

**IP-guard产品测试用例**

目录

[一、IP-guard功能模块简介 1](#_Toc10483)

[二、测试环境介绍 4](#_Toc4113)

[2.1 IP-guard系统的组成架构 4](#_Toc30148)

[2.2 产品测试软硬件配置 4](#_Toc32503)

[2.3 测试软件版本说明 5](#_Toc21035)

[三、产品安装及卸载 5](#_Toc29464)

[3.1 安装部署总览 5](#_Toc19430)

[3.2 安装SQL Server 5](#_Toc11564)

[3.2.1 SQL Server安装前准备 5](#_Toc10998)

[3.2.2 SQL Server安装步骤 10](#_Toc24245)

[3.3 部署IP-guard服务器 14](#_Toc18003)

[3.3.1 安装程序及注册码获取渠道 14](#_Toc10330)

[3.3.2 安装服务端 15](#_Toc4939)

[3.3.3 服务端注册 16](#_Toc19541)

[3.3.4 设置检验码 17](#_Toc27858)

[3.4 安装IP-guard控制台 18](#_Toc15614)

[3.5 安装IP-guard客户端 18](#_Toc14918)

[3.5.1 创建客户端 18](#_Toc12533)

[3.5.2 客户端安装 19](#_Toc6528)

[3.6 卸载安装程序 21](#_Toc29065)

[3.6.1 客户端卸载 21](#_Toc3614)

[3.6.2服务器和控制台卸载 21](#_Toc32064)

[四、功能操作测试 22](#_Toc2154)

[4.1基本模块 22](#_Toc10155)

[4.1.1 了解控制台的基本操作 22](#_Toc26711)

[4.1.2 熟悉主体功能 23](#_Toc26871)

[4.1.3 设置第一条策略 24](#_Toc1371)

[4.1.4 查看操作日志及基本事件 25](#_Toc25297)

[4.1.5 终端安全检测 26](#_Toc19001)

[4.1.6 策略管理及日志导出 27](#_Toc3478)

[4.1.7审计管理员操作日志 28](#_Toc11251)

[4.2移动存储管控 29](#_Toc22509)

[4.2.1 移动存储设备的使用信息及分类管理 29](#_Toc15744)

[4.2.2 移动存储设备注册管理 30](#_Toc5173)

[4.2.3移动存储设备读写权限控制 31](#_Toc28153)

[4.2.4制作企业内部加密U盘 32](#_Toc10869)

[4.2.5公私两用U盘加解密的设置 33](#_Toc11605)

[4.3应用程序管控 34](#_Toc31404)

[4.3.1应用程序使用审计 34](#_Toc21490)

[4.3.2应用程序使用管控 35](#_Toc31406)

[4.3.3应用程序安装卸载管理 36](#_Toc19325)

[4.4 网络控制 37](#_Toc13306)

[4.4.1非法终端访问控制 37](#_Toc10538)

[4.4.2部门访问隔离 38](#_Toc21969)

[4.4.3阻断非法端口 39](#_Toc10216)

[4.5 资产管理 40](#_Toc6835)

[4.5.1 IT资产管理（硬件） 40](#_Toc29583)

[4.5.2 IT资产管理（软件） 41](#_Toc20462)

[4.5.3软（硬）件变更统计 42](#_Toc21993)

[4.5.4软件分发管理 43](#_Toc17124)

[4.5.5补丁管理 44](#_Toc20123)

[4.5.6软件卸载管理 45](#_Toc1325)

[4.6 远程维护 46](#_Toc8005)

[4.6.1实时查看客户端计算机的运行状态 46](#_Toc30404)

[4.6.2控制台远程控制客户端 47](#_Toc8549)

[4.6.3远程文件传送 48](#_Toc26326)

[4.7 文档加密 49](#_Toc31862)

[4.7.1文档加密基本设置 49](#_Toc10223)

[4.7.2加密文档安全区域与访问权限 50](#_Toc17894)

[4.7.3加密文档直接解密、外发 52](#_Toc6800)

[4.7.4加密文档申请解密流程设置 53](#_Toc8658)

[4.7.5安全密码设置 54](#_Toc2423)

[4.7.6临时离线申请 55](#_Toc29367)

[4.7.7长期离线设置 57](#_Toc19740)

[4.7.8外发文档设置 58](#_Toc22379)

[4.7.9外发文档浮水印设置 59](#_Toc6198)

[4.7.10邮件白名单解密设置 60](#_Toc29212)

[4.7.11容灾时间设置 61](#_Toc7491)

[4.7.12备用服务器设置 62](#_Toc2100)

[4.7.13加密文档备份服务器设置 63](#_Toc32099)

[4.7.14业务系统上传解密下载加密 64](#_Toc19010)

[4.8 慧眼风险审计报表 65](#_Toc13069)

[4.8.1统计表 65](#_Toc19557)

[4.8.2趋势表 69](#_Toc32612)

[4.8.3综合数据统计表 72](#_Toc15045)

[4.8.4征兆事件统计表 73](#_Toc22324)

[4.8.5征兆事件趋势表 74](#_Toc29472)

[4.8.6周期报表 75](#_Toc29923)

[4.8.7邮件报告设置 76](#_Toc13173)

[五、测试总结 77](#_Toc7896)

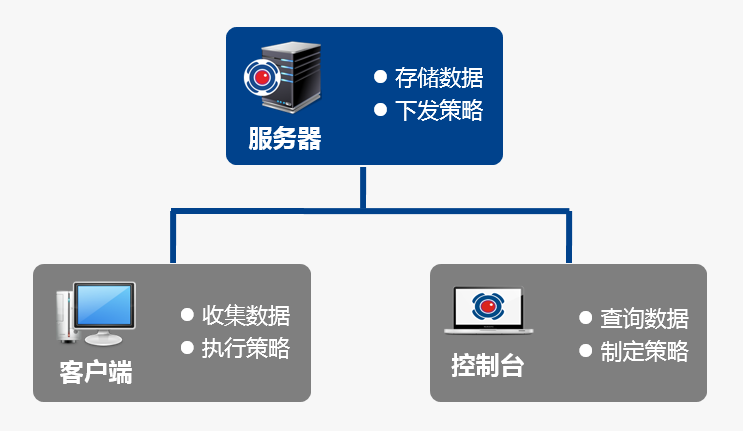
# 一、IP-guard功能模块简介

IP-guard企业信息监管系统，是一款领先的内网安全软件，它能够协助企业解决最棘手的内网安全问题，借助IP-guard强大的功能，企业能够有效地进行用户行为管理，防范信息泄露，营造健康安全的网络环境，下面对功能模块进行简单介绍。

|  |  |
| --- | --- |
| 功能模块 | 功能简介 |
| 基本模块 | 1. 基本模块是IP-guard系统架构的基础，能够收集客户端的基本信息，为客户端的组织化管理提供平台，并构建合理的账户管理机制； 2. 控制台可以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操作； 3. 记录客户端计算机的开机/关机，用户登入/登出，拨号等的事件； 4. 禁止用户对计算机系统的操作权限，并能够绑定计算机的IP/MAC地址； 5. 检查计算机的杀毒软件、软件安装、系统补丁、域用户身份等项目是否符合安全检测的条件； 6. 设置当客户端计算机系统的状态变化时进行及时报警； |
| 文档操作管控 | 1. 记录文档从创建到删除过程中所有操作； 2. 控制终端对文档的读取、修改、删除等操作； 3. 对机密文档的敏感操作进行自动备份。 |
| 文档打印管控 | 1. 限制打印机的使用； 2. 记录打印内容； 3. 设置打印浮水印、二维码。 |
| 设备管控 | 1. 管理U盘、移动硬盘、光驱、刻录机等移动存储设备的使用，防止内部信息被随意带出公司； 2. 管理通讯接口、无线网卡、3G网卡、即插即用网卡等网路设备的使用，避免非法外联带来的风险； 3. 管理声卡、摄像头等设备的应用，避免工作时间分散注意力； 4. 限制其他一切外设的使用，规范企业的外设使用。 |
| 移动存储管控 | 1. 记录移动存储设备的使用，以及移动存储的文档操作日志； 2. 对移动存储设备进行注册管理； 3. 对移动存储设备进行读、写权限控制； 4. 对可指定移动存储设备进行格式化为加密盘，只能在内部使用； 5. 对复制在移动存储设备的文件进行自动加密，加密文档只能在授权的计算机上解密使用。 |
| 应用程序管控 | 1. 可自动统计用户各种应用程序的使用情况； 2. 对工作外的应用程序可分时间段限制； 3. 可禁止运行特定程序； 4. 管理终端电脑的软件安装和卸载。 |
| 屏幕监控 | 1. 可实时查看单用户或多用户的桌面行为； 2. 查看屏幕历史，并能将屏幕记录导出播放； 3. 可灵活设置屏幕记录频率。 |
| 网络控制 | 1. 限制外网计算机与内网计算机的通讯，建立网络隔离区； 2. 开放内网计算机之间的相互访问。 |
| 网页浏览管控 | 1. 可查看内网计算机的所有网页浏览行为； 2. 禁止或分时段限制访问特定网站； 3. 禁止通过HTTP、Ftp协议上传文件。 |
| 即时通讯管控 | 1. 记录即时通讯工具的所有聊天记录； 2. 对通过即时通讯工具外发的文档进行备份； 3. 可禁止通过即时通讯工具外发文档。 |
| 邮件管控 | 1. 记录所有发出邮件的内容； 2. 限定用户只允许使用指定邮箱发送邮件； 3. 强制设置用户发送邮件时必须要抄送给指定人员。 |
| 流量管控 | 1. 统计员工计算机的网络流量； 2. 分时段控制计算机的网络流量。 |
| 资产管理 | 1. 统计计算机软硬件及其它资产的使用及变更情况； 2. 及时为网内所有计算机同步安装最新微软补丁； 3. 集中部署ERP、OFFICE等软件到客户端计算机，或集中运行脚本程序； 4. 集中卸载公司禁止的软件。 |
| 远程维护 | 1. 管理员在控制台远程查看受控计算机基本信息及运行状态，分析故障原因并进行相关维护操作； 2. IT管理员直接操作客户端计算机快速排除故障或进行操作演示； 3. IT管理员从客户端收集故障样本，或分发文件到客户端计算机。 |
| 敏感内容识别 | 1. 建立敏感信息分类库 2. 扫描终端包含敏感信息的文档 3. 含敏感信息的文档外传控制 4. 敏感文档新建加密、落地加密 |
| 文档云备份 | 1. 支持即时备份和定期备份终端的重要文件 2. 支持备份一个文件的多个历史副本 3. 支持对备份的文件进行预览和搜索 4. 可将备份的文件快速恢复到终端计算机 5. 支持对备份文件的操作进行操作审计 |
| 文档加密 | 1. 重要文档从生成即强制加密，保护文档安全 2. 对加密文档，限制剪切板、截屏、打印等操作 3. 对不同部门、不同级别的人员分配不同的加密文档权限，达到部门隔离、等级隔离的效果 4. 严格控制解密、外发管理，限制外发文件的查看期限、查看次数等，防止二次泄密 5. 邮件白名单自动解密文档，为加密文档流通提供便利 6. 离线权限设置，保证移动办公的文档安全 7. 通过容灾时间和备用服务器保证终端在遇到IP-guard服务器故障和网络故障时依然能够运行 8. 通过明文备份服务器，防范终端加密文档损坏的风险 9. 敏感信息文档落地加密 |

# 二、测试环境介绍

## 2.1 IP-guard系统的组成架构



* 服务器：下发策略、存储数据；
* 客户端：执行策略、收集日志数据并上传至服务器；
* 控制台：设置策略及查看数据。

## 2.2 产品测试软硬件配置

搭建IP-guard测试环境请参考如下建议配置：

* 将IP-guard服务端安装在性能较好的服务器上；
* 将客户端软件安装需要管控的计算机上；
* 将管理控制台安装在管理员电脑上。

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 硬件环境 | 软件环境 | 备注 |
| **服务器** | **CPU：**双核或双CPU；  **内存：**4G或以上内存；  **硬盘：**200GB以上的硬盘空间；  **网卡：**1000MB 网卡； | **操作系统：**Windows 2003 Server SP1 简体中文版或Windows 2008 Server SP1；  **数据库：**Microsoft SQL Server 2005 SP4或Microsoft SQL Server 2008 SP1； |  |
| **客户端** | **CPU：**单核或双核CPU；  **内存：**2G或以上内存；  **硬盘：**50GB或以上的硬盘空间；  **网卡：**100MB 网卡； | **操作系统：**Windows XP、Windows 7、Windows 8、Windows 10版本均可； |  |
| **控制台** | **CPU：**单核或双核CPU；  **内存：**1G或以上内存；  **硬盘：**20GB或以上的硬盘空间；  **网卡：**100MB 网卡； | **操作系统：**Windows XP、Windows 7、Windows 8、Windows 10版本均可； |  |

## 2.3 测试软件版本说明

此测试用例适用于大部分IP-guard正式发行版本，我们依据2020年1月份的发布版【4.35.0909.0】进行编制，如发现操作步骤与本测试用例不一致，请以系统操作界面为准，如若遇到操作困难，您可以先联系我司的销售人员或技术人员，我们将协助配合测试。

# 三、产品安装及卸载

## 3.1 安装部署总览

## 3.2 安装SQL Server

**SQL Server安装测试的环境：**

操作系统：Windows Server 2008

数据库：SQL Server 2008 R2

### 3.2.1 SQL Server安装前准备

在运行 SQL Server 2008 R2安装程序之前，可能需要手动安装如下几个组件：

1. Windows Installer 4.5

2、.NET Framework 3.5 (VISTA以上版本，请使用.NET Framework 3.5 SP1)

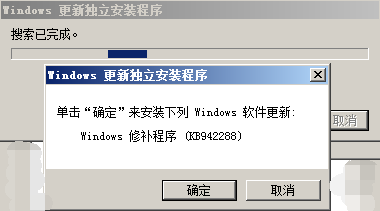
3、Windows Power Shell

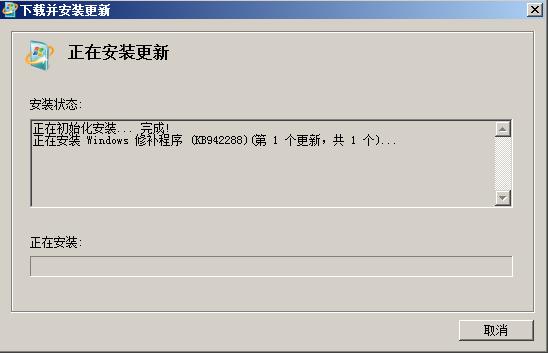
注意：

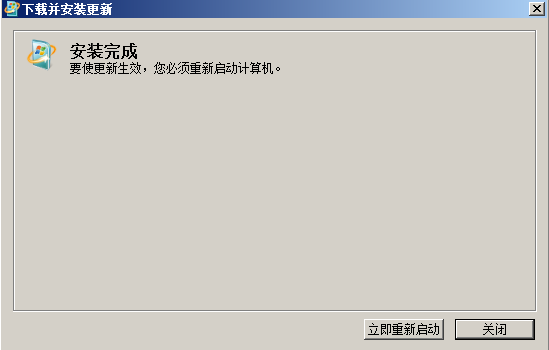
Windows Installer 4.5 和.NET Framework 3.5（或 .NET Framework 3.5 SP1）安装完成后，需要重启系统才能开始SQL Server 2008 R2的安装。

安装Windows Installer

运行Windows Installer安装程序，安装步骤如下：

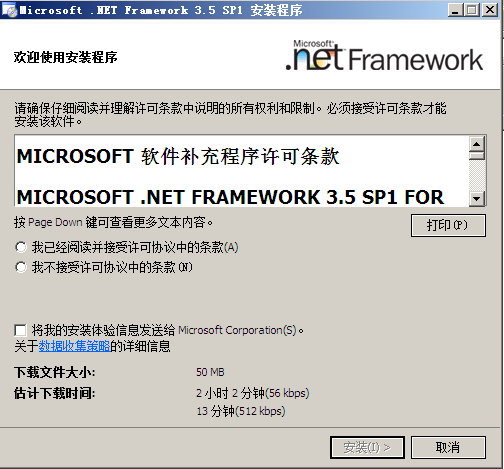






安装.NET Framework

运行.NET Framework安装程序，安装过程需要连接互联网，安装步骤如下：







安装Windows PowerShell

Windows Power Shell安装步骤如下：

1. 打开‘控制面板’
2. 打开‘程序和功能’
3. 打开‘启动或关闭Windows功能’
4. 勾选‘Windows Power Shell’选项，进行安装



### 3.2.2 SQL Server安装步骤

下面以SQL Server 2008 R2 Express为例子进行安装演示。

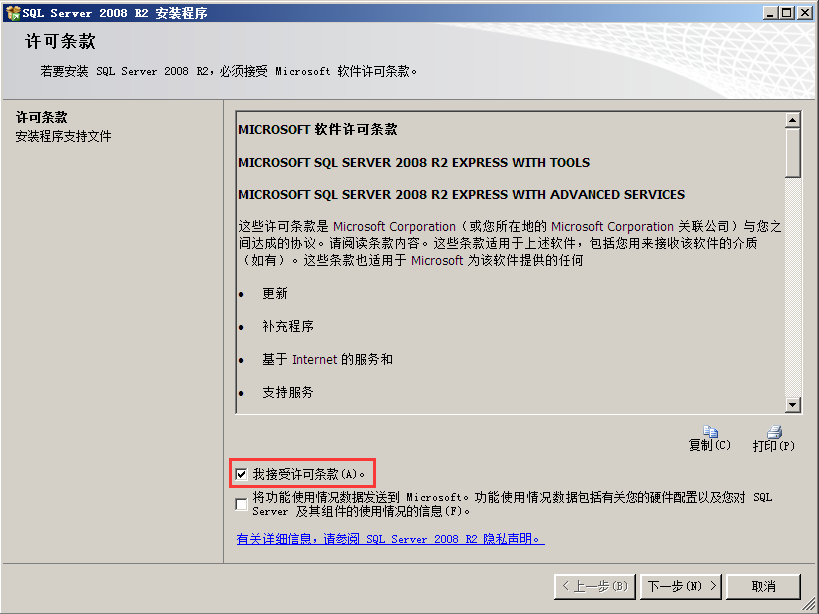
* **Step 1：**运行SQL Server 2008 R2安装程序，解压后，可能弹出无法继续安装的提示信息，安装这些程序的步骤，请参考4.2.1章节内容；



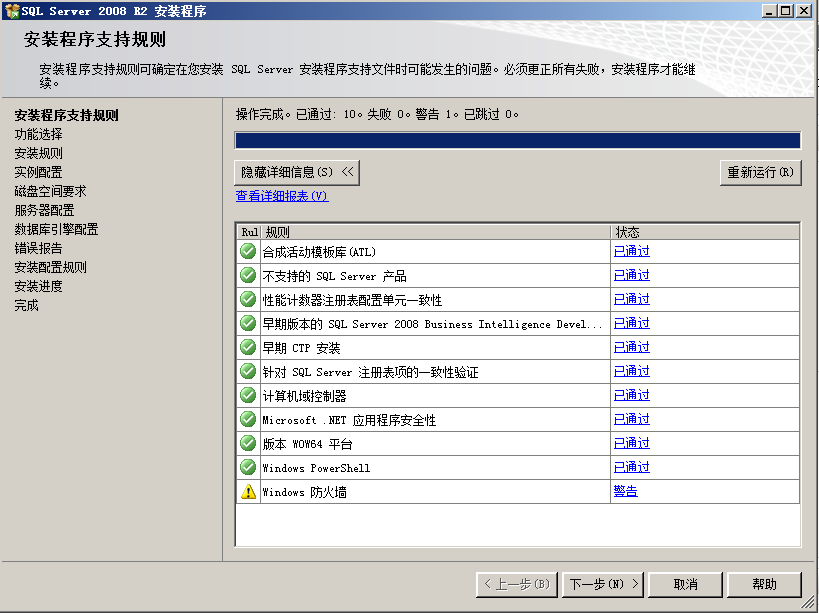
* **Step 2：**安装完成.NET Framework和Windows Installer后，再运行SQL Server 2008 R2安装程序，在弹出安装中心交互页面中，点击‘全新安装或向现有安装添加功能’；



* **Step 3：**勾选‘我接受许可条款’，单击‘下一步’按钮继续；

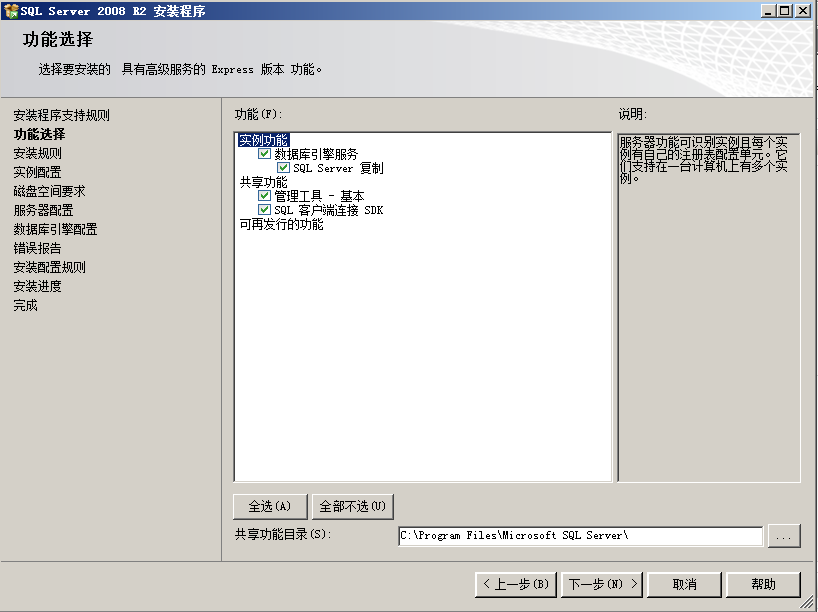


* **Step 4：**安装程序规则检查，检查通过后，单击‘下一步’按钮继续；

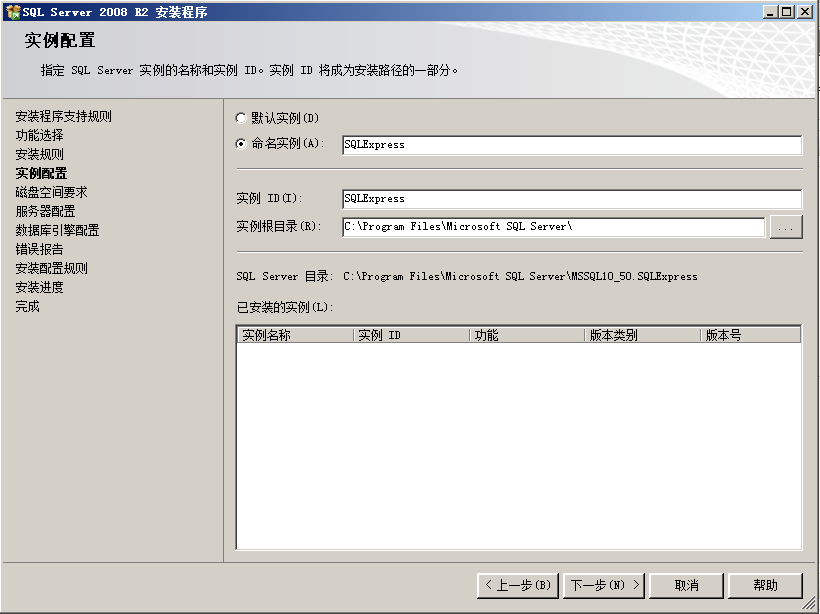


注意：如果操作系统未安装Windows PowerShell，无法通过安装程序规则检查，安装Windows PowerShell方法请参考4.2.1章节的内容。

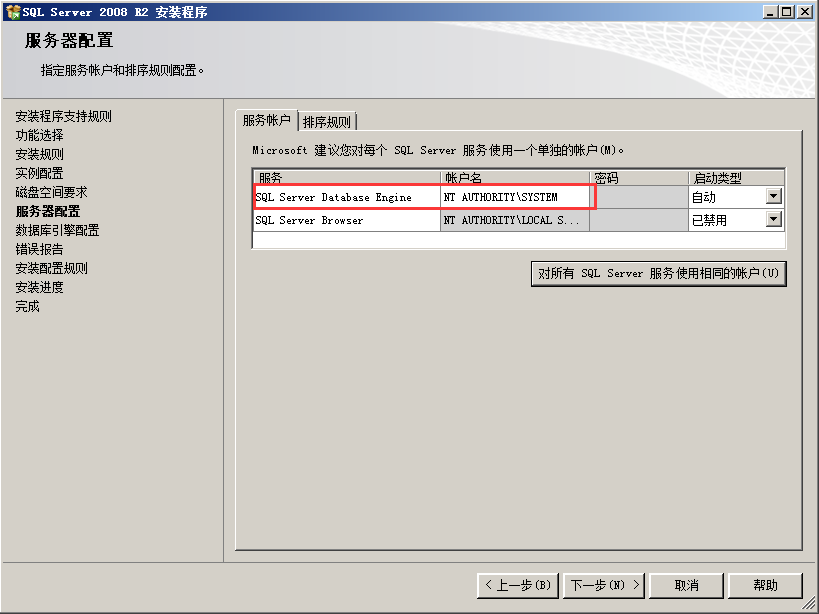
* **Step 5：**功能选择，勾选全部 点击‘下一步’按钮继续；



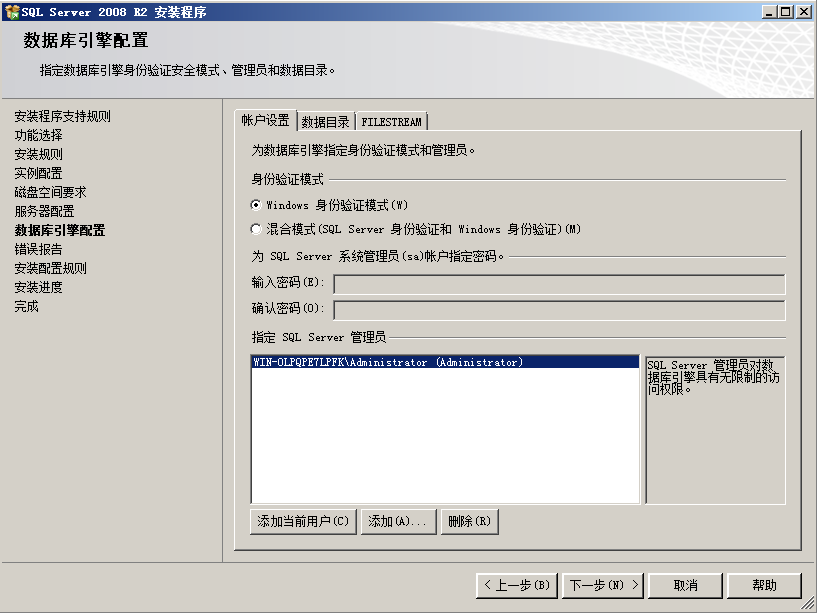
* **Step 6：**实例配置，维持默认命名实例即可，点击‘下一步’按钮继续；



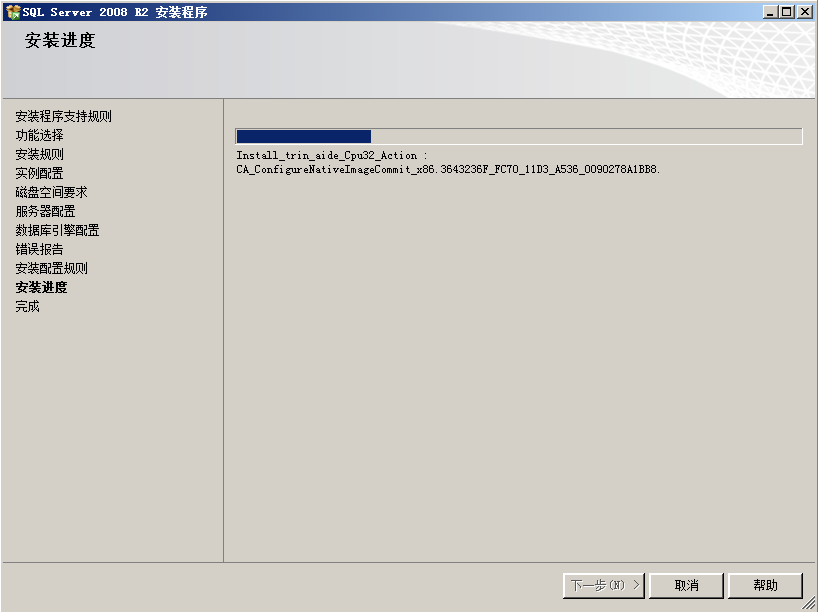
* **Step 7：**服务器配置，SQL Server服务账户必须使用NT AUTHORITY\SYSTEM，排序规则维持默认（不区分大小写），单击‘下一步’按钮继续；

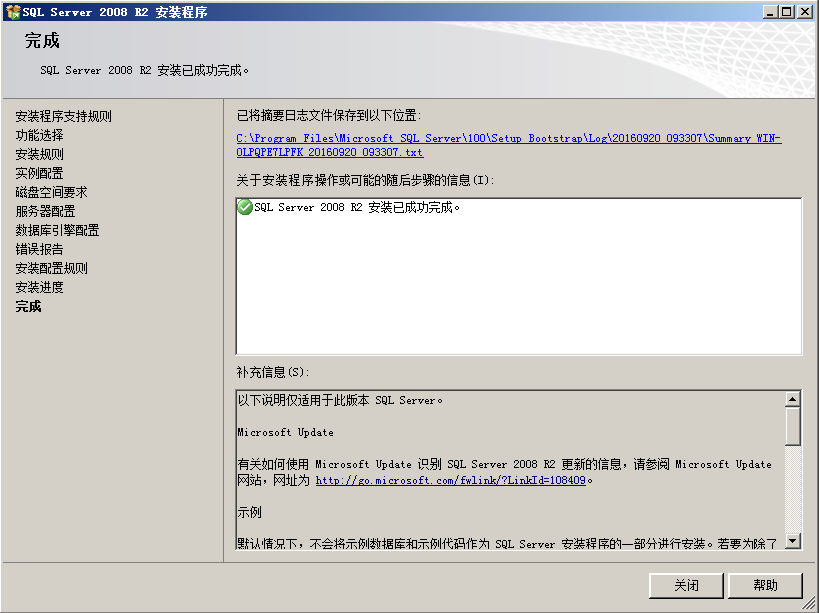


* **Step 8：** 数据库引擎配置，身份验证模式、管理员和数据目录，都可维持默认，点击‘下一步’按钮继续；



* **Step 9：**执行安装进度，至此，SQL Server 2008 R2安装完成；





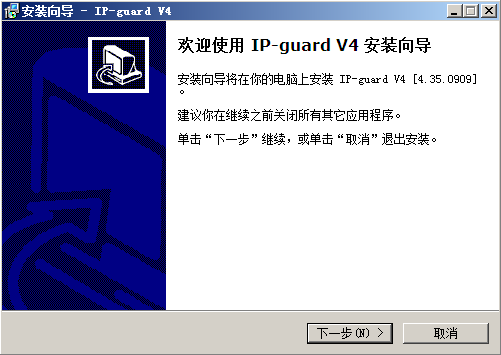
## 3.3 部署IP-guard服务器

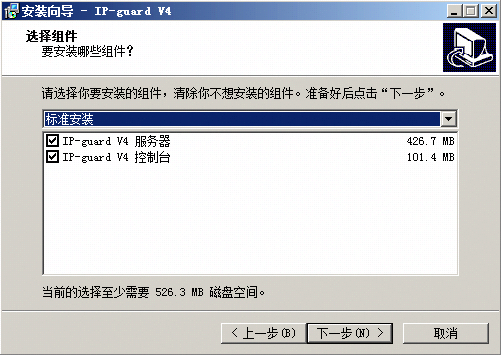
### 3.3.1 安装程序及注册码获取渠道

请与IP-guard厂商或经销商索取IP-guard安装程序及注册码信息。

### 3.3.2 安装服务端

运行服务端安装程序，选择组件，选择‘标准安装’，按照安装向导一步一步完成安装。



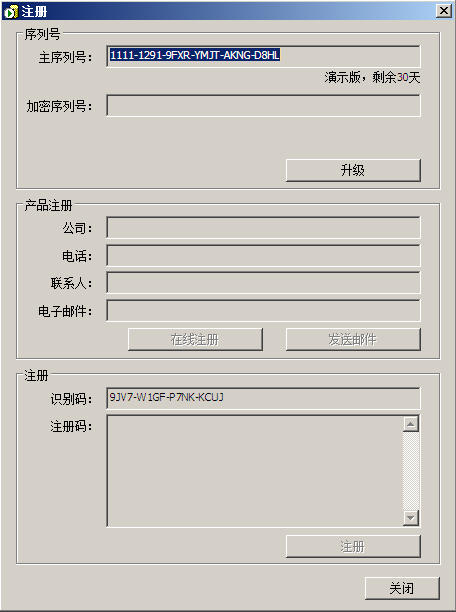




### 3.3.3 服务端注册

启动注册

等待服务器桌面右下角的服务控制器图标变成实心的绿色，说明服务端启动完成。此时可以右键单击【服务控制器】图标，选择“工具->注册”输入管理员密码（默认密码为空）进入注册界面。



点击【升级】按钮，主序列号和加密序列号栏会变成可编辑状态，输入主序列号、加密序列号，点击【确定】按钮，再输入产品注册信息（公司、电话、联系人和电子邮件），点击【在线注册】，完成注册。如果注册过程遇到问题，请联系IP-guard厂家或经销商。

注意：在线注册要求IP-guard服务器必须连接互联网，如果服务器无法联网，请联系IP-guard厂家或经销商提供注册码。

### 3.3.4 设置检验码

检验码是IP-guard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IP-guard服务器接管企业内的客户端。

**设置方法：**

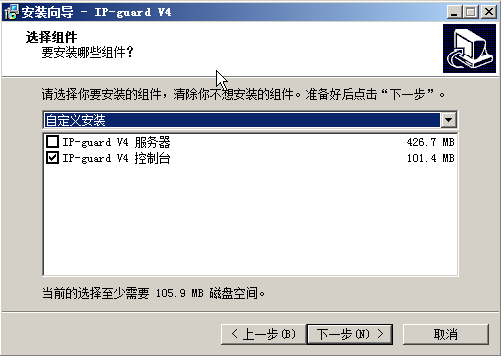
IP-guard服务完成注册后，右键单击【服务控制器】选择菜单“工具->检验码”，系统会要求输入管理员的账号和密码（默认密码为空）才能设置检验码，两次输入检验码，点击【确定】按钮，检验码设置成功。

Warning 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更换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。

## 3.4 安装IP-guard控制台

在4.3.2章节，安装IP-guard服务端时，已经同时安装了IP-guard控制台。

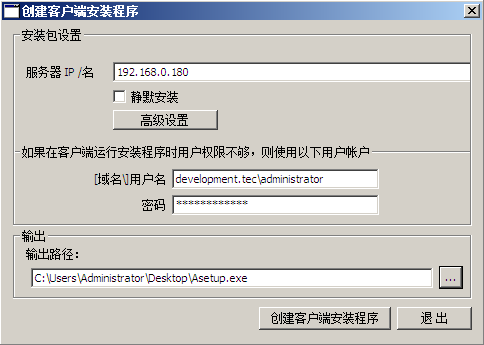
为了方便管理员使用，也可在管理员计算机上单独安装IP-guard控制台，通过运行IP-guard安装程序，仅勾选“IP-guard V4 控制台”即可。



## 3.5 安装IP-guard客户端

### 3.5.1 创建客户端

客户端安装程序需要在IP-guard服务器上创建。点击“开始->所有程序->IP-guard V4->创建客户端安装程序”打开客户端生成工具（右键以管理员身份运行）。客户端安装程序的参数包括：



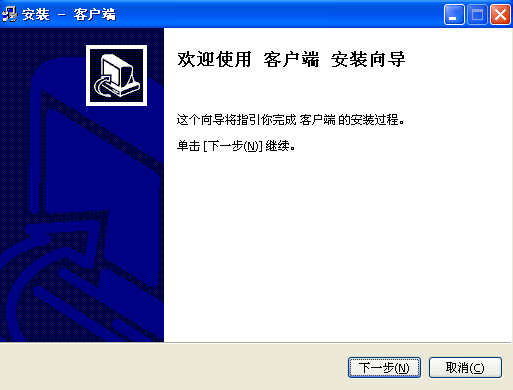
|  |  |
| --- | --- |
| **名称** | **说明** |
| 服务器IP/名 | 系统默认是当前服务器的IP地址，如果服务器有多个IP地址，请输入一个客户端能连接成功的IP地址。 |
| 静默安装 | 选中该复选框，客户端安装程序为静默安装，不会出现安装界面。  不选中该复选框，则为非静默安装包，会出现安装界面。 |
| 用户名和密码 | 如果安装客户端程序需要管理员权限，则在这里输入具有计算机管理员权限的用户名和密码，这样客户端程序在user权限下也能安装成功。如果计算机本身具有安装软件的权限，则此项不需要设置。 |
| 输出路径 | 该路径为客户端安装程序的存放路径。 |

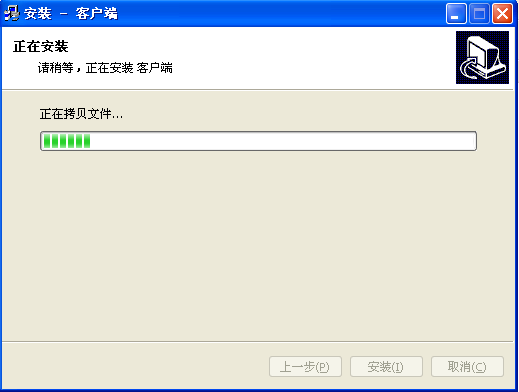
注意：如果客户端计算机上安装了防火墙软件，或在网络上部署了防火墙设备，请确认IP-guard服务器开放了8237端口，客户端开放了 8235端口，控制台开放了8236端口。

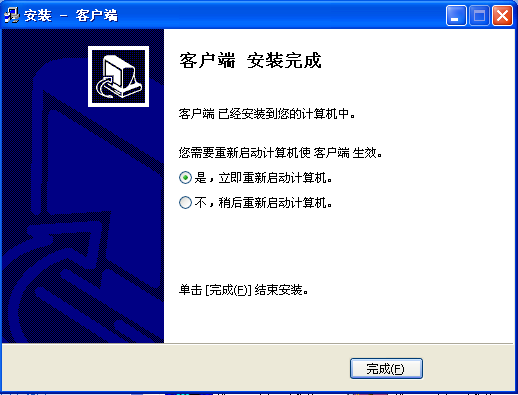
### 3.5.2 客户端安装

客户端程序安装在每一台需要被管控的计算机上，客户端的安装方式主要有三种：手工安装、域脚本安装和自带的远程安装模式。

手动安装客户端，右键以管理员身份运行客户端安装程序，安装完成，请重启计算机，操作步骤如下图：







注意：在产品试用阶段，一般不会部署太多的客户端，我们可以使用手工安装客户端，这样更加方便。

## 3.6 卸载安装程序

### 3.6.1 客户端卸载

系统管理员可以通过登录控制台，选中希望卸载的客户端，在菜单“控制->卸载客户端”来卸载客户端程序。

### 3.6.2服务器和控制台卸载

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。

注意：卸载前，请确认通过IP-guard系统加密的文件已经全部解密。如果文件依然处于加密状态，卸载系统后，用户将不能再打开加密文件。

# 四、功能操作测试

## 4.1基本模块

### 4.1.1 了解控制台的基本操作

|  |  |
| --- | --- |
| 测试目的 | 了解控制台基本操作 |
| 适用场景 | 让管理员熟悉控制台的基本操作，为后续测试提供方便。 |
| 用例描述 | 1. 登录控制台熟悉基本框架并修改密码； 2. 通过控制台组建公司的组织架构； 3. 建立多个管理账号，共同管理客户端。 |
| 测试步骤 | 1. 打开IP-guard 控制台，输入账号密码（账号为：Admin，密码默认为空）； 2. 选择工具-修改密码，输入新的密码； 3. 选择工具-重新登录，回到登录界面，使用Admin和修改后的密码登录； 4. 控制台左侧计算机树中，选择整个网络(右键)-新建组，重命名为测试组（可根据需要自由设置名称），并将未分组的计算机移动到测试组中； 5. 选择工具-账户，点击图标新建一个名称为test的管理员帐号，选择常规，可以设置类型、登录和账户管理等权限。选择功能权限，给予相应的管理权限。选择管理范围，可以设定test账号可以管理哪些计算机。选择加密功能，可以赋予加密相关的权限（需先在常规选项卡中，勾选具有加密功能管理权限），点击确定完成设置； 6. 打开控制台，用新建的test管理员帐号登录，并查看操作权限是否和给予的权限一致。 |
| 预期结果 | 1. 使用admin账号和空密码可以登录控制台； 2. 修改密码后，输入账号和修改后的密码，控制台登录成功； 3. 在控制台左侧，客户端出现在未分组，并且可移动到新建的分组中； 4. 管理账户（test）可以成功登录，并且具备管理员赋予的权限。 |
| 测试结果 | 满足：马 部分满足： 不满足： |
| 备注 |  |

### 4.1.2 熟悉主体功能

|  |  |
| --- | --- |
| 测试目的 | 获取客户端基础信息，执行基本控制，进行系统报警 |
| 适用场景 | 帮助管理员熟悉基本模块的主要功能。 |
| 用例描述 | 1. 获取客户端的基本信息，包括：计算机名称，网络地址，操作系统，登录用户，当前状态等； 2. 对客户端执行锁定、关闭、重启、注销和发送通知信息等操作； 3. 当客户端的系统状态发送变化时进行报警。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 在控制台左边的计算机树中，选中某台计算机； 3. 选择统计-基本信息，下方会显示这台计算机的基本信息； 4. 在控制台左边的计算机树中，选中某台计算机，右键-控制，可以选择发送通知消息、锁定计算机、解锁、注销用户、关闭计算机、重新启动和卸载客户端等操作； 5. 在控制台左边的计算机树中，选中某台计算机，选择策略-系统报警，点击红色+号标识新建一条策略，在右边的属性栏选择动作为报警，再勾选需要报警的内容，比如：插入存储设备、计算机名称改变、磁盘空间不足、磁盘通电异常等： 6. 点击绿色勾状图标，保存该策略； 7. 然后在客户端尝试插入存储设备或修改计算机名等操作。 |
| 预期结果 | 步骤3：查看到计算机名、IP/MAC、操作系统、登录用户等信息；  步骤4：可以成功对计算机执行相关的操作；  步骤5：设置策略后，客户端进行相关操作时，控制台弹出报警信息。 |
| 测试结果 | 满足： 部分满足： 马 不满足： |
| 备注 |  |

### 4.1.3 设置第一条策略

|  |  |
| --- | --- |
| 测试目的 | 学习如何设置第一条控制策略 |
| 适用场景 | 帮助管理员熟悉策略的设置。 |
| 用例描述 | 1. 可尝试对操作系统的30项内容进行控制，包括控制面板、计算机管理、系统、网络、IP/MAC绑定、ActiveX控件等； 2. 通过设置禁止策略，使用户不能使用某项功能。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 在控制台左边的计算机树中选中测试组； 3. 选择策略-基本策略，点击红色+号标识新建一条策略； 4. 在右边的属性栏选择动作为禁止，勾选任务管理器； 5. 点击绿色勾状图标，保存该策略； 6. 然后在客户端计算机任务栏尝试打开“任务管理器”； 7. 在控制台最左边的计算机树中，选择测试组内的某台计算机； 8. 选择策略-基本策略，点击红色+号标识新建一条策略； 9. 在右边的属性栏选择动作为允许，勾选任务管理器； 10. 点击绿色勾状图标，保存该策略； 11. 然后在客户端计算机任务栏尝试打开“任务管理器”。 |
| 预期结果 | 1到5步骤可以实现测试组内所有的计算机都不能打开“任务管理器”；  7到10步骤可以让被选中的计算机（比如：计算机A）能打开“任务管理器”。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 | 策略执行优先级是计算机优先于分组，策略的执行顺序是从上往下执行。 |

### 4.1.4 查看操作日志及基本事件

|  |  |
| --- | --- |
| 测试目的 | 查看操作日志及基本事件 |
| 适用场景 | 学习如何查看日志，以及如何通过设置策略实现日志记录 |
| 用例描述 | 客户端日志的记录：   1. 系统默认记录客户端产生的几乎所有日志记录； 2. 通过日志记录策略来控制日志记录的类型； 3. 如果希望不记录某些日志，可添加一条新策略，设置为不记录，勾选不需要记录的日志项，保存策略即可。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 在控制台左侧的计算机树中选择测试组内的计算机； 3. 选择日志-基本事件，可以查看基本事件日志，也可以在右侧的查询框内通过各种条件进行查询； 4. 选择策略-日志记录，点击红色+号标识新建一条策略； 5. 右边的属性栏选择动作为不记录，勾选系统启用/关闭点击绿色勾状图标，保存该策略； 6. 重启这台客户端计算机后，回到日志-基本事件，查看基本事件日志与策略设置的预期结果是否匹配。 |
| 预期结果 | 步骤3中能查看到计算机系统重启、关闭和用户登录、注销的日志；  设置步骤5后，再次查看只有用户登录日志，没有系统启动、关闭日志。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 | 日志策略默认是记录几乎所有的日志，如不想记录某些日志，可以再建立一条不记录日志的策略叠加在默认策略之上。 |

### 4.1.5 终端安全检测

|  |  |
| --- | --- |
| 测试目的 | 终端安全检测 |
| 适用场景 | 保证终端必须满足企业规定的安全要求才能接入网络，保证终端计算机具备合格的安全基线。 |
| 用例描述 | 1. 设置计算机安全检测条件，可以检测包括：杀毒软件、软件安装、程序运行、系统服务运行、系统补丁、域用户身份、其他自定义条件； 2. 对客户端下发安全检测策略，实时进行检测； 3. 对不满足安全检测条件的客户端进行警告、阻断网络、阻断接入。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 选择安全检测—安全检测条件，进入安全检测条件类别页面； 3. 点击按钮，新建安全检测条件，条件名为“测试组安全检测条件”，选择杀毒软件检查→必须运行杀毒软件→必须运行以下任一杀毒软件，点击添加，输入杀毒软件名称“腾讯御点系统防护”，勾选病毒库更新到最新； 4. 选择系统补丁检查，点击添加，勾选补丁ID； 5. 选择“域用户身份验证”，勾选“启用域用户身份检查功能”，在必须登录以下任意域用户的文本框中输入“域名\用户名”，用户名支持通配符，禁止登录以下任意域用户的文本框中可以不输入内容，点击“确定”，退出“安全检测条件”设置界面，关闭“安全检测条件类别”页面； 6. 在控制台左侧选中某台计算机，点击“安全检测—>安全检测设置”，新建一条策略，选择“测试组安全检测条件”，在右侧属性栏内，可以勾选“警告”，输入警告信息“请检查不符合安全检测的内容”，勾选“显示检测结果”，勾选“阻断网络”、输入“例外地址”（指即使安全检测不通过，依然希望计算机访问的地址，比如：杀毒软件安装包、补丁文件的存放地址）； 7. 保存策略。 |
| 预期结果 | 1. 如果计算机安装了杀毒软件、补丁，成功登录域用户，则计算机会提示“安全检测通过”，并且用户可以访问网络； 2. 如果安全检测不通过，则弹出警告信息，并阻止计算机访问网络，此时计算机只能访问例外地址下载对应的安装包。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 | 测试步骤，第3点，需要输入杀毒软件名称，请从以下位置获取杀毒软件名称，操作系统→控制面板→系统和安全→操作中心→安全→病毒防护。 |

### 4.1.6 策略管理及日志导出

|  |  |
| --- | --- |
| 测试目的 | 策略管理及日志的导出 |
| 适用场景 | 学习策略的灵活应用和日志导出操作。 |
| 用例描述 | 1. 支持策略导出，同样也支持策略导入； 2. 策略可以在组织架构通过复制实现迁移，增强策略应用的灵活性； 3. 支持日志导出格式包括：\*.xlsx，\*.xls，\*.csv，\*.html。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 在计算机树中选中一台计算机； 3. 选择策略-日志记录，选中某条策略-右键导出选中策略，把策略文件导出到本地硬盘中； 4. 在左侧的组织架构中选择整个网络，在策略-日志记录页面中，右键空白处选择导入，导入刚刚导出的策略文件（\*.xml）； 5. 选择测试组内的计算机，在策略-日志记录页面中选择一条策略，右键-复制到，在弹出窗口中选择需要复制到测试组； 6. 选择测试组，查看是否新增了一条策略； 7. 选择测试组内的计算机，切换到日志-基本事件页面，选中任意一条日志右键-导出-本页记录，指定保存路径为桌面，可保存为各种文件类型（\*.html ,\*.xls，\*.xlsx和\*.csv格式）。 |
| 预期结果 | 1. 策略可以灵活自如的导出、导入，也可以复制到其他计算机或分组； 2. 能导出各种格式的日志文件。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.1.7审计管理员操作日志

|  |  |
| --- | --- |
| 测试目的 | 审计管理员操作日志 |
| 适用场景 | 审计管理员可以审查管理员的操作行为，通过这种方式了解管理员的行为是否合规。 |
| 用例描述 | 1. 审计所有管理员在控制台上的操作日志，并且支持查询和导出； 2. 日志记录遵循时序原则，根据管理员的操作步骤进行记录； 3. 支持按管理员的账户分别进行记录； 4. 日志支持导出和打印，日志导出格式：\*.xls，\*.xlsx，\*.csv，\*.html。 |
| 测试步骤 | 1. 打开IP-guard控制台； 2. 使用audit账号登录；（初始密码为空）； 3. 控制台左侧的管理员列表，列出了所有管理员账户； 4. 选择admin账号，可以查看到右侧的审计日志区域会显示admin账号的所有操作行为； 5. 选择日志，右键-导出-所有满足条件的记录，可以导出不同格式（\*.xls、\*.xlsx、\*.csv、\*.html）； 6. 选择日志，右键-打印，可以将日志记录打印出来。 |
| 预期结果 | 选中Admin，能看到Admin修改密码、设置策略的日志，且各项记录的数据正确，并且可以导出和打印日志记录。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 | 审计账号audit只负责审计管理员的操作行为，没有其他任何操作权限。 |

## 4.2移动存储管控

### 4.2.1 移动存储设备的使用信息及分类管理

|  |  |
| --- | --- |
| 测试编号 | 移动存储设备的使用信息及分类管理 |
| 适用场景 | 了解移动存储的使用情况，对移动存储进行分类。 |
| 用例描述 | 对新接入的移动存储设备进行实时的信息获取，同时可以将接入过的移动存储进行分类管理。   1. 移动存储设备的信息记录； 2. 查看移动存储使用情况，显示接入/拔出、时间、计算机和使用用户； 3. 灵活方便的分类管理。 |
| 测试步骤 | 1. 在计算机A上插入一个U盘，大约2-3分钟之后，拔出U盘； 2. 登录控制台； 3. 在日志-移动存储操作页面中，可以看到有插入和拔出的记录； 4. 在顶部功能菜单，分类管理-移动存储-未注册可以看到此U盘的详细信息。 |
| 预期结果 | 在计算机上拔插移动存储后能记录拔插的日志并统计移动存储的相关详细信息。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 未测试 |

### 4.2.2 移动存储设备注册管理

|  |  |
| --- | --- |
| 测试编号 | 移动存储设备注册管理 |
| 适用场景 | 所有U盘进行注册管理，限制非法U盘在公司内部使用。 |
| 用例描述 | 1. 对合法U盘进行注册，记录U盘使用者信息 2. 注册管控，未注册的U盘禁止使用 |
| 测试步骤 | 1. 登录控制台； 2. 在分类管理—>移动存储中，进入移动存储库； 3. 对于已经在客户端插入过的U盘，可以在未注册分组中找到U盘信息，选中该U盘右键点击，选择注册； 4. 对于在控制台电脑是正常使用的U盘，可以点击操作—>本地移动存储信息，选中U盘，点击右上角进行注册； 5. 已注册的U盘可以在已注册分组内找到，然后进行分组管理； 6. 启用控制，点击操作—>注册管控，勾选启用，勾选警告，输入提示信息“该U盘未注册，请联系管理员。” |
| 预期结果 | 在计算机A和其他安装客户端计算机，插入已注册的U盘，可以正常使用；插入未注册U盘，不能使用，并弹出提示信息。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 未测试 |

### 4.2.3移动存储设备读写权限控制

|  |  |
| --- | --- |
| 测试编号 | 移动存储设备读写权限控制 |
| 适用场景 | 需要将外来的移动存储设备接入到内网计算机上工作，对这类移动存储设备使用只读权限打开，一方面方便来访者正常工作需要，另一方面控制好信息出口。 |
| 用例描述 | 1. 对于企业内授权U盘使用正常； 2. 对于外来未授权U盘接入企业计算机时以只读方式打开，防止外来U盘携带走企业机密信息泄密。 |
| 测试步骤 | 1. 登录控制台； 2. 在左侧计算机树中选择计算机A； 3. 选择高级-移动存储授权，点击红色+号标识新建一条策略在，右边的属性栏勾选可读，取消可写选项，移动存储选择未注册； 4. 点击绿色勾状图标**，**保存该策略； 5. 在测试的计算机上接入一个未曾接入过的U盘，对U盘进行读、写操作，测试是否成功。 |
| 预期结果 | 接入U盘只读打开，写入数据失败。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 未测试 |

### 4.2.4制作企业内部加密U盘

|  |  |
| --- | --- |
| 测试编号 | 制作企业内部加密U盘 |
| 适用场景 | 保证U盘只能在企业内部使用，防止因U盘随意外带造成的泄密。 |
| 用例描述 | 1. 对企业内部使用的U盘进行全盘加密，防止因丢失、有意或无意被带出时泄漏机密信息； 2. 加密U盘在企业内部正常使用。 |
| 测试步骤 | 1. 登录控制台，并在控制台所在的计算机插入测试用存储设备； 2. 选择分类管理-移动存储，在弹出的新界面中选择操作-本地移动存储信息，点击修改图标，对该移动存储设备进行加密盘格式化，在确认可以进行格式化后点击确定，操作完成后该移动存储盘变成了加密盘； 3. 在左侧计算机树中选择计算机A； 4. 选择高级-移动存储授权，点击红色+号标识新建一条策略在，右边的属性栏勾选可读和可写选项，移动存储类型选择加密盘； 5. 点击绿色勾状图标，保存该策略； 6. 在安装了客户端并设置允许权限的机器上可以正常使用，如果需要在未安装客户端或者没有权限的机器上打开加密盘，需要先格式化加密盘； 7. 将该移动存储分别插入安装了客户端并设置有权限的计算机和未安装客户端的计算机上打开加密盘，测试是否能正常使用。 |
| 预期结果 | 在安装了客户端并设置了权限的计算机上能正常使用该移动存储盘；未安装客户端的计算机上无法使用该移动存储，如果需要使用，需要格式化加密盘。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 加密盘插在非客户端计算机上会提示需要格化式，点击“确定”将会格式化加密盘为普通U盘。  未测试 |

### 4.2.5公私两用U盘加解密的设置

|  |  |
| --- | --- |
| 测试编号 | 公私两用U盘加解密的设置 |
| 适用场景 | 由于企业员工自备的U盘一般都公私两用，即携带私人资料，也装载公司文档，所以需要防止其拷贝公司重要文档外带泄密，又要不影响正常使用U盘拷贝私人资料。 |
| 用例描述 | 1. 公私两用U盘在企业环境之外使用时不自动加解密拷贝的文档，方便拷贝私人文档； 2. 企业内部计算机拷贝文档到公私两用U盘时自动加密文档，从公私两用U盘拷贝资料到企业内部计算机时自动解密文档； 3. 在企业环境之外不能打开公私两用U盘内已经加密的文档。 |
| 测试步骤 | 1. 登录控制台； 2. 在左侧计算机树中选择计算机A； 3. 选择高级-移动存储授权，点击红色+号标识新建一条策略，取消可读与可写两个选项； 4. 再新建一条策略，右边的属性栏勾选上可读与自动解密、可写与自动加密四个选项，移动存储选择公私两用的U盘分类（请预先做好分类）； 5. 点击绿色勾状图标，保存该策略； 6. 在测试的计算机上接入一个属于公私两用U盘分类里的U盘，拷贝公司资料，并将U盘内文档拷贝到未安装客户端计算机上使用，打开刚拷贝的公司文档，再测试打开私人文档，查看是否成功； 7. 将U盘重新接入测试机，将U盘内公司文档拷贝到计算机打开，测试是否成功。 |
| 预期结果 | 在非测试计算机查看拷贝的公司文档显示乱码，查看私人文档正常，再回到测试计算机将公司文档拷贝出来查看，显示正常，其他非指定的移动存储设备无法进行读写操作。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 加解密动作是在文档拷贝到移动盘或拷出移动盘的过程完成的，因此文档拷贝到移动盘上存储时为加密状态，直接在移动盘上打开该文档是无法执行解密操作的，即打开失败，需拷贝到客户端计算机上方能自动解密打开。  非加密文档可直接在移动盘上打开。  即使已经安装客户端，如果没有自动解密的权限，从U盘拷贝文件出来也无法打开。  未测试 |

## 4.3应用程序管控

### 4.3.1应用程序使用审计

|  |  |
| --- | --- |
| 测试编号 | 应用程序使用审计 |
| 适用场景 | 统计用户使用各种应用程序的百分比，并清晰的图表形式输出统计结果，根据此功能可以精准的分析员工工作效率。 |
| 用例描述 | 1. 统计应用程序使用时间及百分比； 2. 合计方式支持，按类别合计、按名称合计、按明细合计、按分项统计； 3. 导出格式支持\*.xls,\*.html,\*.csv等； 4. 输出方式支持柱状图和饼状图。 |
| 测试步骤 | 1. 在计算机A上打开一个应用程序，如IE，然后再关闭； 2. 登录IP-guard控制台； 3. 隔3-5分钟后，把控制台页面切换到日志-应用程序，可以查看到有IE启动、退出的记录； 4. 在左侧的计算机树中选择计算机A，把控制台页面切换到统计-应用程序，分别选择按类别合计、按名称合计、按明细合计、按分项统计几种模式； 5. 根据每个合计模式对应查看显示结果是否正确。 |
| 预期结果 | 1. 能查看到IE的启动、停止记录； 2. 能查看精准的图表分析。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.3.2应用程序使用管控

|  |  |
| --- | --- |
| 测试编号 | 应用程序使用管控 |
| 适用场景 | 在企业中，管理者可以限制和工作无关的应用软件使用，例如一些BT、迅雷下载工具，聊天工具以及游戏类的软件。 |
| 用例描述 | 1. 通过进程名称来禁止程序运行； 2. 通过应用程序分类来禁止程序运行。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 在左侧计算机树中选择计算机A； 3. 选择策略-应用程序，点击红色+号标识新建一条策略，在右边的属性栏选择模式为禁止，点开应用程序在弹出的窗口中选择图标填写相应的应用程序名称（如：QQ.EXE）或者选择图标选择相应的分类； 4. 点击绿色勾状图标，保存该策略； 5. 在测试的计算机尝试运行分类中或者填写进程名称的程序。 |
| 预期结果 | 被禁止的程序不能运行。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.3.3应用程序安装卸载管理

|  |  |
| --- | --- |
| 测试编号 | 应用程序安装卸载管控 |
| 适用场景 | 企业内部管理，需要统一管理用户计算机上的软件的安装和卸载，与工作无关的软件禁止安装，已经安装好的办公软件禁止卸载。 |
| 用例描述 | 1. 禁止安装与工作无关的软件； 2. 禁止卸载工作软件。 |
| 测试步骤 | 1. 登录控制台； 2. 在分类管理—>软件安装包，新增软件安装包（安装包文件需要事先下载）； 3. 在分类管理—>软件卸载，新增软件，软件可以手动输入，也可以从应用程序分类库中导入； 4. 选择计算机A； 5. 选择策略—>软件安装管理，点击右上角编辑，进入软件安装管理设置界面； 6. 勾选“禁止全部软件的安装”，然后在下方输入允许安装的软件； 7. 勾选“禁止以下软件的卸载”，然后在下方输入禁止卸载的软件； 8. 在计算机A上，进行软件的安装和卸载。 |
| 预期结果 | 在计算机A上，只有允许安装的软件才能安装，其他软件不能安装；被禁止卸载的软件无法卸载。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

## 4.4 网络控制

### 4.4.1非法终端访问控制

|  |  |
| --- | --- |
| 测试编号 | 非法终端访问控制 |
| 适用场景 | 禁止未安装客户端的计算机访问已经安装客户端的计算机，允许内网客户端计算机之间互访。 |
| 用例描述 | 1. 禁止未安装客户端计算机与客户端计算机通讯； 2. 允许客户端计算机之间的正常通讯。 |
| 测试步骤 | 1. 登录控制台； 2. 在最左边的计算机树中选择计算机A； 3. 选择高级-网络控制，点击红色+号标识新建一条策略，在右边属性栏选择模式禁止； 4. 再增加一条策略，选择模式允许，勾选上对方是客户端，其他为默认选项； 5. 点击绿色勾状图标，保存该策略； 6. 已安装客户端计算机B，一台未装客户端计算机C，分别访问计算机A的共享，测试是否可以成功访问共享。 |
| 预期结果 | 计算机B可以访问计算机A共享文件，而计算机C则不能访问计算机A的共享。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.4.2部门访问隔离

|  |  |
| --- | --- |
| 测试编号 | 部门访问隔离 |
| 适用场景 | 在企业里面，有些部门的计算机是非常重要的，不允许部门之外的计算机访问。 |
| 用例描述 | 禁止已安装客户端计算机与核心部门的客户端计算机通讯。 |
| 测试步骤 | 1. 登录控制台； 2. 在最左边的计算机树中选择整个网络； 3. 选择高级-网络控制，点击红色+号标识新建一条策略，在右边属性栏选择模式禁止，网络地址范围选择局域网； 4. 再增加一条策略，选择模式允许，勾选上对方是客户端，属于相同分组，其他为默认选项； 5. 点击绿色勾状图标，保存该策略； 6. 已安装客户端其他部门的计算机B，已安装客户端的同部门计算机C，分别访问受保护部门计算机A的共享，测试是否可以成功访问共享。 |
| 预期结果 | 计算机B不可以访问计算机A共享文件，而计算机C能访问计算机A的共享。 |
| 测试结果 | 满足： 部分满足： 马 不满足： |
| 备注 |  |

### 4.4.3阻断非法端口

|  |  |
| --- | --- |
| 测试编号 | 阻断非法端口 |
| 适用场景 | 为了保护内网安全，企业需要禁止一些互联网的恶意端口或下载端口 |
| 用例描述 | 禁止已安装客户端的计算机通过非法端口进行通讯或下载文件。 |
| 测试步骤 | 1.登录控制台；  2.在最左边的计算机树中选择整个网络；  3.选择高级-网络控制，点击红色+号标识新建一条策略，在右边属性栏选择模式禁止，端口范围选择需要禁止的端口，如：21端口，网络地址范围选择互联网；  4.点击绿色勾状图标，保存该策略；  5.测试是否可以执行FTP下载。 |
| 预期结果 | 互联网上不可以使用FTP下载，在局域网可以执行FTP下载。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 未测试 |

## 4.5 资产管理

### 4.5.1 IT资产管理（硬件）

|  |  |
| --- | --- |
| 测试编号 | IT资产管理（硬件） |
| 适用场景 | 企业规模不断扩大，使得IT资产的种类与数量爆发性的增长，IT管理者面临着以有限的人力管理海量IT资产的困境。 |
| 用例描述 | 1. 自动收集内网计算机的各项硬件信息； 2. 支持以多种参数对网内IT资产查询； 3. IT资产报表输出功能，支持导出格式：\*.html、\*.xls、\*.csv等。 |
| 测试步骤 | 1. 登录控制台； 2. 在菜单栏选择资产管理-硬件资产，进入资产管理界面，右侧的界面中会列出网内所有计算机硬件的基本信息（可以点击按钮将您需要结果选项选出，则会在表中列出）； 3. 选中一台计算机双击可以进入此台计算机的资产管理界面或者在控制台左侧的计算机树中选择一台计算机-右键-资产信息； 4. 在此台客户端计算机上用硬件检测工具或者在设备管理器中作对比，查看统计情况； 5. 在工具栏点击按钮或者在资产管理界面右键导出，即可生成一张IT资产表； 6. 点击按钮或者选择菜单文件-新建查询，设置名称为test,查询条件为：硬盘容量（实例属性）> 60G； 7. 点击确定后查看结果。 |
| 预期结果 | 1. 能够精准的统计出网内计算机的硬件信息并导出； 2. 能查询出硬盘容量大于60G的计算机。 |
| 测试结果 | 满足： 部分满足： 马 不满足： |
| 备注 | 没有找到硬盘容量（实例属性）-马 |

### 4.5.2 IT资产管理（软件）

|  |  |
| --- | --- |
| 测试编号 | IT资产管理（软件） |
| 适用场景 | 统计软件资产信息 |
| 用例描述 | 1. 自动收集内网计算机的各项软件信息； 2. 支持以多种参数对网内IT资产查询； 3. IT资产报表输出功能，支持导出格式：\*.html、\*.xls、\*.csv等。 |
| 测试步骤 | 1. 登录控制台； 2. 在菜单栏选择资产管理-软件资产，进入资产管理界面，右侧的界面中会列出网内所有计算机软件的基本信息（可以点击按钮将您需要的基本信息成列出来）； 3. 选中一台计算机双击可以进入此台计算机的软件资产管理界面或者在控制台左侧的计算机树中选择一台计算机-右键-资产信息**，**点击应用软件可以看到此计算机上所有安装的软件； 4. 在工具栏点击按钮或者在资产管理界面右键导出，即可生成一张软件IT资产表； 5. 点击按钮或者选择菜单文件-新建查询，设置名称为test,查询条件为：操作系统（实例属性）（自己定义一个日期）； 6. 点击确定后查看结果。 |
| 预期结果 | 1. 能够精准的统计出网内计算机的软件信息并导出； 2. 能查询出在您自定义日期前安装的计算机。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.5.3软（硬）件变更统计

|  |  |
| --- | --- |
| 测试编号 | 硬（软）件变更统计 |
| 适用场景 | 自动记录和统计企业内部计算机软硬件资产变更，提供一目了然的软硬件资产变更列表，让系统管理员通过控制台便可对资产变动了如指掌。 |
| 用例描述 | 1. 客户端计算机软、硬件配置发生变动时，即时报警告知管理员； 2. 统计客户端计算机对软硬件配置变动的日志记录； 3. 实时精准的资产信息可避免资产遗失。 |
| 测试步骤 | 1. 登录控制台； 2. 在菜单栏选择资产管理-硬件资产变更，进入资产管理界面，右侧的界面中会列出网内所有计算机里面硬件变更信息； 3. 点击按钮并在弹出的菜单窗口中选择您的查询条件，并点击查询查看查询结果； 4. 在菜单栏选择资产管理-软件资产变更，进入资产管理界面，右侧的界面中会列出网内所有计算机里面软件变更信息； 5. 点击按钮并在弹出的菜单窗口中选择您的查询条件，并点击查询查看查询结果； 6. 卸载一个软件等几分钟后，选择日志-资产变更，查看是否有记录； 7. 选择策略-日志记录，点击红色+号标识新建一条策略，动作（不记录），勾选软件变更，点击绿色勾号图标，保存策略； 8. 安装步骤6里面卸载的软件，在选择日志-资产变更，查看是否有记录。 |
| 预期结果 | 1. 能记录和查询出计算机软硬件变更信息； 2. 设置日志策略后可不记录。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.5.4软件分发管理

|  |  |
| --- | --- |
| 测试编号 | 软件分发管理 |
| 适用场景 | 自动给客户端计算机批量分发安装应用软件包，从而简化了传统软件分发的繁琐程序，减轻管理员批量部署程序的负担。 |
| 用例描述 | 1. 满足大型网络软件统一部署； 2. 对分发过程有明晰的跟踪和记录。 |
| 测试步骤 | 1. 登录控制台； 2. 进入到资产管理界面，选中软件分发-分发程序包，新建一个分发程序包，名称为：QQ安装、文件信息中的分发模式为安装软件、文件列表添加：QQ的安装程序（网上下载安装程序）、检测和必要条件中检测条件为：安装的软件包含腾讯QQ，点击保存； 3. 选中软件分发-分发任务，程序包名称选择刚新建的程序包QQ安装，目标计算机选择计算机A，点击确定。 |
| 预期结果 | 计算机A 弹出QQ安装界面。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 | 软件安装程序如果支持静默安装，分发任务后，会自行在后台安装；  如果不支持静默安装，则会弹出安装的交互界面。  检测条件是检查软件是否成功安装的标准；  必要条件是执行本程序包所必须具备的条件。 |

### 4.5.5补丁管理

|  |  |
| --- | --- |
| 测试编号 | 补丁管理 |
| 适用场景 | 自动扫描计算机的补丁安装情况，并可根据实际所需为计算机自动下载安装微软补丁，自动统计补丁安装情况。 |
| 用例描述 | 1. 自动检测安装，减少系统管理员的工作量； 2. 统一下载补丁并按需安装，减少网络的承载压力。 |
| 测试步骤 | 1. 登录控制台； 2. 进入资产管理选中补丁管理-计算机模式，然后查看计算机A的补丁信息； 3. 选择没有下载的补丁的计算机，右键设置为下载； 4. 选择计算机A中没有安装的补丁，右键设置为安装； 5. 选择补丁管理-补丁模式，可以查看网内计算机所需要的所有补丁列表。 |
| 预期结果 | 下载补丁，并可安装补丁成功。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 使用补丁管理功能，IP-guard服务器必须能联网，需要从微软下载检测包和补丁安装包。  未测试 |

### 4.5.6软件卸载管理

|  |  |
| --- | --- |
| 测试编号 | 软件卸载管理 |
| 适用场景 | 用户安装了与工作无关的软件，为了进行应用程序标准化管理，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。 |
| 用例描述 | 1. 卸载全部计算机指定软件； 2. 卸载任务持续执行。 |
| 测试步骤 | 1. 登录控制台； 2. 进入资产管理—>软件卸载界面； 3. 选择软件模式，点击腾讯QQ，可以发现安装腾讯QQ的计算机； 4. 右键腾讯QQ，点击卸载，进入卸载界面； 5. 选择计算机A，任务模式：持续执行和立即执行； 6. 计算机A和B安装腾讯QQ。 |
| 预期结果 | 1. 在计算机A上安装腾讯QQ后，会立即被卸载； 2. 在计算机B上安装腾讯QQ后，不会被卸载。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

## 4.6 远程维护

### 4.6.1实时查看客户端计算机的运行状态

|  |  |
| --- | --- |
| 测试编号 | 实时查看客户端计算机的运行状态 |
| 适用场景 | 在控制台上像本地一样在控制台上查看计算机相关信息，方便进行故障查看与诊断。 |
| 用例描述 | 1. 查看正在运行的应用程序、进程； 2. 性能、设备管理； 3. 系统服务、磁盘管理； 4. 共享文件夹、计划任务； 5. 用户和组。 |
| 测试步骤 | 1. 登录控制台； 2. 在左侧的计算机树里面选择计算机A； 3. 选择维护-应用程序，可以查看该计算机的应用程序列表； 4. 在客户端计算机上右键任务栏-启动任务管理器-应用程序，与控制台上显示的应用程序列表进行对比是否与之一样； 5. 按照步骤3、4 分别查询进程、性能、设备管理、系统服务、磁盘管理等计算机内部信息，并验证是否与计算机一样； 6. 在计算机A上新建一个共享文档test； 7. 在控制台上，选择维护-共享文档；查看是否多出一个共享文件夹test。 |
| 预期结果 | 查询出的结果与计算机上显示一致。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.6.2控制台远程控制客户端

|  |  |
| --- | --- |
| 测试编号 | 控制台远程控制客户端 |
| 适用场景 | 系统管理员可以通过IP-guard控制台直接远程控制和操作任意一台计算机，可以在控制台给计算机做远程协助。 |
| 用例描述 | 1. 及时故障处理，提高管理员的工作效率； 2. 多种远程方式，便于高效管理； 3. 密码授权。 |
| 测试步骤 | 1. 登录控制台； 2. 在左侧的计算机树中选择计算机A，右键-控制-远程控制； 3. 此时计算机A会弹出确认窗口，单击确认查看是否能够远程控制； 4. 在计算机A上按住组合键shift+alt+ctrl（按住不放）输入“ocularrm”，对该计算机设置远程控制密码； 5. 在控制台上选择此计算机，右键-控制-远程控制，在弹出的对话框中输入密码查看是否能远程控制。 |
| 预期结果 | 用户确认和密码确认两种方式都可以远程控制。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.6.3远程文件传送

|  |  |
| --- | --- |
| 测试编号 | 远程文件传送 |
| 适用场景 | 实现远程文件的传输，方便故障处理时上传工具，完善远程协助的机制。 |
| 用例描述 | 1. 双方确认才可以传送文件； 2. 密码授权； 3. 加密传输。 |
| 测试步骤 | 1. 登录控制台； 2. 在左侧的计算机树中选择计算机A，右键-控制-远程文件传输在弹出的提示窗口确认后等待计算机A确认； 3. 双方确认后会弹出一个类似于FTP的对话框； 4. 传送一些文件到远程机器，观察传送速度； 5. 从远程机器传送一些文件到本地机器，观察传送速度。 |
| 预期结果 | 文件成功传送，且传送速度正常。 |
| 测试结果 | 满足： 部分满足： 马 不满足： |
| 备注 | 80M的文件传输速度稍慢 |

## 4.7 文档加密

### 4.7.1文档加密基本设置

|  |  |
| --- | --- |
| 测试编号 | 文档加密设置基本设置 |
| 适用场景 | 重要的文档需要加密管理，从源头上保护文档安全。 |
| 用例描述 | 针对企业内重要的文档资料，以Word为例，添加自动加解密策略。  1.设置word为授权软件，用户生成Word文档或打开原有Word文档修改保存后自动加密；  2.加密用户可以打开Word加密文档；  3.非加密用户打开加密文档失败，保护文档信息安全。 |
| 测试步骤 | 1. 登陆控制台； 2. 选择计算机A，右键选择加密功能管理，选择授权透明加密，这个时候计算机A桌面右下角会出现一个加密客户端； 3. 然后继续在控制台上选择加密—>加密授权设置，点击右上角编辑按钮； 4. 在加密权限设置界面选择授权软件，勾选办公软件-word，模式默认为：自动加解密、禁止打印、剪切板、截屏等；点击确认退出； 5. 右键点击计算机A，选择加密管理功能，点击启用透明加密； 6. 在计算机A上，新建一个word文档或打开原有的word文档，修改文档内容，保存文档，查看文档是否成功加密； 7. 在计算机A上，打印word文档，将word文档的内容复制到记事本txt文件中，使用QQ截图截取word文档内容； 8. 将该文档拷贝到未安装客户端计算机上打开文档，测试是否成功。 |
| 预期结果 | 1. 计算机A保存的文档会自动加密； 2. 计算机A无法进行打印、复制、截图等操作； 3. 未安装客户端的计算机无法打开加密文档。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.7.2加密文档安全区域与访问权限

|  |  |
| --- | --- |
| 测试编号 | 加密文档安全区域与访问权限 |
| 适用场景 | 不同级别和不同部门的加密文档进行隔离，即本部门的加密文档在其他部门内无法直接访问。 |
| 用例描述 | 1. 禁止不同部门之间加密文档未授权情况下互相传阅； 2. 禁止同一部门不同职位级别之间的加密文档未授权情况下互相传阅； 3. 同一部门相同或更高级别用户、授权用户操作加密文档不受影响； 4. 默认五个级别：普通、内部、秘密、机密，绝密。 |
| 测试步骤 | 1. 登陆控制台； 2. 在工具栏找到点击文档安全管理—安全区域，点击按钮添加安全区域，添加两个安全区域，研发部和财务部； 3. 在左侧的计算机树中选中计算机A； 4. 选择加密—>加密授权设置； 5. 在加密授权设置界面中，选择安全区域，勾选指定安全区域与相应级别，勾选研发部 +普通； 6. 在加密授权设置界面中，选择加密文档默认安全属性，勾选对新产生的加密文档设置默认安全属性，修改设置权限和访问权限为研发部 +普通（访问权限里的公共安全区域要将其删除），点击确认退出； 7. 在左侧的计算机树中选中计算机B； 8. 重复步骤 4，5，6 ，安全区域更改为财务部 +普通； 9. 设置计算机A和计算机B的word为授权软件，并启用加密； 10. 在计算机A新建一个word文档A1，编辑保存；在计算机B新建一个word文档B1，编辑保存。将文档A1拷贝到计算机B上，将文档B1拷贝到计算机A上； 11. 在左侧的计算机树中选中计算机B； 12. 重复步骤 4，5，6 ，安全区域更改为研发部 +秘密； 13. 在计算机A新建一个word文档A2，编辑保存；在计算机B新建一个word文档B2，编辑保存。将文档A2拷贝到计算机B上，将文档B2拷贝到计算机A上。 |
| 预期结果 | 1. 计算机A生成加密文档A1、A2 的安全属性为研发部 +普通； 2. 第七步时，计算机B 生成的加密文档B1 的安全属性为财务部+普通； 3. 第九不时，计算机A无法打开文档B1，计算机B无法打开文档A1； 4. 第十步时，计算机B生成的加密文档B2的安全属性为研发部 +普通； 5. 第十一步时，计算机A无法打开文档B2，计算机B可以打开文档A2。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 | 1. 不同区域的权限不能互相访问； 2. 高等级权限可以访问低等级的文档，低等级权限不能访问高等级文档； 3. 系统默认的安全区域：公共安全区域+普通，为最低权限，所有加密用户都能访问。 |

### 4.7.3加密文档直接解密、外发

|  |  |
| --- | --- |
| 测试编号 | 加密文档直接解密、外发 |
| 适用场景 | 公司的文档进行了加密，但加密文档需要发送给公司之外的人员。 |
| 用例描述 | 1. 加密文档直接右键解密； 2. 加密文档直接右键外发。 |
| 测试步骤 | 1. 登录控制台； 2. 在左侧的计算机树中选中计算机A； 3. 选择加密—>加密授权设置； 4. 在加密授权设置界面中，选择常规，勾选允许直接解密文档，勾选允许直接外发文档，点确认退出； 5. 在计算机A上，右键点击加密的文档A1，选择文档加密系统，点击解密； 6. 在计算机A上，右键点击加密文档A2，选择文档加密系统，点击外发，进入创建外发文档界面，外发对象默认不选，外发配置勾选限制打开次数，最大打开次数为3次，其他选择默认，点击创建，默认选中生成可以执行文件，其他默认，选择路径，点击确定； 7. 将解密后的文档A1和外发文档A2\_docx.exe 拷贝到未安装客户端的计算机上打开。 |
| 预期结果 | 1. 未安装客户端的计算机，可以打开文档A1； 2. 未安装客户端的计算机也可以打开外发文档A2\_docx.exe，但是最多只能打开3次，打开3次后无法打开。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.7.4加密文档申请解密流程设置

|  |  |
| --- | --- |
| 测试编号 | 加密文档申请解密流程设置 |
| 适用场景 | 执行严格的解密申请流程，防止明文文档过多而无限制传播带来泄密风险。 |
| 用例描述 | 1. 创建审批管理员账户； 2. 创建申请流程； 3. 用户提交解密申请。 |
| 测试步骤 | 1. 登陆控制台； 2. 选择工具—账户，进入账户管理界面； 3. 点击按钮，新建账户，命名为 test1，常规页面，勾选具有加密功能管理权限，管理范围勾选测试组，加密功能勾选流程管理，点击确定退出； 4. 按照步骤3，创建账户，test2； 5. 选择申请管理—加密申请管理-审批流程管理，点击按钮，创建流程，基本设置中，申请类型选择解密申请或者全部，申请对象勾选测试组，文件设置、文档安全属性、外发对象、外发配置、临时离线默认； 6. 环节设置，点击按钮，创建环节，审批人员选择test1、test2 ，点击确定； 7. 然后点击完成，勾选刚刚新建的流程，点击右上角按钮，保存策略； 8. 使用test1或者test2 账户登录控制台，密码默认为空（也可以在加密客户端上-审批管理平台上登录输入账号密码登录），如在加密客户端上登录审批账号，需要在加密-加密授权设置里面勾选允许登录审批平台； 9. 在计算机A，右键点击加密文档，点击申请解密，输入申请理由，点击申请； 10. 审批员在控制台上收到申请信息后，查看申请信息，点击批准； 11. 管理员批准后，计算机A桌面右下角会弹出通知气泡，点击进入查看界面，点击完成申请，加密文档解密。 |
| 预期结果 | 计算机A加密文档可以解密。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.7.5安全密码设置

|  |  |
| --- | --- |
| 测试编号 | 安全密码设置 |
| 适用场景 | 提高加密系统的安全性，在客户端电脑进行敏感操作时，需要输入安全密码才能完成。 |
| 用例描述 | 1. 解密或者外发时需要输入密码； 2. 客户端离线后，登录加密系统需要输入安全密码； 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。 |
| 测试步骤 | 1. 给计算机A和B设置允许直接解密的权限，在控制台加密-加密授权设置，勾选允许允许直接解密文档； 2. 在计算机A上，右键点击托盘加密系统图标，点击常规选项，在安全密码设置中设置安全密码，安全密码初始为空；点击确认退出； 3. 在计算机A上右键解密一个加密文档，查看是否需要输入安全密码；注销加密系统（需要在加密-加密授权设置-常规的最下面勾选“允许客户端注销加密系统”），然后在客户端电脑任务栏图标，再右键开启加密功能，这时会提示是否输入安全密码； 4. 登录控制台； 5. 选择计算机B； 6. 选择加密—加密参数设置，点击编辑进入设置界面，在安全密码设置中，勾选必须设置安全密码； 7. 在计算机B上，右键解密一个文档，查看是否需要安全密码。 |
| 预期结果 | 1. 计算机A在解密和登录加密系统时，需要输入安全密码； 2. 计算机在解密文档时，需要输入安全密码，安全密码初始为空，必须要设置安全密码后，才能解密文档。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.7.6临时离线申请

|  |  |
| --- | --- |
| 测试编号 | 临时离线申请 |
| 适用场景 | 加密客户端出差办公时离开公司环境，既要防止因计算机丢失或被盗等原因造成的泄密，同时也不能影响出差用户工作。 |
| 用例描述 | 1. 离线计算机在授权时间内可打开加密文档，保证其工作正常进行； 2. 超出离线授权时间后生成文档不加密，不影响用户使用； 3. 超出离线授权时间后不能打开加密文档，保护文档安全。 |
| 测试步骤 | 1. 流程设置参考用例 5.17.4； 2. 在计算机A，右击右下角任务栏的加密图标，选择临时离线-申请；在临时离线窗口选择临时离线到期日期与时间，填写申请理由**，**点击申请提交离线申请信息； 3. 管理员登录控制台，收到申请信息，点击点击批准或拒绝下发审批结果； 4. 计算机A右下方有临时离线审批信息报警提示，点击报警信息，或右击右下角任务栏的加密图标，选择查看加密申请情况-临时离线申请，查看申请与审批信息； 5. 在计算机A分别测试，离线申请被拒绝与批准两种情况，客户端离线时是否能正常打开加密文档，离线超过申请日期后加密文档能否正常打开。 |
| 预期结果 | 1. 临时离线申请被批准后，客户端离线则进入紧急模式，能正常打开加密文档； 2. 临时离线申请被拒绝或者超过申请日期后，离线计算机不能打开加密文档。 |
| 测试结果 | 满足： 马 部分满足： 不满足： |
| 备注 |  |

### 4.7.7长期离线设置

|  |  |
| --- | --- |
| 测试编号 | 长期离线设置 |
| 适用场景 | 对于需要长期出差办公的用户，为了保证加密功能的正常使用，又要保护笔记本电脑的安全，防止丢失、被盗而导致泄密。 |
| 用例描述 | 1. 离线计算机在授权时间内离线授权登入后，可打开加密文档，保证其工作正常进行； 2. 离线计算机在授权时间内未离线授权登入则不可打开加密文档，防止因计算机丢失等原因导致文档泄密； 3. 未离线授权登入或超出离线授权时间后生成文档不加密； 4. 超出离线授权时间后不能打开加密文档，保护文档安全。 |
| 测试步骤 | 1. 登录控制台； 2. 选择计算机A； 3. 选择加密—长期离线授权，点击编辑按钮，进入长期离线授权设置界面； 4. 勾选启用离线授权，输入离线授权原因：长期出差，设置起始时间和结束时间；勾选允许直接解密文档，加密功能启用方式选择强制手动登录；勾选允许客户端注销加密系统； 5. 授权软件设置全部勾选，点击确定退出； 6. 在计算机A上，断开网络，然后右击右下角加密图标选择启用加密，输入安全密码，完成授权登入； 7. 在被测计算机上，测试授权登入后，打开加密文档是否成功，未授权登入时或者超过授权日期时打开加密文档是否成功。 |
| 预期结果 | 离线授权登入后，能正常打开离线授权软件范围以内的加密文档，超出授权日期或未离线授权登入则无法打开所有加密文档。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.7.8外发文档设置

|  |  |
| --- | --- |
| 测试编号 | 外发文档设置 |
| 适用场景 | 加密文档在发送给公司之外的人员时，需要防止二次泄密。 |
| 用例描述 | 1. 生成外发文档； 2. 打开外发文档。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 选择计算机A； 3. 选择加密—加密授权设置，点击编辑，进入设置界面，勾选允许直接外发文档，点击确认退出； 4. 在计算机A上，右键点击一个加密文档，选择文档加密系统—外发，进入创建外发文档界面； 5. 文档信息，可以点击，添加多个文档；外发对象保持默认；外发配置勾选限制打开次数，最大开发次数 3次；其他选择保留默认； 6. 点击创建，勾选生成可执行文件（.exe），点击确定，生成外发文档； 7. 将外发文档拷贝到非加密计算机打开。 |
| 预期结果 | 在非加密计算机可以打开外发文档，阅读文档内容；但是最多打开3次，打开3次后外发文档无法开，同时，外发文档不能打印、复制粘贴、截图、修改等。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 外发文档的申请流程与加密文档的解密申请流程设置类似。 |

### 4.7.9外发文档浮水印设置

|  |  |
| --- | --- |
| 测试编号 | 外发文档浮水印设置 |
| 适用场景 | 为了提高版权意识，可以在外发文档中设置外发文档浮水印，打开外发文档时，会自动带有浮水印信息。 |
| 用例描述 | 设置外发文档浮水印。 |
| 测试步骤 | 1. 登录IP-guard控制台； 2. 选择计算机A； 3. 选择加密—加密参数设置，点击编辑进入设置界面，拖动至最下方，窗口浮水印设置，选择启用外发文档浮水印，勾选启用策略，文字内容“test”,颜色选择红色，创建者信息选择计算机名称，阅读者信息选择用户名称，点击确定退出； 4. 在计算机A上创建一个外发文档，然后打开，查看是否有浮水印信息。 |
| 预期结果 | 计算机A上创建的外发文档带有浮水印信息。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 浮水印是由管理员在控制台统一设置，用户不能修改。 |

### 4.7.10邮件白名单解密设置

|  |  |
| --- | --- |
| 测试编号 | 邮件白名单解密设置 |
| 适用场景 | 为了提高加密文档的外发的效率，减少审批管理员的工作量，对于可信任的用户和合作商，希望邮件发送加密文件时自动解密文档。 |
| 用例描述 | 1. 在邮件客户端（foxmail、outlook）使用指定白名单邮箱发送加密文档给指定白名单合作商邮箱时，自动解密附件的文档，接收方可正常打开文档； 2. 使用非指定白名单邮箱发送加密文档给非指白名单合作间邮箱不解密附件文档，接收方无法正常打开文档； 3. 支持标准协议邮件白名单解密外发。 |
| 测试步骤 | 1. 登录控制台； 2. 选择计算机A； 3. 选择加密—加密参数设置，点击编辑进入设置界面，点击邮件白名单设置中，点击编辑邮箱地址规则设置，模式选择解密附件，在接受邮件白名单中输入Q邮箱地址；在发送邮箱白名单中，输入 A邮箱地址；点击确定退出； 4. 在计算机A中，使用A邮箱发送一封带加密文档附件的邮件给Q邮箱；然后在计算机A中使用A邮箱发送一封带加密文档附件的邮件给B邮箱。（此时的Q和B是没有启用文档加密的） |
| 预期结果 | 1. Q邮箱收到的附件是明文的，可以打开； 2. B邮箱收到的附件是加密的，不可以打开。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.7.11容灾时间设置

|  |  |
| --- | --- |
| 测试编号 | 容灾时间设置 |
| 适用场景 | 当企业经常会出现短暂的网络故障，导致主服务器与客户端经常会出现短暂的断开连接，如何保证加密系统正常运行。 |
| 用例描述 | 1. 网络或服务器出现故障后，在容灾时间内，加密客户端正常工作； 2. 故障时间超过容灾时间后，加密客户端无法正常使用加密功能； 3. 故障解除后，加密客户端连接服务器正常工作。 |
| 测试步骤 | 1. 登录控制台； 2. 选择计算机A； 3. 选择加密—加密参数设置，点击编辑进入设置界面，设置加密容灾时间 30分钟，（实际使用时，建议设置3天），点击确定退出； 4. 在计算机A上，断开网络，测试在容灾时间内，加密系统是否可以正常工作；超过容灾时间后，加密系统是否可以正常工作。 |
| 预期结果 | 1. 容灾时间内，加密系统可以正常运行； 2. 容灾时间外，加密系统停止运行。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.7.12备用服务器设置

|  |  |
| --- | --- |
| 测试编号 | 备用服务器设置 |
| 适用场景 | 在其他计算机上安装备用服务器，并设置与IP-guard主服务器相连，以防止主服务器故障时整个加密系统陷入崩溃，保证加密工作正常进行。 |
| 用例描述 | 1. 主服务器正常工作时，加密客户端连接主服务器正常运行； 2. 主服务器出现故障时，加密客户端连接备用服务器继续工作。 |
| 测试步骤 | 1. 登录控制台； 2. 选择菜单栏文档安全管理-备用服务器管理，进行相关设置； 3. 允许范围建议勾选全部IP地址，点击连接密码，设置连接的服务器为IP-guard主服务器IP，并设置连接密码，点击确定； 4. 返回备用服务器计算机B，右击桌面右下角任务栏备用服务器图标选择工具-设置连接参数； 5. 服务器连接设置主服务器地址为IP-guard主服务器IP，输入上述设置连接密码，主动轮洵勾选启动主动轮询，点击确定完成配置； 6. 测试当主服务器停止运行时，备用服务器是否有效工作，即客户端能否正常使用加解密功能。 |
| 预期结果 | 备用服务器安装成功，并且与主服务器连接成功，备用服务器服务启动成功，并且当主服务器故障等原因停止运行时备用服务器有效工作。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.7.13加密文档备份服务器设置

|  |  |
| --- | --- |
| 测试编号 | 加密文档备份服务器设置 |
| 适用场景 | 在其他计算机上安装文档备份服务器，防范终端加密文档丢失导致文档无法找回的风险。 |
| 用例描述 | 1. IP-guard授权文档备份服务器； 2. 客户端的加密文档可以备份到文档备份服务器。 |
| 测试步骤 | 1. 登录控制台； 2. 选择文档安全管理 - 文档备份服务器管理，在备份服务器列表中选择，然后设置授权范围 -测试组，点击授权； 3. 选择计算机A； 4. 选择加密—文档备份设置，点击编辑按钮，勾选启用加密文档自动备份任务，其他默认，点击确定退出； 5. 在计算机A，操作几个office类型的文档，过一段时间后，在备份服务器上查看是否有备份信息。 |
| 预期结果 | 文档备份服务器安装成功，并且通过主服务器授权成功，在计算机A设置备份策略后，文档备份服务器可以备份加密文档。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.7.14业务系统上传解密下载加密

|  |  |
| --- | --- |
| 测试编号 | 业务系统上传解密下载加密 |
| 适用场景 | 企业有自己的业务系统如OA、ERP、SVN等，上面存储有公司的核心数据文档，需要对其进行管控，防止员工下载泄密。 |
| 用例描述 | 1. 实现业务系统上传解密下载加密，保护业务系统数据安全 |
| 测试步骤 | 1. 登陆控制台； 2. 选择计算机A，右键选择加密功能管理，选择授权透明加密，这个时候计算机A桌面右下角会出现一个加密客户端； 3. 选择计算机A，在策略-客户端配置，新增一条客户端配置策略security\_proxy=1，此客户端配置策略是在没有安全网关的时候配置的，如有安全网关硬件进行测试，则不需要配置此策略； 4. 选择加密-安全通讯设置，点击右上角编辑按钮； 5. 在安全通讯设置，勾选启用对应用系统的保护； 6. 在安全进程，新增一个进程（如IE浏览器iexplore.exe），加密模式选择强制模式； 7. 在安全进程，新增一个进程（如谷歌浏览器chrome.exe），加密模式选择智能模式； 8. 智能模式设置-受保护服务器地址填写对应的业务系统IP:端口（如192.168.1.20:8282），或者填写域名，注意不需要加https，直接填IP或域名即可； 9. 在计算机A上，将一个加密文件test.docx上传到受保护业务系统192.168.1.20:8282上,然后在线打开， 10. 在一台没有安装加密客户端的电脑计算机D上，访问192.168.1.20:8282，将test.docx下载到本地； 11. 在计算机A上，从保护业务系统192.168.1.20:8282下载一个文档test1.xlxs。 |
| 预期结果 | 1. 计算机A使用IE浏览器和谷歌浏览器可以访问受保护的业务系统，使用其他浏览器无法访问受保护的业务系统 2. 计算机A使用IE浏览器访问受保护业务系统的时候，不能访问其他非受保护的地址，IE浏览器设置的是强制模式 3. 计算机A使用谷歌浏览器访问受保护业务系统的时候，可以访问其他非受保护的地址，谷歌浏览器设置的是智能模式 4. 在计算机D上，下载test.docx，下载下来是明文的，可以正常打开 5. 计算机A使用IE浏览器和谷歌浏览器可以在线打开预览之前上传的test.docx文件，下载来的文件，也是加密的。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 | 如需要防止非法用户（如计算机D没有安装客户端）访问受保护的业务系统，需要使用安全网关硬件来管控。 |

## 4.8 慧眼风险审计报表

### 4.8.1统计表

|  |  |
| --- | --- |
| 测试编号 | 统计表（打印、即时通讯、上网浏览、文档操作管控、移动存储、应用程序、邮件） |
| 适用场景 | 对计算机/用户在时间段内操作行为进行统计，通过统计数据发现内网风险。 |
| 用例描述 | 对文档打印、即时通讯聊天、网页浏览、文档操作、文档通过移动存储插拔、文档拷贝情况、应用程序使用情况、邮件发送/接收情况、资产情况进行统计。 |
| 测试步骤1 （打印统计表） | 1. 打开控制台，登录报表控制台； 2. 左边导航栏，双击查询，双击打印报表查询，选择标准打印统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计、按计算机+打印机统计、按打印机统计、按用户+打印机统计中的其中一种类型； 5. 可勾选按组统计； 6. 点击打印机，可选择参与统计的打印机； 7. 在右侧，可选择按照打印次数和打印页数进行统计； 8. 选择高级按钮，可选择更多条件进行统计； 9. 点击统计； 10. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤2 （即时通讯统计表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击即时通讯报表查询，选择标准即时通讯统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计、按聊天工具统计、按计算机+聊天工具统计、按用户+聊天工具统计中的其中一种类型； 5. 可勾选按组统计； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤3 （上网浏览统计表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击上网浏览报表查询，选择标准上网浏览统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计、按网站统计、按计算机+网站统计、按用户+网站统计中的其中一种类型； 5. 可勾选按组统计； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤4 （文档操作统计表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击文档操作报表查询，选择标准文档操作统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计中的其中一种类型； 5. 可勾选按组统计； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤5 （移动存储操作统计表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击移动存储报表查询，选择标准移动存储操作统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计、按移动存储统计、按计算机+移动存储统计、按用户+移动存储统计中的其中一种类型； 5. 可勾选按组统计； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤6 （应用程序运行统计表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击应用程序报表查询，选择标准应用程序运行统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计、按应用程序统计、按计算机+应用程序统计、按用户+应用程序统计中的其中一种类型； 5. 可勾选按组统计； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤7 （邮件统计表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击邮件报表查询，选择标准邮件统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计中的其中一种类型； 5. 可勾选按组统计； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 预期结果 | 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、资产报表都能查询到对应的统计数据，统计数据符合用户实际操作情况。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.8.2趋势表

|  |  |
| --- | --- |
| 测试编号 | 趋势表（打印、即时通讯、上网浏览、文档操作管控、移动存储、应用程序、邮件） |
| 适用场景 | 展现计算机/用户在某个时间段内操作行为的变化趋势，通过统计数据发现内网风险。 |
| 用例描述 | 对文档打印、即时通讯聊天、网页浏览、文档操作、文档通过移动存储插拔、文档拷贝情况、应用程序使用情况、邮件发送/接收情况进行统计，发现内网安全风险趋势变化情况。 |
| 测试步骤1（打印趋势表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击打印报表查询，选择标准打印趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按标准趋势表、按计算机统计、按用户统计、按打印机统计中的其中一种类型； 5. 可选择统计周期，按天、周、月、季度、年； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤2 （即时通讯趋势表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击即时通讯报表查询，选择标准即时通讯趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按标准趋势表、按计算机统计、按用户统计、按聊天工具统计中的其中一种类型； 5. 可选择统计周期，按天、周、月、季度、年； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤3 （上网浏览趋势表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击上网浏览报表查询，选择标准上网浏览趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按标准趋势表、按计算机统计、按用户统计、按网站统计中的其中一种类型； 5. 可选择统计周期，按天、周、月、季度、年； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤4 （文档操作趋势表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击文档操作报表查询，选择标准文档操作趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按标准趋势表、按计算机统计、按用户统计中的其中一种类型； 5. 可选择统计周期，按天、周、月、季度、年； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤5 （移动存储操作趋势表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击移动存储报表查询，选择标准移动存储操作趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按标准趋势表、按计算机统计、按用户统计、按移动存储统计中的其中一种类型； 5. 可选择统计周期，按天、周、月、季度、年； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤6 （应用程序运行趋势表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击应用程序报表查询，选择标准应用程序运行趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按标准趋势表、按计算机统计、按用户统计、按应用程序统计中的其中一种类型； 5. 可选择统计周期，按天、周、月、季度、年； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 测试步骤7  （邮件趋势表） | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击邮件报表查询，选择标准邮件趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按标准趋势表、按计算机统计、按用户统计中的其中一种类型； 5. 可选择统计周期，按天、周、月、季度、年； 6. 选择高级按钮，可选择更多条件进行统计； 7. 点击统计； 8. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 预期结果 | 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、资产报表都能查询到对应的统计数据，能按照时间陈列趋势图，统计数据和趋势图符合用户实际操作情况。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.8.3综合数据统计表

|  |  |
| --- | --- |
| 测试编号 | 标准综合数据统计表 |
| 适用场景 | 对计算机/用户在时间段内多种操作行为进行统计，通过统计数据发现内网风险。 |
| 用例描述 | 对文档打印、即时通讯聊天、网页浏览、文档操作、文档通过移动存储插拔、文档拷贝情况、应用程序使用情况、邮件发送/接收情况进行综合统计，同时呈现不同操作行为的统计数据。 |
| 测试步骤 | 1. 打开控制台，登录报表控制台； 2. 左边导航栏，双击查询，双击综合统计报表查询，选择标准综合数据统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计中的其中一种类型； 5. 选择高级按钮，可选择更多条件进行统计； 6. 点击统计； 7. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 预期结果 | 能够对打印页数、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、上网浏览时间和报警次数进行统计，统计数据符合用户实际操作情况。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.8.4征兆事件统计表

|  |  |
| --- | --- |
| 测试编号 | 征兆事件统计表 |
| 适用场景 | 依据征兆条件对计算机/用户行为进行统计，产生征兆事件（低、重要、严重），发现潜在安全风险 |
| 用例描述 | 对打印操作、文件操作、移动存储操作、邮件、上网浏览、即时通讯、应用程序等日志设置一定的阈值，当操作行为达到阈值时，产生一个征兆事件，并对征兆事件进行统计。 |
| 测试步骤 | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击征兆事件报表查询，选择标准征兆事件统计表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机+征兆级别统计、按用户+征兆级别统计、按征兆类型+征兆级别统计、按计算机+征兆类型统计、按用户+征兆类型统计中的其中一种类型； 5. 选择高级按钮，可选择更多征兆条件进行统计； 6. 点击统计； 7. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 预期结果 | 当打印操作、文件操作、移动存储操作、邮件、上网浏览、即时通讯、应用程序等操作行为达到阈值时，能统计到征兆事件，征兆事件的数量符合实际操作行为。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.8.5征兆事件趋势表

|  |  |
| --- | --- |
| 测试编号 | 征兆事件趋势表 |
| 适用场景 | 展现时间段内用户操作行为产生征兆事件的情况，发现潜在安全风险 |
| 用例描述 | 对打印操作、文件操作、移动存储操作、邮件、上网浏览、即时通讯、应用程序等日志设置一定的阈值，当操作行为达到阈值时，产生一个征兆事件，并展示征兆事件在时间段内的变化趋势。 |
| 测试步骤 | 1. 登录报表控制台； 2. 左边导航栏，双击查询，双击征兆事件报表查询，选择标准征兆事件趋势表； 3. 在查询条件中选择日期，计算机/用户； 4. 在统计类型中可选择按计算机统计、按用户统计、按征兆级别统计、按征兆类型统计中的其中一种类型； 5. 选择高级按钮，可选择更多征兆条件进行统计； 6. 点击统计； 7. 在统计图表中右键—统计图设置，可选择需要参与统计的项目。 |
| 预期结果 | 当打印操作、文件操作、移动存储操作、邮件、上网浏览、即时通讯、应用程序等操作行为达到阈值时，能统计到征兆事件，征兆事件的数量符合实际操作行为。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.8.6周期报表

|  |  |
| --- | --- |
| 测试编号 | 周期报表 |
| 适用场景 | 依据用户自定义的条件，系统定时生成各种周期统计报表，可快速查看已经生成的统计数据。 |
| 用例描述 | 1. 选择需要产生周期报表的模块 2. 设置统计条件 3. 选择统计数据的呈现方式 4. 设置统计的周期 |
| 测试步骤 | 1. 登录报表控制台； 2. 左边导航栏，右键点击报表，可选择新建报表，选择从模板创建、从报表创建、从查询条件创建；（以“从模板创建”为例） 3. 进入创建报表页面，在左边栏中，选择模块，点击下一步（N）； 4. 在高级条件设置中，设置统计条件，点击下一步（N）； 5. 在报表统计类型设置中设置报表的呈现方式，点击下一步（N）； 6. 在设置报表的周期中选择时间范围和报表的生成时间，点击下一步（N）； 7. 点击完成即可。 |
| 预期结果 | 系统依据设定的条件按照规定时间产生报表。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

### 4.8.7邮件报告设置

|  |  |
| --- | --- |
| 测试编号 | 邮件报告设置 |
| 适用场景 | 管理员不希望登录报表控制台设置条件查看统计数据，而是系统自动将统计数据通过邮件发送给管理员。 |
| 用例描述 | 1. 设置需要发送哪些报表模块 2. 设置接收报表的邮件地址 |
| 测试步骤 | 1. 登录报表控制台； 2. 在工具栏，右键点击报表，选择邮件报告； 3. 进入邮件报告设置页面，在左边栏中，选择新建按钮； 4. 在右边栏填写配置名称，在报表设置中选择报表； 5. 在邮件设置中填写邮件标题、收件人地址、选择报表的呈现方式（将报表添加到正文、报表以附件的形式发送），可选择压缩附件，设置解压密码； 6. 点击保存即可。 |
| 预期结果 | 系统依据设定的条件按照规定时间发送报表给指定的邮件地址。 |
| 测试结果 | 满足： 部分满足： 不满足： |
| 备注 |  |

# 五、测试总结

在所有功能模块用例的测试过程中，根据测试步骤进行测试，实际结果与预计的结果一致。