员和审计员的列表，选择其中一个管理员，则审计日志将显示该管理员的所有操作日志。

审计日志视图提供了打印、导出功能以保存有用的统计日志，也提供了删除功能以便删除无用的审计日志。

字段名称	说明
打印/打印预览	选择菜单“**文件->打印/打印预览**”打印当前的审计日志；
导出	选择菜单“**文件->导出**”导出审计日志，导出有 2 种方式，右键“**导出->本页记录**”、“**导出->所有满足条件的记录**”；
删除	选择菜单“**文件->删除**”删除审计日志，删除有 3 种方式，单击右键“**删除->选中的记录**”、“**删除->本页记录**”、“**删除->所有满足条件的记录**”。

18.3 使用审计控制台

审计控制台设置

选择菜单“**工具->选项**”，可进行审计控制台设置。勾选“在管理员名称后显

示管理员描述信息”，重启代理控制台后，在管理员结构树视图中，管理员名字后会显示管理员描述。

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。

审计日志记录的内容包括：

字段名称	说明
时间	管理员操作控制台的具体时间；
计算机	管理员登录控制台所在的计算机名称；
网络地址	管理员登录控制台所在计算机的 IP 地址；
管理员	管理员的账户名称；
管理员描述	管理员的账号描述；
描述	管理员对控制台的操作描述信息。

审计日志查询

审计管理员可以通过时间范围、管理员名称、操作描述来查询需要的日志信息。

查询条件	说明
时间范围	设置一个时间范围，查询一个时间段内的审计日志；
管理员名称	查询指定管理员的审计日志，管理员列表在管理员栏中查看；
操作描述	根据审计日志的描述信息查询指定操作的审计日志。

设置审计员账户

选择菜单“**工具->账户**”，系统审计员可以查看和添加新的审计员账户并设置其功能权限。

字段名称	说明
常规	指定审计员的类型，审计员登录的模式等。与控制台管理员账户设置的意义相似；
功能权限	功能权限包括审计日志的保存及删除；
文件	包括导出数据和打印的权限；
删除	是指删除日志数据的权限。

文档云备份服务器	登录云备份服务器 WEB 审计端的权限
管理对象	选择该审计员可以审计的管理员，使该审计员有权限查看选择的管理员的操作日志；可同时选择多个。系统审计员可以审计所有的管理员。

第十九章. 文档安全管理

19.1 术语介绍

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、Visual Studio 等。

在加密系统中，使用授权软件编写的文档会自动加密，使用授权软件打开加密文档时会自动解密。非授权软件无法查看加密文件，未开启客户端加密功能的计算机也无法查看加密文件。

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。

安全区域默认有公共安全区域，可增加自定义区域，如市场部、财务部。安全级别共有五个等级：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。

在控制台的加密权限设置中，可设置客户端能访问安全区域和级别。在加密文档的文档属性中，可设置能访问此文档的安全区域和级别。例如，客户端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。

在线与离线

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。例如：笔记本电脑在企业内接上局域网能连上服务器，为在线状态；笔记本电脑带回家连不上服务器，为离线状态。

一般情况下，客户端离开企业环境，是不允许加解密文件的。如果确实需要使用加密文件，可设置离线权限。

在控制台的加密权限设置界面，可设置客户端在线时的权限；在控制台的离线权限设置界面，可设置客户端离线时的权限。

备用模式

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

解密

企业内的加密文档有时候需要发给企业外部人员，此时文档需要手工解密成普通的文档，对方才能查看。

有解密权限的员工，可直接解密文档。无解密权限的员工，可向管理员申请解密，管理员审批通过后方可解密。

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，而且希望防止二次泄密，则可以把文档生成外发文档。

有外发权限的员工，可直接生成外发文档。无外发权限的员工，可向管理员申请外发，管理员审批通过后方可生成外发文档。

企业外部人员需安装外发查看器才能查看外发文档。

19.2 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

19.3 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。

加密授权模式	说明
透明加密	客户端的文件打开自动解密，保存自动加密。
只读加密	客户端只能以只读方式打开加密文件,不可以修改加密文档；客户端修改非加密文件，保存后该文件不会被加密。

客户端默认是未启用加密授权的，在计算机的基本信息中有一行显示加密授权状态，为未授权。管理员可根据实际需要，控制台上的计算机栏、基本信息和计算机管理中启用或禁用加密授权。

已启用透明加密的客户端，在计算机树上的图标左下角有个小锁标志。在计算机的基本信息中有一行显示加密授权状态，为透明加密授权。

已启用只读加密的客户端，在计算机树上的图标左下角有个绿色小球标志。在计算机的基本信息中有一行显示加密授权状态，为只读加密授权。

对于 Mac 客户端、Linux 客户端，仅支持透明加密模式。

计算机栏：

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。

基本信息：

在 IP-guard 控制台的基本信息中，选择一个计算机组，可查看组内所有计算机的信息。选中一个或多个计算机，右键选择“**加密管理功能->启用加密授权**”，

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。

计算机管理：

在 IP-guard 控制台中，选择菜单“**工具->客户端管理->计算机管理**”进入计算机管理查看窗口。

图标按钮	操作
	启用透明加密授权。
	启用只读加密授权。
	取消计算机的加密授权。

注意 禁用客户端的加密授权后，计算机中的加密文档将无法查看。如需要禁用加密授权，请先把计算机中的加密文档全部解密。

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。

19.4 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 Windows、Mac、Linux 授权软件。

图标按钮	操作
	导入授权软件库。
	导出授权软件库。
	添加自定义授权软件。
	修改自定义授权软件设置。
	删除自定义授权软件。

	恢复自定义授权软件设置。
	保存修改。

如果需要使用的授权软件，在授权软件库不存在，可添加自定义授权软件。

字段名称	说明
名称	自定义的授权软件名称，可以修改，名称不能为空。
图标	点击“…”按钮选择该自定义授权软件的图标。
描述	对该自定义授权软件的描述说明。
关联进程	该授权软件的关联进程，一个软件可以匹配多个进程。如：winword.exe; Excel.exe。多个用 “; ”隔开 【高级应用】如果想匹配版本信息，可以使用如下规则： “匹配项 1=值 1|匹配项 2=值 2|匹配项 3=值 3|匹配项 4=值 4”，多个用“;”隔开。没有“=”表示进程名称。 例如： ProcessName=Winword.exe| InnerName=WinWord| OriginalName=WinWord.exe;
加密文件	打开自动解密，保存自动加密的文件，多个用 “; 隔开
过滤文件	打开自动解密，保存不会加密的文件，多个用 “;”隔开

19.5 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。

图标按钮	操作
	添加安全区域，也可输入描述信息；
	修改安全区域名称和描述信息
	删除安全区域。

默认有一个公共安全区域，无法修改和删除。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。

19.6 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。

图标按钮	操作
	导入外发对象信息，已存在的外发对象和授权信息将忽略，导入的授权信息均为未认证；
	导出当前外发对象信息，包括授权信息；
	添加外发对象，也可输入描述信息；
	修改外发对象名称和描述信息；
	删除外发对象；
	导入外发计算机识别码，该识别码用于将外发文档绑定到外发对象的指定机器上使用；
	可以选择导入外发计算机识别码，该识别码用于将外发文档绑定到外发对象的指定机器上使用； 可以导入选择外发 USBKey 识别码，该识别码用于将外发文档绑定到外发对象的指定 USBkey 上，要插入该 USBKey 的机器才可以打开此外发对象的外发文档；
	可对外发 USBkey 进行相关管理。

修改状态栏的选中和未选中状态，可以启用和禁用对应的外发对象。

授权情况

目前支持三种外发对象授权方式。

授权方式	说明
通用授权	针对计算机的授权方式。该授权方式下，无需绑定外发计算机，任意计算机只要导入外发对象下生成的通用授权证书，都能打开发给此外发对象的外发文件。

绑定计算机授权	针对计算机的授权方式。该授权方式下，需要通过计算机识别码绑定计算机信息，则发给此外发对象的外发文件只有绑定了识别码的计算机可以查看。
绑定外发 USBKey 授权	针对外发 USBKey 的授权方式。该授权方式下，通过外发 USBKey 识别码绑定外发 USBKey 信息，则发给此外发对象的外发文件，只有插入了该外发 USBKey 的机器可以查看。

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

说明 外发计算机识别码的获取方法详情请参考外发查看器章节中的授权->识别码获取小节内容。

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 1.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。

2.外发 USBKey 识别码的获取方法详情请参考外发查看器章节中的授权->识别码获取小节内容。

通用授权和绑定授权的切换

通用授权和绑定授权不能同时存在。启用了通用授权时，绑定授权会被禁用；同理，启用了一个或以上的绑定授权时，通用授权会被禁用。

如果先是使用了通用授权，管理过程中需要变为严格的管控，则可导入计算机的识别码，生成绑定授权并启用。此时之后绑定了识别码的机器才能查看外发给此外发对象的外发文件。

如果目前已是绑定授权，需要放宽管理尺度，则可生成通用授权并启用（若原来已存在通用授权则直接启用）。此时，只要是导入通用授权证书的任何机器都能查看外发给此外发对象的外发文件。此前绑定的机器无需再导入授权文件也可以查看。

19.7 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。

功能按钮说明

图标按钮	说明
	导入，导入外发配置模板文件；
	导出，把外发配置模板导出保存成文件；
	新建，点击该按钮新增加一个模板；
	删除，点击该按钮删除选中的模板；
	复制，点击该按钮复制选中的模板；
	恢复，取消新建或修改模板时点击该按钮；
	保存，设置或修改模板后需保存才会生效。

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。

19.8 加密权限设置

加密权限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。可以针对 Windows 客户端、Mac 客户端、Linux 客户端进行加密权限设置。

图标按钮	说明
	修改选中计算机或用户的加密权限；
	删除选中计算机或用户的加密权限。
	可以选择导出策略文件、导入策略文件、将当前策略复

制到其他客户端。

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。

常规

常规权限	说明
允许申请解密文档	默认的加密权限，可以向管理员申请解密文档；
允许直接解密文档	直接把加密文档解密的权限，不需要通过管理员审批；
备份解密文档	备份解密的文件，备份的是解密之前的加密文件；
备份的范围	解密在此大小范围内的文档才会备份；
允许申请外发文档	可以向管理员申请申请外发文档；
更多高级设置	客户端申请外发文件时，对外发对象的选择范围以及外发配置进行限定； 其中，外发配置可点击  按钮在已有外发模板中选择，也可以手动设置，点击  按钮可将当前设置保存成外发模板；
外发对象	客户端申请外发时只能向指定的外发对象外发文件；同时还可设置申请外发时必须指定至少一个外发对象。

常规权限	说明
文件权限	客户端申请外发时，对文件的各项权限只能做指定的设置。 打印、虚拟打印、剪贴版、截屏、编辑修改、自动删除指定如下： 无限制：客户端在申请外发文件时，此项权限可以自由设置为允许或者禁止； 禁止：客户端在申请外发文件时，此项权限为“禁止”且不可更改； 允许：客户端在申请外发文件时，此项权限为“允许”且不可更改； 最大打开次数、有效时间指定如下： 无限制：客户端在申请外发文件时，此项权限可以自由选择是否设置最大打开次数、有效时间； 输入值：**次数** 输入 1-99 的正整数，则客户端申请外发文件时，允许打开次数仅可设置为输入值且不可更改； **有效时间** 输入 1-1000 的正整数，则客户端申请外发文件时，有效时间不能超过输入值的天数； 过滤文件指定如下： 禁止：客户端在申请外发文件时，不允许设置过滤文件； 输入值：输入文件类型，多个类型使用逗号分隔，如 *.dwg,*.dxf，则客户端在申请外发文件时可以选择是否过滤文件，若选择了“允许过滤”，设置过滤文件类型必须在此处指定的文件类型范围内。
允许直接外发文档	直接生成外发文档，不需要通过管理员审批；
更多高级设置	客户端直接外发文件时，对外发对象的选择范围以及外发配置设定进行限定。详细可参见允许申请外发文档的更多高级设置，两者类同。
备份外发文档	对外发的文档进行备份；
备份的范围	在此大小范围内的外发文档才会备份；
允许提取客户端权限内的外发文档	可提取访问权限在自身权限内的外发文档；

常规权限	说明
允许提取更高权限的外发文档	可提取访问权限高于自身权限的外发文档；
允许申请修改加密文档安全属性	能向管理员申请修改加密文档安全属性；
允许直接修改加密文档安全属性	直接修改加密文档安全属性，不需要通过管理员审批。
允许登录代理管理员	可以在客户端上使用管理员帐户登录代理管理员，进行解密审批和外发审批。
允许客户端注销加密系统	客户端在线时可以注销加密系统，注销后，所有加密功能被停用。重新登入加密系统后，加密功能正常。
加密登录方式	勾选“允许客户端注销加密系统”，则客户端处才能注销加密系统， 允许客户端自行设置：客户端处“加密图标右键-选项-加密系统登入设置”中，在线和离线的登入可按自己意愿进行设置； 强制手动登入：客户端处“加密图标右键-选项-加密系统登入设置”中，在线和离线的登入设置被指定为“强制手动登入”且不可更改； 自动登入：客户端处“加密图标右键-选项-加密系统登入设置”中，在线和离线的登入设置被指定为“自动登入”且不可更改；

说明 针对 Linux 客户端、Mac 客户端，设置加密常规权限时，仅“允许申请解密文档”、“允许直接解密文档”设置生效，其他设置当前暂不支持。

授权软件

对于透明加密授权，需要手动选定授权软件；只读加密授权，以只读方式打开一个加密文档时，客户端会自动把打开加密文档的软件设置为授权软件。

目前授权软件有四种加密工作模式。

工作模式	说明
自动加解密	可以查看加密文件，并且使用此软件编写的文件，都会被加密。

智能加解密	可以查看加密文件。 使用此软件修改加密文件并保存，该文件仍为加密文件； 使用此软件修改非加密文件并保存，该文件仍为非加密文件。
只读加密	可以查看加密文件，无法使用此软件修改保存加密文件。
只解密不加密	可以查看加密文件，并且使用此软件修改后保存的文件，都会变成非加密文档。

此外，还可以设置使用各授权软件时是否允许打印、虚拟打印、截屏和剪贴板。该设置同时对透明加密授权以及只读加密授权生效。

说明 1.针对 Linux 客户端、Mac 客户端，设置授权软件加密模式时，仅“自动加解密”、“只解密不加密”设置生效，若设置为其他设置则效果相当于“自动加解密”。

2.对于只读加密授权，只读打开加密文件时的程序若并未设置为授权软件，则打印、虚拟打印、截屏以及剪贴板都会被禁止。

安全区域

指定客户端能打开的文档的安全区域和级别。例如：客户端只有市场部机密级别的权限，则他可以打开市场部机密级别和机密级别以下的文档，不能打开财务部任何安全级别的文档。

加密文档默认安全属性

默认情况下加密文档的加密属性是公共区域普通级别，可以设置所有文档或特定的文档具有指定的安全区域和级别。

选项	说明
安全属性	
设置权限	设置加密文件默认的设置权限；
访问权限	设置加密文件默认的访问权限；
文件范围	
包含文件	在此范围中的文件使用已设置的默认安全属性； 输入文件名或路径，可使用通配符。如：*.doc、c:*等。

排除文件	在此范围中的文件不使用设置的默认安全属性； 输入文件名或路径，可使用通配符。如：*.txt、c:*等。

注意　此设置只对新生成的加密文件有效。已存在的加密文件不会修改其安全属性。

19.9 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。

加密参数各项设置，完成后需要保存才可以生效。

图标按钮	说明
	修改选中计算机或用户的加密参数设置；
	删除选中计算机或用户的加密参数设置。
	可以选择导出策略文件、导入策略文件、将当前策略复制到其他客户端。

注意　以下加密参数的各项设置项中，如无特殊说明，则代表仅针对 Windows 客户端生效，针对 Linux 客户端、Mac 客户端不生效。

应急设置

容灾时间

容灾时间是为应急而设定。设置了“容灾时间”的客户端，如因网络故障或服务器故障导致客户端与服务器之间无法正常连接，而客户端又没有长期离线授权策略，那么，该客户端就可在容灾时间范围内进入备用模式，依照其在线权限进行加解密操作。

说明　此设置对 Mac 客户端、Linux 客户端也生效。

允许复制少量文本

对于设置了禁止剪贴板的授权软件，使用该软件打开文档时，不可以将内容复制到非授权软件中。有时企业内部会因为业务的需要，要在这类的授权软件文

档中的少量内容复制到其他地方，此时则可设置允许复制少量文本。

设置时填入为允许复制的字数，如：5，则允许复制 5 个字的内容。

显示设置

隐藏加密标记

设置了“**隐藏加密标记**”的客户端上，所有的加密文档上均不再显示加密小锁图标。用户从视觉上无法判定哪些是加密文档，哪些是非加密文档。

隐藏加密客户端界面

设置了“**隐藏加密客户端界面**”的客户端上，右下角托盘图标处的加密系统图标将被隐藏。用户将无法进行依托于加密图标菜单中的操作。

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。

安全密码输入设置

管理员可以对客户端的安全密码输入设置进行限制，具体设置项说明如下：

设置项	说明
允许客户端自行设置	默认情况下为此项；客户端的“安全密码输入设置”，可按自己意愿进行设置；

每次操作都必须输入	选择此项，则客户端的“安全密码输入设置”被指定为“每次操作都必须输入”且不可更改；
登入安全对象后只需输入一遍	选择此项，则客户端的“安全密码输入设置”被指定为“登入安全对象后只需输入一遍”且不可更改；
登入操作无需再输入安全密码	选择此项，则客户端的“安全密码输入设置”被指定“登入操作无需再输入安全密码”且不可更改；

密码错误次数验证

勾选此项后，在客户端执行需要输入安全密码的操作时，会对密码错误次数进行验证。

设置项	说明
在限定时间内	可设置一个具体的时间，单位为分钟，默认为 20 分钟 0 时代表不限时间；
密码错误达到	指输入密码错误的次数，默认为 5；
密码输入锁定时间	密码错误次数达到指定次数后，指定时间内安全密码输入框不可用；默认锁定 10 分钟；0 代表不锁定；
密码输入锁定报警	密码错误次数达到指定次数后，控制台会有报警信息，级别为最低，默认勾选；

设置后，在指定时间内，密码错误达到指定的次数，密码输入框将会被锁定指定时长。

密码最长使用期限

管理员可以指定安全密码可以使用的天数。如指定为 30 天，则从该密码设置成功起的 30 天内，该密码可以正常使用，超过 30 天则会提示密码已达期限，需要修改安全密码。若控制台设置时客户端的安全密码已存在，则从控制台设置成功后的时刻开始计算期限。

加密文档缩略图设置

设置加密文档缩略图，可实现在资源管理器中显示加密文档的缩略图和预览图。

设置选项	说明
显示缩略图	设置是否显示加密文档缩略图。
显示的文件类型	选择显示缩略图的加密文档类型。
排除的文件类型	选择不显示缩略图的加密文档类型。
显示预览图	设置是否显示加密文档预览图。
显示的文件类型	选择显示预览图的加密文档类型；

设置选项	说明
排除的文件类型	选择不显示预览图的加密文档类型；

说明 *.jpg *.jpeg *.jpe *.bmp *.gif *.png*.tif *.tiff，上述类型的加密文件默认显示缩略图和预览图。

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。

设置选项	说明
邮箱地址规则设置	设置白名单邮箱地址规则，可设置多条规则；
附件文件名称	对指定附件名称做控制。可设置包含的附件文件名，也可设置排除的附件文件名； 设置时输入文件名，支持通配符，支持输入多个，以“,” “;”作为分隔符；
备份解密的附件文件	如果勾选了“备份解密的附件文件”，则此处会显示为“是”，否则显示为“否”；
备份范围	备份的密文附件大小限制，默认为 0-100000 KB；超过此范围的附件不会备份。

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。

设置选项	说明
规则名称	设置邮箱规则名称；
模式	选择模式，可选择解密附件和不解密附件； 解密附件：符合本规则的邮件，加密的附件会被解密； 不解密附件：符合本规则的邮件，加密的附件不会被解密； 默认为解密附件模式；
接收邮箱	设置收件人的邮箱，包括收件人也包括抄送人和密送人的邮件地址； 可设置包含的邮箱，以及排除的邮箱，排除邮箱优先于包含邮箱；

设置选项	说明
	排除范围中的邮箱属于不匹配本策略，继续匹配下一条策略。 支持直接输入邮箱地址，以及选择邮箱分类进行控制： 点击，添加邮箱地址，可以输入完整的邮箱地址，如“123@qq.com” ，可以使用通配符输入一类邮箱地址，如*@126.com，多个设置使用“,”隔开。设置后可点击进行修改； 点击，添加邮箱分类；
允许排除范围外的收件人解密	对接收邮箱排除范围之外的收件人邮箱地址做控制。 一封有多个收件人的邮件： 1.属于包含范围内的收件人，收到的附件一定解密； 2.属于排除范围内的收件人，收到的附件一定不会解密； 3.既不属于包含范围，也不属于排除范围的收件人： 勾选此项，则这些收件人收到的附件会解密； 不勾选此项，则这些收件人收到的附件不会解密
发送邮箱	设置发件人的邮箱； 可设置包含的邮箱，以及排除的邮箱，排除邮箱优先于包含邮箱； 排除范围中的邮箱属于不匹配本策略，继续匹配下一条策略。 支持直接输入邮箱地址，以及选择邮箱分类进行控制： 点击，添加邮箱地址，可以输入完整的邮箱地址，如“123@qq.com” ，可以使用通配符输入一类邮箱地址，如“*@126.com” ，多个设置使用“,”隔开。设置后可点击进行修改； 点击，添加邮箱分类；

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 1

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

邮件白名单规则使用示例 2

企业相关情况

1.公司内工作使用公司内部邮箱，员工的沟通交流和工作文件流转等均通过内部邮件；

2.内部邮箱的后缀统一为@innerdept.com。

需要实现

内部员工的邮件交流，除了发送给特定的几位领导（li@innerdept.com, zhang@innerdept.com）的邮件需要解密附件，其余情况均不解密附件。

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 li@innerdept.com, zhang@innerdept.com，排除邮箱为

空，不勾选"允许排除范围外的收件人解密"

发送邮箱：包含*@innerdept.com，排除邮箱为空

日志策略

客户端默认会记录所有的加密文档操作日志。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，此时可通过日志策略来控制加密文档操作日志的记录。

设置选项	说明
记录日志	默认为记录文档操作日志，不勾选则为不记录，勾选此项的前提下，才可以对操作类型和文件范围进行设置；
记录的操作类型	默认为记录全部类型，可根据需求进行选择；
记录的文件范围	
包含文件	此范围内的文件，其加密操作会记录；输入文件名或路径，可使用通配符。如：*.doc、c:*等。
排除文件	此范围内的文件，其加密操作不会被记录；输入文件名或路径，可使用通配符。如：*.doc、c:*等。

说明 此设置对 Mac 客户端、Linux 客户端也生效。

扩展功能

加密新建文件

加密新建文件功能，可以对指定目录下新出现的文件和修改过的文件进行自动加密，加密后文件安全属性为“公共安全区域”-“普通”级别。

设置选项	说明
加密新建文件	设置是否启用加密新建文件功能
排除范围	设置指定目录和指定文件类型不会被自动加密。支持多条设置，新建设置默认为本地硬盘目录的所有文件。
加密范围	设置指定目录和指定文件类型会自动加密。多支持多条设置，新建设置默认为本地硬盘目录的所有文件。

目前支持本地硬盘和网络盘。目录必须是一个确定的合法的客户端本地磁盘路径,支持通配符“*”和通用路径{sd}。如：{sd}users*\Documents。注意，“*”在目录中仅能表示一层文件夹。{sd}代表系统盘根目录，如 C:\，必须使用小写字母，{sd}后直接接文件夹名，不能加“\”。

文件类型支持通配符“*”和“?”。

若部署了文档备份服务器，则启用了“**加密文档自动备份任务**”的客户端，通过加密新建文件策略而加密的文件也会自动备份。

加密授权软件只解密不加密文件

管理员可以对授权软件设置只解密不加密的文档。

设置选项	说明
进程	设置的授权软件的进程名，支持通配符，多个进程以“,”分隔；
文件	增加设置的过滤文件，支持路径和后缀，如 E:\work*.dat；支持通配符和通用路径；支持“,”作为分隔符。

说明 1.仅对授权进程在使用过程中修改的文件生效，对直接手工加密、加密新建文件功能、全盘扫描加密功能的操作对象文件不生效；

2.此设置中的不加密文件，比授权库中的加密文件优先。

窗口浮水印

外发文档浮水印

可以设置客户端生成的外发文档带有水印信息。包括：自定义文字、外发文件创建者信息、外发文件阅读者信息等。水印信息在打开外发文档时的可视窗口中显示。

设置选项	说明
外发文档浮水印	设置是否启用外发文档浮水印；
文字内容	设置浮水印的文字内容；
字体类型	设置浮水印内容文字的字体类型；
字体大小	设置浮水印内容文字的字体大小；
字体颜色	设置浮水印内容文字的字体颜色；
透明度	设置浮水印内容文字的透明度；
创建者信息	选择浮水印内容中显示外发文件创建者信息，包括：计算机名称、IP 地址、用户名称、创建时间；

设置选项	说明
阅读者信息	选择浮水印内容中显示的外发文件阅读者信息，包括：计算机名称、IP 地址、用户名称、阅读时间；

外发文档浮动窗口标题

可以设置客户端生成的外发文档打开查看时带有浮动窗口，并可设置浮动窗口标题内容。浮动窗口可在打开的文件区域内任意拖动位置。

设置选项	说明
外发文档浮动窗口标题	设置是否启用外发文档浮动窗口标题；
文字内容	设置外发文档浮动窗口标题的文字内容；
字体颜色	设置外发文档浮动窗口标题文字的字体类型；
背景颜色	设置外发文档浮动窗口标题区域的背景颜色；
显示关闭按钮	勾选此项，则浮动窗口会出现关闭按钮，用户可手动关闭浮动窗口； 不勾选此项，则浮动窗口会不出现关闭按钮，浮动窗口在关闭对应的外发文件前无法手动关闭；
显示进程类型图标	勾选此项，则会显示外发文档进程类型图标； 不勾选此项，则不会显示；
显示权限	勾选此项，则鼠标移动至浮动窗口，会显示当前外发文件的权限； 不勾选此项，则不会显示。

外发文档边框

可以设置客户端生成的外发文档，在打开查看时程序窗口带有边框，便于用户区分打开的文件是普通文件还是外发文件。可设置边框颜色和边框大小。

设置选项	说明
外发文档边框	设置是否启用外发文档边框；
边框颜色	设置边框颜色；
边框大小	设置边框大小，输入 1-10 的正整数，数值越大，边框线条越粗。

外发文档网络设置

外发文档默认禁止访问网络，当碰到某些外发文档在使用时必须使用网络，否

则无法正常查看的情况时，管理员可以设置放开某些指定进程对指定网络的访问。

设置选项	说明
外发文档允许网络	设置是否启用外发允许网络策略；
允许网络	设置进程和对应允许的网络。可设置多条策略，每条策略包含一个进程名和一组网络地址。 网络地址格式为：IP 或 IP:Port，多 IP 地址之间以英文逗号“,”分隔；不支持 IP 地址段、端口段。 例如：进程设置为 CATIA.exe，允许网络设置为 192.168.7.230:8090。则在查看外发文件时，允许 CATIA.exe 访问 192.168.7.230:8090。

申请文档上传设置

启用设置

开启申请文档上传设置，勾选启用设置，符合条件的文档将会上传至申请文档存储服务器。

设置选项	说明
启用设置	设置是否启用申请文档上传至文档存储服务器。
文档存储服务器地址	输入文档存储服务器地址（只支持 https 协议，故端口填 https 协议的端口号）；
包含文件	此范围内的文件，会被上传至文档存储服务器；在给定的预定义文件类型中选择或者点击“ ”按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。
排除文件	此范围内的文件，不会被上传至文档存储服务器；在给定的预定义文件类型中选择或者点击“ ”按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。
文件大小	设置上传文件的大小范围；可自定义设置，文件大小仅限于 0 至 2000000kb 之间。

19.10 长期离线授权设置

长期离线授权设置是对启用加密授权的客户端在连不上服务器时的权限设置。例如公司高层经常需要在公司外办公时，要保证能正常查看和编辑加密文档，则可设置长期离线授权。

图标按钮	说明
	修改长期离线权限；
	删除长期离线权限；
	导出离线授权文件。
	可以选择导出策略文件、导入策略文件、将当前策略复制到其他客户端。

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 Windows 客户端、Mac 客户端、Linux 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 Windows 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。

说明 Mac 客户端、Linux 客户端当前不支持离线授权导入。

19.11 安全通讯设置

安全通讯设置是配合硬件安全网关功能的设置，需要在已部署安全网关的前提下设置本策略，否则将出现无法上网等异常现象。

图标按钮	说明
	修改安全通讯设置；
	删除安全通讯设置；
	可以选择导出策略文件、导入策略文件、将当前策略复

制到其他客户端。

具体设置项说明:

应用系统保护

设置选项	说明
启用对应用系统的保护	勾选此项，则对客户端启用应用系统保护；
安全进程窗口标志	填入具体的内容，如：安全进程，则打开安全进程时，进程窗口上会显示此内容；
例外网络范围	设置为强制模式的安全进程，仅可以访问受保护的应用系统服务器，其他网络地址无法访问，支持输入网络地址和域名； 若想让安全进程访问其他的网络地址，可以设置为例外网络范围；支持 ip 段输入，多个输入使用逗号隔开，如：192.168.1.1-192.168.1.100,192.168.2.102；
安全进程	设置安全进程，点击 进行添加，需要输入进程名和加密模式； 进程名：输入需要设置为安全进程的进程名，一条配置支持输入多个进程名，使用逗号隔开，如 iexplore.exe, TortoiseProc.exe。输入多个并保存后会自动分成多条； 加密模式：分为强制模式和智能模式； 强制模式下，安全进程只能访问受保护的应用服务器和例外网络范围内的服务器，其他地址无法访问； 智能模式下，安全进程既可以访问受保护的应用服务器，也可以访问其他非受保护地址。 如果是选择智能模式，则需要配置以下“智能模式设置”相关设置项；
智能模式设置	本设置针对选择了智能模式的安全进程生效；
受保护服务器	输入受保护的应用系统服务器，支持以下格式输入： IP:端口，如：192.168.2.104:8080； IP:端口段，如：192.168.2.104:8080-8079； IP 段:端口，如：192.168.2.1-192.168.2.255:8080； IP 段:端口段，如：192.168.2.1-192.168.2.255:1000-8079； 域名，如：jira5.development.tec；

设置选项	说明
	说明：这里设置的受保护服务器，需和安全网关设备中设置的受保护应用系统服务器一致。否则智能模式的安全网关进程无法访问受保护的应用系统服务器；
上传控制	勾选此项，则对上传操作进行控制；
上传限制大小	设置上传限制的文件大小，超过该大小的文件将被限制上传；
上传控制白名单	设置上传白名单地址，则启动上传控制时，上传到白名单地址的文件不受限制； 可以输入 ip 或者 ip 带端口，支持多个输入，多个输入使用逗号隔开，如 192.168.1.1,192.168.1.2:80。

网络共享文档保护

设置选项	说明
启用对网络共享文档目录保护	勾选此项，则对客户端启用网络共享文档目录保护；
安全网关地址	设置安全网关的 IP 地址，点击  进行添加；
受保护的共享文档目录	设置受保护的共享文档目录，点击  进行添加；输入具体的目录路径，如：\\192.168.1.1\release\ 不支持通配符。
文件白名单设置	设置为文件白名单的文件，从受保护的网络共享文档目录中复制出来不加密。 勾选“PE 文件”，则 PE 类文件如 exe，dll 等，被设置为文件白名单； 勾选“指定文件类型”，并输入文件类型，支持多个输入，多个输入使用逗号隔开，如：*.txt,*png ，这些文件类型会被设置为文件白名单；
进程白名单设置	只有授权进程可以直接在受保护网络共享文档目录中打开文件。如果想让非授权进程也可直接在受保护网络共享文档目录中打开文件，则需要设置进程白名单。 输入进程名，支持通配符，支持多个输入，多个输入使用逗号隔开，如：notepad.exe,*word.exe。

注意 受保护的共享文档目录，若既可以通过域名访问，也可以通过 IP 访问，则两个地址都要添加，如 \\192.168.1.1\release\ 和 \\server\release\ 都要添加，否则通过未添加的方式访问时不

受控制。

19.12 加密文档操作日志

加密文档操作日志可记录：

1.Windows 客户端加密文件，解密文件，生成外发文件，修改文档安全属性，解密申请，外发文件申请和修改文档安全属性申请等相关日志。

2.Mac 客户端、Linux 客户端加密文件、解密文件的日志。

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。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。

19.13 全盘扫描

用户可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。

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。

说明 Mac 客户端、Linux 客户端暂不支持全盘扫描功能。

19.13.1 全盘扫描任务设置

全盘扫描加密任务

设置全盘扫描加密任务步骤：

5) 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；

6) 在“常规”选项卡中，对常规项目进行设置；

7) 切换至“高级”选项卡中，对高级项目进行设置；

8) 设置完成后，点击“确定”按钮，扫描加密任务创建成功。

常规设置说明：

设置选项	说明
任务名称	当前任务的任务名。系统会自动填上默认值，可以修改。
选择对象	可进行目标计算机选择。此前选中的客户端机器在此处被勾选上，也可以增加或去除选择对象。
包含文件	此范围内的文件，会被扫描加密； 可以在给定的预定义文件类型中选择；也可点击  按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。
排除文件	此范围内的文件，不会被扫描加密； 可以在给定的预定义文件类型中选择；也可点击  按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。
过滤文件	默认会排除一些系统文件，点击  按钮可已查看具体被过滤的文件。如果不想过滤这些文件，可在包含文件中添加。

说明 包含文件、排除文件、过滤文件之间的优先级为“排除范围>包含范围>过滤文件”。

高级设置说明：

设置项	说明
任务选项	设置任务执行的内容；
明文加密成密文	扫描到明文则加密成密文；

密文变更安全属性	扫描到密文则变更安全属性，可以选择以下三种变更： **公共-普通变更安全属性**：只变更文档的加密属性中的访问属性只有“公共-普通”的加密文件。 **低级别变更高级别安全属性**：系统会对加密文档的原设置属性与新设置的设置属性进行对比，原设置权限低于新的设置权限则变更。 **强制变更安全属性**：无论原文档是什么安全属性，都会变更为新设置的安全属性。
文件安全属性	设置文件被加密后的安全属性，包括设置权限和访问权限，加密后的文档的安全属性和此处设置一致。
性能设置	任务进行时的性能设置。
扫描速度任务优先	扫描速度会快，对系统性能会有一定影响；建议在执行任务时间为非工作时间时，选择此项。
系统性能优先	扫描速度会放慢，对计算机的资源消耗不会太高，保证系统性能；执行任务时间为工作时间时，建议选择此项。
仅在空闲时扫描	客户端空闲时才会扫描并对指定文件加密，其余时间不扫描不加密； 客户端空闲指：控制台上显示该客户端的状态为“正在运行（空闲）”。
扫描时段	设置任务开始扫描加密的时间。在下拉菜单中选择符合要求的时间分类； 此处下拉菜单中选择分类的即为时间类型管理中的各分类。
文件大小	此大小范围内的文件才会被加密。

说明

1. 包含文件为空，或者选定计算机对象为空时，扫描加密任务不可创建。
2. 管理员创建加密任务并设置文档安全属性时，受其本身的安全区域和级别限制。
3. 全盘扫描加密任务创建成功后，则无法修改任务设置，请在创建任务时务必确认好每项设置。

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。

常规设置说明：

设置选项	说明
任务名称	当前任务的任务名。系统会自动填上默认值，可以修改。
选择对象	可进行目标计算机选择。此前选中的客户端机器在此处被勾选上，也可以增加选择对象。在查询栏中输入对象名称，可模糊匹配快速定位到对象，点击一次查找则定位到下一个匹配对象。
包含文件	此范围内的文件，会被扫描解密；默认解密所有文件； 可以在给定的预定义文件类型中选择；也可点击  按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。
排除文件	此范围内的文件，不会被扫描解密； 可以在给定的预定义文件类型中选择；也可点击  按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。

高级设置说明：

设置项	说明
文件安全属性	设置解密访问权限为指定安全属性的加密文件。
全部区域全部级别	选择此项，则属于全部区域和全部级别的加密文件都会被解密。
全部区域指定级别	选择此项，并指定级别，则属于全部区域且为指定级别的加密文件会被解密。
指定区域指定级别	选择此项，并设置指定的安全区域和级别，则访问权限属于或低于此设置的加密文件会被解密。
性能设置	任务进行时的性能设置。
扫描速度任务优先	扫描速度会快，对系统性能会有一定影响；建议在执行任务时间为非工作时间时，选择此项。

系统性能优先	扫描速度会放慢，对计算机的资源消耗不会太高，保证系统性能；执行任务时间为工作时间时，建议选择此项。
仅在空闲时扫描	客户端空闲时才会扫描并对指定文件解密，其余时间不扫描不解密； 客户端空闲指：控制台上显示该客户端的状态为“正在运行（空闲）”。
扫描时段	设置任务开始扫描解密的时间。在下拉菜单中选择符合要求的时间分类； 此处下拉菜单中选择分类的即为时间类型管理中的各分类。
文件大小	此大小范围内的文件才会被解密。

说明

1. 选定计算机对象为空时，扫描解密任务不可创建。
2. 管理员创建解密任务并设置文档安全属性时，受其本身的安全区域和级别限制。
3. 全盘扫描解密任务创建成功后，则无法修改任务设置，请在创建任务时务必确认好每项设置。

19.13.2 查看任务信息

对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，正在执行的任务为当前任务，等待执行的任务为后续任务，当前任务执行完后，后续任务自动变为当前任务。

当前任务信息

在全盘扫描功能界面的上半视图中，可以查看每台客户端当前执行任务的基本信息。

内容项	说明
计算机	客户端的计算机名称。
组	客户端所在分组的名称。
扫描功能	扫描功能的状态：启用/禁用；启用时可执行全盘任务，禁用时全盘任务暂停； 扫描功能默认为开启状态。

内容项	说明
当前任务	客户端当前执行的全盘任务名称。
当前任务状态	客户端当前执行的全盘任务状态； 1. 当扫描功能为启用时，当前任务会执行，状态为“启动” 2. 当扫描功能为禁用时，当前任务会暂停，状态为“暂停” 3. 在任务启动和暂停的过程中，对应会有“正在启动”/“正在暂停”的状态 4. 当扫描任务执行完成后，状态为“完成”
开始时间	客户端当前执行的全盘任务开始执行的时间。
进度	客户端当前执行的全盘任务的完成进度，会根据当前进度自动更新。

其他任务信息

选中一台客户端，在全盘扫描功能界面下半视图的“**任务信息**”选项卡中，除了可以查看该台客户端当前任务，也可以查看后续任务的任务信息，明细包括创建该加密任务时对应的各项设置内容。

说明 全盘扫描任务仅执行一次，执行完毕后不会保留，将执行后续任务。

特殊：

一台客户端最后一个任务（无后续任务）执行完成后，会保留在全盘扫描功能界面该客户端的当前任务信息中。此时对该计算机执行“先禁用扫描功能，再启用扫描功能”的操作，会重新执行该任务，适用于需定时执行同一任务的使用情形。

19.13.3 查看任务日志

在全盘扫描功能界面，选中一台客户端，在下半视图的“**任务日志**”选项卡中，可以查看该客户端执行任务的日志。通过工具栏上的刷新按钮进行刷新。

内容项	说明
时间	该条任务日志产生的时间。
任务名称	当前执行的任务名称。
内容	包括：当前任务完成的百分比，当前扫描的目录，该任务的主要信息（包含条件、排除条件）

19.13.4 启用/禁用扫描功能

禁用

计算机的扫描功能默认为启用状态。在全盘扫描功能界面，选中一台或多台客户端，点击禁用按钮，或是右键菜单中选择“**禁用扫描功能**”，则目标客户端的扫描功能会被禁用，正在进行的任务将暂停。

启用

选中一台或多台禁用了扫描功能的客户端，点击启用按钮，或是右键菜单中选择“**启用扫描功能**”，则目标客户端的扫描功能会被启用，此时若有暂停的任务，该任务将继续执行，后续任务也会按次序执行。

19.13.5 删除任务

选中一台或多台客户端，点击删除按钮，或是右键菜单中选择“**删除计算机任务**”，则目标客户端的所有任务都会被删除，包括当前任务和后续任务。

19.13.6 查询计算机任务

查询

点击查询按钮，弹出查询对象选择对话框，选择指定的计算机或者计算机组，点击【**确定**】按钮，则计算机列表中仅会出现符合查询条件的计算机，可进行针对性查看。

模式

点击模式切换按钮，可以选择显示所有的计算机，也可以选择仅显示有任

务的计算机。

19.14 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：

8) 客户端使用右键菜单或扫描工具申请解密；

9) 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；

10) 双击申请记录，可查看申请信息和文件内容；

11) 若要批准，点击【**批准**】按钮，反之点【**拒绝**】按钮；

12) 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。

删除申请

具有删除解密申请权限的管理员，可以删除解密申请。在解密申请视图中，选择一条或多条申请，根据需要选择一种删除模式：删除选中的记录、删除本页记录、删除所有满足条件的记录。

说明 任何状态的解密申请均可以删除，已审批但未分发的申请被删除后，审批结果不会继续分发到客户端。

19.15 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。

删除申请

具有删除外发申请权限的管理员，可以删除外发申请。在外发申请视图中，选择一条或多条申请，根据需要选择一种删除模式：删除选中的记录、删除本页记录、删除所有满足条件的记录。

说明 任何状态的外发申请均可以删除，已审批但未分发的申请被删除后，审批结果不会继续分发到客户端。

19.16 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；

删除申请

具有删除临时离线申请权限的管理员，可以删除临时离线申请。在临时离线申请视图中，选择一条或多条申请，根据需要选择一种删除模式：删除选中的记录、删除本页记录、删除所有满足条件的记录。

说明 任何状态的临时离线申请均可以删除，已审批但未分发的申请被删除后，审批结果不会继续分发到客户端。

19.17 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。

删除申请

具有删除安全属性变更申请权限的管理员，可以删除安全属性变更申请。在安全属性变更申请视图中，选择一条或多条申请，根据需要选择一种删除模式：删除选中的记录、删除本页记录、删除所有满足条件的记录。

说明 任何状态的安全属性变更申请均可以删除，已审批但未分发的申请被删除后，审批结果不会继续分发到客户端。

19.18 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。

图标按钮	说明
	一个管理员既可以是委托者，也可以是受托者；可切换查看委托的情况以及受托的情况。系统管理员还可以切换查看所有管理员的委托情况。
	进行审批权限委托设置；
	删除委托的权限，即收回委托的权限。

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。

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。

注意 受委托的权限，不能被委托或代委托给其他管理员。

19.19 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，“**申请管理->加密申请管理->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。

功能按钮说明

图标按钮	说明
	查找，点击该按钮可按条件查询对应的审批流程；

	新建，点击该按钮新增加一条流程；
	编辑，点击该按钮编辑选中的流程；
	删除，点击该按钮删除选中的流程；
	复制，点击该按钮复制选中的流程
	上移，将选中的流程上移一个位置；
	下移，将选中的流程下移一个位置；
	替换，选中具体的流程后点击该按钮，可设置替换新的审批人；
	恢复，取消新建或修改流程时点击该按钮；
	保存，设置或修改流程后需保存才会生效。

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。

流程条件包括以下：

字段名称	说明
基本设置	流程的基本信息设置；
流程名称	新建的流程的名称，不能输入已存在的流程名。不输入时，则默认为“审批流程”，其后新建的流程默认名称为“审批流程_1”、“审批流程_2”，以此类推；
申请类型	能匹配此流程的申请类型，可勾选全部也可选择其中某一类或几类；
申请对象	能匹配此流程的申请对象，可以选择计算机、用户，也可以选择角色；
文件设置	对文件属性进行设置，此处如果不设置则表示不限制；
文件数量	申请的文件数在设定的数量范围内的申请才能匹配此流程。数值范围在[0,100000]之间。
文件总大小	申请的文件的总大小在设定的范围内的申请才能匹配此流程。数值范围在[0,100000000]之间。

文件路径\文件类型	文件路径\文件类型与设置的相匹配的申请才能匹配此流程。此处可以设置文件路径也可设置文件类型，两者也可混合设置。各条件间用“,”或“;”分隔，支持通配符，如*.doc，*.txt,c:\test*等。各条件之前是“或”的关系
文档安全属性	点击按钮即可弹出条件设置框，可以设定文件的“设置权限”和“访问权限”；若勾选了“满足上述任一条件即可”，则与设置的任一条件相符合即可匹配此流程，不勾选则必须与设置的条件完全一致方能匹配； 此处如果不设置则表示不限制；
外发对象	选择外发对象；若勾选了“满足上述任一条件即可”，则与设置的任一条件相符合即可匹配此流程，不勾选则必须与设置的条件完全一致方能匹配； 此处如果不设置则表示不限制；
外发配置	点击按钮即可弹出条件设置框，可以设置外发属性（打印、虚拟打印、剪贴板、截屏、编辑修改）以及对应条件（禁止/允许）；若勾选了“满足上述任一条件即可”，则与设置的任一条件相符合即可匹配此流程，不勾选则必须与设置的条件完全一致方能匹配； 此处如果不设置则表示不限制；
临时离线	选择延时时长的区间，时长的单位有分钟、小时和天可以选，最多不能超过 1000 天。 此处如果不勾选“临时离线”则表示不限制。

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。流程环节设置包括以下：

字段名称	说明
环节名称	新增的环节名称，格式不限，必填，不能与已有的重复；
审批人员	此环节的所有审批人员，可选择多个审批人，必选；
审批通过条件	此环节通过的条件，可选择“必须由全体审批人员批准通过”，或者“必须由指定人数的审批人批准通过”。指定的人数不能大于全部审批人员的人数。任意一人拒绝申请此环节不能通过。

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。

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。若删除流程时，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。

说明 **原审批人只能在选中的流程中包含的审批人中选择，新审批人可以在所有用户中选择。替换审批人后，原先属于此流程的未完成的申请都会失效。**

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。

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。

注意 加入到流程中的审批者账号，可能会出现权限变更或者被删除的情况。在已启用的流程中，如果某一环节中，存在且拥有加密管理权限的管理者小于必要批准人数，则该条流程失效。
对于失去加密管理权限的环节审批者，即使重新赋予其加密管理权限，该流程也不会重新生效。

19.20 自动审批设置

管理员可以根据需要赋予对应的审批员自动审批的权限，开启功能后客户端提交给对应审批员的申请会自动批准。

审批员需要有“**允许设置自动审批**”的权限才能开启自动审批，管理员可在控制台“**工具->账户管理->加密功能->流程管理**”中，勾选“**允许设置自动审批**”，赋予审批员自动审批的权限。

开启自动审批

审批员登录控制台“**流程管理->自动审批设置**”，点击编辑按钮，勾选“**启用自动审批功能**”选项，并点击确定，开启自动审批功能。客户端提交给对应审批员的申请会自动批准。

查看申请明细

当申请是自动审批通过时，控制台“**加密申请管理**”中查看申请明细以及客户端的“**查看加密申请情况->查看申请信息**”中，申请明细显示的审批动作为：批准申请（自动）。

19.21 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。

说明 Mac 客户端、Linux 客户端暂不支持远程文档管理功能。

19.22 智能终端加密管理

选择菜单“**文档安全管理->智能终端加密管理**”，管理员可以查看安装安全查看器的智能终端设备，并可以对这些设备进行管理。

19.22.1 基本操作

查看基本信息

在左侧视图中选中一台智能设备，在右侧选择“**基本**”选项卡，数据显示会显示该智能设备的基本信息。

1） 智能终端基本信息

字段名称	说明
概要信息	
名称	该台智能终端的名称，默认和终端申请授权时填入的使用者一致，在控制台可以进行重命名；
使用者	该智能终端申请授权时输入的使用者名称；
组	该智能终端所在的分组；
最后在线时间	该智能终端最后一次与服务器的通讯时间；
授权状态	该智能终端的授权状态，分为：等待审批，已授权，已拒绝授权，已取消授权，已通用授权，已过期，已删除；
申请信息	对该智能终端申请授权时填入的申请理由；
授权有效时间	对该智能终端授权时设置的授权有效时间；
授权认证间隔	对该智能终端授权时设置的授权认证间隔；
设备信息	

字段名称	说明
App 信息	该智能终端安装的 IP-guard 相关 APP 信息；
智能终端名	该智能终端名称；
状态	该智能终端的当前状态，分为：在线和离线；
离线天数	该智能终端的离线天数；
网络地址	该智能终端的 IP 地址；
操作系统	该智能终端的操作系统；
设备型号	该智能终端的名称；
设备厂商	该智能终端的厂商；

2） 智能终端组基本信息

在智能终端栏中选择一个分组，右侧选择“**基本**”选项卡，数据显示会显示该智能终端分组的基本信息。

如果选择整个网络，会显示所有的智能终端分组，单击数据显示区右上角的【展开】按钮“”，可以查看这些组下所有智能终端的信息列表。

分组操作

在智能终端架构数中，默认只有一个【未分组】。当有智能终端申请授权后，会自动出现【等待审批】和【未授权】分组，该台申请的智能终端将显示在这两个分组下。当管理员对该台智能终端做出审批操作后，该设备将会在【等待审批】分组中移除，如果审批结果为拒绝，则该设备将继续留在【未授权】分组中，如果审批结果为启用授权，则该智能终端设备会在从【未授权】分组移动到【未分组】。

在智能终端结构树中，所有智能设备在首次授权成功后，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，将这些智能终端在逻辑上划分到不同的分组中。

新建分组

在智能终端结构树，选择根结点“**智能终端**”或某个分组，选择菜单“**文件->新建组**”， 则会在智能终端结构树中出现一个新的组节点，为可编辑状态，输入组名称，将相关已授权的智能终端该到该组。管理员可以按照相同的办法建立多级的分组结构。

提示 默认存在一个“**未分组**”组，新出现的授权智能终端都被归类为“**未分类**”组。“**未分类**”组不能删除，不能重命名，也不能在“**未分类**”内新建子组。

指定分组和改变分组

当需要为智能终端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智能终端，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，这样我们所选择的智能终端(组)就会属于我们指定的组了。

查找

通过查找功能，管理员可以快速定位到指定的智能终端，并且查看其相关的信息。

在智能终端结构树中，选择“**文件->查找**”打开查找对话框。输入查询条件，查询条件支持名称（智能终端结构树中显示的名称）、网络地址、操作系统、授权状态、状态，支持模糊查询。查找出来的智能终端在下面的列表中显示，双击其中一台智能终端可直接跳转到该智能终端的数据显示画面。

重命名

为了方便管理，管理员可以将智能终端名称改为便于管理和查看的名称。选择要更改名字的智能终端，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。

删除

对于不再需要接受管理智能终端，可以在控制台上将其删除。选择“**文件->删除**”，可以选中的智能终端删除，如果是智能终端组，则包括该组中所有的子组和智能终端。删除操作会删除该智能终端的授权，安全查看器将无法正常使用，其授权页面会提示“你的授权已被删除，请联系管理员”。

恢复

对于已删除组里的智能终端，可以在控制台上将其恢复。选择“**文件->恢复**”，可以将智能终端恢复到原分组，授权状态也将恢复成删除前的状态。

19.22.2 授权管理

启用授权

使用智能终端上的安全查看器进行申请授权后，该设备将出现在“**等待审批**”分组。选中一台授权状态为“**等待审批**”的智能终端，右键菜单中选择“**授权管理->启用授权**”，指定授权设置并点击【**确定**】按钮后便可授权成功。

授权设置包括以下：

设置项	说明
授权时间设置	智能终端的授权时间设置
认证间隔	勾选此项，并输入指定天数，则启用授权后，该智能终端上安装的安全查看器需要在指定的天数内至少需要连接服务器一次；若指定天数内都没有连接过服务器，则智能终端上已授权的安全查看器则会无法继续使用，提示“授权认证已超期，请联系管 不勾选此项，则启用授权后，该终端一直不连接服务器也可正常使用安全查看器； 默认该项为勾选状态，指定天数默认为 7 天；
授权有效时间	勾选此项，并选择上日期，则该指定日期前智能终端的授权有效，超过指定日期该授权过期，安全查看器无法使用；不勾选此项，则智能终端的授权没有时间限制，将一直生效； 默认该项为不勾选；
分组设置	智能终端授权后分组设置
选择分组	可选择分组，选定并启用授权后，该智能终端设备划分到此处选择的分组。

拒绝

选中一台授权状态为“**等待审批**”的智能终端，右键菜单中选择“**授权管理->拒绝**”，输入拒绝理由并点击【**确定**】按钮后便可拒绝成功。拒绝后，该智能终端的授权状态将变为“**已拒绝**”，拒绝理由将在安全查看器的授权状态页面上显示。

暂停授权

对于授权状态为“**已授权**”的智能终端，管理员可以在右键菜单中选择“**授权管理->暂停授权**”，暂停该智能终端的授权。

智能终端被暂停授权后，安全查看器将无法正常使用，其授权页面会提示“你的授权已被暂停，请联系管理员”。

取消授权

对于授权状态为“**已授权**”,“**已暂停**”,“**已过期**”的智能终端，管理员可以在右键菜单中选择“**授权管理->取消授权**”，取消该智能终端的授权。

智能终端被取消授权后，授权状态将变为“**已取消**”，安全查看器将无法正常使用，其授权页面会提示“你的授权已被取消，请联系管理员”。

修改授权信息

对于授权状态为“**已授权**”,“**已暂停**”,“**已过期**”的智能终端，管理员可以在右键菜单中选择“**授权管理->修改授权信息**”，修改该智能终端的授权信息，可修改的信息和启用授权时可设置的信息一致。

19.22.3 加密设置

加密设置

智能终端的加密设置，主要是对其安全区域的设置，可指定智能终端能打开查看的加密文档的安全区域和级别,不属于权限范围内的安全区域和级别的文档，在该智能设备上无法打开。

例如：智能终端只有市场部机密级别的权限，则在此智能终端上，使用安全查看器可以打开市场部机密级别和机密级别以下的文档，不能打开财务部任何安全级别的文档。

水印设置

管理员通过设置水印类型和水印内容，可以使安全查看器查看文件时带上自定的文字或二维码，有效地保护文档版权。

水印的设置包括：

设置项名称	说明
启用水印策略	勾选此项，则启用安全查看器水印策略；
水印内容	设置水印内容。有文字水印和二维码水印供选择；
文字水印	勾选此项，则水印添加文字内容；需要设置：文字内容，字体大小、字体颜色以及透明度；其中文字内容包括使用者，当前日期，自定义内容；

二维码水印	勾选此项，则水印添加二维码信息；需要设置二维码内容和透明度，其中二维码内容包括当前日期，使用者，自定义内容；
参数设置	设置相关参数；
水印样式	设置水印样式。有 3 种样式可供选择，在左侧可查看预览效果；
文档	设置启用水印的文档，默认为全部文档，可选择仅查看加密文档时启用水印。

19.23 USBKey 管理

加密 USBkey 作为提升用户加密权限的工具，通过在客户端机器上插入加密 USBKey 实现加密各项权限的变更。

选择菜单“**文档安全管理->USBKey 管理**”，管理员可以保存 USBKey 信息，并对这些 USBKey 进行管理。

说明 USBKey功能仅支持在Windows客户端上使用。Mac客户端、Linux 客户端当前暂不支持。

19.23.1 注册

加密 USBKey 必须注册之后才可以正常使用。注册方式有两种：

本地注册

在控制台机器上插入加密 USBKey，选择菜单“**文档安全管理->USBKey 管理**”打开 USBKey 库，选择“**操作->本地 USBKey 信息**”，可以看到该加密 USBKey 信息。选中该加密 USBKey，按图标按钮“”，选择“**注册**”，输入注册信息，完成后按图标按钮“”保存。

远程注册

在远程客户端机器上插入加密 USBKey，通过控制台打开 USBKey 库，选择“**操作->远程 USBKey 信息**”，在“**远程客户端**”选择到插着加密 USBKey 的客户端后，可以看到该客户端上插入的加密 USBKey 信息，选中该加密 USBKey，按图标按钮“”，选择“**注册**”，输入注册信息，完成后按图标按钮“”保存。

注册时需要输入的信息包括以下：

选项	说明
常规	一些常规的记录信息，可选填；
设备 ID	显示设备的 ID 信息，无法修改；
有效期至	默认不勾选，即不限制有效时间； 勾选此项并指定日期，则超过该时间后加密 USBKey 的状态变为“已过期”，无法使用；
USBKey 分类	该加密 USBKey 注册后归到的分类；
备注信息	记录该加密 USBKey 的使用者相关信息； 包括：设备标号，所属部门，设备使用人，职位信息，联系方式，备注信息；
功能权限	该 USBKey 所带有的功能权限，使用该加密 USBKey 的客户端将会在当前状态权限下，叠加加密 USBKey 的权限；
在线加密权限	加密在线权限，使用该加密 USBKey 的客户端若连接不上服务器，则也将拥有对应加密在线权限；
直接解密权限	直接解密文档的权限
直接外发权限	直接外发文档的权限
全部安全区域与级别	安全区域与级别为全部的权限；
使用范围	设置可以使用该加密 USBKey 的计算机和用户。

19.23.2 基本操作

本地 USBKey 信息中各项操作说明：

图标按钮	说明
	刷新本地加密 USBKey 列表；
	保存按钮，将加密 USBKey 信息保存到分类库；
	USBKey 数据及密码相关操；
重置密码	将加密 USBKey 的使用密码重置为初始密码，初始密码在“**操作-> USBKey 密码设置**”中设置； 对于被锁定的加密 USBKey，执行重置密码操作，修改密码为初始密码的同时也会对其解除锁定；

重置数据	为了防止加密 USBKey 被伪造，加密 USBKey 注册之后会有一串随机数。非法的操作可能会导致 USBKey 的随机数和服务器保存的不一致，如果随机数不一致，加密 USBKey 无法正常使用。 重置数据可将恢复加密 USBKey 注册的随机数。
恢复出厂设置	将加密 USBKey 恢复到出厂时的初始设置。恢复出厂的加密 USBKey 可以在其他服务器上注册；
	加密 USBKey 注册相关操作；
注册	注册加密 USBKey；
禁用	加密 USBKey 注册成功后默认为启用状态，执行禁用操作后该加密 USBKey 将无法使用；
启用	对已禁用的 USBkey 执行启用操作，该加密 USBKey 将恢复正常使用
修改注册信息	此操作可修改注册时填写的常规信息，功能权限，使用范围；
删除	删除加密 USBKey 后，USBKey 库中将删去该加密 USBKey 的信息，下次插入该加密 USBKey 将视为未注册。
自动更新识别码	勾选此项，若插入的加密 USBKey 使用旧识别码是会自动更新；不勾选此项，若插入的加密 USBkey 使用的是旧的识别码，则会弹出提示选择是否更新。默认为不勾选。

说明 远程 USBKey 信息中各项操作也类同。

注意 恢复出厂设置仅能在本地 USBKey 信息中操作。

USBKey 的属性说明

加密 USBKey 的属性内容包括：

属性名称	说明
设备 ID	加密 USBKey 的 ID 信息；
注册状态	分别为以下： 未注册：该加密 USBKey 未注册，无法使用； 已授权：该加密 USBKey 已注册，可以使用； 已禁用：该加密 USBKey 已被禁用，无法使用； 已过期：改加密 USBKey 已过期，无法使用；

使用范围	注册时设置的可以使用该加密 USBKey 的计算机和用户；
权限	注册时设置的该加密 USBKey 所带有的功能权限；
过期时间	注册时设置的该加密 USBKey 的过期时间；
首次注册时间	该加密 USBKey 首次注册的时间；
最后修改时间	该加密 USBKey 最后一次修改注册信息的时间；
上次操作时间	该加密 USBKey 上一次操作的时间；
上次操作的计算机	上一次操作该加密 USBKey 的计算机
备注	注册时设置的该加密 USBKey 的备注信息；
设备名称	注册时设置的加密 USBKey 的名称信息；
设备编号	注册时设置的加密 USBKey 的编号信息；
部门	注册时设置的加密 USBKey 所属部门信息；
设备使用人	注册时设置的加密 USBKey 的使用人名称；
职位信息	注册时设置的加密 USBKey 的使用人的职位信息；
联系方式	注册时设置的加密 USBKey 的使用人的联系方式信息；
查看使用情况	右键单击一条加密 USBKey 信息选择“**查看使用情况**”查看该加密 USBKey 的使用情况。

19.23.3 安全性设置

USBKey 密码设置

打开 USBKey 库，选择“**操作-> USBKey 密码设置**”，可以对加密 USBKey 的密码使用进行管理设置。

设置项说明如下：

设置项	说明
初始登录密码	执行重置密码时密码将被重置为初始登录密码，初始为 123456；
首次登录须修改密码	勾选此项，则使用该加密 USBKey 首次登录时，必须要修改密码；

密码错误次数验证	勾选此项并指定最大错误次数，则登录加密 USBKey 时输入错误密码达到最大次数后该加密 USBKey 将被锁定。被锁定的加密 USBKey 将无法使用，需要执行重置密码操作方可解锁。

USBKey 识别码设置

识别码可以看做是加密 USBKey 的使用凭证，加密 USBKey 出厂时带有默认识别码，服务器也会将默认识别码分发给客户端。加密 USBkey 识别码和客户端处的识别码相匹配时，该加密 USBKey 方可在该客户端上使用，否则无法使用。在服务器所在机器上登录控制台，打开 USBKey 库，选择“**操作-> USBKey 识别码设置**”， 可以对加密 USBKey 的识别码使用进行管理设置。

功能按钮说明如下：

按钮文字	说明
修改	修改 USBKey 的识别码，点击进入设置界面后，可以选择是使用默认的识别码，或是自定义识别码，自定义识别码亦可以选择自行输入或者随机生成；
备份	可备份自定义识别码；
导入	导入已备份的识别码。

如果不想使用 USBkey 的默认识别码，可修改为自定义识别码。执行修改操作后，该 USBkey 所使用修改后识别码，同时服务器会将修改后的识别码同步至客户端，保证客户端处始终都持有最新的识别码。

修改了识别码后，其他未修改识别码的 USBkey 在已更新了最新识别码的客户端上将无法使用。可在控制台本地 USBKey 信息或远程 USBKey 信息中更新 USBkey 识别码。

提示 在服务器机器以外的机器登录控制台，不会出现**识别码设置**菜单。

19.23.4 日志查看

在 USBKey 库，选中一个加密 USBKey 信息，右键菜单选择“**查看使用情况**”，可以查看该加密 USBKey 的使用操作日志，包括注册 USBKey、修改 USBKey 注册信息，删除 USBKey 信息，插入 USBKey，拔出 USBKey 等。

在 USBKey 库选择“**操作->USBKey 操作日志**”，可以查看所有加密 USBKey

的操作日志。

19.23.5 离线使用

对于离线的客户端机器，仅能保存离线前的加密 USBKey 授权信息。在其离线后再注册或修改权限的加密 USBKey，无法在该离线客户端上使用。此时，管理员可在 USBKey 库选择“**操作->导出 USBKey 授权文件**”，导出授权文件，把文件发给客户端，在客户端导入。

19.24 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。

修改密码

点击“**修改连接密码**”，可设置备用服务器和主服务器之间的连接密码。具体步骤如下：

控制台菜单“**文档安全管理**”->“**备用服务器管理**”->“**修改连接密码**”；设置了连接密码后，备用服务器才能成功连接到主服务器，通过主服务器验证，获取主服务器的授权。

说明 Windows 客户端、Mac 客户端、Linux 客户端均能在主服务器出现问题时被备用服务器接管。

19.25 自定义密钥

用户可自行选择客户端加密文件时的加密算法，同时可设置自定义密钥，备份密钥信息。

加密算法设置

登陆控制台，“文档安全管理→文档加密算法设置”，进入文档加密算法设置对话框，点击“加密算法”分组框处的“**修改**”。

可以使用默认的文档加密算法，也可以自定义文档加密算法，目前有四种加密算法可供选择：DES、3DES、AES128、AES256 。

加密密钥设置

“文档安全管理→文档加密算法设置”，进入文档加密算法设置对话框，点击“加密密钥”分组框处的“**修改**”。

可以使用默认的文档加密密钥，也可以自定义文档加密密钥。

使用自定义文档加密密钥时，勾选“**生成新的自定义密钥**”的话，可选择随机生成或是手动输入一个新密钥作为自定义密钥；不勾选“**生成新的自定义密钥**”的话，则使用原有自定义密钥中最新的密钥作为当前的自定义密钥。备注信息为必填。

所有的密钥都会保存，加密时使用最新的进行加密，而解密时会使用所有的密钥逐个尝试解密，以保证不同时期加密的文件都能正常解密。

备份自定义加密密钥

文档加密算法算法设置对话框“加密密钥”分组框处，点击“**备份**”，可将密钥信息导出备份到指定位置；点击“**导入**”，可将已备份的密钥信息导入，导入时可以选择用“**本地自定义密钥作为当前自定义密钥**”，或者是用“**导入自定义密钥作为当前自定义密钥**”。

若重新部署服务器，想导入旧服务器中备份的密钥信息作为自定义密钥并且使用该自定义密钥，则可参照以下操作：

1) 导入备份密钥时，在弹出的选择对话框中选择“**导入自定义密钥作为当前自定义密钥**”；

2) 在加密密钥设置中，选择“**使用自定义文档加密密钥**”，随后无需勾选“**生成新的自定义密钥**”，直接点击“**确定**”完成设置即可。

说明 设置的密钥同时对Windows客户端、Mac客户端、Linux客户端生效。

注意 此功能的使用需要两个前提条件：

1. 服务器需注册正式序列号；
2. 需在服务器环境下启动控制台。

19.26 加密文档备份

用户可部署加密文档备份服务器，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。

说明 备份服务器支持Windows客户端、Mac客户端、Linux客户端的文件备份。

19.26.1 文档备份服务器

安装

加密文档备份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。直接双击运行安装程序进行安装，具体操作步骤如下：

1) 双击 IPguardBackup.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；
4) 选择开始菜单的快捷方式的目录，点击【**下一步**】；
5) 确认设置无误，点击【**安装**】，复制文件结束后系统安装完毕，单击【**完成**】按钮完成安装。

查看备份服务器状态

加密文档备份服务器的运行图标，显示当前备份服务器运行时的状态，具体状态有：

图标状态	说明
	文档备份服务器正在启动；
	文档备份服务停止；
	未设置运行参数，包括连接参数、备份设置、空间设置；或未与服务器进行授权验证；
	与服务器连接成功，已获得授权；
	与服务器连接成功，未获得授权；
	与服务器断开连接；或是达到空间报警限制；
	与服务器断开连接，未获得授权
	停止备份；或是通讯错误；

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“**状态**”，可以查看备份服务器更加详细的状态情况。

服务器参数设置

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。

参数	内容
连接参数	
服务器地址	指定所要连接的服务器地址。
本机域名或 IP	备份服务器和客户端在同一网络时，此处可不填； 备份服务器和客户端在不同网络时，此处需填写备份服务器所在局域网的公网 IP，且备份服务器所在局域网需开启 8249 端口映射方可成功备份。
备份库路径	指定备份的加密文档的存储路径。
历史副本	勾选并指定历史副本最多保留的数量，则会备份副本，且仅保留最新的指定数量的副本。

剩余空间管理

自动清理	勾选“**自动清理**”并指定剩余空间大小和历史副本数量，则当剩余空间小于指定大小时，仅保留最新的指定数量的副本。
自动清理指定天数前的备份文档和副本	勾选此项，并设置天数，则满足条件的备份文档和副本将会被删除。
发送警报	备份路径所在盘的剩余空间低于此处设置值则会报警。
停止备份	备份路径所在盘的剩余空间低于此处设置值则停止备份。

说明 发送警报限制和停止备份限制同时存在时，前者设置的值应大于后者。

查看运行日志

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**”->“**运行日志**”，可以查看备份服务器工作状态的相关日志。

备份文档管理工具

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。

19.26.2 文档备份管理

授权

设置完加密文档备份服务器的连接参数之后，需要在连接到相应服务器的控制台上对其进行授权。

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**】。成功之后，文档备份服务器的状态会相应的变为“已授权”。点击【取消授权】，文档备份服务器会变回“未授权”状态。

设置范围

备份文档的机器范围，默认为无。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**】，完成设置。

设置模式

备份文档的模式，默认为明文模式。各模式说明如下：

模式	说明
明文模式	触发备份操作的文档，备份到备份服务器上将以明文形式保存；
密文模式	触发备份操作的文档，备份到备份服务器上将以密文形式保存
原文模式	触发备份操作的文档，备份到备份服务器上将保持其原有属性，即明文备份为明文，密文备份为密文。

选择模式后，点击【**确定**】，完成设置。

设置备份条件

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。

图标按钮	说明
	修改选中计算机的文档备份条件；
	删除选中计算机的文档备份条件。

修改备份条件时，勾选“**启用加密文档自动备份任务**”，则修改加密文档、把非加密文档加密，都会根据下面的备份限制条件对该计算机的加密文件进行备份，各限制条件包括：

选项	说明
包含文件	在此范围中的文件会备份；输入文件名或路径，可使用通配符。如：*.doc、c:*等。
排除文件	在此范围中的文件不会备份；输入文件名或路径，可使用通配符。如：*.doc、c:*等。 排除文件优先于包含文件。
备份范围	在此大小范围内有加密操作的文件会备份。
备份间隔	以此时间范围内，多次修改文件，仅备份一次。
备份流量	上传备份文档时的流量不会超过此数值。
备份时段	在此时段内才向备份服务器上传备份；如：14:00-18:00。
定期扫描备份	是否定期对加密文件进行扫描备份。

选项	说明
扫描日期	指定定期扫描的日期。
扫描时段	指定定期扫描的开始时间和结束时间。 若结束时未扫描完，则下次开始时会接着上次结束时的位置继续扫描； 若未指定结束时间，则开始扫描后直到所有文件扫描结束为止。
允许客户端开启/关闭备份功能	勾选此项，则在对应的客户端处可以自行设置是否备份文件。该项默认为不勾选。

说明 扫描时段内扫描到的需要备份的文档，也会等到进入备份时段后才会备份至备份服务器。

查看文档备份日志

控制台“**文档安全管理**”->“**文档备份操作日志**”，可查看文档备份操作日志。

第二十章. Windows 加密客户端

20.1 客户端运行状态

客户端启用加密功能后，在系统托盘处显示图标。

图标状态	说明
	启动；
	停止；
	离线；
	离线授权；
	备用模式。

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。

20.2 资源管理器

在资源管理器中，安全属性为“公共区域普通级别”的加密文件，右下角图标为不带条纹的小锁图标；其余安全属性的加密文件，右下角图标为带条纹的小锁图标。

在资源管理器中，选择一个加密文件，点击鼠标右键，可弹出加密相关菜单，能执行解密、申请解密、外发、申请外发等功能，在“**属性**”对话框的“**加密**”选项卡中，可以查看修改文档安全属性能功能。

20.3 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。

20.4 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。同时可将此次设置的安全属性设为默认值，下次加密时无需重复修改。

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。

有解密权限的客户端，能加密所有文件；

没有解密权限的客户端，不能加密 windows 目录、program files 目录的文件和一些 PE 文件，如*.exe ,* .ini,* .bat,* .cmd 等，其余文件可以加密。

20.5 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。

20.6 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。

20.7 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。

20.8 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) 添加文件夹时，子文件夹也会一并添加进来，原有的层次结构保持不变。

4) 在任一级目录选择添加文件或文件夹时，会以当前所在目录为父目录。双击文件夹可以进入子级目录查看，点击  … 或者  可以返回上层目录；

5) 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。

6) 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：可设置外发文档是否允许打印、虚拟打印、剪贴板复制、截屏、修改、限制打开次数、最大打开次数、起始有效时间、结束有效时间，是否自动删除、同步标准时间，查看时是否需要密码、添加水印，是否允许过滤指定的文件类型，是否自动隐藏有效期、打开次数限制和修改权限等功能。

   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。

7) 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

 说明

1.是否启用水印以及水印内容设置，由管理员在控制台“**文档安全管理->加密参数设置->窗口浮水印->外发浮水印**”中设置，客户端在外发/申请外发时仅能查阅，无法更改。

2.设置外发配置时，勾选了过滤的文件类型，查看生成的外发文件时对源文件进行另存为操作，保存为过滤的文件类型，则保存下来的文件为明文。另存为非过滤文件类型的文件为密文。

3.当设置了有效时间或最大打开次数时，“**自动删除**”才可设置。设置了“**自动删除**”，则外发文档超过有效时间或达到最大打开次数后，该外发文档会在下一次打开时自动删除。

客户端外发模板管理

客户端把自己常用的外发配置做成模版并管理模版。

直接外发或者申请外发时，在“**外发配置**”标签页中点击按钮，可进入客户端外发模板管理界面。

使用同控制台外发配置模板管理。

说明

1.每个客户端只能使用、管理自己创建的常用外发配置，无法查看到其他客户端创建的；不过，可以导入其他客户端导出的配置。

2.如果客户端选中的"常用外发配置" 跟控制台下发的外发配置策略冲突，以控制台的为准。

20.9 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。

20.10 外发提取

外发提取，即将外发文件中的加密文件提取出来。

有外发提取权限的客户端，在资源管理器中，选择一个外发文件，右键菜单，选择“**文档加密系统**”->“**提取外发文档**”，提取出对应权限的加密文件。

扫描工具中对外发文件直接右键“**提取外发文件**”，亦可提取出外发文件中的加密文件。

20.11　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。

20.12　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。

20.13 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。**

20.14 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。

文字按钮	说明
查看	查看解密申请和离线申请的详细信息。
导入审批	离线时，导入控制台提供的审批文件，以获取审批结果。
离线申请	生成离线申请文件，发给控制台进行审批。
取消申请	取消解密/外发申请。

解密申请

可查看解密申请的时间、状态、文件名、大小、数量、安全区域和级别等信息。

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

可查看外发申请的时间、状态、文件名、大小、数量、安全区域和级别等信息。

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

可查看安全属性变更申请的时间、状态、文件名、大小、数量、安全区域和级别等信息。

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

可查看临时离线申请的时间、状态、文件名、大小、数量、安全区域和级别等信息。

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。

20.15 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。

当前授权进程

透明加密授权下，显示当前打开加密文档的授权软件；显示的进程列表会按照从 A-Z 的顺序对名称进行排序。只读加密授权下，显示当前只读打开加密文档的授权软件，以“!”标识。

当前安全对象

显示当前客户端的加密授权信息，包括常规权限、授权软件、安全区域、加密文档默认安全属性，这些信息与控制台上的加密授权设置一致。

查看加密系统日志

显示系统日志，报告加密文档失败、解密文档失败、以及加密系统事件。

其中加密系统事件如：只读加密授权下以只读方式打开加密文档。

查看离线信息

显示长期离线授权时间、临时离线授权时间和容灾剩余时间。

20.16 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。

20.17 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。

20.18 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。

20.19 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。

20.20 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。

20.20.1 安全密码设置

设置安全密码

安全密码的作用在于：

1. 为防止有别人使用此客户端非法解密文件，客户端应该要设置一个密码对文件解密或者外发进行控制，在每次解密或者外发时需要输入密码。
2. 客户端离线后，使用安全密码登陆离线授权模式后才能正常使用离线加解密权限，增强客户端离线状态下加密文档的安全保护。
3. 客户端在线时注销加密系统后，加密功能停用，使用安全密码重新登入加密系统后方可正常使用加密功能，增强加密系统使用的安全性。

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。

20.20.2 安全密码输入设置

点击“选项”对话框中的“**安全密码输入设置**”，可设定安全密码的输入模式：

选项	说明
每次操作都需输入	每一次解密文件、外发文件时都必须输入安全密码才能成功。
首次操作需要输入	客户端启动，在第一次登入加密系统或第一次解密文件、外发文件时需要输入安全密码，接下来的解密文件、外发文件操作均不需要再输入安全密码。

加密系统登入后无需再输入	客户端启动，在线时登入加密系统或离线时登入离线授权模式后，解密文件、外发文件操作均不需要输入安全密码

20.20.3 加密系统登入设置

在线登入设置

客户端如果有注销加密系统权限，在注销之后加密功能会停用。需要重新登入加密系统方可正常使用加密功能。

可选择客户端启动时，加密系统的登入模式。参数说明:

选项	说明
强制手动登入	客户端每次启动时，都处于加密系统注销状态，需要手动输入正确的安全码，才可登入加密系统。
沿用上一次的状态	客户端上一次在线时为注销加密系统状态，则启动后，仍旧为注销加密系统状态； 客户端上一次在线时为登入加密系统状态，则启动后，仍旧为登入加密系统状态；
自动登入	每次启动后都自动登入加密系统。

离线登入设置

客户端如果有离线加解密权限，则在客户端离线后，需要登入离线授权模式后，才能正常执行离线加解密权限。

可选择登入离线授权模式，参数说明：

选项	说明
强制手动登入	客户端每次启动后，都处于离线授权模式登出状态，需要手动输入正确的安全码，才可登入离线授权模式。
沿用上一次的状态	客户端上一次离线时为离线授权模式登出状态，则启动后，仍旧为离线授权模式登出状态； 客户端上一次离线时为离线授权模式登入状态，则启动后，仍旧为离线授权模式登入状态；
自动登入	客户端每次启动后都自动登入离线授权模式。

20.20.4 数据保存设置

在选项中可设定客户端系统日志的保存时间。默认是 3 天。

20.20.5 解密申请浮动窗口设置

可设置是否显示申请解密浮动窗口，是否记录上次浮动窗口位置，并可调节浮动窗口的透明度。

20.20.6 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。

20.20.7 右键菜单设置

默认情况下，选中一个文档，第一级右键菜单中含有“申请解密”、“申请外发”功能菜单项，其余功能项放在“文档加密系统”下的二级菜单。可以根据使用习惯进行设置，可设置制定的功能项会出现在右键菜单中的一级菜单中。

20.21 加密 USBKey 使用

20.21.1 登入 USBKey 认证

客户端插入加密 USBKey 之后，会自动弹出登入 USBKey 认证窗口。

登录的对话框中包含以下内容：

字段	说明
设备	要登入的加密 USBKey 设备；

密码	初始密码为 123456，登入 USBKey 认证后可以修改密码，右键客户端加密图标“**USBKey 管理->修改登入密码**”中修改密码
记住密码	勾选此项，则登入 USBKey 认证时会记住此次的密码。 登入 USBKey 认证后，可以右键客户端加密图标，选择“**USBKey 管理->清除记住的密码**”，确认删除记住的密码，则下次登入 USBKEy 认证模式时将需要输入密码；
自动登录	勾选此项，则下次选择登入 USBKey 认证时，使用上一次密码自动登录。 若选择“**USBKey 管理->清除记住的密码**”，确认删除记住的密码，下次登入 USBKEy 认证时不会自动登录。

登入 USBKey 认证后，客户端的权限变为自身权限叠加加密 USBKey 所带权限。

右键客户端加密图标，选择“**USBKey 管理->登出 USBKey 认证**”，登出 USBKey 认证后，客户端将不再拥有加密 USBKey 所带权限。

20.21.2 查看 USBKey 信息

右键客户端加密图标，选择“**USBKey 管理->查看 USBKey 信息**”，可以查看插在客户端上的加密 USBKey 信息，包括设备 ID、状态、首次注册时间、有效期、权限、最后修改时间。

20.21.3 导入 USBKey 授权文件

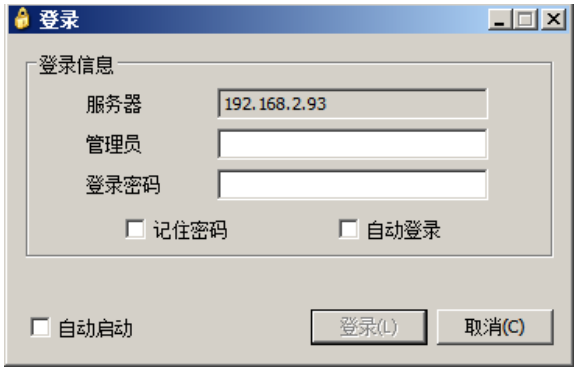
在系统托盘的客户端图标处，选择右键菜单“**导入 USBKey 授权文件**”，选择一个由控制台生成的 USBKey 授权文件导入，即可更新本地 USBKey 库信息。

20.22 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。

20.22.1 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“**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**”。

若同时勾选“**自动启动**”和“**自动登录**”，并输入正确的管理员帐户和密码后，则下次客户端启动并且连上服务器后，代理控制台能在后台自动登录启动，但不会弹出代理控制台主界面，用户可以在客户端托盘图标菜单中调出。

20.22.2 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。

20.22.3 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**”。

20.23 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。

第二十一章. Linux 加密客户端

Linux 客户端暂时仅支持加密的部分功能。

21.1 加密文档扫描工具

在 Linux 客户端下，当前不支持右键菜单操作，无法像 Windows 客户端那样右键执行加解密操作。加密、解密、申请解密、申请临时离线均需要在加密文扫描工具中操作。

在有界面的 Linux 系统下，客户端托盘图标选择右键菜单“**扫描本地文件**”，可启动扫描工具。

说明　在某些 Linux 版本下，如 Ubuntu12.04 以上版本，托盘处无法显示客户端图标。当发现托盘处无客户端图标时，在终端中执行以下命令后可启动扫描工具：/usr/local/bin/LSDHelper。

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。

在无界面的 Linux 系统，可以运行 LSDHelper_CUI 来使用扫描工具。

扫描的指令	说明
-p	源文件路径，不可省略
-o	目标存储路径，省略时默认为源文件路径（省略是指指令“-x”和参数“xxx”一起省去）
-t	要扫描的文件类型，省略时为全部类型文件
-e	只搜索加密文件，省略时为搜索加密和非加密文件
-s	不搜索子文件夹，省略时默认为搜索子文件夹
-l	列出所描到的文件，省略时默认不列出
-E	按扫描条件加密，省略时为只扫描
-D	按扫描条件解密，省略时为只扫描（客户端需拥有解密

说明 1.指令中的所有字符均为英文形式，区分大小写，指令“-x”和参数“xxx”之间用单空格隔开。用户可以根据需要选取指令进行组合。

2.程序启动一次只执行一条指令。

Linux 命令扫描示例 1

要扫描某个目录下（如/root/Desktop/test）的所有文件，可在终端输中入命令：

LSDHelper_CUI -p /root/Desktop/test

按 Enter 后结果返回扫描到的文件总数。

Linux 命令扫描示例 2

要扫描某个目录下（如 root/Desktop/test）某个类型（如 txt）的文件，并且显示详细的文件信息，可在终端中输入命令：

LSDHelper_CUI -p /root/Desktop/test -t txt -l

按 Enter 后结果返回 txt 文件的详细信息，包括文件名、目录、状态、大小、修改时间。

21.2 加密

在扫描工具的扫描结果中，选择一个或多个非加密文件，右键菜单选择“**加密**”，可以把此文件加密，加密后的文件默认为公共安全区域普通级别且在 Linux 下无法修改安全属性。

如果是无界面的 Linux 系统，可通过命令进行加密。

Linux 命令加密示例

要加密某个目录下（如 root/Desktop/test）某个类型（如 txt）的文件，可在终端输中输入命令：

LSDHelper_CUI -p /root/Desktop/test -t txt -E

21.3 解密

在扫描工具的扫描结果中，选择一个或多个加密文件，右键菜单选择“**解密**”，可以把此文件解密。

如果是无界面的 Linux 系统，可通过命令进行解密。

Linux 命令解密示例

要解密某个目录下（如 root/Desktop/test）的所有文件，可在终端输中输入命令：

LSDHelper_CUI -p /root/Desktop/test -D

21.4 申请解密

没有解密权限的客户端，可在扫描结果中，选择一个或多个加密文件，右键菜单选择“**申请解密**”，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**”中选择“**完成申请**”进行解密。

如果是无界面的 Linux 系统，无法进行申请解密操作。

说明　　Linux 加密客户端目前不支持离线申请解密。

21.5 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**”，或是在打开扫描工具后，点击 按钮，在菜单中选择“**查看申请情况**”，可查看解密的申请和审批情况。

文字按钮	说明
完成申请	在申请批准以后执行完成申请，解密申请批准后完成申请即为将文件解密。
查看	查看解密申请的详细信息。
取消申请	取消解密申请。

解密申请

可查看解密申请的时间、状态、文件名、大小、数量、安全区域和级别等信息。

选中一条申请记录，点击【**查看**】可查看申请的详细信息。并可执行解密取消申请等操作。

已批准的加密申请，可点击【**完成申请**】按钮进行解密，可选择解密到源文件目录，也可以到其他目录。

第二十二章. Mac 加密客户端

Mac 客户端暂时仅支持加密的部分功能。

22.1 加密文档扫描工具

在 Mac 客户端下，当前不支持右键菜单操作，无法像 Windows 客户端那样右键执行加解密操作。加密、解密、申请解密、申请临时离线均需要在加密文扫描工具中操作。

在 Mac 系统下，客户端托盘图标选择右键菜单“**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。

22.2 加密

在扫描工具的扫描结果中，选择一个或多个非加密文件，右键菜单选择“**加密**”，可以把此文件加密，加密后的文件默认为公共安全区域普通级别且在 Mac 下无法修改安全属性。

22.3 解密

在扫描工具的扫描结果中，选择一个或多个加密文件，右键菜单选择“**解密**”，可以把此文件解密。

22.4 申请解密

没有解密权限的客户端，可在扫描结果中，选择一个或多个加密文件，右键菜单选择“**申请解密**”，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**”中选择“**完成申请**”进行解密。

说明　　Mac 加密客户端目前不支持离线申请解密。

22.5 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**”，或是在打开扫描工具后，点击按钮，在菜单中选择“**查看申请情况**”，可查看解密的申请和审批情况。

文字按钮	说明
完成申请	在申请批准以后执行完成申请，解密申请批准后完成申请即为将文件解密。
查看	查看解密申请的详细信息。
取消申请	取消解密申请。

解密申请

可查看解密申请的时间、状态、文件名、大小、数量、安全区域和级别等信息。

选中一跳申请记录，点击【**查看**】可查看申请的详细信息。并可执行解密取消申请等操作。

已批准的加密申请，可点击【**完成申请**】按钮进行解密，可选择解密到源文件目录，也可以到其他目录。

第二十三章. U 盘加密客户端

将 U 盘制作成 U 盘加密客户端，在任意计算机上插入 U 盘加密客户端时则可正常使用加密功能，无需另外安装客户端，实现加密功能的方便快捷使用。

23.1 启动和退出

启动

在计算机上插入 U 盘加密客户端，打开 U 盘，运行其中的 USDAgent.exe。对于首次使用该 U 盘客户端的计算机，程序需要初始化，等待初始化完成后，重启计算机。

首次使用的 U 盘客户端，在重启后需先运行 U 盘中的 USDConf.exe，点击**【在线更新策略】**按钮，此时会弹出对话框输入服务器 IP，输入并确定后会自动向服务器获取策略并导入。策略导入成功后，运行 U 盘中的 USDAgent.exe，弹出 U 盘加密客户端登录对话框。

登录的对话框中包含以下内容：

字段	说明
可移动盘	当前 U 盘客户端的盘符信息；
设备名称	设备名称，即在授权改 U 盘加密客户端时设置的名称；
密码	初始密码为 123456，登录后可以修改密码，在加密托盘图标右键菜单“**高级->修改密码**”中修改密码；
记住密码	勾选此项，则登录 U 盘加密客户端时会记住此次登录用户的密码。 登录后，可以在加密托盘图标右键菜单“**高级->清除记住的密码**”，点击**【确定】**按钮立即清除，下次 U 盘加密客户端时将需要输入密码；
自动登录	勾选此项，则下次启动 U 盘加密客户端时，使用上一次的密码自动登录。 若执行过“**清除记住的密码**”操作则下次登录时不会自动登录；

重置密码	忘记登录密码时，点击“**重置密码**”，将界面中的原始操作码发给管理员。 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，生成操作码后发给用户，用户输入操作码后，点击【**确定**】按钮重置密码。 执行重置密码后，登录密码即被重置为初始值，即为123456。

说明　首次使用的 U 盘客户端，需要先导入一次策略后才能启动，对于非首次使用的 U 盘客户端则无需此步骤。

登录成功后，系统托盘会出现加密客户端图标，加密等相关功能的使用同加密客户端。

退出

在系统托盘的客户端图标上，选择右键菜单“**安全退出**”，即可退出 U 盘加密客户端。

23.2 更新策略

自动更新

U 盘加密客户端启动运行且能与服务器通讯，会自动同步服务器设置的策略。

在线更新策略

运行 U 盘中的 USDConf.exe，点击【**在线更新策略**】按钮，策略更新工具将服务器当前最新的策略更新到 U 盘中。

说明　在线更新策略功能可在未启动 U 盘解密客户端时操作。

离线更新策略

当 U 盘加密客户端离线时，更新策略的具体步骤如下：

1) 管理员登录控制台，在计算机树上选中该 U 盘加密客户端，右键菜单中选择“**策略导出**”，也可以在“**工具->客户端管理->U 盘加密客户端管理**”中选中该 U 盘加密客户端，右键菜单中选择“**导出策略文件**”，导出策略文件，文件格式为 ipz；

2) 用户拿到策略文件，运行 U 盘中的 USDConf.exe，点击【**导入策略**】按钮，选择策略文件导入；

3) 导入后需要退出 U 盘加密客户端并再重新登录即可。

第二十四章. 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。

24.1 安装

运行安装程序，选择安装目录，直到程序安装完毕。

24.2 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。

授权外发 USBKey

具体步骤：

1) “**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，选择“**USBKey 管理**”；

3) 点击【加载】，导入授权文件，并填写公司信息。

4) 在授权列表中可看到此外发 USBKey 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。

24.3 时间同步

同步时间功能能够防止用户通过修改系统时间，延长使用有时间限制的外发文档，从而更好的控制外发文档的使用权限。

同步时间有两种方式

方式	说明
直接连接到互联网	当计算机可以连接互联网时，选择此方式，点击【更新】按钮，便可直接连到互联网以同步正确的互联网时间
使用时间同步工具	当计算机无法连接互联网时，选择此方式。在一台能连接互联网的机器上运行时间同步工具，把外发查看器中的操作码输入到时间同步工具中，生成确认码，再在外发查看器的中输入确认码，点击【更新】，即可同步时间。

24.4 USBKey 管理

外发 USBKey 管理功能可对外发 USBKey 进行相关管理。在机器上插入外发 USBKey，会自动获取外发 USBKey 的 ID、识别码信息以及授权列表信息。

密码设置

外发 USBKey 默认密码为空，可以修改密码。

功能按钮	说明
修改密码	修改外发 USBKey 的登入密码，需要输入旧密码以及修改后的密码；

清除记住的密码	在登入外发 USBKey 时如果勾选了“**记住密码**”，则下次选择登入外发 USBKey 认证时，使用上一次密码自动登录； 清除记住的密码操作，可删除记住的密码，下次登入 USBKEy 认证时不会自动登录。

24.5 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。

查看多级目录的外发文件时，双击文件夹可以进入子级目录查看，点击 … 或者 可以返回上层目录。

针对一些三维设计类软件，如 UG、Proe，不同厂商的产品，生成文件格式的标准不一，打开不同厂商的文件时，经常需要先将文件导入软件以转换成相同格式方可查看。若拿到不同厂商文件格式的文件制成的外发文件时，查看外发文件可按以下步骤操作：

1）打开外发文档，点击**【打开程序】**；

2）选择打开文件的程序，选择后选择**【确定】**按钮；

3）等待所选程序启动后，在该程序中“**文件-打开**”，在外发文档所在目录中找到释放的文件，选中打开即可。

对于使用 USBKey 的机器，要先插入对应外发对象授权的 USBKey，启动外发查看器后，登入外发 USBKey，方可查看外发文件。

说明	当外发USBKey的密码为空时，启动外发查看器时会自动登入外发 USBKey。

第二十五章. 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。

一个主服务器可以有部署多个备用服务器，一个备用服务器在运行时只能连接一个主服务器。

25.1 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。

25.2 查看备用服务器状态

备用服务器的运行图标，显示当前备用服务器运行时的状态，具体状态有：

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；
	与服务器断开连接并进入备用模式；
	授权错误，备用服务器无法与主服务器连接；

选择备用服务器的右键菜单“**状态**”，可查看到当前备用服务器是否已与主服务器建立连接，是否获得备份授权，以及备用服务器获取主服务器上所有客户端信息的更新时间。

25.3 登录密码设置

在备用服务器的运行图标上点击右键，在右键菜单“**工具**”->“**设置登录密码**”，可以设定在使用备用服务器时，是否需要使用密码。

设置登录密码后，在使用备用服务器右键菜单“**工具**”中的各个子菜单时，需要输入密码才能成功操作。

登录密码可以在备用服务器的右键菜单“**工具**”->“**设置登录密码**”中进行修改。

25.4 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。

25.4.1 服务器连接设置

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。

25.4.2 主动轮询

主动轮询功能，可应用在两个方面：

1) 加密系统进入备用模式状态，网络正常，但客户端显示为离线状态，无法进入备用模式，在线策略不生效时，可开启备用服务器的主动轮询功能，

让备用服务器自动连接客户端；

2) 主服务器未部署备用服务器便出现异常，可在安装备用服务器后，开启备用服务器的主动轮询功能，让备用服务器自动连接客户端。

开启主动轮询功能的具体操作：

在备用服务器系统托盘图标上点击右键“**工具**”->“**设置连接参数**”，点击“**主动轮询**”标签页，勾选“**启动主动轮询**”。

默认情况下，主动轮询会自动检测所有网段中的客户端。如果设定了检测范围，则只检测设定 IP 范围内的客户端。

25.5 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。

25.6 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。

25.7 创建备用模式授权文件

备用服务器进入备用模式后，若客户端由于网络问题或其他未知因素无法正常连接到备用服务器，则可以在备用服务器中生成备用模式授权文件，导入到客户端中，强制客户端进入备用模式。

备用模式授权文件只能在备用服务器进入备用模式时生成。步骤如下：

1) 备用服务器系统图标上单击右键“工具”->“高级”->“创建备用模式授权文件”，进入“生成离线备用模式授权文件”对话框；

2) 设定文件密码。设定文件密码后，客户端在导入紧急授权文件时，需要输入密码才能成功导入。该步骤可以忽略，但为了避免不合法的客户端导入紧急授权文件，执行在线加解密策略，建议设定文件密码；

3) 设定有效期限。设定有效期限后，客户端导入的紧急授权文件，只在文件有效期内生效，过期后，需重新生成备用模式授权文件，重新导入。

25.8 超级授权

若您的备用服务器未部署完成，主服务器便出现问题无法正常运行，请使用备用服务器的超级授权功能，向我们发出申请。

超级授权与备用服务器是一对一的关系，一台备用服务器上发出的超级授权申请，审批后，只能用于备用服务器自身，不能用于另外的备用服务器。

如果此时您需要部署多台备用备用服务器，请在各个备用服务器上各自生成申请文件，发送给我们。

25.8.1 申请超级授权

具体操作步骤如下：

1) 安装备用服务器并运行；

2) 在备用服务器的系统图标上点击右键“**工具**”->“**高级**”->“**超级授权**”，进入超级授权申请对话框；

3) 在对话框中输入主服务器的序列号，点击【**创建申请文件**】，然后将生成

的申请文件，通过邮件发送给我们；

25.8.2 设置超级授权

我们会根据您的申请文件，为您生成一份超级授权文件并发送给您，您可以使用这份超级授权文件，在备用服务器的系统图标上点击右键->工具->高级->设置超级授权，在超级授权设置对话框中，定位到超级授权文件，点击**【设置超级授权】**按钮，导入超级授权文件。

您可以在导入超级授权文件的同时，输入主服务器上的检验码；也可以在成功导入超级授权文件之后，再输入检验码。

超级授权文件导入成功后，备用服务器进入备用模式。

25.8.3 设置检验码

为保证主服务器上的客户端能成功连接上备用服务器，请在备用服务器的系统图标上点击右键“**工具**”->“**高级**”->“**设置检验码**”，在弹出的检验码设置对话框中，填入主服务器的检验码。

通过超级授权文件，进入备用模式的备用服务器，不需要设置主服务器的连接参数，但是必须开启主动轮询功能。

第二十六章. 申请文档存储

客户端提交解密、外发和安全属性变更申请的申请文档支持上传到申请文档存储服务器，客户端离线时，审批人审批预览可以读取申请文档存储服务器或客户端上的文件。

26.1 安装与部署

26.1.1 安装

1）右键以管理员权限运行安装包程序 OapprBackup.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，有默认安装路径，用户也可以自定义安装路径，路径设置好后，点击【**下一步**】继续；

4）设置 HTTPS 页面中导入证书文件 server.crt 和 KEY 文件 server.key，并设置 HTTPS 的端口，默认端口为 443，点击【**下一步**】继续；

5）选择组件界面，默认为标准安装，会默认安装 MySQL 数据库，点击【下一步】继续；

6）选择开始菜单的安装目录，设置完毕后点击【**下一步**】继续；

7）确认设置无误后，点击【**安装**】，开始安装；

8）等待安装过程，安装完成后，会弹出提示，点击【**完成**】即可。

26.1.2 初始化

安装申请文档存储服务器完成后，使用内置账号 admin，密码为空，通过浏览器登录申请文档存储服务器管理端，

服务器地址填写例子：

1、IP+ http 默认端口：http://192.168.2.112:9001

2、IP+ https 默认端口：https://192.168.2.112:443

https://192.168.2.112

3、IP+ 非默认端口：http://192.168.2.112:8086

https://192.168.2.112:8089

登录成功后，在“**存储设置**”页面点击 按钮，输入已存在的数据存储路径名，如 D:\backup，仅支持一个盘符路径，如设置多个仅识别第一个。

说明 1. http 默认端口为 9001，https 默认端口为 443。

2.数据存储路径必须设置，申请文档上传功能才能正常开启。

26.1.3 启用申请文档上传

初始化申请文档存储服务器后，需要在控制台上启用申请文档上传设置。控制台“**计算机->加密->加密参数设置->申请文档上传设置**”，勾选启用设置，输入申请文档存储服务器地址，开启申请文档上传至指定的申请文档存储服务器中。

26.2 WEB 管理端

26.2.1 登录

在登录页面输入账户和密码登录申请文档存储服务器管理端，内置账户为 admin，密码为空。

登录成功，可点击页面导航右上角的“admin”，选择“**修改密码**”对账号密码进行修改。

26.2.2 首页

登录成功后，会默认显示首页。首页中显示上传文档概述，包括当天上传数量、当天上传大小、历史上传总数量和历史上传总大小。

26.2.3 存储设置

存储设置页面，可以对数据存储路径和磁盘空间管理进行各项参数的设置。点击 按钮进行编辑，完成后可点击“**保存**”按钮保存，或点击“**取消**”按钮撤销修改。

参数设置说明：

设置项	说明
数据存储路径	备份文档的存储路径，输入已存在的路径名，如D:\backup，仅支持一个盘符路径，如设置多个仅识别第一个。
自动清理	当磁盘空间少于设置值时自动清理备份文档，单位 MB，会在 1 分钟内执行清理操作，默认不设置。
自动清理指定天数前的文档	设置天数，系统会自动清理最后备份时间为设置天数前的备份文档，在每天 00:00 时刻检测清理，设置天数必须为大于 0 的整数，默认不设置。
发送警报	磁盘空间少于设置值时报警，登录申请文档存储系统会弹出空间不足，单位 MB；
停止上传	磁盘空间少于设置值时停止上传，单位 MB，默认设置值为 1024MB。

说明

1.数据存储路径必须设置，申请文档上传功能才能正常开启。

2.为了保证申请文档存储服务器可以正常工作，请确保每项参数设置正确。

第二十七章. 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。支持部署多个文档云备份服务器,每台客户端机器的备份文档仅可上传至一台备份服务器。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。

27.1 安装与部署

安装文档云备份服务器后，执行相关的初始化操作，并设置相关策略后，功能方能正常使用。

27.1.1 安装

文档云备份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。直接双击运行安装程序进行安装，具体操作步骤如下：

1) 双击 FileCloudBackupServer.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;
4) 设置文档云备份服务器的端口，默认为 80，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【**安装**】,
7) 若当前环境没有安装 Mysql 数据库，安装程序会自动安装上 Mysql
   若当前环境已经安装 Mysql 数据库，则会弹出 Mysql 确认界面，需要输入 Mysql 的用户和密码，点击点击【**下一步**】;
8) 等待安装过程，最后单击【**完成**】按钮完成安装。

安装完毕后，在系统托盘处显示文档云备份服务器图标。

说明 使用安装程序安装的 Mysql，用户名为 root，密码为 mysql。

查看文档云备份服务器状态

文档云备份服务器的运行图标，显示当前服务器运行时的状态，具体状态有：

图标状态	说明
	文档云备份服务器正在启动；
	文档云备份服务器停止；
	未进行文档云备份服务器初始化；
	与服务器连接成功，已获得授权；
	与服务器连接成功，未获得授权；
	与服务器断开连接；
	与服务器断开连接，未获得授权
	停止备份；或是通讯错误；

选择文档云备份服务器托盘图标的右键菜单“**状态**”，可查看到当前文档云备份服务器的启动运行状态，是否已与主服务器建立连接，是否获得备份授权等信息。

查看文档云备份服务器运行日志

选择文档云备份服务器托盘图标的右键菜单“**工具->运行日志**”，可以查看云备份服务器工作状态的相关日志。

修改文档云备份服务器端口

选择文档云备份服务器托盘图标的右键菜单“**工具->选项**”中修改，修改完后需要重启文档备份服务器，具体操作为托盘处右键菜单“**文档份服务器-停止**”，停止服务器，随后选择“**文档份服务器-启动**”。

27.1.2 初始化云备份服务器

安装部署完文档云备份服务器后，首次登陆需进行初始化设置，在浏览器中输入服务器地址，此时弹出初始化界面进行初始化。

服务器地址填写的例子：

1、IP+默认端口 80：192.168.2.203

2、IP+非默认端口 8080：192.168.2.203:8080

3、域名+映射端口：tec.oicp.net:10941

4、前面加 http： http://192.168.2.203

首次登录的初始化界面需要输入以下信息：

参数	内容
IP-guard 服务器地址	连接的 IP-guard 服务器地址，如：192.168.2.236；
账户	拥有“文档云备份服务器->设置配置权限”的管理员账号；
密码	管理员的密码。

首次登录成功后需要重启文档云备份服务器。

27.1.3 云备份服务器参数设置

登录云备份服务器 WEB 管理界面，“**设置**”->“**参数设置**”中设置好各项参数，为了保证云备份服务器可以正常工作，请确保每项参数都有设置且设置正确。

27.1.4 授权云备份服务器

初始化文档云备份服务器后，需要在连接到相应服务器的 IP-guard 控制台上对其进行授权。

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**】。成功之后，文档备份服务器的状态会相应的变为“已授权”。点击【**取消授权**】，文档备份服务器会变回“未授权”状态。

27.1.5 设置备份范围

备份文档的机器范围，默认为无。控制台“**工具**”->“**服务器管理**”->“**文档备份服务器管理**”，选中文档云备份服务器，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**】，完成设置。

则选定的计算机的文档将会备份到此文档云备份服务器。

27.1.6 设置关联用户

文档云备份服务器仅会备份存在关联用户的计算机文档。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。对于没有自动关联用户的客户端机器，管理员可在控制台“**工具**”->“**服务器管理**”->“**用户系统管理**”->“**关联信息**”中，手动进行关联。

27.1.7 设置备份策略

计算机默认不启用文档备份。登录控制台“**高级**”->“**文档云备份**”，可以设置策略启用或停止计算机的文档备份，并设置备份的条件。

图标按钮	说明
	修改选中计算机的文档云备份策略；
	删除选中计算机的文档云备份策略。

修改备份条件时，勾选“**启动文档云备份任务**”，则修改、新增文档都会根据下面的备份限制条件将该计算机的文件备份到文档云备份服务器，各限制条件包括：

选项	说明
包含文件	在此范围中的文件会备份；输入文件名或路径，可使用通配符。如：*.doc、c:*等。
排除文件	在此范围中的文件不会备份；输入文件名或路径，可使用通配符。如：*.doc、c:*等。 排除文件优先于包含文件。
备份范围	在此大小范围内有新增、修改操作的文件会备份。
备份间隔	以此时间范围内，多次新增或修改文件，仅备份一次。
备份流量	上传备份文档时的流量不会超过此数值。
备份时段	在此时段内才向文档云备份服务器上传备份；如：14:00-18:00。
定期扫描备份	是否定期对文件进行扫描备份。

选项	说明
扫描日期	指定定期扫描的日期。
扫描时段	指定定期扫描的开始时间和结束时间。 若结束时未扫描完，则下次开始时会接着上次结束时的位置继续扫描； 若未指定结束时间，则开始扫描后直到所有文件扫描结束为止。

说明

1. 修改文档包括：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。
2. 扫描时段内扫描到的需要备份的文档，也会等到进入备份时段后才会备份至备份服务器。

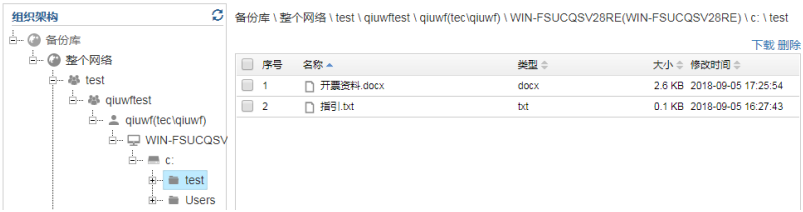
27.2 WEB 管理端

27.2.1 首页

通过浏览器登录文档云备份服务器后，进入 WEB 管理端界面首页。首页主要展示文档备份服务器的授权状态、备份概述、磁盘空间。

27.2.2 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。



右侧视图中的备份文件按其在客户端上实际的存储路径展示，选择指定的目录，右边显示该目录下的备份文件。点击文件名称，可以查看文件详细信息，如果该文件有副本，点击；勾选单个或多个文件，点击“**下载**”可将选中文件下载至本地，点击“**删除**”可将选中文件从文档云备份服务器上删除。

27.2.3 文件查找

左侧为查询栏，右侧视图显示查询结果。默认显示的查询条件为文件名称，点击“**高级查询**”右边的>，会显示更多查询条件。查询条件包括：

字段名称	说明
文件名称	文件的名称；
用户	文件的操作用户，单次查询仅能选择一个用户；
计算机	此查询项须选定用户后方可选择，指定该用户下的计算机；
修改时间	文件的修改时间，可以设置时间段；
文件大小	文件的大小，可以设置大小区间。

查询结果视图中对文件的操作，同备份浏览视图中对文件的操作。

27.2.4 设置

角色管理

角色管理用于分角色管理和设置域用户的权限。此界面分为上下视图，上方视图为角色列表，下方视图为查看/设置设置项界面。

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。

各设置项说明如下：

设置项	说明
角色名称	设置角色的名称；
备注	设置该角色的备注信息；
已分配对象	设置该角色的分配对象，点击设置框后方的…按钮选择用户，可通过模糊查找功能快速定位到目标对象；

用户权限	设置角色的文档权限；
查看文档	是否可以查看备份文档的权限，默认为允许； **允许**：该角色的分配用户可以打开备份文档进行查看； **禁止**：该角色的分配用户无法查看文档； **不设置**：该角色的分配用户此权限受其继承的父组角色权限影响，若继承的权限为“允许”则为“允许”，所继承的权限为“禁止”则为禁止，若无继承权限，“不设置”相当于“禁止”；
下载文档	是否可以下载备份文档的权限，默认为不设置； **允许**：该角色的分配用户可以下载备份文件； **禁止**：该角色的分配用户无法下载备份文件； **不设置**：该角色的分配用户此权限受其继承的父组角色权限影响，若继承的权限为“允许”则为“允许”，所继承的权限为“禁止”则为禁止，若无继承权限，“不设置”相当于“禁止”；
删除文档	是否可以删除备份文档的权限，默认为不设置； **允许**：该角色的分配用户可以删除备份文件； **禁止**：该角色的分配用户无法删除备份文件； **不设置**：该角色的分配用户此权限受其继承的父组角色权限影响，若继承的权限为“允许”则为“允许”，所继承的权限为“禁止”则为禁止，若无继承权限，“不设置”相当于“禁止”；
管理范围	设置该角色的管理范围，属于该角色的用户，仅能管理此范围内的备份文档。默认为空，当管理范围为空时，属于该角色的用户，其管理范围为其本身； 点击设置框后方的…按钮选择管理范围，可通过模糊查找功能快速定位到目标对象。

在上方视图的角色列表选中一个角色，下方视图的设置项将显示该角色的设置值且为不可编辑状态。选中一个角色，最右边点击，设置项将变成可编辑状态，可对角色的各项设置进行修改，修改后需保存。点击，则可删除该角色。

角色权限优先级

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。

例如以下场景：

1.测试部分组下有用户 A，该用户 A 同时属于角色甲和角色乙；

2.角色甲的用户权限为：查看文档（允许）、下载文档（禁止）、删除文档（禁止），管理范围为：空（即只能查看自己的备份文档）；

3.角色乙的用户权限为：查看文档（允许）、下载文档（禁止）、删除文档（允许），管理范围为：测试部分组。

用户 A 登录文档云备份服务器，可以看到所有测试部分组下的用户的备份文档。用户 A 对自己的备份文档，可以查看，无法下载，无法删除；对其他测试部分组用户的备份文档，可以查看，无法下载，可以删除。用户权限管理

用户的文档云备份服务器权限管理。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权限，包括所属角色，管理范围，查看/下载/删除备份文档的权限。可通过模糊查询快速定位到目标用户。

所属角色一列中，若角色的字体为黑色，代表该角色在创建时，分配对象选择的是该用户/用户组的父组，此角色是继承而来的（以下称继承角色）；若角色的字体为蓝色，代表该角色在创建时，分配对象直接选择了该用户/用户组（以下称直接角色）。在右侧视图中选中一条记录，鼠标移至所属角色一列会出现 按钮，点击后可增加或移除角色，继承角色无法移除。当用户属于多个角色时，选中该用户，右侧视图中默认仅看到所属角色信息，管理范围和其他文档权限均为空，点击用户名称前的【+】展开查看具体每个角色的权限。

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，默认情况下所有管理员都不受控制，可以选择设置黑名单或者白名单。

点击进行设置，勾选对应的设置项，并输入管理员名称，多个管理员名称之间使用“ ;”或“;”或“,”或 “,”隔开，完后点击保存。

设置项	说明
以下管理员禁止登录	此范围内的管理员都无法登录文档云备份服务器；
以下管理员允许登录	仅有此范围内容的管理员可以正常登录文档云备份服务器，其他管理员不能登录云备份服务器。。

说明　管理员黑名单中可以设置 admin，当设置为 admin 时，admin 登录仅有设置管理员黑白名单设置的权限，没有其他权限。

27.2.5 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，或者点击“**取消**”撤销修改。

参数说明如下：

参数	内容
授权设置	IP-guard 服务器授权设置；
IP-gurd 服务器地址	此处为云备份服务器初始化时输入的 IP-guard 服务器地址； 若初始化后 IP-guard 服务器地址有变，可在此处修改，对于新输入的地址，建议先测试是否可连接成功，测试连接时需输入具有“**文档云备份服务器->设置配置权限**”的 IP-guard 管理员账号和密码；
域账号密码验证设置	云备份服务器支持计算机关联的域用户登录查看自己的备份文件信息，需要设置对应域服务器的相关信息； 设置完后建议先测试是否可连接成功，测试连接时需输入具有等于域服务器权限的域用户账号和密码；
域服务器地址	域服务器的 IP 地址；
域名	域服务器名称；
是否为 AD 域	当前支持 AD 域服务器和 LDAP 服务器，如果是 AD 域服务器则选择“**是**”，如果是 LDAP 服务器选择“**否**”；
组织架构同步设置	云备份服务器定期会向 IP-guard 服务器同步用户组织架构，可进行同步设置；
同步间隔	定期同步间隔默认为 1 天，可修改，也可点击“**立即同步**”按钮即时同步；
最后同步时间	显示云备份服务器最后一次与 IP-guard 服务器同步的时间；
备份存储设置	设置备份文档的存储参数；
数据存储路径	备份文档的存储路径，在编辑的状态下点击，输入已存在的路径名，如 D:\backup，支持设置多个盘符路径，带有标识的为当前存储路径，当前存储路径无法继续存储时，如满足空间不足停止备份条件时，则会转到下一个存储路径存储。

历史副本数量	勾选“**历史副本数量最多保留**”并设置具体个数，则备份文档的历史副本超过指定个数后，最早的副本将会被删除，保持副本数为指定个数；
磁盘空间清理	磁盘空间清理设置项，包括以下： 1.可设置当磁盘空间少于指定值时，保留指定数量的历史副本，默认该设置不启用； 2.可设置自动清理按最后备份时间为指定天数前的备份文档和副本，设置后在每天 00:00 时刻检测清理，设置天数必须为大于 0 的整数，默认该设置不启用； 3.可设置当存储路径剩余空间少于指定值时发送警报，默认该设置不启用； 4.可设置当存储路径剩余空间少于指定值时停止备份，若设置了多个盘符路径，则每个盘符磁盘空间少于设置值时会停止备份，自动跳转到下一个盘符，直到全部磁盘都占用完；该设置默认为 4GB；
端口映射设置	
域名	不在同一网络中的设备（包括 IP-guard 服务器和客户端）访问云备份服务器需要通过域名方可成功通讯，保持功能正常。请在此输入不同网络的设备可成功访问云备份服务器的域名。

说明 1.存储路径仅支持云备份服务器本地路径

2.为了保证云备份服务器可以正常工作，请确保每项参数都有设置且设置正确。

27.2.6 系统日志

在顶部导航栏中点击“**系统日志**”，进入系统日志查询页面。系统日志记录了自动清理文档的操作日志，用户可以查询到相应时间段内系统执行自动清理文档操作的记录。默认显示一个月内的清理日志。

查询条件参数说明：

查询条件项	说明
起始时间	查询清理日志时间段内的起始日期；
终止时间	查询清理日志时间段内的终止日期；

操作类型	清理日志的操作类型，目前只有自动清理磁盘的操作类型；
描述	日志中的描述内容，包括清理文档个数，释放空间大小，可支持模糊查询；

输入查询条件后，点击“**查找**”按钮查询，查询结果列表属性包括有操作日志类型、时间和详细信息。列表每页最多显示 25 行内容，超过 25 行内容会形成下一页，可点击“**上一页**”、“**下一页**”按钮进行翻页。

说明 系统执行了一次自动清理的操作，都会记录一条清理的日志。

27.3 WEB 审计端

WEB 审计端主要是对管理员操作文档云备份服务器的一种日志记录，方便查询管理员在文档云备份服务器上做过什么操作。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。

27.3.1 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。

审计日志记录的内容包括：

字段名称	说明
操作日志	操作日志的类型；
时间	操作的具体时间
登录计算机	登录文档云备份服务器所在的计算机名称；
登录用户	登录文档云备份服务器的用户名称；
详细信息	管理员对控制台的操作描述信息。

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。

字段名称	说明
时间范围	设置一个时间范围，查询一个时间段内的审计日志；

操作类型	管理员的操作日志类型；
文件名称	管理员操作的文件名称。

27.3.2 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，默认情况下所有审计管理员都不受控制，可以选择设置黑名单或者白名单。

点击进行设置，勾选对应的设置项，并输入审计管理员名称，多个审计管理员名称之间使用“;”或“;”或“,”或 “,”隔开，完后点击保存。

设置项	说明
以下审计员禁止登录	此范围内的管理员都无法登录文档云备份服务器；
以下审计员允许登录	仅有此范围内容的管理员可以正常登录文档云备份服务器，其他管理员不能登录云备份服务器。。

说明 管理员黑名单中可以设置 audit，当设置为 audit 时，audit 登录仅有设置管理员黑白名单设置的权限，没有其他权限。

27.4 文档云备份扫描工具

管理员在控制台上可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，并将指定的文件备份至文档云备份服务器。一台客户端可以设置多个扫描任务，任务按照创建顺序依次执行。

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。

说明 Mac 客户端、Linux 客户端暂不支持文档云备份扫描任务功能。

27.4.1 扫描任务设置

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。

常规设置说明：

设置选项	说明
任务名称	当前任务的任务名。系统会自动填上默认值，可以修改；
选择对象	可进行目标计算机选择；
扫描路径	默认填写的是“本地磁盘（_local）”，即代表全盘；若不想扫描全盘，只想扫描指定的路径，可以编辑此处，多个路径用“;”隔开，如输入 C:\;D:\ ，则代表仅扫描 C 盘和 D 盘；
包含文件	此范围内的文件，会被扫描备份； 可以在给定的预定义文件类型中选择；也可点击 按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等；
排除文件	此范围内的文件，不会被扫描备份； 可以在给定的预定义文件类型中选择；也可点击 按钮进行手动输入，支持通配符。如：*.doc、c:*、D:\test*.txt 等。

说明 包含文件、排除文件之间的优先级为“排除范围>包含范围”。

高级设置说明：

设置项	说明
性能设置	任务进行时的性能设置。
扫描速度任务优先	扫描速度会快，对系统性能会有一定影响；建议在执行任务时间为非工作时间时，选择此项。
系统性能优先	扫描速度会放慢，对计算机的资源消耗不会太高，保证系统性能；执行任务时间为工作时间时，建议选择此项。

仅在空闲时扫描	客户端空闲时才会扫描并对指定文件加密，其余时间不扫描不加密； 客户端空闲指：控制台上显示该客户端的状态为“正在运行（空闲）”。
扫描时段	设置任务开始扫描加密的时间。在下拉菜单中选择符合要求的时间分类； 此处下拉菜单中选择分类的即为时间类型管理中的各分类。
备份流量	上传备份文档时的流量不会超过此数值。
文件大小	此大小范围内的文件才会被扫描备份。

说明

1. 包含文件为空，或者选定计算机对象为空时，扫描备份任务不可创建。
2. 全盘扫描备份任务创建成功后，则无法修改任务设置。请在创建任务时务必确认好每项设置。

27.4.2 查看任务信息/任务日志

全盘扫描备份任务创建后，分解为多个任务会下发到每台计算机。一台客户端可能会被设置多个扫描备份任务，则任务按照创建顺序依次执行。

查看任务信息

在文档云备份扫描任务界面的上半视图中，可以查看分解后的任务的基本信息。

内容项	说明
任务名称	全盘扫描备份任务的名称。
计算机	客户端的计算机名称。
计算机组	客户端所在分组的名称。
用户	客户端机器最后登录的用户名称。
用户组	客户端机器最后登录的用户所在分组名称。
关联用户	客户端机器的关联用户名称。
计算机状态	客户端机器的运行状态。
开始时间	客户端执行此全盘任务的开始时间。
结束时间	客户端执行此全盘任务的结束时间。

内容项	说明
任务状态	客户端当前执行的全盘扫描备份任务状态； 1. 当任务创建后，如果当前客户端没有前序任务，则状态为“正在启动”，当任务初始化相关的工作完成后，状态会变为“已启动”； 2. 若当前客户端有前序任务正在执行，则后续任务的状态会一直维持为“正在启动”，直到自己变为当前任务后则会变为“已启动”； 3. 任务执行过程中，若执行了禁用任务操作，则状态为“暂停”；启用了该条暂停的任务后，状态会重新变为“已启动”； 4. 在任务启动和暂停的过程中，对应会有“正在启动”/“即将暂停”的状态 5. 当扫描任务执行完成后，状态为“完成”
文件数量	客户端当条扫描任务中扫描的文件总个数；
文件大小	客户端当条扫描任务中扫描的文件总大小；
进度	客户端执行此扫描备份任务的完成进度，会根据当前进度自动更新。

选中一条任务，在文档云备份扫描界面下半视图的“**任务信息**”选项卡中，可以查看该台客户端此任务的详细信息，明细包括创建该任务时对应的各项设置内容。

查看任务日志

在文档云备份扫描界面，选中一条任务，在下半视图的“**任务日志**”选项卡中，可以查看该客户端执行任务的日志。通过工具栏上的刷新按钮进行刷新。

内容项	说明
时间	该条任务日志产生的时间。
任务名称	当前执行的任务名称。
内容	包括：当前任务的状态进程，任务执行结果等。

27.4.3 其他任务操作

禁用/开启任务

计算机的扫描任务创建后默认为启用，在文档云备份扫描任务界面，选中一条或多条任务，点击禁用按钮，或是右键菜单中选择“**禁用扫描任务**”，则目标任务会暂停。

选中一条或多条被禁用的任务，点击启用按钮，或是右键菜单中选择“**开启扫描惹怒**”，则目标任务会启动。

删除任务

选中一条或多条任务，点击删除按钮，或是右键菜单中选择“**删除扫描任务**”，则目标任务会被删除。

查询任务

点击查询按钮，弹出查询对象选择对话框，选择指定的计算机或者计算机组，点击【**确定**】按钮，则任务列表中仅会出现符合查询条件的任务，可进行针对性查看。

27.5 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，日志包括的内容有：

属性名称	说明
类型	上传日志类型，包括开始扫描、扫描结束、开始上传文件、上传文件成功、上传文件失败、中止上传；
时间	该条日志产生的时间；
计算机	客户端计算机的名称
计算机组	客户端计算机所在的计算机分组
用户	客户端计算机产生此条日志时登录的用户名称；
用户组	客户端计算机产生此条日志时登录的用户所在的用户组；
关联用户	客户端计算机的关联用户名称；

文件	上传备份的文件名称；
备份服务器	文件备份到的文档云备份服务器信息，包括计算机名和IP；
备份大小	上传备份的文件大小；
描述	当上传备份失败时，会显示错误原因和错误代码。

第二十八章. 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。

28.1 术语介绍

周期报表

根据指定的周期，自动定期生成符合指定条件的报表。

查询

选择报表类型，输入查询条件，实时统计并生成报表。

统计表和趋势表

每种模块的报表都提供统计表和趋势表。统计表展示满足各项查询条件的统计结果，趋势表展示选定时间区间内各项数值的走势。

为了方便使用，系统已经分别针对周期报表和查询报表，预定义了各类型的统计表以及趋势表，并按报表类型分组。

28.2 报表控制台

28.2.1 登录报表控制台

登录控制台，选择菜单“**工具->登录报表系统**”，启动报表控制台。

报表控制台界面包括：

界面区域	说明
菜单栏	包含了本系统的所有菜单，是各功能窗口的入口；
工具栏	包含了一些常用的功能；

导航栏	位于窗口的左边，显示所有的周期报表、查询报表和分组信息； 为了方便使用，系统已经预设了所有报表类型的统计表以及趋势表，并按报表类型分组；
数据显示区	是本系统的核心视图，所有的数据都在数据显示区查看； 数据显示区分为三部分；
查询栏	查询栏，提供查询条件；
图表栏	位于查询栏下方，显示查询结果统计图的区域；
数据栏	位于图表栏下方，显示具体的查询结果数据。

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。

28.2.2 数据显示区

数据显示区包含很多通用内容。

结果视图

所有的报表和查询结果，默认在数据显示区平分显示统计图和列表数据，上方为统计图，下方为列表数据。在数据显示区右键菜单中选择“**结果视图->最大化统计图**”，则仅显示统计图，选择“**结果视图->最大化列表**”，则仅显示列表数据。

统计图

统计图的右上方，可以选择显示的数据条数和切换显示图样。数据条数默认为全部，可选择仅显示前 5，前 10，前 20，以及自定义显示数值。统计报表默认显示图样为柱状图，趋势报表默认为折线图，在数据显示区右键菜单中选择“**统计图**”亦可切换显示图样。

数据显示区右键菜单中选择“**统计图设置**”，可以设置显示图例项，以及水平轴标签显示数量。

列表

统计图下方会以列表形式显示具体的数据，列表中可以选择需要显示的列。右

键点击列头，可选择增加或减少显示的数据列。

明细信息

在每个报表的统计结果列表中，双击一条数据或是选中一条数据，右键菜单中选择“**明细**”，可查看具体的明细信息。综合数据报表包含了多种类型数据，选中一条数据，双击不同的单元格，查看的是该单元格对应数据的明细信息。

在明细信息列表中，双击一条明细信息，可查看具体的日志记录内容。

28.2.3 辅助功能

导入导出

生成的报表和查询结果，以及对应的明细表，均可以导出保存为电子文档。

报表和查询结果

在周期报表或查询结果的数据显示区单击右键“**导出->导出统计报表**”，可选择导出当前的统计信息，包括图表。右键“**导出->导出明细表**”，可导出当前所有统计信息的明细数据。

明细结果

双击一条数据进入明细信息界面，右键“**导出->导出本页记录**”只会导出当前页的日志，默认是 20 条记录，和控制台每页的显示条数一致，管理员可以在控制台“**工具->选项->控制台设置->日志查看**”中修改每页显示的最大记录数。右键“**导出->导出所有记录**”会导出所有记录。

导出的文档可以保存为 4 种格式：文本文件(.CSV)、HTML 文件、MHT 文件、EXCEL 文件。

打印、打印预览

生成的报表和查询结果，均可打印出来存档，在数据显示区单击右键“**打印**”，用户可以将当前统计结果打印输出，右键“**打印预览**”，可以做打印预览。

28.3 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； 除了预设了移动存储操作报表外，还按统计条件预设了三个存储相关的报表： 1.标准移动存储操作分组统计表：按计算机组统计 U 盘使用情况 2.标准移动存储插入次数分组统计表：按计算机组统计 U 盘插入次数 3.标准移动存储插入次数统计表：按计算机统计 U 盘插入次数 以上三个报表均都能通过同一个报表修改统计条件得到，
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；
资产报表	软、硬件资产数据统计；
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； 外传文档统计表，外发文件行为的综合数据统计，外发行为包括邮件、U 盘、上传、打印。

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。

28.4 报表通用设置

创建周期报表和创建查询时，需要进行条件设置和统计设置。

设置	说明
条件设置	包含计算机范围、用户范围，和高级条件设置，不同类型的报表对应的高级条件不同；
统计设置	包含统计类型选择和具体统计设置。

28.4.1 条件设置

条件设置包括计算机范围、用户范围和高级条件设置。其中，不同类型的报表对应的高级条件不同。

高级条件中有一个通用的条件，即时间类型，用于设置统计的时间范围，选择时间分类，下拉列表中显示的为控制台“**分类管理->时间类型**”中的所有分类。

下面说明各类型报表的其他高级条件。

打印报表

高级条件	说明
打印机类型	有本地、共享、网络和虚拟打印机四种类型。默认选择本地、共享、网络三种打印机；
打印机（包含）	包含在统计范围内的打印机名称。可以指定网内某台计算机上的打印机，如：“\\server*”表示\\server上的所有打印机；“SomePrinter”为名称为SomePrinter 的打印机；
打印机（不包含）	不包含在统计范围内的打印机名称；
打印任务（包含）	包含在统计范围内的打印任务名称，支持通配符；
打印任务（不包含）	不包含在统计范围内的打印任务名称，支持通配符；
应用程序（包含）	包含在统计范围内的打印程序名称，支持通配符，也支持选择应用程序分类；
应用程序（不包含）	不包含在统计范围内的打印程序名称，支持通配符，也支持选择应用程序分类；
页数大于	输入一个正整数，大于该值的打印记录被统计；

页数小于	输入一个正整数，小于该值的打印记录被统计。

即时通讯报表

高级条件	说明
聊天工具	包含在统计范围内的聊天工具；
聊天类型	包含在统计范围内的聊天类型，可选择单聊和多聊；
聊天内容（包含）	包含在统计范围内的聊天内容，支持通配符；
聊天内容（不包含）	不包含在统计范围内的聊天内容，支持通配符；
用户 ID 或昵称（包含）	包含在统计范围内的用户 ID 或昵称，支持通配符；
用户 ID 或昵称(不包含）	不包含在统计范围内的用户 ID 或昵称，支持通配符；

上网浏览报表

高级条件	说明
网站（包含）	包含在统计范围内的网站名称，支持通配符；
网站（不包含）	不包含在统计范围内的网站名称，支持通配符。

文档操作报表

高级条件	说明
源文件路径（包含）	包含在统计范围内的源文件路径，支持通配符；
源文件路径(不包含）	不包含在统计范围内的源文件路径，支持通配符；
源文件名（包含）	包含在统计范围内的源文件名称，支持通配符；
源文件名（不包含）	不包含在统计范围内的源文件名称，支持通配符；
源盘符类型	包含在统计范围内的源盘符选择，可选硬盘、软盘、光盘、可移动盘和网络盘；
文件大小大于（>=KB）	输入一个正整数，大于该值的文件大小被统计；
文件大小小于（>=KB）	输入一个正整数，小于该值的文件大小被统计；
目标文件路径(包含）	包含在统计范围内的目标文件路径，支持通配符；
目标文件路径（不包含）	不包含在统计范围内的目标文件路径，支持通配符；
目标文件名（包含）	包含在统计范围内的目标文件名称，支持通配符；

目标文件名（不包含）	不包含在统计范围内的目标文件名称，支持通配符；
目标盘符类型	目标盘符选择，可选硬盘、软盘、光盘、可移动盘和网络盘。
操作类型	可选复制、移动、删除、访问、修改、上传和下载；
应用程序（包含）	包含在统计范围内的应用程序名称，支持通配符，也支持选择应用程序分类；
应用程序（不包含）	不包含在统计范围内的应用程序名称，支持通配符，也支持选择应用程序分类。

移动存储报表

高级条件	说明
加密盘类型	可选全部、非加密盘、加密盘和专用盘；
移动存储	包含在统计范围内的移动存储，可选择移动存储库的一个或多个移动存储或移动存储分类；
移动存储（不包含）	不包含在统计范围内的移动存储，可选择移动存储库的一个或多个移动存储或移动存储分类；
移动存储操作类型	包含在统计范围内的移动存储操作，分别有：插入、复制到、移动到、复制出、移动出、删除、访问、修改、上传、下载；
源文件路径（包含）	包含在统计范围内的源文件路径，支持通配符；
源文件路径（不包含）	不包含在统计范围内的源文件路径，支持通配符；
源文件名（包含）	包含在统计范围内的源文件名称，支持通配符；
源文件名（不包含）	不包含在统计范围内的源文件名称，支持通配符；
文件大小大于（>=KB）	输入一个正整数，大于该值的文件大小被统计；
文件大小小于（>=KB）	输入一个正整数，小于该值的文件大小被统计；
目标文件路径（包含）	包含在统计范围内的目标文件路径，支持通配符；
目标文件路径（不包含）	不包含在统计范围内的目标文件路径，支持通配符；
目标文件名（包含）	包含在统计范围内的目标文件名称，支持通配符；
目标文件名（不包含）	不包含在统计范围内的目标文件名称，支持通配符；
应用程序（包含）	包含在统计范围内的应用程序名称，支持通配符，也支持选择应用程序分类；
应用程序（不包含）	不包含在统计范围内的应用程序名称，支持通配符，也支持选择应用程序分类。

应用程序报表

高级条件	说明
应用程序（包含）	包含在统计范围内的应用程序名称，支持通配符，也支持选择应用程序分类；
应用程序（不包含）	不包含在统计范围内的应用程序名称，支持通配符，也支持选择应用程序分类。

邮件报表

高级条件	说明
邮件方向	包含在统计范围内的邮件方向，可选择接收或发送；
带附件	可选择带附件或不带附件；
发件人（包含）	包含在统计范围内的发件人的邮箱地址，支持通配符；
发件人（不包含）	不包含在统计范围内的发件人的邮箱地址，支持通配符；
收件人（包含）	包含在统计范围内的收件人的邮箱地址，支持通配符，收件人也包括抄送人和密送人的邮件地址；
收件人（不包含）	不包含在统计范围内的收件人的邮箱地址，支持通配符，收件人也包括抄送人和密送人的邮件地址；
主题（包含）	包含在统计范围内的邮件主题，支持通配符；
主题（不包含）	不包含在统计范围内的收件人的邮箱地址，支持通配符，收件人也包括抄送人和密送人的邮件地址；
邮件大小大于（>=KB）	输入一个正整数，大于该值的邮件大小被统计；
邮件大小小于（>=KB）	输入一个正整数，小于该值的邮件大小被统计；
邮件附件名称(包含)	包含在统计范围内的邮件附件名称，支持通配符；
邮件附件名称（不包含）	不包含在统计范围内的邮件附件名称，支持通配符；

加密文档操作报表

高级条件	说明
操作类型	包含在统计范围内的操作类型，分别有：加密文件、解密文件、生成外发文档、修改文档安全属性、申请解密文件、申请生成外发文档、申请修改文档安全属性。

文件名称	包含在统计范围内的文件名称，支持通配符；
应用程序	包含在统计范围内的应用程序名称，支持通配符；
文件大小大于（>=KB）	输入一个正整数，大于该值的文件大小被统计；
文件大小小于（>=KB）	输入一个正整数，小于该值的文件大小被统计；

策略日志报表

高级条件	说明
策略日志类型	可选统计的策略,包括基本策略、应用程序控制策略、网页浏览控制策略、设备控制策略、打印控制策略、屏幕控制策略、日志记录策略、远程控制策略、流量控制策略、网络控制策略、邮件控制策略、即时通讯文件传送策略、即时通讯文件传送策略、上传控制策略、文档控制策略、系统报警策略、移动存储授权策略；
报警级别	包含在统计范围内的报名级别，可选一般、重要、严重
报警内容（包含）	包含在统计范围内的报警内容，支持通配符；
报警内容（不包含）	不包含在统计范围内的报警内容，支持通配符。

征兆报表

高级条件	说明
征兆条件	包含在统计范围内的征兆条件。

综合报表

包括以上除征兆报表外其他所有类型报表的高级条件设置。

外传文档报表

包括打印报表、邮件报表、移动存储报表、文档操作报表的高级条件设置。

28.4.2 统计设置

统计设置包含统计类型选择和具体统计设置。其中，个别设置项因报表类型不同而不同。

通用设置项

设置项	说明
统计类型选择	
按计算机统计	含有两种方式： 按计算机统计，以每个计算机为对象统计一组结果； 按计算机组统计，以每个计算机组作为对象统计一组结果，该结果是包含该组内所有计算机统计结果的总和；
按用户统计	含有两种方式： 按用户统计，以每个用户为对象统计一组结果； 按用户组统计，以每个用户组作为对象统计一组结果，该结果是包含该组内所有用户统计结果的总和；
具体统计设置	
计算机组统计级别	选择数据统计到到计算机分组的第几级别；
用户组统计级别	选择数据统计到到计算机分组的第几级别；

打印报表统计类型

设置项	说明
统计类型选择	
按打印机统计	以每台打印机为对象统计一组结果；
按计算机+打印机统计	以计算机（组）和打印机为对象统计，一个计算机（组）对应一台打印机有一组数据；
按用户+打印机统计	以用户（组）和打印机为对象统计，一个用户（组）对应一台打印机有一组数据；
具体统计设置	
打印机设置	选择统计的打印机；

说明 按计算机+打印机统计，按用户+打印机统计时，打印机数据中的打印次数和打印页数需要在统计视图右上方切换查看。

即时通讯报表

设置项	说明
统计类型选择	
按聊天工具统计	以每个聊天工具为对象统计一组结果；

按计算机+聊天工具统计	以计算机（组）和聊天工具为对象统计，一个计算机（组）对应一个聊天工具有一组数据；
按用户+聊天工具统计	以用户（组）和聊天工具为对象统计，一个用户（组）对应一个聊天工具有一组数据；
具体统计设置	
聊天工具设置	选择统计的聊天工具；

 说明　　按计算机+聊天工具统计，按用户+聊天工具统计时，聊天工具数据中的语句数和字符数需要在统计视图右上方切换查看。

上网浏览报表

设置项	说明
统计类型选择	
按网站统计	含有两种方式： 1.按网站统计，以每个网站为对象统计一组结果； 2.按网站分类统计，以每个网站分类作为对象统计一组结果，该结果是包含该分类内所有网站的总和；
按计算机+网站统计	含有四种方式： 1.按计算机+网站统计； 2.按计算机+网站分类统计； 3.按计算机组+网站统计； 4.按计算机组+网站分类统计； 以计算机（或计算机组）和网站（或网站分类）为对象统计，一个计算机（或计算机组）对应一个网站（或网站分类）有一组数据；
按用户+网站统计	含有四种方式： 1.按用户+网站统计； 2.按用户+网站分类统计； 3.按用户组+网站统计； 4.按用户组+网站分类统计； 以用户（或用户组）和网站（或网站分类）为对象统计，一个用户（或用户组）对应一个网站（或网站分类）有一组数据；
具体统计设置	
网站分类级别设置	选择数据统计到网站分类的第几级别；

网站设置	选择统计的网站，支持通配符输入。

文档操作报表

文档操作报表统计类型仅含有通用的统计类型设置。

设置项	说明
统计类型选择	
按文档统计	以每个文档的操作为对象统计一组结果。统计的操作包括：创建、复制、移动、重命名、恢复、删除、访问、修改、上传、下载、刻录。

说明 按文档统计，涉及的查询范围和数据量很大，查询过程会有一定耗时，请使用时尽量设置更为精准查询条件。

移动存储报表

设置项	说明
统计类型选择	
按移动存储统计	含有两种方式： 1.按移动存储统计，以每个移动存储为对象统计一组结果； 2.按移动存储分类统计，以移动存储分类作为对象统计一组结果，该结果是包含该分类内所有移动存储统计结果的总和；
按计算机+移动存储统计	含有四种方式： 1.按计算机+移动存储统计； 2.按计算机+移动存储分类统计； 3.按计算机组+移动存储统计； 4.按计算机组+移动存储分类统计； 以计算机（或计算机组）和移动存储（或移动存储分类）为对象统计，一个计算机（或计算机组）对应一个移动存储（或移动存储分类）有一组数据；

按用户+移动存储统计	含有四种方式： 1.按用户+移动存储统计； 2.按用户+移动存储分类统计； 3.按用户组+移动存储统计； 4.按用户组+移动存储分类统计； 以用户（或用户组）和移动存储（或移动存储分类）为对象统计，一个用户（或用户组）对应一个移动存储（或移动存储分类）有一组数据；
具体统计设置	
移动存储分类级别设置	选择数据统计到移动存储分类的第几级别。

 说明　　按计算机+移动存储统计，按用户+移动存储统计时，移动存储数据中的插入次数写入，读取、删除、访问、修改文件等数据需要在统计视图右上方切换查看。

应用程序报表

设置项	说明
统计类型选择	
按应用程序统计	含有两种方式： 1.按应用程序统计，以每个应用程序为对象统计一组结果； 2.按应用程序分类统计，以应用程序分类作为对象统计一组结果，该结果是包含该分类内所有应用程序统计结果的总和；
按计算机+应用程序统计	含有四种方式： 1.按计算机+应用程序统计； 2.按计算机+应用程序分类统计； 3.按计算机组+应用程序统计； 4.按计算机组+应用程序分类统计； 以计算机（或计算机组）和应用程序（或应用程序分类）为对象统计，一个计算机（或计算机组）对应一个应用程序（或应用程序分类）有一组数据；

按用户+应用程序统计	含有四种方式： 1.按用户+应用程序统计； 2.按用户+应用程序分类统计； 3.按用户组+应用程序统计， 4.按用户组+应用程序分类统计 以用户（或用户组）和应用程序（或应用程序分类）为对象统计，一个用户（或用户组）对应一个应用程序（或应用程序分类）有一组数据；
具体统计设置	
应用程序分类级别设置	选择数据统计到应用程序分类的第几级别；
应用程序设置	选择统计的应用程序，支持通配符。

邮件报表

邮件报表统计类型仅含有通用的统计类型设置。

加密文档操作报表

加密文档操作报表统计类型仅含有通用的统计类型设置。

硬件资产报表

设置项	说明
统计类型选择	
按 CPU 型号统计	含有一种方式： 1.按计算机组+CPU 型号统计； 以计算机组和 CPU 型号为对象统计，一个计算机组对应一个 CPU 型号有一组数据；
按内存型号统计	含有一种方式： 1.按计算机组+内存型号统计； 以计算机组和内存型号为对象统计，一个计算机组对应一个内存型号有一组数据；
按硬盘驱动器型号统计	含有一种方式： 1.按计算机组+硬盘驱动器型号统计； 以计算机组和硬盘驱动器型号为对象统计，一个计算机组对应一个硬盘驱动器型号有一组数据；

按主板型号统计	含有一种方式： 1.按计算机组+主板型号统计； 以计算机组和主板型号为对象统计，一个计算机组对应一个主板型号有一组数据；
按显示卡型号统计	含有一种方式： 1.按计算机组+显示卡型号统计； 以计算机组和显示卡型号为对象统计，一个计算机组对应一个显示卡型号有一组数据；
按计算机型号统计	含有一种方式： 1.按计算机组+计算机型号统计； 以计算机组和计算机型号为对象统计，一个计算机组对应一个计算机型号有一组数据；
按计算机制造商统计	含有一种方式： 1.按计算机组+计算机制造商型号统计； 以计算机组和计算机制造商型号为对象统计，一个计算机组对应一个计算机制造商型号有一组数据；
具体统计设置	
计算机组统计级别设置	选择数据统计到计算机组分类的第几级别。

软件资产报表

设置项	说明
统计类型选择	
按Windows系统软件统计	含有一种方式： 1.按计算机组+系统软件统计； 以计算机组和系统软件为对象统计，一个计算机组对应一个系统软件有一组数据；
按杀毒软件统计	含有一种方式： 1.按计算机组+杀毒软件统计； 以计算机组和杀毒软件为对象统计，一个计算机组对应一个杀毒软件有一组数据；
按操作系统统计	含有一种方式： 1.按计算机组+操作系统统计； 以计算机组和操作系统为对象统计，一个计算机组对应一个操作系统有一组数据；

按应用软件统计	含有一种方式： 1.按计算机组+应用软件统计； 以计算机组和应用软件为对象统计，一个计算机组对应一个应用软件有一组数据；
具体统计设置	
计算机组统计级别设置	选择数据统计到计算机组分类的第几级别。

硬件资产变更报表

设置项	说明
统计类型选择	
按计算机+资产类别统计	含有两种方式： 1.按计算机+资产类型统计； 2.按计算机组+资产类型统计； 以计算机（或计算机组）和资产类型为对象统计，一个计算机（或计算机组）对应一个资产类型有一组数据；
具体统计设置	
计算机组统计级别设置	选择数据统计到计算机组分类的第几级别。

征兆报表

设置项	说明
统计类型选择	
按计算机+征兆级别统计	含有两种方式： 1.按计算机+征兆级别统计； 2.按计算机组+征兆级别统计； 以计算机（或计算机组）和征兆级别为对象统计，一个计算机（或计算机组）对应一个征兆级别有一组数据；
按用户+征兆级别统计	含有两种方式： 1.按用户+征兆级别统计； 2.按用户组+征兆级别统计； 以用户（或用户组）和征兆级别为对象统计，一个用户（或用户组）对应一个征兆级别有一组数据；
按征兆类型+征兆级别统计	以征兆类型和征兆级别为对象统计，一个征兆类型对应一个征兆级别有一组数据；

按计算机+征兆类型统计	含有两种方式： 1.按计算机+征兆类型统计； 2.按计算机组+征兆类型统计； 以计算机（或计算机组）和征兆类型为对象统计，一个计算机（或计算机组）对应一个征兆类型有一组数据；
按用户+征兆类型统计	含有两种方式： 1.按用户+征兆类型统计； 2.按用户组+征兆类型； 以用户（或用户组）和征兆类型为对象统计，一个用户（或用户组）对应一个征兆类型有一组数据；
具体统计设置	
征兆条件设置	选择统计的征兆条件。

综合数据报表

综合报表统计类型仅含有通用的统计类型。

外传文档报表

外传文档报表统计类型仅含有通用的统计类型。

28.5 报表统计内容

各报表支持的统计内容如下：

打印报表

打印报表能统计的内容包括：打印次数、打印页数。

邮件报表

邮件报表能统计的内容包括：发送邮件数量、发送邮件大小、接收邮件数量、接收邮件大小、邮件数量、邮件大小。

移动存储报表

移动存储操作报表、标准移动存储操作分组统计表、标准移动存储插入次数分

组统计表、标准移动存储插入次数统计表能统计的内容包括：插入次数、写入移动盘文件数量、写入移动盘文件大小、读取移动盘文件数量、读取移动盘文件大小、删除文件数量、删除文件大小、修改文件数量、修改文件大小、访问文件数量、访问文件大小。

文档操作报表

文档操作报表能统计的内容包括：上传文件数量、上传文件大小、下载文件数量、下载文件大小、删除文件数量、删除文件大小、复制文件数量、复制文件大小、移动文件数量、移动文件大小、修改文件数量、修改文件大小、访问文件数量、访问文件大小。

应用程序报表

应用程序报表能统计的内容包括：开机时间、活动时间、活动时间百分比、应用程序时间、应用程序时间百分比。

上网浏览报表

上网浏览报表能统计的内容包括：上网浏览时间、上网浏览时间百分比。

策略日志报表

策略日志报表能统计的内容包括：报警次数。

即时通讯报表

即时通讯报表能统计的内容包括：聊天语句数、聊天字符数、聊天会话数。

加密文档操作报表

加密文档操作报表能统计的内容包括：加密文件数量、加密文件大小、解密文件数量、解密文件大小、生成外发文件数量、生成外发文件大小、修改文档安全属性数量、修改文档安全属性大小、申请解密文件数量、申请解密文件大小、申请生成外发文件数量、申请生成外发文件大小、申请修改文档安全属性数量、申请修改文档安全属性大小。

资产报表

硬件资产报表能统计的内容：CPU 型号、内存型号、硬盘驱动器型号、主板性号、显示卡型号、计算机型号、计算机制造商，默认为 CPU 型号。

软件资产报表能统计的内容：Windows 系统软件、杀毒软件、操作系统、应用软件，默认为应用软件。

硬件资产变更报表能统计的内容：主板、显示卡、CPU、内存和硬盘驱动器，默认全部显示。征兆报表

征兆报表能统计的内容：征兆次数。

综合报表

综合报表能统计的内容包括：打印页数、发送邮件大小、写入移动盘文件大小、上传文件大小、应用程序时间、上网浏览时间、报警次数。

外传文档报表

外传文档报表能统计的内容包括：外传文件数量、外传文件大小、发送附件数量、发送附件大小、写入移动盘文件数量、写入移动盘文件大小、上传文件数量、上传文件大小、打印次数、打印页数。

28.6 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。

28.7 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。

周期的设置内容说明如下：

设置	说明
报表数据时间范围	数据的起始时间范围，包含开始日期和结束日期；
报表生成时间	生成周期报表的时间，设置之后将在该时间生成数据时间范围内的统计数据；

报表生成前进行预统计	勾选此项，并设置开始统计时间和统计时间间隔，则会从开始统计时间开始计算，达到统计时间间隔时长后便会成预先生成这段时间内的统计数据。

报表生成前进行预统计示例说明

创建了一个周期为月的打印统计表，选定的月周期设置如下：

开始时间为本月 1 日，结束时间为本月 31 日，报表生成时间为本月 31 日 23:59。

以 10 月份的数据为例，不勾选“报表生成前预统计” 时，该报表将会在 10 月 31 日 23:59 生成 10 月份的打印统计表数据，在此之前该打印统计表数据显示区中的报表日期选择中不会出现 10 月份以供选择。

如果管理员想在 10 月份中每周都能查询到截止至当前的统计数据，可以

1.勾选上“报表生成前预统计”；

2.设置开始统计时间，如可设置为本月 7 日；

3.统计时间间隔为 1 周；

设置后，该打印月报会在 10 月 7 日生成从 10 月 1 日到当前时间（10 月 7 日）的统计数据，一周后会再生成 10 月 1 日到当前时间（10 月 14 日）的统计数据，以此类推，新的预统计结果会覆盖上一次的预统计结果，直到报表生成时间 10 月 31 日，生成最终的周期报表结果。此时每次预统计的结果都更接近最终的报表结果。

说明　对于在邮件设置中选中会发送邮件的报表，只有在报表生成时间生成的最终结果会发送邮件，周期过程中生成预统计的结果不会发送邮件。

28.8 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。征兆条件包含了常规和过滤条件两项。常规中设置时间间隔和级别阈值，过滤条件中设置相关的过滤项。创建征兆报表或趋势表时需选择征兆条件，符合过滤条件且在指定时间间隔内达到征兆级别阈值的数据将会统计出来。

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。支持 U 盘复制日志、打印操作日志、即时通讯日志、上网浏览日志、文档操作日志、应用程序运行日志、邮件日志作为征兆数据类型。默认定义了邮件日志、U 盘

复制日志、打印操作日志、文档操作日志类型的征兆条件。系统默认定义的征兆条件可以修改，可以删除。

28.9 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。

28.9.1 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。

28.9.2 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。

报表日期选择下拉菜单中，会列出已统计的时间范围项，如 2016 年 9 月份时创建周期报表，选择的周期为标准月，到了指定时间生成报表后，下拉菜单中出现 2016 年 9 月，到了 10 月再生成新的报表，下拉菜单中会再出现 2016 年 10 月。

统计类型下拉菜单中，可以切换统计类型来查询，在创建周期报表时设置了哪些统计类型，则此处下拉菜单中便会出现对应的类型。

选择了报表日期和统计类型后，会显示相应的统计图结果，统计图的右上方，可以选择显示的数据条数和显示图样，默认显示全部数据，统计表默认为柱状图，趋势表默认为折线图。

统计图下方会有具体的数据，双击一条数据，可查看具体的明细内容。选中数据列头，右键可增加或减少显示的数据列。

28.9.3 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。

28.9.4 启用和暂停

报表生成后默认为启用状态，即会按照设置的周期时间生成指定数据的报表。若想停止生成报表，则可选中目标报表，右键菜单中选择“**暂停**”。若想恢复定期生成报表，右键菜单中选择“**启用**”。

28.9.5 其他操作

数据显示区统计条件的右边，可对选中统计报表进行以下操作。

保存统计条件

点击“**保存**”，可以保存当前选中的统计条件，下一次再选中该表，则自动显示上一次保存的统计条件以及对应的统计结果。能保存的条件如默认显示列、图形类型、显示数量等。

查看报表信息

点击“**报表信息**”，可以查看当前报表的重要信息，包含条件设置和统计设置。

用户修改过的条件设置内容和统计设置内容会显示，系统默认条件不会显示，如果想查看完整的信息，可选中该报表，右键菜单中选择“**修改报表**”进行查看修改。

28.10 查询

28.10.1 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。

28.10.2 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。

查询条件包含以下日期、计算机范围、用户范围和高级条件。统计类型中，如果是趋势表查询，则还会出现统计的单位选择，供选择的时间单位有：天、周、月、季度、年。如查询条件中选择前一月，若统计类型中选择按天，则每一天的统计总量作为一组结果，若统计类型中选择按周，则每一周的统计总量作为一组结果。

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。

28.10.3 其他操作

查询数据显示区统计条件的右边，可对选中查询进行以下操作。

重置

点击“**重置**”，可以将当前界面上的查询条件和统计类型恢复为上一次保存的内容。

保存

点击“**保存**”，可保存当前界面上的查询条件和统计类型，下一次再选中该查询，则自动显示上一次保存的查询条件和统计类型。

保存结果

选定一组查询条件和统计类型，统计出结果后，点击“**保存结果**”，设置完名称后，可在“**报表->数据中心**”找到该报表结果。

另存为模板

点击“**另存为模板**”，设置名称后会弹出创建模板的对话框，创建的模板会沿用当前选中查询的查询条件和统计类型，亦可根据实际使用微调。另存为的模板可在“**报表->模板管理**”找到。

生成报表

点击“**生成报表**”，弹出创建周期报表对话框，创建的周期报表会沿用当前选中查询的查询条件和统计类型，亦可根据需要进行修改。

28.11 历史报表

28.11.1 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。

28.11.2 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。

功能按钮说明

图标按钮	说明
	查找按钮，点击弹出查找框，可根据报表名称和报表状态查询历史任务；
	启用按钮，可以启动一个已暂停的任务；
	停用按钮，可以暂停一个进行中的任务；
	添加按钮，可以创建一个新的历史报表任务；
	删除按钮，可以删除一个选定的任务，对于未执行完的任务，删除后未生成的报表不会再生成。

历史报表任务建立完后，会即刻执行生成报表任务，状态为“**进行中**”。

在同一时间，只能执行一个任务。当同时存在多个任务时，则以任务添加的先后顺序执行，后添加的任务状态为“**等待中**”。当前一个任务执行完成状态变为“**已完成**”后，或是前一个任务被停用状态变为“**已暂停**”后，状态为“**等待中**”且最早添加的任务状态将开始执行，状态变为“**进行中**”，以此类推。

28.12 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。

图标按钮	操作
	添加邮件报告配置。
	删除邮件报告配置。

报表邮件需要设置以下参数：

参数	说明
配置名称	用户自己定义的一种对该邮件配置的描述；
报表	选择需要邮件发送的周期报表；
邮件标题	设定发送的邮件报告标题；
收件人地址	接收报表邮件信息的邮箱地址；
将报表添加到正文	勾选则邮件正文中会添加报表数据内容，包括条件设置和统计类型，统计图结果和数据结果；
生成明细表	勾选则邮件正文中会添加报表数据的明信信息；
报表以附件发送	勾选则报表以附件形式发送，可指定附件类型；
邮件正文	输入的内容会在邮件正文中出现；
发送测试邮件	发送一封测试邮件到收件人邮箱。
压缩附件	勾选则会将报表以附件形式发送一个压缩文件，可设置此压缩文件的解压密码；

注意 所选的报表生成即发送，即所选报表最后一次统计完成时立即发送只含此报表的邮件。

28.13 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。

系统默认显示所有的报表，管理员也可以设置各种查询条件进行查询。

查询条件	说明
数据时间范围	报表所统计的数据的时间范围，可设置起始时间和终止时间；
报表范围	选择报表或查询的范围，默认为全部；
报表类型	报表类型，默认为全部；
报表周期	选择报表周期，可选年、季度、月、周、天，默认为全部。

注意 数据时间范围指的是报表中统计的数据的时间范围，不是报表生成的时间范围。

如 2016 年 11 月 1 日生成了 2016 年 9 月 1 日至 2016 年 9 月 30 日的打印报表，查询时起始时间选择 2016 年 11 月 1 日，无法查询到该打印报表，因为目标报表的数据范围不包含 2016 年 11 月 1 日，起始时间应选择 2016 年 9 月 1 日或更早的时间。

第二十九章. WEB 控制台

29.1 登录 WEB 控制台

在浏览器地址栏输入服务器地址，进入登录页面。

服务器地址填写的例子：

1、IP+默认端口 80：192.168.2.203

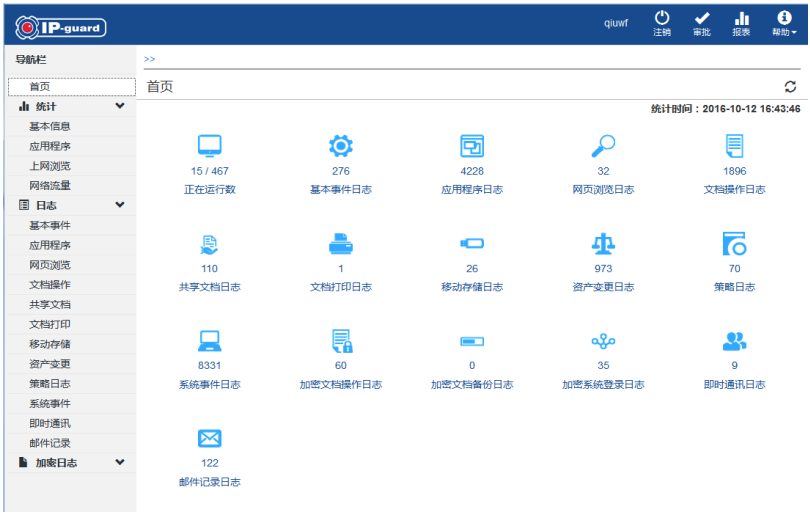
2、IP+非默认端口 8080：192.168.2.203:8080

3、域名+映射端口：tec.oicp.net:10941

4、前面加 http： http://192.168.2.203

29.2 WEB 控制台简介

登录 WEB 控制台后，界面如下图所示：



WEB 控制台界面包括：

界面区域	说明
功能栏	位于页面顶端右边，可以查看当前登录管理员信息，以及进行相关功能操作；
导航栏	位于功能栏左下方，包含了本系统的所有菜单，可快速导航各功能；
计算机栏/用户栏	位于导航栏右边，默认隐藏，点击导航栏右上方的 >> 按钮可展开，显示所有安装了客户端的计算机、用户列表和以及分组信息；
数据显示区	是本系统的核心视图，所有的数据都在数据显示区查看；
图表栏	只有统计功能包含图表栏，是显示统计图的区域；
查询栏	位于数据显示区内顶端，提供时间范围作为通用查询条件，在高级查询中可以选择更多的查询条件。

说明 1. Admin 和 Audit 账户不允许登录 WEB 控制台；
2.WEB 控制台仅支持日志的查看及查找，不支持修改与删除。

29.3 计算机和用户操作

点击数据显示区首行中的 >> 按钮，默认隐藏的计算机和用户树会展现出来。

当前针对计算机和用户，仅支持查看基本信息以及查找。

查看基本信息

在导航栏中选择“**统计->基本信息**”，选择计算机（组）或用户（组），可查看基本信息，基本信息包括的内容和控制台上一致。

查找

点击结构树视图上方的 图标，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。

29.4 首页

首页显示整个网络各项日志的统计信息。统计的数据包括：正在运行的客户端数、基本事件日志、应用程序日志、网页浏览日志、文档操作日志、共享文档日志、文档打印日志、移动存储日志。

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。

双击一个统计数据类型图标，可以跳转至具体日志信息界面。

29.5 统计

统计信息展示应用程序、上网浏览和网络流量的统计报告以及统计图表，以供对员工的工作情况进行评估。

选择导航栏“**统计**”，可分别查询在某一段时间计算机(组)或用户(组)的应用程序、上网浏览、网络流量使用情况，系统默认统计当天的各项使用情况，每项统计模式支持与控制台一致，数据展示仅支持柱状图。

29.6 日志

选择导航栏“**日志**”，可查询到各操作日志，包括：基本事件日志，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，系统事件日志，即时通讯日志，邮件记录日志。

选中一条日志，点击末尾的“**明细**”，可查看该条日志具体的内容。

29.7 加密日志

选择导航栏“**加密日志**”，可查看加密系统相关的各操作日志，包括：文档操作日志，文档备份日志，加密系统登录日志。

选中一条日志，点击末尾的“**明细**”，可查看该条日志具体的内容。

第三十章. WEB 审批

登录 WEB 控制台，点击页面顶部菜单栏右侧的“**审批**”，可进入到审批管理界面，此时点击页面顶部菜单栏右侧登录账户信息处，自动会出现下拉菜单，选择“**控制台**”即可返回 WEB 控制台界面。

WEB 审批支持桌面申请管理和加密申请管理的审批。

30.1 桌面申请管理

在页面顶部的菜单栏，选择“**桌面申请管理**”，切换的到桌面申请管理视图。

桌面申请管理包含水印申请，打印申请，设备申请，移动存储申请。

查看待审批申请

选择菜单栏下方左侧的“**等待审批**”，可查看等待当前登录管理员审批的申请。

等待审批界面左上角有“**查询条件**”折叠按钮，默认是折叠的，点击后可以选择条件进行查询，支持的查询条件有申请类型、申请时间范围、流程名称。

注意 修改查询条件后可以点击“重置”按钮进行恢复，但是时间范围是不会恢复到默认状态的。

查看申请总览

选择菜单栏下方左侧的“**申请总览**”，默认可查看一个月内所有的申请信息。也可以使用查询条件进行查询，支持的查询条件有状态、申请类型、申请时间范围、审批人、流程名称。

审批

双击一条申请，或者点击该条申请后的 按钮，会打开该申请的明细页面，可查看的信息包括申请信息，申请内容，有效时间，审批信息，变更历史。管理员能执行同意，拒绝，否决三种操作，不能更改申请的其他信息。选中多条申请，点击列表上方左侧的【**批量审批**】按钮，可进行批量审批。

30.2 加密申请管理

在页面顶部的菜单栏，选择“**加密申请管理**”，切换的到加密申请管理视图。

加密申请管理包含解密申请、离线申请、外发申请、安全属性变更申请。

查看待审批申请

选择菜单栏下方左侧的“**等待审批**”，可查看等待当前登录管理员审批的申请。

等待审批界面左上角有“**查询条件**”折叠按钮，默认是折叠的，点击后可以选择条件进行查询，支持的查询条件有申请类型、申请时间范围、文件名、流程名称。

注意 修改查询条件后可以点击“重置”按钮进行恢复，但是时间范围是不会恢复到默认状态的。

查看申请总览

选择菜单栏下方左侧的“**申请总览**”，默认可查看一个月内所有的申请信息。也可以使用查询条件进行查询，支持的查询条件有状态、申请类型、申请时间范围、文件名、审批人、流程名称。

审批

双击某条申请，或者点击该条申请后的 按钮，会打开该申请的明细页面，可查看的信息包括申请信息，文件信息，审批信息，管理员能执行同意或拒绝两种操作，不能更改申请的其他信息。选中多条申请，点击列表上方左侧的【**批量审批**】按钮，可进行批量审批。

下载文件

解密申请、外发申请和安全属性变更申请支持文件下载，打开申请的明细界面，在“**文件信息**”标签页，选中某个文件，点击 按钮下载该文件。

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，目前只支持只支持 txt，doc，docx，ppt，pptx，pdf 文件的预览，打开申请的明细界面，在“**文件信息**”标签页，选中某个文件，点击 按钮预览该文件。

注意 当客户端在线且文件存在时方可正常下载和预览成功，若客户端已离线，或文件已被修改、重命名、删除，则无法下载或预览并有相应提示。

第三十一章. WEB 报表

登录 WEB 控制台，点击页面顶部菜单栏右侧的“**报表**”，可进入到报表界面，此时点击菜单栏右侧登录账户信息处，自动会出现下拉菜单，选择“**控制台**”即可返回 WEB 控制台界面。

说明 WEB 报表仅支持已生成报表的查看，不支持查询和其他功能设置。

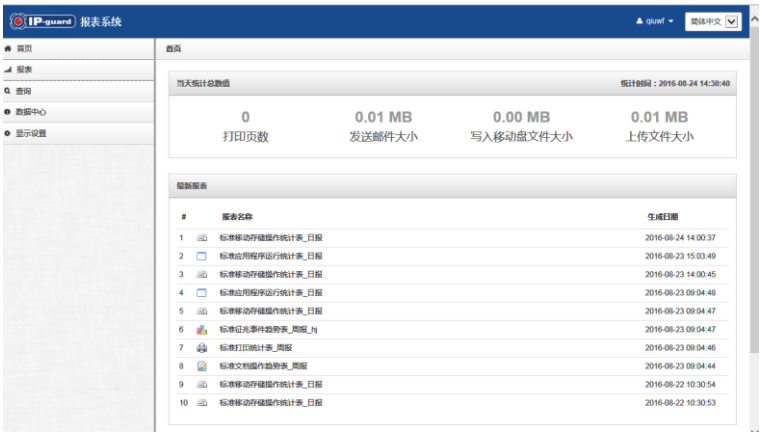
31.1 首页

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



31.2 报表

在左侧导航栏中，选择“**报表**”，会向下展现出报表结构树，可以查看已有报表数据，可以选择报表日期、统计类型、统计图样、统计数量等条件来展示数据。点击“**报表信息**”可以查看当前报表的重要信息，包含条件设置和统计设置。

支持的报表类型包括：打印报表，即时通讯报表，上网浏览报表，文档操作报表，移动存储报表，应用程序报表，邮件报表，策略日志报表、加密文档操作报表、征兆报表，综合报表。每种支持的报表均包含统计表和趋势表。

31.3 数据中心

在左侧导航栏中，选择“**数据中心**”，会在右边的数据显示区将会显示各个报表的信息，包括报表名称，报表分组，数据时间范围，报表类型，报表周期，生成日期。双击一个报表，会启动新窗口显示报表的详细数据。

第三十二章. 安全查看器

安全文档查看器，可以实现移动智能设备在授权情况下正常查看加密的文档，无授权则无法查看加密文档，降低泄密风险的同时能很好的适应和推动智能办公的普及。

32.1 软硬件环境

安全查看器支持的操作系统以及硬件建议配置如下表：

项目	基本要求
智能终端类型	智能手机、平板
操作系统	Android 4.0.3 及以上版本； iOS 6.0 及以上版本
配置	最低配置 内存 512M 建议配置 内存 1GB
支持查看的加密文档类型	文本（pdf,txt,c,h,cpp,hpp,doc,docx,xls,xlsx,ppt,pptx）、 图片（bmp,png,jpg） 网页（htm,html） 特殊：iwork（pages,key,numbers）

32.2 安装

通过浏览器输入安全文档查看器的下载地址，或者在手机浏览器中通过扫描二维码直接跳转网站，可选择下载支持 Android 系统或者 iOS 系统的版本。

安全文档查看器下载地址：

http://www.tec-development.com/apps/download.html

安全文档查看器下载的二维码：

注意 iOS 系统安装安全文档查看器 APP 后需要对其进行“信任”操作：

iOS 8.0 以上 9.0 以下的系统：安装后打开，会直接弹出提示是否信任该应用，直接点击【**信任**】即可；

iOS 9.0 以上的系统：安装后打开，会弹出提示“未受信任的企业级开发者”，需要在“设置-通用-描述文件”信任该应用；

32.3 授权

安全查看器需要连接上服务器，并通过管理员授权后，才能打开加密文档。

具体步骤如下：

1) 运行安全查看器，输入服务器地址，支持填写 IP 或域名，输入完毕后点击【**连接**】按钮；

2) 进入授权状态界面，点击【**申请授权**】；

3) 在申请授权页面，输入使用者信息和申请理由，点击【**提交**】。提交成功后会自动返回授权状态页面，状态栏显示为“**你的申请已提交，正等待审批中**”。

管理员在控制台通过申请，对该设备启用授权后，安全查看器的授权状态页面状态栏将变更显示为“**申请被批准，授权成功**”，可点击【**进入**】按钮，转至

安全查看器主界面。

32.4 查看加密文件

授权成功后，打开安全查看器进入主界面。选择“**存储**”，进入到加密文档的存放位置，如果目标路径下的文件众多，可以点击当前路径下方的“**搜索**”，输入文件名称进行快速定位，支持模糊查找。点击加密文件，可自动跳转至文档内容页面。

除了在安全查看器中打开加密文件，也可以在其他 APP 中，点击加密文件，在弹出的打开方式中选择安全查看器，则也会启动安全查看器打开加密文档。

说明　　安全文档查看器中的搜索功能当前只支持当前目录的搜索。

32.5 加密/解密文件

安全查看器中可以对文件进行加密、解密操作。

加密

安全查看器加密功能默认开启，加密文件的安全属性统一为“**公共-普通**”。

安全查看器主页面中的底部导航栏中会显示“**加密**”按钮，选择文件，点击“**加密**”按钮，能将文件加密，已加密的文件会显示带小锁的文件图标。

解密

安全查看器解密功能默认不开启，管理员需要在控制台对设备设置智能终端策略，“**智能终端加密管理->加密->常规**”中勾选“**允许直接解密文档**”启用解密功能。

安全查看器主页面中的底部导航栏中会显示“**解密**”按钮，选择加密文件，点击“**解密**”按钮，能将文件解密，已解密的文件不会显示带小锁的文件图标。

32.6 分享文件

在安全查看器主界面中选择文件，点击“**更多->分享**”，弹出分享方式选择界面，可将相应的文件分享到其他 APP。分享出去的文件加解密状态保持不变。

32.7 最近和收藏

最近

安全查看器主界面，选择“**最近**”，列表中将按打开文件时间列出最近查看过的文件，点击文档可直接查看。点击左上角的“**清空**”可将最近列表清空。

收藏

在“**最近**”列表中，文档的最右边都有一个☆，代表收藏状态，灰色为未收藏，蓝色为已收藏，点击该☆，状态将在未收藏和已收藏之间切换。

在安全查看器主界面，选择“**收藏**”，列表中显示已收藏的文档，方便以后快速定位常用文档，收藏列表点击文档可直接查看。点击左上角的“**编辑**”，选中指定的文档，点击“**删除**”，最后点击“**保存**”，则选中的文件将在收藏列表中删除。

32.8 设置

安全查看器主界面，选择右上角的设置图标，可以对安全查看器的一些常规使用进行设置。

选项	说明
仅在 WIFI 下通讯	开启此项，则仅在智能终端连接 WIFI 时才与服务器通讯，不开启此项，则只要有网络连接都会与服务器通讯；
修改服务器地址	选择此项，会转到服务器地址设置页面，可修改连接服务器地址；
设置密码	设置使用密码，需要输入密码才能使用安全查看器。 设置过密码后，选择此项，可以对密码进行修改； 默认使用安全查看器的密码为空，即运行安全查看器无需输入密码直接可以使用。
关于	选择此项，可以查看当前安全查看器的版本信息。

32.9 重置密码

设置了使用密码，则每次打开安全查看器时将进入密码登入界面，输入正确的密码后点击**【进入】**按钮，转至安全查看器主界面。

若忘记了登录密码，可按以下步骤重置密码：

1) 点击安全查看器密码登入页面上的“**重置密码**”，进入重置密码页面；

2) 页面中会显示一串原始操作码，请把原始操作码报告给管理员；

3) 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；

4) 管理员确认后点击**【生成确认码】**;

5) 管理员将确认码告诉用户，用户在安全查看器中输入正确的确认码，点击**【确定】**，直接进入安全查看器界面。

执行重置密码后，登录密码即被重置为初始值，即为空。

第三十三章. 安全审批 APP

安全审批 APP，可实现在智能终端上，对桌面安全管理和文档安全管理的申请进行审批。

33.1 软硬件环境

安全审批 APP 支持的操作系统以及硬件建议配置如下表：

项目	基本要求
智能终端类型	智能手机、平板
操作系统	Android 4.0.3 及以上版本； iOS 6.0 及以上版本
配置	最低配置 内存 512M 建议配置 内存 1GB

33.2 安装

通过浏览器输入安全审批 APP 的下载地址，或者在手机浏览器中通过扫描二维码直接跳转网站，可选择下载支持 Android 系统或者 iOS 系统的版本。

安全审批 APP 下载地址：

http://www.tec-development.com/apps/download.html

安全审批 APP 下载的二维码：

注意 iOS 系统安装安全审批 APP 后需要对其进行“信任”操作：
iOS 8.0 以上 9.0 以下的系统：安装后打开，会直接弹出提示是否信任该应用，直接点击【**信任**】即可；
iOS 9.0 以上的系统：安装后打开，会弹出提示“未受信任的企业级开发者”，需要在“设置-通用-描述文件”信任该应用；

需要安装部署了 Web 审批服务器，安全审批 APP 才能使用。

33.3 登录

首次运行安全审批 APP 后，需要输入 Web 审批服务器地址，具有审批权限的管理员账号及密码。

服务器地址填写格式为：WEB 服务器 IP/域名:端口号。

其中，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；

服务器地址填写的例子：

1、IP+默认端口 80：192.168.2.203

2、IP+非默认端口 8080：192.168.2.203:8080

3、域名+映射端口：tecyexh.oicp.net:10941

4、前面加 http： http://192.168.2.203

安全审批 APP 退出登录后，仍会记住上次登录的服务器地址和管理员账号，下次登录时只需输入正确密码，即可登录；

说明 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。

33.4 申请管理

申请管理支持桌面申请管理和加密申请管理，可在界面上方的“**桌面申请管理**”和“**加密申请管理**”切换进行查看和审批。

33.4.1 桌面申请管理

桌面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。

查看待审批申请

点击“**等待审批**”，切换至等待审批申请列表，点开一条申请，可以查看该条申请具体的申请信息。

通过查询功能可快速定位到指定的申请。

快速查询

查询条件只支持对“流程名”的查询；在编辑框中输入流程名，点击 即可。

高级查询

高级查询的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、时间以及流程名。点击【重置】，可以重置查询条件为默认情况。

查看申请总览

点击“**申请总览**”，切换至全部申请列表，默认显示一个月内的申请。点开一条申请，可以查看该条申请具体的申请信息。

申请总览也可通过查询功能可快速定位到指定的申请，查询功能使用同等待申请列表。

审批申请

管理员选择一条申请，双击进入详细信息页面，进行审批操作，点击“**同意**”，则该申请被批准，点击“**拒绝**”，则该申请被拒绝。

支持打印申请、浮水印申请、设备申请、移动存储申请的审批。

说明　　不支持修改申请信息。

33.4.2　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。

查看待审批申请

点击“**等待审批**”，切换至等待审批申请列表，点开一条申请，可以查看该条申请具体的申请信息。

通过查询功能可快速定位到指定的申请：

快速查询

查询条件只支持对“流程名”的查询；在编辑框中输入流程名，点击 即可。

高级查询

高级查询的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、时间以及流程名。点击【重置】，可以重置查询条件为默认情况；

查看申请总览

点击“**申请总览**”，切换至全部申请列表，默认显示一个月内的申请。点开一条申请，可以查看该条申请具体的申请信息。

申请总览也可通过查询功能可快速定位到指定的申请，查询功能使用同等待申请列表。

审批申请

管理员选择一条申请，双击进入详细信息页面，进行审批操作，点击“**同意**”，则该申请被批准，点击“**拒绝**”，则该申请被拒绝。

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。

说明 当前不支持修改申请信息。

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 文件暂时不支持。

点击一条申请进入详细信息页面，点击“**文件信息**”处的，可查看申请的文件的详细情况，默认显示文件名和文件大小；点击可显示文件的安全属性；点击按钮可以预览此文件。

说明 1.预览文件功能，需要 Web 服务器在部署时要安装 JAVA 和 OpenOffice 组件；

2.若客户端当前不在线或文件已被移动，无法预览文件。

33.5 设置

安全审批 APP 主界面，选择右上角的图标，下拉菜单中选择“设置”，可以对安全审批 APP 的一些常规使用进行设置。

选项	说明
接收新消息通知	默认开启，与其他通知设置（仅在 WIFI 下通知、声音和振动）相关联；关闭“接收新消息通知”后，其他通知设置均被收起，无法设置，APP 不会接收新的申请通知；
仅在 WIFI 下通知	默认不开启；开启后，只有在 WIFI 环境下，才接收新的申请通知；数据流量环境下，不接收新的申请通知；
声音	默认开启，声音为默认值，不可修改；

振动	默认开启，振动则是系统自带；
关于	选择此项，可以查看当前安全审批 APP 的版本信息。

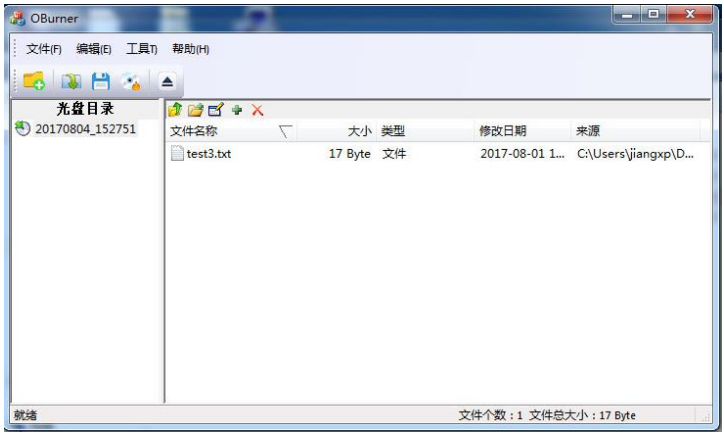
说明 平板设备不支持振动，不显示“振动”项。

第三十四章. 专用刻录工具

刻录工具 OBurner 为 IP-guard 专用刻录工具，简单易用，可完成绝大部份的刻录工作。此专用刻录工具需要在装有 IP-guard 客户端的机器上方可正常使用刻录功能，在无客户端的机器上无法进行刻录，仅可操作配置文件。

34.1 界面简介

双击运行专用刻录工具 OBurner.exe，进入刻录工具主界面，如下图：



主界面包括工具界面包括：

界面区域	说明
菜单栏	包含了本系统的所有菜单，是各功能窗口的入口；
工具栏	包含了一些常用的功能：新建、打开、保存、刻录、弹出光盘；
光盘显示区	左侧为光盘目录层级结构，选择某个层级节点，右侧视图中将出现该层目录下的文件和文件夹信息； 右侧视图上方的功能键，可对当前层级目录下的文件和文件夹进行相关操作；

状态栏	位于工具的最下方，显示了当前所有待刻录文件的总个数和总大小。

工具栏功能按钮说明：

图标按钮	说明
	新建按钮，新建一个空的光盘目录，也可看成是新建一个配置文件；
	打开按钮，打开已有的配置文件；
	保存按钮，将当前光盘目录保存成配置文件；
	刻录按钮，将当前光盘目录下的内容刻录进光盘；
	弹出光盘按钮，可弹出光驱取出光盘。

光盘显示区右侧视图功能图标说明：

图标按钮	说明
	在当前目录下（非根目录），返回上一层目录；
	在当前目录下，新建文件夹；
	对选中文件或者文件夹进行重命名；
	添加文件或文件夹到当前目录中；
	删除选中的文件或文件夹。

34.2 刻录

使用专用刻录工具刻录光盘的步骤如下：

1) 在安装了客户端的机器上运行启动 OBurner.exe，同时在该机器上接入光驱，放入光盘；

2) 在专用刻录工具中，按刻录需求构建光盘目录；

   菜单栏中选择“编辑->添加”，选择文件或者文件夹加入，也可直接将目

标文件或文件夹拖拽进光盘显示区的右侧视图完成添加；

3) 构建完光盘目录后，菜单栏中选择“**工具->刻录**”，也可点击工具栏上的刻录按钮，弹出“刻录设置”界面；

其中：

选择刻录机：下拉选择连入客户端并且用于刻录光盘的刻录机；

写入速度：刻录过程光盘写入速度，有最快、24X、20X、16X、10X 多种速度可选；

光盘格式：ISO-9660 和 UDF；

刻录份数：刻录的光盘数量；

备注信息：此次刻录的相关备份信息，为必填项；

4) 完成刻录设置后，点击【刻录】按钮，开始刻录；

5) 刻录过程中有进度显示，以查看到当前刻录的进度、已用时间、剩余时间、光盘写入速度和刻录份数。当刻录进度为 100%时表示刻录完成。

6) 刻录完成后，菜单栏中选择“**工具->弹出光盘**”，也可点击工具栏上的弹出光盘按钮，弹出光盘刻录机取出光盘。

注意 刻录设置选择光盘格式时，ISO-9660 单个文件刻录大小最大不超过 2G，UDF 则无此限制。

34.3 配置文件

配置文件主要用户保存当前的目录内容和对应的文件信息，方便日后重复刻录。对于已经构建好的光盘目录，可以在菜单栏“文件->保存”，或是点击工具栏上的保存按钮，将当前目录信息保存为配置文件。

下次刻录时，菜单栏“文件->打开”，选择此前保存的配置文件，会根据目录导入文件，此时可直接刻录。

若当前打开的配置文件中的目录，较保存时已发生变化，会弹出提示，如果是整个待刻录文件夹变化则会提示文件夹下每一个文件的变化情况。其中，操作类型为“修改”的提示说明该路径下的文件内容编辑修改过，操作类型为“缺少”的提示说明该路径下的文件已被删除或重命名。

若待刻录文件提示变化后不保存配置文件，之后每次重新打开都会提示，在未保存的情况下直接刻录文件，刻录的文件内容是修改后的最新内容（缺少的文件不会刻录），并且自动保存配置文件中的待刻录文件为最新内容。

第三十五章. 准入网关

IP-guard 的桌面管理系统可以详细地对计算机的操作行为进行详细的审计和严格的控制，但是仍然有一些用户通过重新格式化并安装操作系统，设置个人防火墙等等手段逃避行为监管。即使当管理员及时发现这类情况，重新再部署桌面管理客户端亦是一件繁琐和恼人的工作。同时，基于管理需要，企业会规定计算机必须符合一定的要求才能正常访问网络，如安装杀毒软件、运行指定的进程等。

准入网关控制系统就是为了解决上述问题而诞生的。

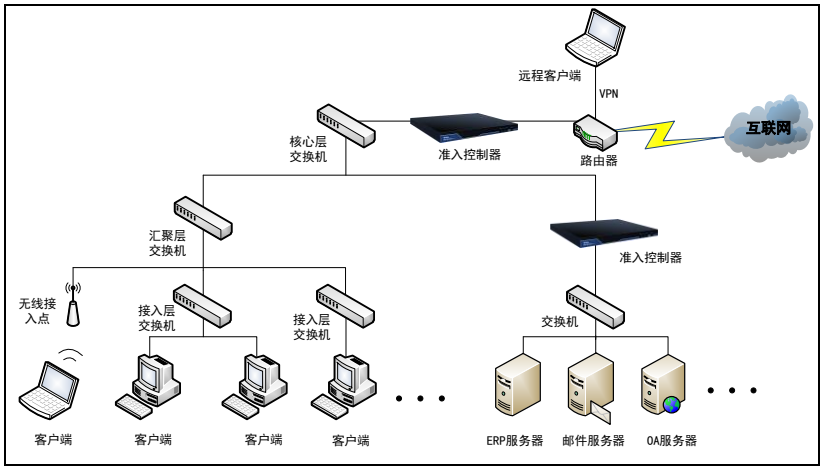
准入网关系统是一套专业的软硬件结合系统，由硬件控制器与桌面管理系统联合工作，可有效的避免内网 PC 脱离桌面管理系统的管控，加强网络准入监管，保证内网安全策略的执行，同时杜绝非法连入带来的外泄风险。

35.1 网络架构

准入网关系统的控制功能主要依托于硬件网关准入控制器（以下称准入设备）。准入设备的工作模式有两种：网桥模式和路由模式。

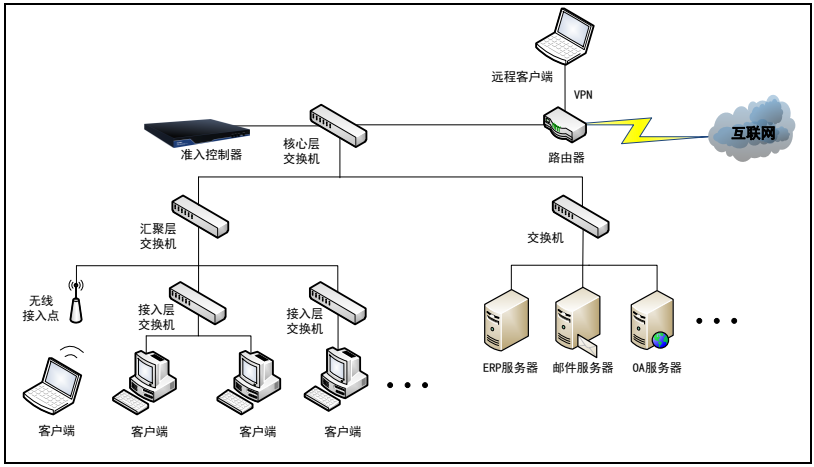
网桥控制模式

使用网桥模式，可以对网络结构和配置不做任何修改，直接将准入设备串接进网络中需要进行控制的地方，多数是重要的应用服务器或者网关处，对通过其的网络通讯进行控制。



旁路控制模式

对核心交换机启用策略路由，对跨网段的访问进行控制。这种控制方式需要核心交换机支持策略路由。



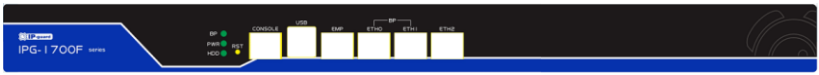
35.2 设备介绍

准入设备有以下几种型号：1700F、2500F、3300F、3500F、4300F、4500F。

1700F：

四个 RJ45 端口，其中包含一组 BYPASS（ETH0 和 ETH1）；

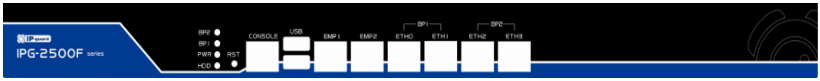
管理端口为 EMP；



2500F：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

管理端口为 EMP1 和 EMP2；



3300F：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

管理端口为 EMP1 和 EMP2；

3500F：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

管理端口为 EMP1 和 EMP2；

4300F：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

两个 SFP 端口 ETH4 和 ETH5；

管理端口为 EMP1 和 EMP2；

4500F：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

两个 SFP 端口 ETH4 和 ETH5；

管理端口为 EMP1 和 EMP2；

说明　　1.所有设备均支持千兆网络；

2. 初始配置使用管理端口：

对于仅有一个管理端口（EMP）的设备，IP 固定为 190.190.190.190；

对于有两个管理端口（EMP1 和 EMP2）的设备， EMP1 的 IP 固定为 190.190.190.190，EMP2 的 IP 固定为 191.191.191.191；

3.BYPASS 功能，可以在控制器断电或死机的情况下，将控制器所连接的两端直接物理上导通，不影响网络的使用。

35.3 设备部署

35.3.1 设置设备 IP

根据实际情况选择控制方式，定好部署准入设备的位置，根据部署点为准入设备定好 IP，确定之后便开始设置准入设备 IP。

有管理端口的设备使用管理端口进行设置。具体步骤如下：

1) 使计算机 A 脱离内网环境，修改计算机 A 的 IP，让它能与准入设备通讯。如：

   IP 地址：190. 190. 0. 1

   子网掩码：255. 255. 0. 0

   默认网关：可不填

2) 使用网线将计算机 A 和准入设备管理端口（若是 IPG-1000 则是任一端口）直连，计算机 A 上使用浏览器访问网址 http://190.190.190.190，能进入到设备管理登录界面；

3) 账号为 admin，密码初始为空，点击【确定】后进入管理界面；

4) 左侧菜单栏中，选择“**网络参数->基本设置**”，选择准入设备连入网络环境的接入模式，并设置相应的 IP 信息，设置完成后保存即可。

IP 修改成功后需要重启设备。

说明 设置 IP 时，2500F 及其以上型号的设备模式选择项中会多出一项“网桥（双机备份[主]）”。网桥模式下采用双机热备的主设备才需要用到此设置。

35.3.2 连入网络前设置

如果选择网桥部署模式，且准入设备部署在以 TRUNK 方式相连的交换机之间，需要设置被阻断时的转发功能，则需要启用准入控制器的 TRUNK 功能。具体可查看“**网络参数->Vlan 设置**”，如不是此种网络环境，无需启用。

如果选择网桥部署模式，且准入设备部署在二层交换机和三层交换机之间，二层交换机上的 PC 有多个网段（非 VLAN），且网关上也有对应这些网段的 IP。设置被阻断时的转发功能，则需要启用多 IP 绑定配置。具体可查看“**网络参数->多 IP 配置**”，如不是此种网络环境，无需启用。

如果选择旁路部署模式，需要对交换机加上策略路由配置，具体请咨询技术工程师。

35.3.3 设备连入网络

设置完准入设备 IP 后，则可以将其连入事先计划好的部署点。

网桥模式

连接方法：使用设备的两个端口将其连入网络；

设备型号	使用的端口
1700F	使用 ETH0、ETH1、ETH2 中任两个；
2500F	使用 ETH0、ETH1、ETH2 中任两个；
3300F	使用 ETH0、ETH1、ETH2 中任两个；
3500F	使用 ETH0、ETH1、ETH2 中任两个；
4300F	使用 ETH0、ETH1、ETH2 中任两个；
4500F	使用 ETH0、ETH1、ETH2 中任两个。

旁路模式

连接方法：使用设备的一个端口连接交换机；

设备型号	使用的端口
1700F	只能使用 ETH0；
2500F	只能使用 ETH0；
3300F	只能使用 ETH0；

设备型号	使用的端口
3500F	只能使用 ETH0；
4300F	只能使用 ETH0；
4500F	只能使用 ETH0。

旁路模式支持将接入口由 ETH0 更改为其他端口，修改方法为：

选择“**系统工具->设置配置管理->高级配置**”，点击“**设置**”，输入以下配置内容

[PRP]

PRP=ethX

其中，X 代表具体的通讯端口号。

设备连入网络后，可以使用浏览器访问准入设备的 IP 地址，如 http://192.168.2.190，进入到设备管理登录界面。

35.4 基本信息

选择“**基本信息**”，可以进行“**开启/停止准入控制功能**”的操作。为了在部署过程中不影响工作，建议设置好准入设备的相关设置以及 IP-guard 安全策略设置后，再启用准入控制功能。

在基本信息中，还能查看准入设备的相关信息，包括通过准入设备的 IP 统计信息、准入设备信息、时间信息。

统计信息包括以下信息：

属性名称	说明
IP 总数	经过准入设备的 IP 总数；
在线数量	持续有通讯通过准入设备的 IP 数量；
阻止数量	被准入设备阻止的 IP 数量。

准入网关信息包括以下信息：

属性名称	说明

软件版本	准入设备的功能软件版本；
出厂版本	出厂时准入设备的功能软件版本；
当前版本	当前功能软件版本，初始为出厂版本，若进行过升级或降级操作，则为操作后的版本；
Web 版本	当前设备的 Web 前端页面版本；
运行平台	功能软件的运行平台信息；
硬件型号	准入设备的硬件型号信息；
校验结果	程序出厂校验结果，均为 OK；

时间信息包括以下信息：

属性名称	说明
当前时间	准入设备当前时间，出厂前都会调整至同网络同步；可在“系统工具→修改时间”中修改；
启动时间	准入设备启动的时间；
运行时间	准入设备最近一次开机到当前持续运行的时间。

35.5 网络参数

35.5.1 基本设置

选择“**网络参数->基本设置**”，可以设置准入设备连接模式以及 IP 地址。设备没有设置 IP 时需使用管理端口连接准入设备进行设置，设备已设置了 IP 则可直接在连入网络的状态下设置。设置并保存后需要重启准入设备才会生效。

35.5.2 Vlan 设置

在网桥运行模式下，如果准入设备部署在以 TRUNK 方式相连的交换机之间，同时设置被阻断时的转发功能，则需要启用准入控制器的 TRUNK 功能

选择“**网络参数->Vlan 设置**”，勾选了“**开启 Trunk**”并添加 VLan 配置即可。

Vlan 配置信息包括以下：

属性名称	说明

ID	VlanID；
IP 地址	添加时需要输入一个对应 VlanID 下不会冲突的 IP 地址；
子网掩码	IP 地址的子网掩码；

提示

1.添加 VLAN 配置时，只能添加 Native Vlan 或 defaultVlan 之外的 VLAN，否则可能会导致网络不正常；

2.在以 TRUNK 的方式连接时，设备的 IP、掩码及网关的配置必须属于 Native Vlan 或 defaultVlan；

3. Native Vlan 或 defaultVlan 如果在交换机上不进行人为的修改时，那就是 Vlan 1。

35.5.3 多 IP 配置

在网桥运行模式下，如果准入设备部署在二层交换机和三层交换机之间，二层交换机上的 PC 有多个网段（非 VLAN），且网关上也有对应这些网段的 IP。设置被阻断时的转发功能，则需要启用多 IP 绑定配置。

选择“**网络参数->多 IP 配置**”，勾选了“**开启多 IP 绑定**”并添加需要绑定的 IP 即可。

多 IP 绑定配置信息包括以下：

属性名称	说明
IP 地址	需要绑定的网段下不会冲突的 IP 地址；
子网掩码	IP 地址的子网掩码；

提示

在增加多 IP 绑定的配置时，对于准入设备 IP 所在的网段不能添加，否则会出现冲突。

35.6 准入网关配置

35.6.1 管理范围

选择“**准入网关配置->管理范围**”设置准入设备管理范围。

管理范围默认为空，即所有计算机有通信经过准入设备时，就会出现在准入设备对应的“**状态信息**”视图内。设置了管理范围后，则只有管理范围内的计算机有通信经过准入设备时，就会出现在准入设备对应的“**状态信息**”视图内。

35.6.2 控制范围

选择“**准入网关配置->控制范围**”设置准入设备控制范围。

控制范围默认为空，即不对任何计算机做控制。设置了控制范围，此范围内没有安装客户端机器以及不符合相关安全条件的客户端将会被阻断，其访问准入设备保护的网络时受限。

35.6.3 例外规则

例外规则，即所有的计算机都能访问的 IP 地址和端口，其中，端口包括 TCP 端口和 UDP 端口。企业内部一些公用服务器，没有敏感信息，对访问的机器没有特别的要求时可以设置为例外 IP 地址；企业内部的一些无固定 IP 地址但有特定的通讯端口，不涉及敏感信息却需要能正常网络通讯的网络设备，可以设置例外 TCP 端口或例外 UDP 端口。选择“**准入网关配置->例外规则**”进行设置。

提示　　例外 TCP 端口和例外 UDP 端口，针对所有 IP 生效。

35.6.4 警告页面

警告页面主要作用在于：未符合准入规定的计算机访问准入设备保护的网络受阻，且访问的目标地址端口属于“转发的端口”时，会被引导至警告页面，可在此页面得知相关的准入需求通告，亦可下载 IP-guard 客户端进行修复，得以

通过网络准入控制的认证，从而保证正常访问准入设备网络。

选择“**准入网关配置->警告页面**”进行设置。警告页面的配置项如下：

属性名称	说明
转发页面	选择使用哪种转发页面；
系统转发页面	警告页面默认为系统转发页面，已预先给定页面，系统警告页面提供访客登录操作。管理员可以修改页面内容，亦可重置为初始给定页面；
其他转发页面	如果想使用已有的 http 服务器网页，亦可以选择其他转发页面，输入网页地址；
转发端口	不符合规定的计算机，访问的目标地址端口属于“转发端口”时，会自动跳转至警告页面。可根据实际需要进行修改。

35.6.5 主动认证

一般情况下，当客户端与服务器断开连接时，准入设备会阻断客户端连接网络；或是客户端开机启动后没有立即连上服务器时，也会造成短暂的网络访问阻断。设置准入设备接收客户端认证信息，则可以解决以上问题。

默认情况下准入设备不会接收客户端认证信息，需要在准入设备网页管理界面选择“**准入网关配置->主动认证**”中勾选“**信任客户端认证**”。

主动认证其他各设置项说明如下：

设置项	说明
信任客户端认证	勾选此项，准入设备将接收客户端发送的主动认证信息；
仅信任所连服务器的客户端主动认证	不勾选此项，则接收所有客户端发送的认证信息； 勾选此项，则只会接收所连服务器的客户端发送的认证信息，不信任其余服务器的客户端发送的认证信息；

禁止网络地址转换（NAT）	禁止网络地址转换：不勾选此项，在 NAT 设备(路由、无线路由等) 架构下，只要其中一台电脑设备主动认证成功，该 NAT 设备下连接的其他电脑设备，也都允许接入受保护网络； 勾选此项，NAT 设备架构下的电脑设备，都无法主动认证成功。 ※ 不支持虚拟环境架构：无论是否勾选此项，只要虚拟环境以 NAT 模式透过实体主机连接网络，则虚拟环境对受保护网络的访问，将与主机相同。
兼容非安全检测客户端	该项默认为勾选上。勾选此项，则接收所有客户端发送的认证信息； 不勾选此项，则只接收支持安全检测功能的客户端发送的认证信息。

35.6.6 白名单

对于一些无法安装客户端的网络终端设备，例如网络打印机，可以在“**准入网关配置->白名单**”通过配置白名单的方式允许这些网络设备接入网络。白名单支持 IP 地址以及 MAC 地址控制。

说明　仅支持与准入网关处于同一 VLAN 的机器设置为 MAC 地址白名单。

35.6.7 黑名单

为了管理上的严格，对于一些合规的客户端，也要控制其对特定环境的访问，此时可以在“**准入网关配置->黑名单**”通过设置黑名单来实现。设置了黑名单的计算机，访问准入设备保护的网络均会被受阻，例外地址可以访问。

35.7 服务器管理

设置服务器与准入设备连接，则服务器上的合规客户端正常连接服务器时，将能正常访问准入设备保护的网络。

在控制台“**工具->准入网关管理**”中成功添加了准入设备后，在准入设备网

页管理界面的“**服务器管理**”可以看到连接上来的服务器。可以修改服务器和准入设备之间的容灾设置，也可以启用/禁用服务器，禁用后服务器和准入设备的连接将断开，容灾设置不生效。

35.8 访客登录管理

35.8.1 访客管理

对于一些临时需要访问准入设备保护网络的外来机器，不方便安装客户端，则可以给予访客账号，在访问受阻转到系统警告页面时，输入访客账号和密码进行认证登录，登录成功则正常访问。

访客具有临时性，登录成功后一定时间内没有网络访问行为，则当前认证登录会失效，下次再访问则需要再进行认证登录。

选择“**访客登录管理->访客管理**”可进行访客账号管理，添加/删除、启用/禁用访客账号，同时也可以修改访客账号。添加访客账号时有如下设置项：

设置项	说明
账号	访客账号的相关信息设置；
账号名	访客账号名称，必填；
密码	访客账号密码，必填，不能为空；
备注	访客账号的备注信息，可不填；
有效时间	访客账号使用的有效时间；
登录	访客登录的相关设置；
仅允许单点登录	不勾选此项，则访客账号可以在多个 IP 上登录成功； 勾选此项，则访客账号在某一 IP 登录成功，在其他 IP 上便不可在登录此账号；
仅允许在指定的 IP 上登录	不勾选此项，则访客账号可以在任意 IP 上登录成功； 勾选此项，并设置指定的 Ip，则该访客账号只能在指定的 IP 上登录，在其他 IP 上无法登录；
不允许在客户端上登录	不勾选此项，则在不合规的客户端上，该访客账号可以登录； 勾选此项，则在不合规的客户端上，该访客账号也不可以登录。

说明　　被设置为黑名单的机器，访客不能登录。

35.8.2 访问范围

当外来人员被授予访客权限以后，默认可以访问准入网关保护的所有网络。选择“**访客登录管理->访问范围**”可对访客账号访问的网络进行限制。

设置项	说明
动作	可以选择禁止或者允许；
IP 地址	访问范围，支持 IP 段输入，多个输入使用逗号隔开，如：192.168.1.1-192.168.1.100,192.168.2.102；
备注	备注信息。

说明　　可以设置多条访问范围，新添加的设置默认添加在列表最末端，设置从上到下匹配，即：一个 IP 匹配到的第一条访问范围设置生效，就不会在继续往后匹配。

35.8.3 高级设置

选择“**访客登录管理->高级设置**”可以设置访客认证机制的配置项。

设置项	说明
心跳链接	系统每隔多长时间去检测一次当前登录访客账户是否有网络访问行为；默认为 1 分钟；
访客网络禁止行为	访客网络访问行为停止达到指定时间后，本次认证失效，下次访问会受阻，需要重新认证登录；默认为 5 分钟。

35.8.4 访客日志

选择“**访客登录管理->访客日志**”可以查看访客账号的日志，提供审计依据。访客日志包含的内容有：时间、网络地址、账户、操作。

属性名称	说明

时间	访客账号执行相关操作的时间；
网络地址	访客账号执行操作的网络地址；
账户	账户名；
操作	此次操作的类型，登录或者注销。

35.9 状态信息

状态信息中，可以查看当前经过准入设备的计算机的相关信息，包括：网络地址、最后在线时间、阻断状态、当前标识。

属性名称	说明
网络地址	计算机的网络地址；
最后在线时间	计算机最后有通讯通过准入设备的时间；
阻断状态	计算机当前的是否为阻断。如果被阻断，阻断状态为“阻断”，如果没有被阻断，阻断状态为空；
当前标识	计算机当前的状态标识。

不同情况的计算机，都会对应一种当前标识，而每种标识都会对应一种阻断状态，具体如下：

当前标识	说明	对应阻断状态
空	没安装客户端	阻断
合规（授权）	安装了客户端，且符合安全策略。当前为服务器授权合规。	空，即不阻断
合规（信任）	安装了客户端，且符合安全策略。当前为发送信任包合规。	空，即不阻断
合规(授权+信任)	安装了客户端，且符合安全策略。当前同时为服务器授权合规和发送信任包合规。	空，即不阻断
客户端（不合规）	安装了客户端，但不符合安全策略	阻断
白名单	设置了白名单的计算机	空，即不阻断
黑名单	设置了黑名单的计算机	阻断
访客	使用访客认证登录访问的网络的计算机	空，即不阻断

灾备开放	由于容灾生效而被准入设备放行通过的计算机。 说明：设备网页管理界面中的“服务器管理”会显示与设备连接的服务器，当设备与服务器的连接出现异常时，容灾设置开始生效。	空，即不阻断

当前标识

一台计算机，可能同时具有多种标识，各标识的优先级如下：

黑名单 > 白名单 > 访客> 客户端（合规和不合规）

当一台计算机的标识超过一种时，则按照优先级高的标识为主，对应该标识的阻断状态。例如，一台不满足安全条件的客户端计算机，同时被设置了白名单，则此时它的当前标识是“**白名单**”，阻断状态为“**空**”。

35.10 系统工具

35.10.1 修改密码

选择“**系统工具->修改密码**”，可以修改登录准入设备的密码。

35.10.2 升级

选择“**系统工具->升级**”，可导入升级包，对准入设备软件进行升级，升级成功后需重启才生效。

35.10.3 设备重启

选择“**系统工具->重启设备**”，点击【**重启准入控制器**】按钮，可以将准入设备重启。

35.10.4 定时重启

选择“**系统工具->定时重启**”，可以启用定时重启功能。勾选“**启用定时重启**”

选项，并设置定时重启的日期（每天或者每周几）和时间，点击【**保存**】按钮即可。则设备将会在设定的时间时点设备会自动重启。

35.10.5 设置时间

选择“**系统工具->时间设置**”，可以修改准入设备的当前时间，修改后保存生效。

35.10.6 恢复出厂设置

选择“**系统工具->恢复出厂设置**”，可将准入设备的设置恢复到出厂时的初始设置。

对于 IPG-1000，也可通过 RESET 键将准入设备的设置恢复到出厂时设置。操作方法为：在设备开机状态下，按住该键五秒以上，随后重启设备。

35.10.7 配置管理

选择“**系统工具->配置管理**”，可实现当前准入设备配置的导入和导出。支持导入导出的配置包括：管理范围、控制范围、例外地址、主动认证、白名单、黑名单、访客列表。

35.10.8 注销

选择“**系统工具->注销**”，可注销本次网页管理界面的登录。

35.11 超级模式

当升级出错导致无法正常运行，或忘记准入设备登录密码等时，可以选择“**系统工具->超级模式**”进入超级模式进行清除登录密码或者恢复出厂操作。

使用超级模式时，需要计算机直连准入设备的管理端口，具体如下：

1) 使计算机 A 脱离内网环境，修改计算机 A 的 IP，让它能与准入设备通讯。如：

IP 地址：190. 190. 0. 1

子网掩码：255. 255. 0. 0

默认网关：可不填

2) 使用网线将计算机 A 和准入设备管理端口直连，在计算机 A 上运行浏览器，访问 http://190.190.190.190/reset，能进入到准入设备超级模式界面；

3) 选择“**清除登录密码**”，则当前准入设备的登录密码会被置为空；选择“**恢复出厂设置**”，则当前准入设备会恢复到出厂设置；

对于 1000 型号的设备而言，没有固定的管理端口，设置了正常连入网络使用的 IP 后，没有端口的 IP 为 190.190.190.190。

1000 设备如果忘记了登录密码，推荐的操作步骤为：

1) 导出当前备份；

IP 地址：190. 190. 0. 1

子网掩码：255. 255. 0. 0

默认网关：可不填

2) 将设备从网络中取出，通过 RESET 键恢复出厂设置；

3) 重新设置 IP 信息，并导入备份后，重新连入网络。

35.12 使用示例

企业相关情况：

1.内网所有的服务器（如 svn 服务器、jira 服务器、网络电话服务器等）均部署在 1 网段；

2.准入网关已采用串联的方式联入网络，IP 为 192.168.2.1，所有非 1 网段机器访问内网服务器都会经过准入网关。

需要实现：

1.员工电脑需要安装了 IP-guard 客户端，同时运行公司内部交流工具 RTX，方可访问内网的服务器；

2.网络打印机和 IP 电话要能正常使用；

3.针对个别领导，无需做以上限制；

4.对于偶尔过来公司交流的合作伙伴，其电脑不适宜安装 IP-guard 客户端，合作伙伴的电脑联入公司无线网络,会使用 192.168.3.1-192.168.3.20 的 IP 地址。

针对以上需求，可以如此设置

准入网关上的设置

① 准入网关配置->控制范围，设置控制范围：包含除了 1 网段外，整个公司的其他网络地址；
② 准入网关配置->例外规则，添加：网络打印机和 IP 电话的 IP 地址；
③ 准入网关配置->警告页面，选择系统警告页面，可按实际修改页面内容；
④ 准入网关配置->白名单，添加：不做限制的领导的机器 IP；
⑤ 访客登录管理->访客管理，添加访客，设置账号名、密码和备注后，在登录设置中，勾选"仅允许在指定 IP 上登录"，并输入指定的 IP：192.168.3.1-192.168.3.20；

IP-guard 控制台上的设置

① 工具->准入网关管理，添加准入网关 192.168.2.1；
② 安全检测->安全检测条件，添加新的安全检测条件：
输入条件名，如"RTX 安装"；
在弹出的安全检测条件设置界面，选择“程序检查”选项卡，勾选"必须启动以下全部程序"，并添加进程：RTX.exe；
③ 对所有客户端，安全检测->安全检测设置，添加一条策略：
安全条件选择前面添加的 RTX 安装"；
在策略右侧的属性中，勾选"阻断接入"；

设置完成后，开启准入网关的控制功能即可。

第三十六章. 安全网关

为了利用信息化技术提高工作效率，很多企业部署了 ERP/OA/CRM/PLM 等信息管理系统，这些应用系统储存着企业的各种重要资料，如客户信息、研发 计划、财务报表等等，所以它们对企业的重要性不言而喻。安全网关的价值正是在于严密保护这些应用系统的安全，不让企业机密轻易泄露。安全网关通过上传解密、下载加密及通讯加密，实现对加密文档上传、下载与传输过程中的全面防护。

安全网关的两大功能为：应用系统保护和文件共享保护。

应用系统保护

保护 OA、PLM、SVN 等应用系统服务器中的文件，未授权的用户和程序无法访问受保护的应用系统服务器，授权用户和程序可以正常访问，且上传文件到服务器该文件会被解密，从服务器上下载文件到本地该文件会被加密。

共享文件保护

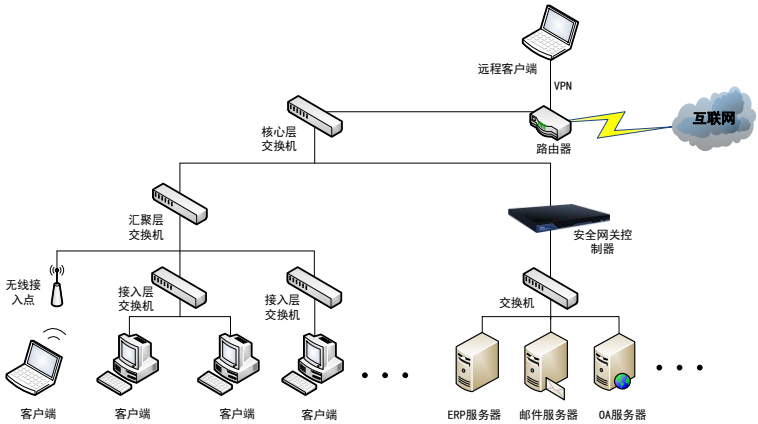
保护共享文件服务器，实现效果和应用系统保护类似，未授权的用户和程序无法访问受保护的共享文件服务器，授权用户和程序可以正常访问。同时可实现，上传文件到共享文件服务器某个目录该文件会被解密，从该目录下载文件到本地该文件会被加密，其他未指定目录下的文档上传和下载则不会做处理。

36.1 网络架构

安全网关的控制功能主要依托于硬件安全网关设备。安全网关设备的工作模式有两种：网桥模式和路由模式。

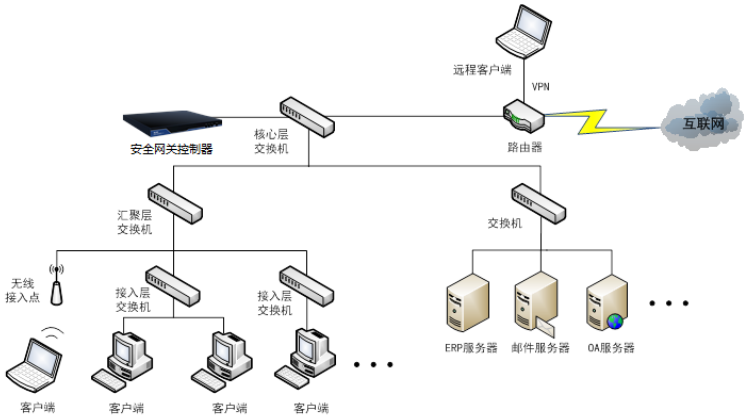
网桥控制模式

使用网桥模式，可以对网络结构和配置不做任何修改，直接将安全网关设备串接进网络中需要进行控制的地方，多数是重要的应用服务器或者网关前。



旁路控制模式

对核心交换机启用策略路由，对跨网段的访问进行控制。这种控制方式需要核心交换机支持策略路由。



36.2 设备介绍

安全网关设备有以下几种型号：1800S、2600S、3400S、3600S、4400S、4800S。

1800S：

四个 RJ45 端口，其中包含一组 BYPASS（ETH0 和 ETH1）；

管理端口为 EMP；

2600S：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

管理端口为 EMP1 和 EMP2；

3400S：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

管理端口为 EMP1 和 EMP2；

3600S：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

管理端口为 EMP1 和 EMP2；

4400S：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

两个 SFP 端口 ETH4 和 ETH5；

管理端口为 EMP1 和 EMP2；

4800S：

六个 RJ45 端口，其中包含两组 BYPASS（ETH0 和 ETH1，ETH2 和 ETH3）；

两个 SFP 端口 ETH4 和 ETH5；

管理端口为 EMP1 和 EMP2；

说明　　1.所有设备均支持千兆网络；

2.初始配置使用管理端口：

对于仅有一个管理端口（EMP）的设备，IP 固定为 190.190.190.190；

对于有两个管理端口（EMP1 和 EMP2）的设备， EMP1 的 IP 固定为 190.190.190.190，EMP2 的 IP 固定为

191.191.191.191；

3.BYPASS 功能，可以在控制器断电或死机的情况下，将控制器所连接的两端直接物理上导通，不影响网络的使用。

36.3 设备部署

36.3.1 设置设备 IP

根据实际情况选择控制方式，定好部署安全网关设备的位置，根据部署点为安全网关设备定好 IP，确定之后便开始设置安全网关设备 IP。

使用管理端口进行设置，具体步骤如下：

1) 使计算机 A 脱离内网环境，修改计算机 A 的 IP，让它能与安全网关设备通讯。如：

IP 地址：190. 190. 0. 1

子网掩码：255. 255. 0. 0

默认网关：可不填

2) 使用网线将计算机 A 和安全网关设备管理端口直连，计算机 A 上使用浏览器访问网址 http://190.190.190.190，能进入到安全网关设备管理登录界面；

3) 账号为 admin，密码初始为空，点击【确定】后进入管理界面；

4) 左侧菜单栏中，选择“**网络参数->基本设置**”，选择安全网关设备连入网络环境的接入模式，并设置相应的 IP 信息，设置完成后保存即可。

IP 修改成功后需要重启安全网关设备。

说明 设置 IP 时，2600S 及其以上型号的设备模式选择项中会多出一项“网桥（双机备份[主]）”。网桥模式下采用双机热备的主设备才需要用到此设置。

36.3.2 连入网络前设置

如果选择网桥部署模式，且安全网关设备部署在以 TRUNK 方式相连的交换机之间,则需要启用安全网关设备的 TRUNK 功能。具体可查看“**网络参数->Vlan 设置**”，如不是此种网络环境，无需启用。

如果选择网桥部署模式,且安全网关设备部署在二层交换机和三层交换机之间，二层交换机上的 PC 有多个网段（非 VLAN），且网关上也有对应这些网段的 IP，则需要启用多 IP 绑定配置。具体可查看“**网络参数->多 IP 配置**”，如不是此种网络环境，无需启用。

如果选择旁路部署模式，需要对交换机加上策略路由配置，具体请咨询技术工程师。

36.3.3 设备连入网络

设置完安全网关设备设备 IP 后，则可以将其连入事先计划好的部署点。

网桥模式

连接方法：使用设备的两个端口将其连入网络；

设备型号	使用的端口
1800S	使用 ETH0、ETH1、ETH2 中任两个；
2600S	使用 ETH0、ETH1、ETH2 中任两个；
3400S	使用 ETH0、ETH1、ETH2 中任两个；
3600S	使用 ETH0、ETH1、ETH2 中任两个。
4400S	使用 ETH0、ETH1、ETH2 中任两个；
4800S	使用 ETH0、ETH1、ETH2 中任两个；

旁路模式

连接方法：使用设备的一个端口连接交换机；

设备型号	使用的端口
1800S	只能使用 ETH0；
2600S	只能使用 ETH0；
3400S	只能使用 ETH0；

设备型号	使用的端口
3600S	只能使用 ETH0；
4400S	只能使用 ETH0；
4800S	只能使用 ETH0；

旁路模式支持将接入口由 ETH0 更改为其他端口，修改方法为：

选择“**系统工具->设置配置管理->高级配置**”，点击“**设置**”，输入以下配置内容

[PRP]

PRP=ethX

其中，X 代表具体的通讯端口号。

设备连入网络后，可以使用浏览器访问安全网关设备的 IP 地址，如 http://192.168.2.190，进入到安全网关设备管理登录界面。

36.4 基本信息

选择“**基本信息**”，可以进行“**开启/停止安全网关功能**”的操作。为了在部署过程中不影响工作，建议设置好安全网关设备的相关设置以及 IP-guard 安全通讯策略设置后，再启用安全网关功能。

在基本信息中，可查看安全网关设备的相关信息，包括控制功能信息，统计信息，安全网关信息，时间信息。

控制功能信息包括以下：

属性名称	说明
安全网关功能	当前安全网关设备的控制状态，分为：启用控制和停止控制；
受保护的应用系统 IP	受保护的应用系统 IP 信息；可在“**安全管理->应用系统保护**”中设置；
受保护的文件共享 IP	受保护的文件共享服务器 IP 信息；可在“**安全管理->文件共享保护**”中设置。

统计信息包括以下信息：

属性名称	说明

IP 总数	经过安全网关设备的 IP 总数；
在线数量	持续有通讯通过安全网关设备的 IP 数量；
阻止名称	被安全网关设备阻止的 IP 数量。

安全网关信息包括以下信息：

属性名称	说明
软件版本	安全网关设备的功能软件版本；
出厂版本	出厂时安全网关设备的功能软件版本；
当前版本	当前功能软件版本，初始为出厂版本，若进行过升级或降级操作，则为操作后的版本；
Web 版本	当前设备的 Web 前端页面版本；
运行平台	功能软件的运行平台信息；
硬件型号	安全网关设备的硬件型号信息；
校验结果	程序出厂校验结果，均为 OK；

时间信息包括以下信息：

属性名称	说明
当前时间	安全网关设备当前时间，出厂前都会调整至同网络同步；可在“**系统工具->修改时间**”中修改；
启动时间	安全网关设备启动的时间；
运行时间	安全网关设备最近一次开机到当前持续运行的时间。

36.5 网络参数

36.5.1 基本设置

选择“**网络参数->基本设置**”，可以设置安全网关设备连接模式以及 IP 地址。设备没有设置 IP 时需使用管理端口连接安全网关设备进行设置，设备已设置了 IP 则可直接在连入网络的状态下设置。设置并保存后需要重启安全网关设备才会生效。

36.5.2 Vlan 设置

在网桥运行模式下，如果安全网关设备部署在以 TRUNK 方式相连的交换机之间，需要启用安全网关的 TRUNK 功能

选择“**网络参数->Vlan 设置**”，勾选了“**开启 Trunk**”并添加 VLan 配置即可。

Vlan 配置信息包括以下：

属性名称	说明
ID	VlanID；
IP 地址	添加时需要输入一个对应 VlanID 下不会冲突的 IP 地址；
子网掩码	IP 地址的子网掩码；

提示

1.添加 VLAN 配置时，只能添加 Native Vlan 或 defaultVlan 之外的 VLAN，否则可能会导致网络不正常；

2.在以 TRUNK 的方式连接时，设备的 IP、掩码及网关的配置必须属于 Native Vlan 或 defaultVlan；

3. Native Vlan 或 defaultVlan 如果在交换机上不进行人为的修改时，那就是 Vlan 1。

36.5.3 多 IP 配置

在网桥运行模式下，如果安全网关设备部署在二层交换机和三层交换机之间，二层交换机上的 PC 有多个网段（非 VLAN），且网关上也有对应这些网段的 IP，则需要启用多 IP 绑定配置。

选择“**网络参数->多 IP 配置**”，勾选了“**开启多 IP 绑定**”并添加需要绑定的 IP 即可。

多 IP 绑定配置信息包括以下：

属性名称	说明
IP 地址	需要绑定的网段下不会冲突的 IP 地址；

子网掩码	IP 地址的子网掩码；

提示　在增加多 IP 绑定的配置时，对于安全网关设备 IP 所在的网段不能添加，否则会出现冲突。

36.5.4 转发规则设置

如果有部署在云端的服务器，想实现公网的机器访问云端服务器时，也受部署在企业内网的安全网关保护，则可以使用安全网关的转发功能。当启用该功能时，安全网关相当与网闸的作用，即云端服务器的 IP 地址不公开，用户仅知道安全网关的地址。访问时直接访问安全网关，然后由安全网关进行地址转换，跳转到云端服务器。

设置转发地址

安全网关 WEB 管理界面，选择“**网络参数->转发规则设置**”，点击“**转发地址设置**”，增加输入转发地址。

转发地址设置信息包括以下：

属性名称	说明
转发地址	只支持 IP，安全网关会占用这个 IP，需设置为与安全网关设备同一网段，不能设置重复的转发地址，可以设置多条转发地址；

设置转发规则

安全网关 WEB 管理界面，选择“**网络参数->转发规则设置**”，点击“**添加**”，设置转发规制，输入目标地址，目标端口、选择转发地址、转发端口、备注信息，保存。

转发规则设置信息包括以下：

属性名称	说明
目标地址	只支持 IP 地址，不支持域名，必须设置；
目标端口	目标地址的相应端口，必须设置；
转发地址	可选择转发地址设置中设置的网络地址，默认为空，必须设置；

转发端口	可下拉选择亦可手动输入，默认为相应端口；下拉选项包括：相应端口和历史端口；手动输入端口，可以任意设置。

提示 支持设置多条转发规则，一条转发地址也可以设置多个转发规则。

36.6 范围设置

设置安全网关功能的相关范围，此处的范围设置针对应用系统保护和文件共享保护同时生效。

36.6.1 管理范围

选择“**范围设置->管理范围**”设置安全网关设备的管理范围。

管理范围默认为空，即所有计算机有通信经过安全网关设备时，就会出现在安全网关设备对应的“**状态信息**”视图内。设置了管理范围后，则只有管理范围内的计算机有通信经过安全网关设备时，就会出现在安全网关设备对应的“**状态信息**”视图内。

36.6.2 控制范围

选择“**范围设置->控制范围**”设置安全网关设备的控制范围。

控制范围默认为空，即不对任何计算机做控制。设置了控制范围，此范围内的机器若使用非安全进程访问受保护的应用系统服务器，将会被阻止。

36.6.3 白名单

对于一些无法安装客户端的网络终端设备，例如网络打印机，可以在“**范围设置->白名单**”通过配置白名单的方式允许这些网络设备访问受保护的服务器。白名单支持 IP 地址以及 MAC 地址控制。

说明 仅支持与安全网关处于同一 VLAN 的机器设置为 MAC 地址白

名单。

36.7 应用系统保护

应用系统保护，结合加密客户端一起使用，实现指定进程方可访问受保护的应用系统服务器，同时，客户端本地密文上传至受保护的应用系统服务器，该文件会被解密，从应用系统服务器上下载文件至客户端本地，该文件会被加密。

36.7.1 保护范围

选择“**应用系统保护->保护范围**”设置安全网关设备保护的应用系统服务器。设置说明如下：

属性名称	说明
IP 地址及端口	设置应用系统服务器 IP 和端口参数，支持设置 IP 端和端口段，格式可参考如下： IP:端口，如 192.168.1.50:8080 IP:端口段，如 192.168.1.50:80-8080 IP 段:端口，如 192.168.1.50-192.168.1.60:80 IP 段:端口段，如 192.168.1.50-192.168.1.60:80-8080
备注	备注信息，可选填。

受保护的应用系统服务器只能通过安全进程访问，所以设置了受保护的应用系统服务器后，需要同时在 IP-guard 控制台对客户端启用加密，同时在“**加密->安全通讯设置->应用系统保护**”中设置启用“**对应用系统的保护**”并设置安全进程。

36.7.2 警告页面

警告页面主要作用在于：未使用安全进程范访问保护范围时，会被引导至警告页面，可在此页面得知相关的通知信息。

选择“**应用系统保护->警告页面**”进行设置。警告页面的配置项如下：

属性名称	说明

系统转发页面	警告页面默认为系统转发页面，已预先给定页面，系统警告页面提供访客登录操作。管理员可以修改页面内容，亦可重置为初始给定页面；
其他转发页面	如果想使用已有的 http 服务器网页，亦可以选择其他转发页面，输入网页地址；

36.7.3 绑定产品

默认情况下不绑定产品 ID，即只要是安全进程均可以访问受保护的应用系统。输入指定的产品 ID 进行绑定，则只有指定的产品 ID 的客户端可以通过安全进程访问受保护的应用服务器，其他产品 ID 的客户端则无法通过安全进程访问。

36.8 文件共享保护

文件共享保护，结合加密客户端一起使用，实现指定机器方可访问受保护的网络共享文档目录，同时，客户端本地密文复制到受保护的的网络共享文档目录，该文件会被解密，从受保护的网络共享文档目录上复制文件到客户端本地，该文件会被加密。

选择“**文件共享保护**”设置安全网关设备保护的文件共享服务器 IP 和端口信息。

文件共享保护各设置项说明如下：

设置项	说明
端口设置	默认端口：选择此项，通用的共享端口 139，445 会受保护；默认此项为选中； 全部端口：选择此项，所有端口都会受保护； 自定义端口：选择此项并输入端口号，则输入的端口号会受到保护；

禁止网络地址转换（NAT）	不勾选此项，在 NAT 设备(路由、无线路由等) 架构下，只要其中一台电脑设备能访问受保护的共享文件夹，该 NAT 设备下连接的其他电脑设备，也将被允许访问受保护的共享文件夹； 勾选此项，NAT 设备架构下的电脑设备，都无法访问受保护的共享文件夹； 此设置不支持虚拟环境架构：无论是否勾选此项，只要虚拟环境以 NAT 模式透过实体主机连接网络，则虚拟环境对共享文件夹的访问权限，将与主机相同。
IP 设置	设置受安全网关保护的文件共享保护服务器的 IP 地址，支持 ip 段输入，多个输入使用逗号隔开，如：192.168.1.1-192.168.1.100,192.168.2.102。

设置了受保护的文件共享服务器，需要同时在控制台对客户端启用加密，同时在“**加密->安全通讯设置->网络共享文档保护**”中设置启用“**对网络共享文档目录的保护**”并设置相关配置，方可正常使用此功能。

36.9 状态信息

状态信息中，可以查看当前经过准入设备的计算机的相关信息，包括：网络地址、启动时间、最后在线时间、白名单、阻止、最后阻止时间、是否允许访问共享文件夹。

属性名称	说明
网络地址	计算机的网络地址；
启动时间	计算机首次有通讯通过安全网关设备的时间；
最后在线时间	计算机最后有通讯通过安全网关设备的时间；
白名单	该计算机如果被设置为白名单，此列会显示“√”，此列空白代表该计算机不是白名单；
阻止	该计算机如果访问受保护的应用系统服务器受阻，此列会显示“√”，此列空白则表示该计算机没有受阻；
最后阻止时间	该计算机最近一次访问受保护的应用系统服务器受阻的时间；

允许访问共享文件夹	该计算机如果能正常访问受保护的共享文件服务器，此列会显示“√”，此列为空白则表示不允许访问共享文件服务器。

36.10 系统工具

36.10.1 修改密码

选择“**系统工具->修改密码**”，可以修改登录安全网关设备的密码。

36.10.2 升级

选择“**系统工具->升级**”，可导入升级包，对安全网关设备软件进行升级，升级成功后需重启才生效。

36.10.3 设备重启

选择“**系统工具->重启设备**”，点击【**重启安全网关**】按钮，可以将安全网关设备重启。

36.10.4 定时重启

选择“**系统工具->定时重启**”，可以启用定时重启功能。勾选“**启用定时重启**”选项，并设置定时重启的日期（每天或者每周几）和时间，点击【**保存**】按钮即可。则设备将会在设定的时间点会自动重启。

36.10.5 时间设置

选择“**系统工具->时间设置**”，可以修改安全网关设备的当前时间，修改后保存生效。

36.10.6 恢复出厂设置

选择“**系统工具->恢复出厂设置**”，可将安全网关设备的设置恢复到出厂时的初始设置。

36.10.7 配置管理

选择“**系统工具->配置管理**”，可实现当前安全网关设备配置的导入和导出。支持导入导出的配置包括：管理范围、控制范围、应用系统保护、文件共享保护、警告页面、绑定产品、白名单。

36.10.8 注销

选择“**系统工具->注销**”，可注销本次网页管理界面的登录。

36.11 超级模式

当升级出错导致无法正常运行，或忘记安全网关设备登录密码等时，可以进入超级模式进行清除登录密码或者恢复出厂操作。

使用超级模式时，需要计算机直连安全网关设备的管理端口，具体如下：

1) 使计算机 A 脱离内网环境，修改计算机 A 的 IP，让它能与安全网关设备通讯。如：

IP 地址：190. 190. 0. 1

子网掩码：255. 255. 0. 0

默认网关：可不填

2) 使用网线将计算机 A 和安全网关设备管理端口直连，在计算机 A 上运行浏览器，访问 http://190.190.190.190/reset，能进入到安全网关超级模式界面；

3) 选择“**清除登录密码**”，则当前安全网关设备的登录密码会被置为空；选择“**恢复出厂设置**”，则当前安全网关设备会恢复到出厂设置；

36.12 使用示例

企业相关情况：

1.OA 系统，主要为日常工作使用，该系统 IP 为 192.168.1.2，端口为 8080；

2.文件共享服务器，用于存放日常工作资料和文档，该文件共享服务器的 IP 为 192.168.1.1，其中\\192.168.1.1\private 目录中的存放着公司重要文档，不能随意外传；

3.安全网关已采用串联的方式联入网络，IP 为 192.168.2.6，所有机器访问 OA 系统和文件共享服务器都会经过安全网关。

需要实现：

1.员工仅能以 IE 浏览器访问 OA 系统，其他浏览器均不能使用，同时 OA 系统上的文档要保持明文，而员工从 OA 系统上下载文件到本地该文件需为密文；

2.仅特定的员工才可以访问文件共享服务器，且 private 目录下的文件，从共享中移动到本地时文件要被加密。

3.针对个别领导，无需做以上限制。

针对以上需求，可以如此设置

安全网关上的设置

① 安全管理->控制范围，设置控制范围包含整个公司的网络地址；
② 安全管理->应用系统保护，添加 IP 地址：192.168.1.2:8080；
③ 安全管理->文件共享保护，选择默认端口，添加 IP 地址：192.168.1.1；
④ 安全管理->白名单，添加不做限制的领导的机器 IP

IP-guard 控制台上的设置

① 对所有客户端启用加密；
② 对所有客户端，加密->安全通讯设置->应用系统保护，设置：
勾选"**启用对应用系统的保护**"；
添加安全进程为 iexplore.exe，加密模式为"**强制模式**"；
③ 针对特定的员工客户端，加密->安全通讯设置->网络共享文档保护，设置：
勾选"**启用对网络共享文档目录的保护**"；
添加安全网关地址：192.168.2.6
添加受保护的共享文档目录为：\\192.168.1.1\private

设置完成后，开启安全网关的控制功能即可。

附录 各模块功能说明

模块	子功能	功能详细介绍
基本功能	基本信息	统计客户端计算机基本信息，包括计算机名称，网络地址，操作系统，登录用户，当前状态等信息。
	基本控制	能够在控制端对网内任意客户端计算机进行锁定、关闭、重启、注销和发送通知信息等。
	基本日志	对客户端计算机的开机/关机，用户登入/登出，拨号等的事件记录。
	系统策略	设置客户端计算机的本地系统的操作权限，包括控制面板，计算机管理，系统管理，网络属性，插件管理等所有计算机属性。并能够将客户端计算机的 IP 与 MAC 地址进行绑定。
	策略报警	设置当客户端计算机系统状态变化时报警，包括硬件异动，存储设备和通讯设备插拔，软件安装卸载，系统信息和网络配置变化等。
	策略日志	记录客户端计算机在执行策略时的操作日志，如禁止、报警、警告和锁定计算机等。
	安全检测的检测功能	检查客户端的状态是否与控制台设置的检测条件相符，检测结果可以在控制台和客户端显示。检测内容包括:杀毒软件使用、补丁、软件安装、程序使用、系统服务状态和其他条件（注册表等）。
应用程序管控	应用程序日志	详细记录应用程序的启动、退出。 记录窗口切换和标题变化，并可以按时间范围，计算机范围，应用程序名称，应用程序路径、窗口标题等多种查询条件进行查询。
	应用程序统计	多种方式统计各种应用程序的使用时间和使用百分比，并以列表和图表两种方式显示。统计方式包括按应用程序类别、名称、明细统计以及按计算机分项统计。
	应用程序控制	可在指定时间内限制指定计算机对指定程序应用，并可在受限程序运行时向控制台报警。

	软件安装管理	控制软件的安装和卸载。
网页浏览管控	网页浏览日志	详细记录每台计算机（用户）浏览网页的网址和标题，并提供查询功能。
	网页浏览统计	多种方式统计网页浏览情况，以列表和图表两种方式显示统计结果。统计方式包括按网站类别、明细统计以及按计算机分项统计。
	网站浏览控制	对指定的客户端在指定的时间范围内访问指定的网站或者网址进行管控。
	上传控制	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。
网络流量管控	网络流量统计	统计客户端在指定时间范围内的网络通讯流量，包括通讯总流量和每种网络协议、地址的详细流量。统计方式包括按地址、协议和端口的类别或明细统计以及按计算机分项统计。
	网络流量控制	通过设置指定时间范围，网络地址和端口范围、发送和接收方向来限制计算机流量速度，保障网络带宽资源的合理使用。
文档操作管控	文档操作日志	记录本机上所有文档操作信息，包括在硬盘、移动存储、网络路径、共享目录上所有文档的创建、访问、修改、复制、移动、删除、恢复、重命名等操作；并可按日志记录的信息进行查询。
	共享文档操作日志	记录本机的共享文档被其它机器的用户操作的信息。
	文档操作控制	控制客户端计算机在指定的磁盘类型或者网络上对指定文档的读取，修改和删除操作的权限。
	文档备份	为防止重要文档被误删或者篡改，可以在文档内容被改变或破坏前进行备份。
文档打印管控	打印操作日志	详细记录所有打印操作的时间、终端、用户、应用程序、页数、打印机类型和名称，并能够根据时间，文件名，计算机等信息进行查询。
	打印内容记录	完整记录在所有类型打印机上的文档打印映像，查看打印的原始内容。

	打印控制	控制应用程序打印权限，阻止非法应用程序打印； 控制终端打印权限，限制终端对指定类型打印机或指定打印机的使用。 备份打印内容。
	水印控制	保护知识产权，在打印的内容上添加水印。
屏幕监控	实时屏幕快照	实时查看客户端的屏幕快照，支持对同时多个用户登录的监控，支持对多显示器的监控，可同时对一组计算机进行集中监控
	屏幕历史记录	记录客户端的历史屏幕画面，根据不同应用实现变频记录；配合日志记录查看当时的屏幕情况；支持将屏幕历史转存为通用视频文件，被其他常用工具播放。
远程维护	远程维护	实时查看客户端的运行信息，远程分析客户端运行状况和故障原因，并可以执行远程操作，帮助解决远程问题。
	远程控制	远程连接到客户端计算机的桌面，直接操作客户端，方便进行远程协助或操作示范。
	远程文件传送	远程打开指定客户端的文件夹，传送文件和搜集故障样本。
设备管控	设备控制	控制客户端各种设备类型的使用权限。 可以禁止任何新增加的设备。 通讯设备：串/并口、SCSI、1394、蓝牙、红外线、MODEM、直接对联线等； 存储设备：软驱、光驱、刻录机、磁带机，移动存储设备等； 通讯设备：串/并口、SCSI、1394、蓝牙、红外线、MODEM、直接对联线等； USB 设备：USB 键盘、鼠标、MODEM、映像设备、存储、光驱、硬盘和其他 USB 设备； 网络设备：无线网卡、即插即用网卡、虚拟网卡等； 其他设备：声音设备、虚拟光驱等。 可以禁止任何新增加的设备。
网络控制	网络通讯控制	通过对网络通讯方向、IP 地址范围、网络端口范围的设置，管理内网计算机使用网络的权限； 控制指定客户端的网络通讯； 控制指定协议和地址范围的网络通讯； 控制与外来计算机的网络通讯。

	入侵检测	检测网络内是否有非法计算机接入并给出报警，同时阻止非法计算机接入网络。
	安全检测的网络控制功能	根据安全检测结果，对不符合安全检测条件的客户端进行断网控制，可以设置例外地址。一旦机子符合安全检测条件，会自动放开控制。
邮件管控	邮件日志	记录标准协议邮件、Exchange 邮件收发的收件人、发件人、正文及完整附件；记录网页邮件、Lotus 邮件发送的收件人、发件人、正文及完整附件。
	邮件控制	通过邮件的发送人、接收人、主题、附件及邮件大小等条件限制，控制发送邮件的账户，阻止向不被允许的收件人发送邮件，阻止发送特定名称或者超出规定大小的附件。
即时通讯控制	即时通讯日志	完整记录 MSN、QQ、TM、RTX、ICQ、Yahoo 通、Sina UC、PoPo、Skype、Lotus Sametime、阿里巴巴贸易通，阿里旺旺等主流即时通讯工具的对话时间，对话人、对话内容等。
	即时通讯传输文档控制	通过文档名称和大小条件的设定，控制通过即时通讯工具向外发送文档，并可以在传输的过程中备份文档（请在文档操作管控中查询）。
资产管理	资产管理	自动扫描并完整记录每台终端软硬件资产信息，详尽记录资产变更信息，可自定义资产属性进行辅助信息管理； 通过自定义资产类别对非 IT 资产进行管理。
	版权管理	对客户端计算机安装的软件进行统计和分类，记录软件采购，统计付费软件的授权使用情况。
	系统补丁管理	自动扫描客户端的微软产品补丁安装情况； 根据策略下载指定的补丁并进行自动分发和安装。
	安全漏洞检查	自动扫描客户端的安全漏洞情况，并提供分析报告和解决方案。
	软件分发	自动部署和安装软件、执行程序或者派送文档，支持断点续传，支持后台安装和交互安装。

	软件卸载	自动扫描目标软件是否安装，执行卸载软件任务。
移动存储管控	移动存储审计	识别曾接入到网内的所有移动存储设备，记录设备详细信息，掌握移动存储设备使用情况。 支持对移动存储设备进行分类管理，可将企业内部移动存储设备按部门划分。
	移动存储授权	控制每一个移动存储设备的读写权限，禁止外来移动存储设备在企业内部使用。
	移动存储加密	将普通移动存储设备格式化为加密盘，只能在内部使用，如加密盘丢失，内部文件也无法打开；将复制到移动存储上的文件自动加密，加密文档只能在授权计算机上解密使用。
	设备注册管理	对移动存储设备的生命周期管理，包括对移动存储设备的注册、分类、挂失、注销等。
报表系统	风险审计报表	统计表：从多种维度统计分析每一项操作行为，包括打印、电子邮件、移动存储、文档操作、程序应用、上网浏览、即时通讯等，帮助快速掌握内网计算机的应用情况。 趋势表：直观展现用户行为的变化趋势。 征兆表：分级征兆预警机制，当行为达到设定的阈值时，自动记录征兆事件及其级别，提醒管理人员关注和处理。
敏感内容识别	敏感内容定义	支持通过关键字和正则式等多种组合定义敏感信息。 支持从样本文档分析提取特征信息，定义敏感信息。
	敏感内容发现	支持通过本地扫描和远程扫描发现敏感信息。 通过全盘扫描在全网内统一检查敏感内容，发现敏感信息。
	敏感内容监视	新建和下载文档到计算机，发现敏感内容，触发报警。 含敏感信息的文档通过流通渠道外传时，发现敏感内容，触发报警。

	敏感内容保护	当含有敏感信息的文档发生外传行为时（如拷贝到移动盘、网络盘，发送邮件、IM传送等），进行阻断或审计。 创建、编辑含有敏感信息的文档时，自动对文档进行加密保护。
文档云备份	自动备份	对终端计算机上的数据进行备份，统一上传到文档云备份服务器进行集中存储和管理。支持定期备份、触发式备份以及全盘扫描备份；备份版本可以根据需要保留一个文档或多个备份版本。
	分级管理	可以对不同用户划分不同的文档管理权限以及划分相应的管理范围，防止无关人员查看重要文档。
	备份审计	可以对文档云备份的所有操作进行日志记录，包括开始上传文件/上传文件成功/上传文件失败/开始扫描/扫描结束等，管理员可以在日志中查看详细的操作过程。
V+ 全向文档加密	透明加密	采用高强度加密技术，对文档进行强制透明加密，使得无论何时何地文档都以密文形式存在。在授权环境中，文档能自动解密,丝毫不影响用户原有的使用习惯；在非授权环境中，加密文档则无法正常打开和使用。在加密文档的使用过程中，能够防止用户通过剪贴板,截屏,虚拟打印等方式窃取加密文档内容。
	权限控制	根据文档的重要程度不同，可将加密文档划归不同的安全区域和级别，以便让不同部门和职位的用户使用，建立分部门分级别的保密机制。 用户可调整文档的区域和级别，对重要文档可采取提高其级别的方法来禁止普通用户的使用。
	离线授权	根据实际需要授予用户离开授信环境后的加密文档的使用权限。 能够单独设置用户离线时能使用的加密软件类别和文档使用权限。
	外发管理	能够对需要进行外发的文档进行加密控制,只允许授权的外部人员查看,防止二次泄密。 能够指定外发文档的查看期限、次数以及使用权限。

	防灾备份	备用服务器设计能够应对各种硬件和系统崩溃的情况，保证加密系统连续运转；同时采用的文档备份服务器能够以明文完整备份所有加密文档，即使意外出现，用户的文档依然完整可用。
	多级审批	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。
加密只读	只读加密	对重要文档进行加密保护。在只读授权环境下，可以打开加密文档，但是无法对文档进行修改和另存为；非只读授权环境下，无法打开加密文档。 在加密文档的使用过程中，能够防止用户通过剪贴板,截屏,虚拟打印等方式窃取加密文档内容。
	权限控制	根据文档的重要程度不同，可将加密文档划归不同的安全区域和级别，以便让不同部门和职位的用户使用，建立分部门分级别的保密机制。 用户可调整文档的区域和级别，对重要文档可采取提高其级别的方法来禁止普通用户的使用。
	离线授权	根据实际需要授予用户离开授信环境后的加密文档的使用权限。 能够单独设置用户离线时能使用的加密软件类别和文档使用权限。
加密安全网关	应用服务器保护	只有安全进程才可以访问受保护的服务器。没有安装客户端的机子，或者没有使用安全进程访问受保护的服务器会被阻止。
	网络共享文件夹保护	对网络共享文件夹，可以实现上传加密文件自动解密，下载文件自动加密。
网络准入控制	准入控制	不合规的计算机不能访问受保护的服务器。 对于不合规的计算机，可设置为白名单或者提供访客账号供临时访问。
	安全检测的准入控制功能	根据安全检测结果，对不符合安全检测条件的计算机进行准入控制，可以设置例外地址。 一旦机子符合安全检测条件，会自动放开控制。

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.com

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

电话（香港）：+852-2950 0067

传真（香港）：+852-2950 0709

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。

TEC Solutions Limited

滔信科技