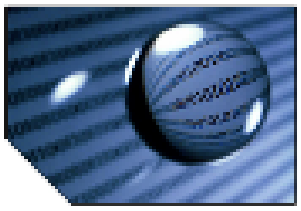
中软统一终端安全管理系统 8.0

系统介绍

中国软件与技术服务股份有限公司

CHINA NATIONAL SOFTWARE & SERVICE CO., LTD.



目　录

第一章　系统概述

随着信息化安全技术的不断发展，各种内网安全管理问题逐步凸现出来。据 IDC 调查报告显示超过 85%的网络安全威胁来自于内部，其危害程度更是远远超过黑客攻击所造成的损失，而这些威胁绝大部分是内部各种非法和违规的操作行为所造成的。

内网安全问题已经引起了各级单位的广泛重视，随着安全意识的不断增强，安全投入逐步增加，但是内网的安全事件却不断地增多。分析其原因我们认为主要有以下几个方面：

- **有章不循，有规不依，企业内网安全合规性受到挑战。**

很多公司明文规定安装操作系统必须打最新的补丁，但是终端用户依然我行我素导致操作系统补丁状况不一，从而给蠕虫病毒、木马程序和黑客软件带来了可乘之机。同时有些单位购买了防病毒软件，但是终端用户没有按照单位统一部署的要求安装防病毒软件，或者有些终端用户虽然安装了防病毒软件，但是没有及时更新病毒库，导致计算机病毒有机可乘。对于终端安全管理，公司建立了很多安全制度，但是终端用户不按照公司安全规定要求，将不安全的计算机接入网络，从而引入了内网安全威胁，企业内网的安全合规性受到了严峻的挑战。

- **谋一时，而未谋全局，终端系统被划分为多个独立的信息安全孤岛。**

各单位在解决各种内网安全问题上，通常缺乏统一、全面的内网安全解决方案。按照“头痛医头，脚痛医脚”的内网安全防护加强思路，采购并部署了多款终端安全管理的产品，比如：身份认证、补丁管理、软件分发、病毒防护软件等等。但是这些终端安全防护软件来自于不同的安全厂商，各种软件之间各自为政，缺乏统一管理、协调工作的机制，最终导致个人桌面系统被划分为一个个独立的信息安全孤岛，因此出现了终端安全管理混乱、内网安全漏洞百出，内网安全事件防不胜防。

- **百花齐放，百家争鸣，终端系统终因难堪负重，系统性能急剧下降。**

为了加强终端安全管理，在个人桌面系统上同时安装了不同厂家的终端代理。每种代理程序都需要实现自我防护、网络通信、运行监控等程序调度机制，需要重复的占用系统有限的 CPU、内存等系统资源，导致个人桌面系统运行速度变慢，系统性能急剧下降。同时，由于不同厂家的软件存在很多功能重叠的部分，而这些重叠部分往往是采用类似技术开发，从而导致不同软件之间频繁发生应用冲突。

◆ **治标不治本，本末倒置，软件购买费用增加，系统维护成本成倍增长。**

通常终端管理软件大致分为三个组件，即：服务器、控制端、客户端代理。每种服务器软件都需要独立的数据库和硬件服务器支撑，无形中增加了软件的部署成本。同时，由于每种软件都有自己的控制台程序，管理员要针对每套系统生成它的控制策略，每套系统的数据审计都是分开的，管理工作非常多，管理员为每天的维护工作疲于奔命，从而导致管理疏忽。

针对以上几种原因，以及中软公司在对企业内网安全管理展开全面调查的基础上，创造性地形成了一套完备的终端安全“一体化”解决方案。在过去的几年里中软公司一直致力于内网安全的研究，并在国内最早提出了一系列的内网安全管理理论体系和解决方案。内网失泄密防护软件--中软防水墙系统的推出填补了国内内网安全管理软件的空白，并获得了若干国家专利局的技术专利。防水墙系统连年获奖，其中在 2006 年“防水墙”被计算机杂志评为 2005 年度新名词。

中软公司早在 2001 年就开始致力于内网失泄密软件的开发，先后向市场推出了中软防水墙系统 7.0 版本、7.0+版本和 7.2 版本。随着内网安全管理的复杂化，中软公司在复用防水墙系统成熟技术的基础上，引入先进的内网安全管理理念和新的内网安全管理技术重新搭建系统体系结构，自主研发了中软统一终端安全管理系统 8.0（CSS United End-Point Management System,简称 UEM8.0）。

该系统是以“木桶原理”为理论依据，以安全策略为驱动，按照 PDR 安全模型的“保护-检测-响应”工作流程循环检测，同时结合保密规定的“等级防护”指导方针，采用多种安全技术实现了对终端主机全方位、多层次的安全防护。按照“保护-检测-响应”的工作流程逐步完善终端安全防护策略，并将事件处理方式和处理流程登录到用户知识库，逐步形成内网事故应急响应流程和共享安全解决方案的知识库。

第二章　体系结构和运行环境

2.1 系统体系结构

系统分为三个组件：客户端、服务器和控制台，系统采用分布式监控，集中式管理的工作模式。组件之间采用 C/S 工作模式，组件的通信是采用 HTTP/HTTPS 加密传输方式。支持任意层级的服务器级联，上下级服务器之间采用 HTTPS 协议进行数据交换。体系结构如图 1 所示。

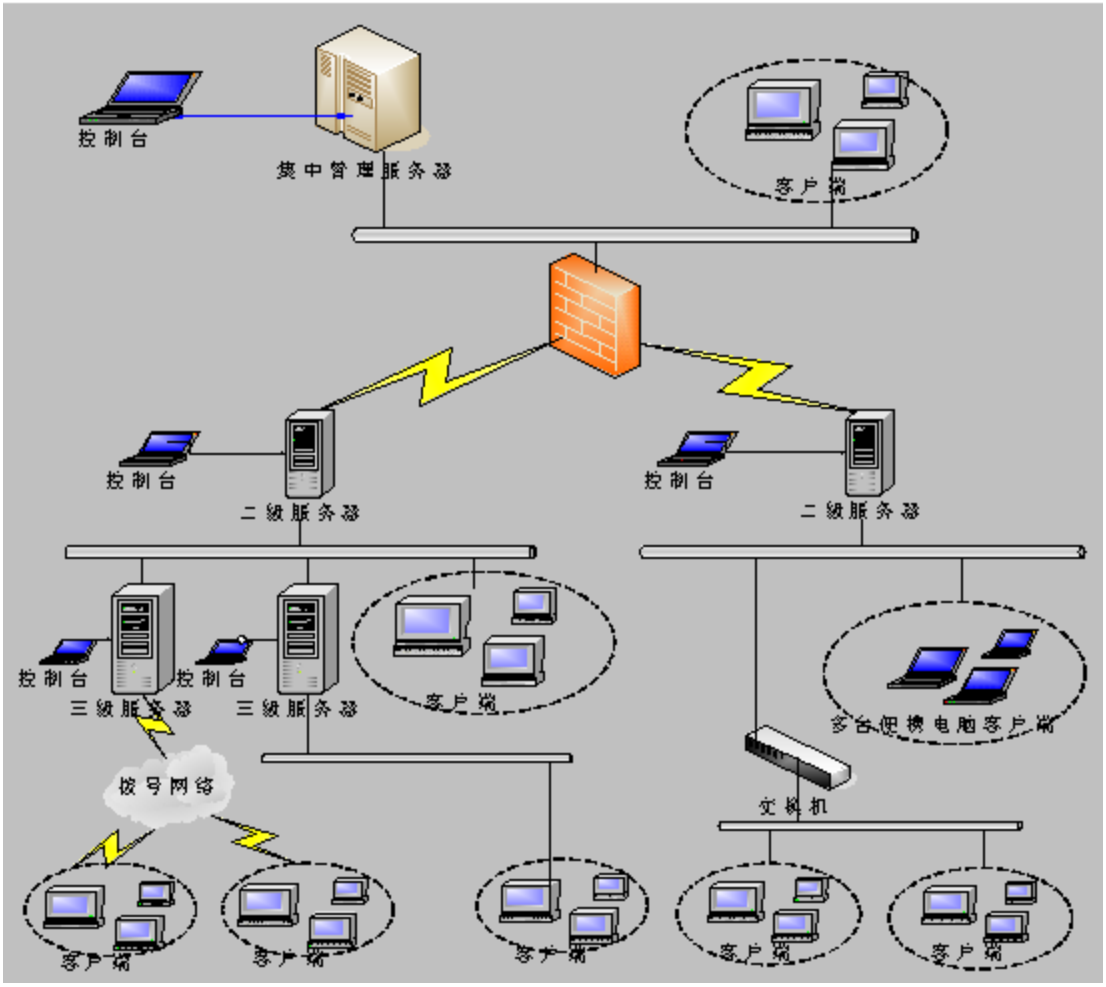


图 1　系统体系结构图

■ **客户端：**安装在受保护的终端计算机上，实时监测客户端的用户行为和安全状态，实现客户端安全策略管理。一旦发现用户的违规行为或计算机的安全状态异常，系统及时向服务器发送告警信息，并执行预定义的应急响应策略。

■ **服务器：**安装在专业的数据服务器上，需要数据库的支持。通过安全认证建立与多个客户端系统的连接，实现客户端策略的存储和下发、日志的收集和存储。上下级服务器间基于 HTTPS 进行通信，实现组织结构、告警、日志统计信息等数据的搜集。

■ **控制台：**人机交互界面，是管理员实现对系统管理的工具。通过安全认证建立与服务器的信任连接，实现策略的制定下发以及数据的审计和管理。

2.2 推荐硬件需求

客户端个数	<200	200-500	500-1000	>1000
服务器主机个数	1	1	1	1+
服务器	CPU P4 3.0 RAM 1GB HDisk 120GB	CPU P4 3.0 AT RAM 2GB HDisk 240GB	CPU P4 3.0 AT RAM 4GB HDisk 480GB	CPU Xeon 1G*4 RAM 4GB SCSI Disk 240GB RAID 5
控制台	CPU P4 2.0 RAM 512MB HDisk 40GB	CPU P4 2.0 RAM 1GB HDisk 40GB	CPU P4 3.0 RAM 1GB HDisk 40GB	CPU P4 3.0 RAM 1GB HDisk 80GB
客户端	CPU P4 2.0/ RAM 512MB/ HDisk 40GB			
审计平台	CPU P4 2.0/ RAM 512MB/ HDisk 40GB			

表格 1　系统推荐硬件需求

2.3 推荐软件需求

	操作系统	所需其他软件支持
服务器	Microsoft Windows Server 2003 / Advanced Server（32/64位）	SQL Server 2000+SP4 SQL Server 2005 SQL Server2008或达梦数据库。硬件“加密锁”驱动程序
控制台	Microsoft Windows Server 2003，Microsoft Windows 2000 Professional / Server / Advanced Server, Microsoft Windows XP	
客户端	Microsoft Windows 2000 Professional / Server / Advanced Server, Microsoft Windows XP Professional，Microsoft Windows Server 2003，Microsoft Windows Vista (Ultimate / Business)，Microsoft Windows7（Ultimate / Enterprise / Business）（32/64 位）	
审计系统	Microsoft Windows 2000 Professional / Server / Advanced Server, Microsoft Windows XP, Microsoft Windows Server 2003	SQL Server 2000+SP4 SQL Server 2005 SQL Server2008或达梦数据库

表格 2　系统软件需求

提示：

- 安全管理系统服务器，包括服务器软件和后台支持数据库。建议在专用主机上安装安全管理系统服务器，并且关闭所有与安全管理系统无关的不必要的服务。支持操作系统为 MS Windows 2003 系列，推荐 Advanced Server 版本。
- 以上操作系统，没有特别说明，仅指 32 位操作系统。

- 安全管理系统客户端不支持 Linux 系统，不能在 windows 双系统下同时安装 UEM 客户端。
- 为保证用户正常使用安全管理系统，最好将安全管理系统服务器、控制台和客户端分别运行于独立的系统之上，同时用户安装前应将 Windows 版本进行升级，安装各自版本最高补丁。

第三章　系统功能

随着内网终端安全地位的合理化，终端安全管理将进一步沿着整合化、平台化、统一化、基础化的方向发展。内网终端安全一体化的需求越来越强烈，终端安全产品的形态将逐步发生变化，最后发展为兼顾安全防御与安全管理。终端安全发展的历史使命终将通过一款“大、一、统”的终端安全产品来实现。所谓“大”就是该产品功能所涵盖的范围大，它不但要包含网络接入认证、系统身份认证、资产管理、补丁管理、软件分发，还要包涵系统运行监控、用户行为监控等终端软件的所有功能。所谓“一”就是一个终端代理、一台服务器就可以实现上述所有功能， 一个网络管理员就可以全局控制整个内网安全。所谓“统”就是指对所有的桌面系统应用**统一的安全策略**，对所有的终端用户采用**统一的终端管理策略**，对终端产生的日志进行**统一的日志分析，**为所有管理员提供**统一的应急响应知识库**。各功能部件之间协调工作，统一管理，形成一个高效有机的安全代理。通过统一的桌面管理平台降低系统的复杂度，提高了个人桌面系统的工作性能，降低了用户的维护管理成本。

针对以上终端计算机用户的安全需求，中软公司对政府、军工和高新技术企业的终端计算机管理问题展开了全面的调查，借鉴中软防水墙系统的开发经验，以等级防护和国家关于涉密计算机管理的相关规定为蓝本，创造性地形成了一款终端安全管理系统，该系统从终端安全管理、终端运维管理、用户行为管理、数据安全管理、系统身份认证管理，同时辅助这些功能系统提供了监控日志的统计与分析功能和系统运行管理功能。

3.1 基本功能

3.1.3 用户身份认证

身份认证是系统应用安全的起点，通过硬件 USBKey 和口令认证登录 Windows 系统用户身份，保证进入 Windows 系统用户身份的合法性；对登录用户权限进行合法性检查，保证用户权限的合规性。具体功能如下：

- **基于 USBKey 的身份认证**，将用户信息和证书内置于 USBKey 硬件中，通过读取 USBKey 中的用户信息实现登录用户身份认证，实现双因子认证，提高了主机身份认证的安全强度。同时为了增强系统的灵活性，对于 USBKey 用户，系统管理员可要求该用户进行 USBKey 和

Windows 双因子认证登录系统，也可允许该用户无需输入 Windows 口令，只使用 USBKey 完成登录认证。

- **登录用户权限合法性检查**，检查登录 Windows 系统的用户权限，当发现登录用户权限与策略设置的登录用户权限不一致时，系统及时阻止非法用户登录，并向服务器发送告警信息。该项功能主要是防止用户通过非法途径提升自身用户权限而达到某种非法目的，例如：策略设置只能是 USER 权限用户登录计算机，如果登录计算机的用户拥有 Administrator 或 PowerUser 权限则系统自动阻止该用户登录。

3.1.2 网络访问控制

规范计算机用户的网络访问行为，根据业务相关性和保密的重要程度建立信任的虚拟安全局域网。网络防护有两个层面的含义：第一是防止用户误操作或蓄意泄漏企业的敏感信息；第二是防止黑客通过互联网透过防火墙非法获取客户端的敏感信息。实现了从网络层到应用层的多层次防护，具体功能如下：

- **网络层防护**：IP 地址访问控制、TCP/UDP/ICMP 协议控制；
- **应用层防护**：HTTP/FTP/TELNET/SMTP/WEBMAIL/BBS/NETBIOS 控制；

控制策略有：禁止访问、自由访问。禁止访问时提供仅开放白名单功能，实现只开放白名单地址，其它地址全部禁止；自由访问时提供黑名单功能，实现只禁止黑名单地址，其它地址全部开放；同时提供三种日志记录模式：记录被禁止的访问、记录未知的访问和记录信任的访问，对 FTP、SMTP 访问控制和文件打印，可以记录文件内容。

3.1.3 非法外联控制

通过对 Modem 的控制实现非法外联的监控。

控制策略有：禁止访问、自由访问和条件访问。禁止访问时提供仅开放白名单功能，实现只开放白名单地址，其它地址全部禁止；自由访问时提供黑名单功能，实现只禁止黑名单地址，其它地址全部开放；同时提供三种层次的记录：记录被禁止的访问、记录未知的访问和记录信任的访问，同时对 FTP、SMTP、和打印可以提供文件备份功能。

3.1.4 接口外设管理

统一配置计算机外设接口的控制策略，动态的关闭与开启外设接口。所能控制的接口有：USB

接口、SCSI 接口、串行总线、并行总线、红外接口、PCMCIA 接口、软盘控制器、火线 1394 接口、无线网卡接口、DVD/CD-ROM 驱动器、蓝牙接口、第二块网卡接口。

接口访问控制的策略分为：允许和禁止两种，在禁止策略下的尝试访问向安全管理系统服务器报警。同时提供了接口设备白名单和黑名单定义的功能，实现在接口禁止或者接口开放情况下某些设备放开或禁止使用。

3.1.5 移动存储介质管理

对移动存储介质的访问进行统一的控制，控制模式可以分为：自由使用、禁止使用、设置为只读、拷贝文件加密、拷贝文件记录日志并备份文件内容等五种控制策略。其中拷贝文件加密为个人加密的加密方式，个人加密只能在当前主机的当前个人用户下才能解密。

3.1.6 CDROM/CDRW/刻录机的控制

对光盘介质的访问进行统一的控制，控制模式可以分为：自由使用、禁止使用。刻录机控制支持：禁止使用、自用使用、只读使用等三种。

3.1.7 辅助硬盘的控制

对计算机上挂接第二块硬盘的访问进行统一的控制，控制模式可以分为：自由使用辅助硬盘和禁止使用辅助硬盘。

3.1.8 打印机管理

根据企业的打印机管理制度和计算机用户业务关系统一制定打印机的管理策略，具体的功能控制项如下：

- **监控用户打印行为：**统一制定计算机用户的打印管理策略，控制模式可以分为：自由使用打印机、禁止使用打印机和允许使用打印机并记录打印文件名称(可选项为备份文件内容)。使用打印机能够基于打印机名称、打印进程以及虚实打印机进行控制。
- **打印行为违规报警：**在禁止打印机策略时如果用户执行打印操作，系统立即向服务器发送违规打印操作信息。

3.2 可信移动存储介质管理

该功能实现了用户对移动存储介质管理的要求，对可信移动存储介质从购买到销毁的整个生命周期进行管理和控制。

可信移动存储介质管理通过授权认证、身份验证、密级识别、锁定自毁、扇区级加解密、日志审计等六个途径对可移动存储设备的数据进行安全防护，使得未通过身份验证的用户或密级不够的主机，不可访问存储在可信移动存储介质上的文件。

- 授权认证：管理员对移动存储介质进行注册授权，写入授权信息。
- 身份验证：客户端使用可信移动存储介质时，对用户的身份信息进行验证。
- 密级识别：客户端使用可信移动存储介质时，需对客户端主机密级进行验证。
- 锁定自毁：客户违规使用可信移动存储介质时，对磁盘进行锁定或自毁，保证数据的安全性。
- 扇区级加解密：文件数据的加解密由系统底层驱动自动进行，对用户是透明的。
- 日志审计：对用户使用可信移动存储介质所产生的日志进行审计和查看。

可信盘的制作和管理主要由系统管理员完成：

- **磁盘的库存管理**

系统管理员完成对普通磁盘的入库登记，以备制作可信盘，或对入库的磁盘进行信息销毁等。

- **磁盘授权管理**

管理员对移动存储介质进行注册授权，写入授权信息，即完成可信磁盘的制作、解锁、回收、以及商旅盘的使用激活与反激活等操作管理，同时当可信磁盘需要跨服务器使用时，可启用该功能。另外，客户端也可通过在线审批方式进行可信磁盘的授权。

- **授权信息管理**

系统管理员可查询可信磁盘信息、撤销可信盘的授权等。

- **可信磁盘文件操作策略定义**

包括定义可信磁盘文件读、写操作的监控策略，以及设置是否允许在可信磁盘上直接运行可执行文件等，以防止病毒的运行和传播。

- **可信磁盘日志审计**

无论是普通可信磁盘，还是商旅磁盘，在磁盘使用过程中所产生的日志都需要上传到服务器中，所要求记录的日志包括：

可信磁盘使用台帐、磁盘锁定与自毁日志、磁盘违规使用日志、磁盘使用口令更改日志、

磁盘的文件操作日志、可信磁盘跨服务器使用功能的启用与关闭日志、以及跨服务器使用过程的日志记录。

3.2 终端接入管理

对接入内网的计算机进行统一的管理，未经许可的计算机不能接入内网，其主要功能如下：

3.2.1 终端接入认证

通过登录用户的用户名和口令检查接入用户的合法性，阻止外来主机在没有得到管理员许可的情况下非法接入内部网络。

3.2.2 终端安全检查

对接入内网的计算机必须通过安全性检查才能访问内部网络资源，主要功能如下：

对通过接入认证的计算机进行安全性检查，检查的策略包括两个方面：防病毒软件检查、操作系统补丁检查和必备软件安装运行检查。如果没有达到安全检查的基准，则系统只能访问内部修复服务器，不能访问内部网络资源。当系统执行自我修复操作后（如：安装操作系统补丁或安装防病毒软件），如果安全状态达到相应的标准那么该计算机即可正常访问内部网络资源。

3.2.3 内网安全扫描

内网安全扫描是终端安全管理系统的一个组件，它的主要功能是扫描局域网内部的存活计算机信息，并对这些计算机进行合法性分析。通过子网配置和参数设置后，各个网段的代理向本网段发送探测数据，并收集数据提取存活主机信息，然后各网段代理分别将本网段数据信息发送至服务器。服务器在分析数据之后，通过控制台显示被探测到主机的相关信息。这些信息包括主机的 IP 地址、Mac 地址、是否安装 UEM 客户端、合法性、一致性、是否例外主机等。该组件可以通过交换机阻断功能或 ARP 欺骗阻断功能来阻断不合法主机，并记录扫描产生的日志信息。

3.3 补丁管理与软件分发管理

3.3.1 补丁分发管理

统一配置终端计算机的补丁管理策略，实现对系统补丁状况的扫描，自动完成补丁分发。系统所支持的补丁包括：Windows 操作系统补丁系列、office 系列办公软件补丁、SQL Server 系列补丁

等微软产品的补丁，具体功能如下：

- **制定统一的补丁管理策略**，通过设置补丁来源确定补丁服务器 WSUS 的地址和 WSUS 统计地址，按照补丁检测周期定期检测客户端补丁安装状况。
- **实现统一的补丁更新管理**，通过设置终端策略实现系统补丁更新，更新模式有两种：手动更新补丁和自动更新补丁。
  - 手动更新补丁模式，通过策略设定对特定补丁的检测，如果客户端没有安装这类的补丁，则根据事先设定的下载优先级从补丁服务器下载补丁并安装补丁。
  - 自动更新补丁模式，通过设定自动更新方式，实现三种方式的安装和下载：通知下载和通知安装、自动下载和通知安装、自动下载和自动安装三种方式，通过设定自动更新时间点和更新完成是否重启计算机等参数实现客户端补丁的自动安装。

3.3.2 软件分发管理

规划企业统一分发的软件安装包，按照统一的软件分发策略，自动完成企业软件的部署，其主要功能如下：

- 软件包管理，按照软件包信息和安装环境创建需要分发的软件包，它包含软件位置、安装环境等相关信息。可支持 MSI、可执行文件、批处理文件三种形式的软件包。
- 软件包分发，选择分发软件包的类型，根据统一设定的分发策略可实现多种类型的软件分发，具体类型如下：
  - 软件下载优先级，根据程序运行的优先级可以设置为：前台、高、中、低四种优先级；
  - 软件下载类型，根据下载的紧迫性要求可以分为：立即下载、时间点下载和分时段下载三种下载模式。而时间点下载有可以设置立即下载的起始时间；分时段下载可以分为多个时段下载，每个时段需要设置起始和终止时间。
  - 安装类型，可以分为静默安装和交互安装两种方式。
  - 安装时间类型，可以分为立即安装、时间点安装和等待 N 分钟后安装。

同时系统对标准格式的安装包在终端主机上安装结果（成功/失败）进行跟踪反馈，管理员可以根据反馈结果形成统计报表。

3.4 终端安全运维管理

按照统一的安全策略监控客户端的运行状况，通过软件自动分发和软硬件资产的统一管理大大节约了企业信息系统的维护成本，通过系统远程帮助控制实现远程维护计算机，清除系统故障。系统具体功能如下：

3.4.1 系统运行状况监控

为管理员随时提供远程终端主机的运行状态变化信息，自动对指定的异常情况进行报警，根据管理员预定义策略及时阻断远程主机的违规行为。具体功能项如下：

- **监控信息管理**，实时监测计算机的资源使用情况，当发现系统资源超过管理员设定的监测阀值时，根据管理员预定义的响应策略阻止用户行为或向服务器发送告警，具体所能监控的信息如下：
  - **计算机名称监控**，禁止计算机用户修改计算机名称的行为。
  - **系统资源监测**，监测 CPU、内存的使用情况，当 CPU、内存超过管理员设置的监测阀值时，系统向服务器发送告警信息；监测硬盘的使用情况，当硬盘空闲空间小于管理员设置的阀值时，系统向服务器发送告警信息。
  - **网络流量监测**，监测计算机网络的实时流量和总流量，当网络流量超过阀值时系统向服务器发送告警信息。
  - **文件共享监测**，监测共享文件夹的添加、删除，当系统共享文件夹发生变化时，系统向服务器发送告警信息。
  - **文件操作监测**，监测用户创建文件、读写文件、重命名文件和删除文件的操作行为，可以设置所监测的文件名、文件后缀和文件路径。
  - **用户和组操作监测**，监测用户和组的添加、删除和属性改变的用户操作行为。
  - **系统服务监测**，监测系统服务的启动和停止的变化情况，并记录日志。
  - **网络配置**，监控系统网络配置的变化情况，禁止用户修改 IP 地址。
  - **系统日志**，设置获取远程计算机的系统日志上传周期。
- **查看系统信息**，及时获取远程主机的资源信息，包括：进程、网络、帐户和组、服务、共享、活动窗口、驱动、硬件、内存、会话信息、系统信息和系统日志。

3.4.2 软硬件资产管理

自动发现和收集计算机上的软硬件资产信息，跟踪软硬件资产信息变化情况，对非授权的软硬件资产的变更产生报警。具体功能相如下：

- **资产信息查看**，自动收集计算机用户的软硬件资产信息。其中硬件信息包括处理器、硬盘、内存、BIOS、光驱、显卡、声卡、网卡、显示器、输入设备、接口控制器、调制解调器、系统端口和插槽共计 14 种类型的硬件资产；软件资产包括系统软件、应用软件两种类型；还包括有操作系统信息和客户端信息。
- **软件管理策略**，规范用户使用软件的范围，通过设置安装程序黑白名单或基线方式保证用户启动进程的合法性。获取计算机用户的软件安装情况，并能对全网的软件安装情况进行统计。
- **硬件管理策略**，定义非法硬件名单，可定义的非法硬件包括：调制解调器、无线网卡、打印机、采集卡、刻录机、软驱、移动存储器、键盘和鼠标。系统一旦识别出非法硬件后立即向服务器发送告警信息。
- **硬件基线设置**，定义硬件设备的运行基线，当发现硬件设备与运行基线不一致时，系统立即向服务器发送告警信息。能定义为基线的硬件设备有 CPU、BIOS、硬盘、网卡、显卡、光驱、内存和声卡。

3.4.3 安全策略管理

按照企业终端计算机安全管理规定，统一配置终端计算机的 Windows 安全策略，实现集中的安全策略配置管理，统一提高终端计算机用户的安全策略基线。系统所能配置的安全策略如下：

- 帐户密码策略监视，统一监视 Windows 密码策略的启用情况和策略参数，对不符合安全策略的状态进行报警。
- 帐户锁定策略监视，统一监视 Windows 帐户锁定策略的启用情况和策略参数，对不符合安全策略的状态进行报警。
- 审核策略监视，统一监视 Windows 审核策略的启用情况和策略参数，对不符合安全策略的状态进行报警。
- 共享策略监视，统一监视 Windows 共享（包含默认共享）情况，对不符合安全策略的状态

进行报警。

- 屏保策略监视，统一监视屏幕保护策略的启用情况和策略参数，对不符合安全策略的状态进行报警。

3.4.4 防病毒软件监测

通过策略设置防病毒软件特征，按照统一的策略监测防病毒软件使用状况，并进行统计分析形成统一的数据报表。具体功能如下：

- **监视防病毒软件的使用状况**，通过防病毒软件的特征监视防病毒软件的安装情况、运行状态和病毒库版本，对不符合安全策略的状态进行报警。
- **防病毒软件监测特征的自定义**，通过对未知防病毒软件的特征自定义实现对未知防病毒软件的监测，其特征包括杀毒程序名称、病毒库版本标识的注册表项等。

3.4.5 网络进程管理

通过对网络进程的统一管理，规范计算机用户的网络行为，实现“外面的网路连接未经许可进不来，里面的网络进程未经许可出不去”。具体功能描述如下：

管理向外发起连接的网络进程，通过设置网络访问进程的黑、白名单，实现对计算机用户访问网络的控制；

管理接收外部连入的网络进程，通过网络进程与本地监听端口绑定，规范计算机用户所提供的网络服务程序，例如“SUFTP.EXE 授权监听端口为 21，如果将 SUFTP.EXE 的监听端口改为 1133，则进程不能对外提供服务”。

实时获取网络进程信息和会话连接状态，当管理员通过控制台获取网络进程信息时，客户端以快照的方式上传当前的网络信息和会话状态。

3.4.6 文件安全删除

通过控制台设置临时文件管理策略，实现临时文件的统一删除管理，系统所能删除的文件包括有：

- 清除 IE 缓存，按照策略定期删除 IE 所产生的临时文件；
- 清除 IE 地址栏，按照策略定期删除 IE 地址栏中的临时信息；

- 清除历史记录，按照策略定期删除历史记录文件；
- 清除 COOKIE，按照策略定期删除系统访问所产生的 COOKIE 文件；
- 清除系统临时目录，按照策略定期删除系统工作的临时目录；
- 清除最近打开的文档，按照策略定期删除系统最近打开文件的记录；
- 清除运行中的运行命令，按照策略定期删除系统运行中记录的用户运行命令；
- 清除回收站，按照策略定期清空回收站中的被删除信息。

同时提供文件安全擦除功能，实现对存储在本地的敏感文件进行安全擦除功能，通过多次数据回填的方式实现敏感文件的安全擦除，经过安全擦除处理后的文件无法通过磁盘剩磁的方式恢复数据。管理员可以配置擦写次数实现统一的文件擦除管理。

3.4.7 进程管理

UEM 系统能够自动收集受控终端的运行进程信息，并对收集的进程信息实施分类管理。通过可信计算策略控制，防范关键进程的重命名行为；另外，UEM 系统对操作系统文件进行完整性校验，并实现强制访问控制，确保操作系统核心系统文件的安全，保证操作系统免被病毒或木马侵袭，实现操作系统的可信。

- **可信计算管理，**通过添加、删除、导入、导出和批量更改分类等操作，对“应用程序库”和“核心文件库”中收集到的进程信息和核心文件信息进行统一管理。
- **可信计算策略，**通过下发“程序控制策略”，监控程序的执行变化情况，阻止非法程序的运行，并记录日志；通过下发“核心文件策略”，监控核心文件的正常运行，防止被非法程序篡改。如果核心文件有变化，系统将会报警，并通过消息方式通知用户。

3.5 远程管理

通过终端用户与服务器相互授权的机制建立终端与服务器之间的信任通信体系，管理员通过服务器实现对终端用户提供帮助，具体功能如下：

- **实时获取客户端主机信息，**通过 UEM 控制台远程实时获取客户端主机的相关的信息：如：驱动信息、硬件信息、进程信息、内存信息、网络连接、活动窗口、服务信息、共享信息、系统信息、用户信息、组信息、会话信息、系统日志等。
- **远程关机、远程注销、远程重启，**通过控制台对远程的客户端主机下发远程关机、远程注

销、远程重启等命令，实现远程对客户端主机的基本管理控制。

- **服务器-客户端远程消息管理**，通过控制台向客户端发送消息通告。支持客户端通过消息传递方式实现客户端和服务器一对一的消息交流。
- **远程协助支持,**能通过控制台连接客户端主机远程协助功能，实现管理员远程协助客户端主机进行故障排除。

3.6 安全存储与传输管理

3.6.1 我的加密文件夹

我的加密文件夹为终端用户提供了个人文件加密存储的文件服务，拖进该文件夹的文件自动生成以.wsd 为后缀的加密文件。当本人访问加密文件夹中的加密文件时，系统会自动解密。

3.6.2 硬盘保护区

硬盘保护区是在本地硬盘上提供一个或多个安全存放本地敏感文件的加密存储空间，用户可视为该文件保险箱为可信空间，并可通过加载或卸载操作以使该保险箱可见或不可见。所有放入保险箱的文件都是自动加密存储的，正常加载以后呈现给用户的是明文，用户感觉不到加解密过程。

3.6.3 文件安全分发

文件安全分发实现了文件在指定范围内（个人、小组、公共用户和指定用户）的自动加密或者自动解密，在指定范围外的用户不能共享这些加密文件。

3.7 安全文档管理

基于透明加解密技术，在客户终端上实施对客户文件的透明加密、透明解密，有效防止内部和外部窃取机密的行为，从根本上解决泄密防范问题。运行在用户桌面电脑中的程序，接受服务器的安全策略，根据策略判断什么样的文件需要加密，什么样的文件不加密；用户执行打开、编辑、存盘等文件操作中，强制执行这些策略。所有这些过程是不改变用户行为习惯，文件的操作者感觉不出以上这些过程的，所以对用户来讲是“透明”的。通过该模块对以下对象进行相应策略设置和日志审计：

- 加密进程控制：设置是否对某进程产生的文档执行强制加解密策略；

- 扫描执行管理：启用扫描加密命令，对指定扩展名的文件进行全盘扫描加密。管理员可以查看当前的扫描加密执行状态，启动、暂停、继续或终止任一次扫描加密任务，并对扫描记录进行审计。
- 工作模式控制：是否允许用户对工作模式的切换设置，在普通模式下不执行文档加密策略，在工作模式下强制执行加密策略。
- 安全文档自解密功能：在策略允许的情况下，支持用户自解密加密文档，且记录申请和带出的日志。
- 安全文档在线审批功能：根据审批规则设置，将需要带出的安全文档，通过审批员网上审批，转化为自解密文件使用。整个申请、审批过程记录日志。
- 安全文档备份与恢复：支持安全文档统一备份策略设置，允许客户端用户自行设置备份策略，实现安全文档的自动备份，防止文档意外破坏。
- 灾难恢复工具：防止系统出现意外或者客户端卸载后，原来加密的文档无法解密。

3.8 安全文档隔离管理

隔离管理分为“个人隔离”和“部门隔离”。“个人隔离”是对用户下发个人隔离策略，该用户产生的指定类型文件为隔离文件（个人隔离），此类文件用户自己可以自由访问，其他用户不能访问。“部门隔离”是将一个或者多个部门添加到一个隔离范围中，这一隔离范围内的用户产生的指定类型文件为隔离文件（部门隔离文件），此类文件可以被范围内的用户自由访问，范围之外的用户禁止访问。

3.9 电子文档权限管理

主动授权管理是控制客户端是否允许通过右键菜单离线制作主动授权文件。主动授权文件是用户主动制作生成的一种加密文件，此类文件本身带有一些制作者主动设置的使用权限，用户访问该文件时受文件中设置的使用权限控制。“主动授权文件”可以通过在线审批方式制作，而对于下发了离线制作主动授权文件策略的用户，也可以通过离线方式自主制作“主动授权文件”。

3.10 文档密级标识与轨迹跟踪管理

该功能利用透明加解密技术实现对电子文件的加密保护，从电子文件自身数据安全，到文件处理环境，到文件传播途径，到文件运动轨迹追踪，实现层层保护，形成严密的、立体的电子文件防护体系。

- **设定电子文件的密级**

通过在线审批机制，用户可以申请设定指定的电子文件的密级，将密级设置为“普通”、“秘密”、“机密”、“绝密”，根据电子文件的密级的不同，采用不同的文件保护方式与控制方式。

- **基于密级文件密级的访问控制**

制定电子文件的密级访问控制策略，当用户密级低于文件密级时，用户对密级文件的访问控制将被禁止，并可以设置对此非法访问产生报警。符合电子文件的密级访问控制的用户，可以自由访问对应的已经定密的电子文件。

- **基于密级文件使用范围的访问控制**

指定密级文件时可以指定密级文件的使用范围。通过设置电子文件的使用范围控制策略。可以控制不同组织的用户对文件的访问。当用户在有权限访问密级文件的组织内，用户可以自由访问密级文件。 当用户不在有对应权限的组织内，用户将被禁止打开密级文件，并且会产生非法使用文件的报警。

- **密级文件在线审批管理**

设置在线审批规则后，对密级文件的创建、修改、销毁、带出操作都可以通过系统的在线审批流程完成。用户只需要通过此管理界面发出申请，密级文件和审批请求会自动发送到审批员所在的机器。审批员通过管理界面，执行审批操作，简化对密级文件的管理流程。

- **密级文件的轨迹追踪**

系统能够全程跟踪密级文件的使用轨迹，能够查询文件在不同计算机间的使用与流转状况。通过轨迹追踪，能够跟踪到密级文件的来源于哪台计算机，也能够追踪到密级文件流转到其他哪些计算机上。

3.11 文件打印审批管理

如果客户端被禁止使用打印机，当用户必须打印文件时，就需要按照审批规则向审批员提交自己的打印申请，待审批员批准后才可以打印。审批员可以查看打印文件，决定是否批准打印。客户端用户无法自行打印文件。

3.12 U盘拷贝审批管理

如果客户端被禁止使用移动存储设备，当用户必须通过移动存储设备带入带出文件时，就需要按照审批规则向审批员提交自己的复制申请，待审批员批准后才可以进行复制操作。复制操作包括带入和带出，带入是指将移动存储设备中文件拷贝到客户端的过程，带出是指将客户端中文件拷贝到移动存储设备的过程。

3.13 光盘刻录审批管理

如果客户端被禁止使用光驱设备，当用户必须通过光驱带入带出文件时，就需要按照审批规则向审批员提交自己的复制申请，待审批员批准后才可以进行复制操作。复制操作包括带入和带出，带入是指将 CDROM 中文件拷贝到客户端的过程，带出是指将客户端中文件拷贝到刻录机的过程。

3.14 系统管理与审计

提供了对响应知识库的管理、系统用户的管理、以及对系统运行参数的设置功能；同时集中统计、显示和分析各种受监控的用户行为日志、违规操作报警日志、主机状态日志、以及 UEM 系统用户的操作日志等。

3.14.1 组织结构管理

对系统管理员角色和权限进行管理，可以添加、修改、删除、审核管理员帐户；对组织结构的人员和计算机进行管理，添加、删除、导入、导出用户和组织等，并对未注册的用户、未注册的主机和长时间未上线的主机进行强制删除等。

在多级服务器部署下，可在上级服务器查看下级服务器的组织结构信息。

3.14.2 统计审计分析

集中统计、显示和分析各种受监控的用户行为日志、违规操作报警日志、主机状态日志、以及 UEM 系统用户的操作日志等。

集中统计、显示和分析客户端程序安装情况以及客户端主机应用的在线和离线策略。

在多级服务器部署下，支持下级服务器警报、软硬件资产的统计数据报表的定时上传和集中显示，统计数据报表上传的频率可通过上级服务器定义。

通过数据表、分布图、对比图、排序图、趋势图、频率图等多种形式展示和分析日志情况，辅助用户做快速分析和判断。

3.14.3 分级报警管理

为用户提供了违规行为的警报等级的定义、警报的归并方式（按时间归并、按累计次数归并）选择等。

在多级服务器部署下，允许上级服务器定义下级服务器实时上传警报的策略。

3.14.4 响应与知识库管理

提供了响应方式定义，支持短信、邮件以及自动向控制台发送消息等多种警报提醒方式；支持事件的解决方案定义，以及警报查询的功能。提供了知识库文件的导入和导出功能。

在多级服务器部署下，可通过定义级联警报策略，要求下级服务器实时上传各类警报，从而在上级服务器可查看下级服务器的实时警报内容。

3.14.5 服务器数据存储空间管理

包括客户端日志文件和安全文档审批的文件存储管理。支持服务器文件存储路径自定义，以及存储空间不够设定的阀值时可采用的措施，如：报警或停止日志接受等。

3.14.6 系统升级管理

支持客户端升级包上传、自动获取以及全部或者局部自动升级；支持控制台升级包上传、自动检测和自动升级功能，以及支持控制台和服务器版本兼容检测。

支持内部安全服务器设置与管理，用户可在 UEM 系统中添加内部防病毒服务器、补丁更新服务器、UEM 服务器等为内部安全服务器，以防因出现安全问题而导致客户端主机断网的情况下，能保证客户端主机与这些安全服务器之间的正常通讯。

3.14.7 B/S管理功能支持

通过网页方式登录控制台，进行简便的系统管理。支持匿名用户登录进行安装软件或者工具的下载；支持客户端用户的添加与搜索、客户端密码修改、客户端本地卸载口令生成、以及客户端安装统计；支持服务器状态查看等。

3.14.8 系统参数设置

实现 UEM 系统运行参数的集中设置，包括服务器运行参数设置和客户端运行参数设置，服务器 IP 地址更改设置，警报报警方式设置，以及是否允许 Key 用户通过非验证的方式注册客户端。

第四章 系统特点

4.1 全面的终端防护能力

以安全策略为驱动，围绕“保护-检测-响应”的循环模式检测终端用户的安全策略合规性行为。从终端安全管理、终端运行维护、用户行为管理、数据安全管理、终端接入管理等六个方面多层次的保障企业内网计算机用户的安全。根据企业的规章制度、行业规定、计算机的风险等级和业务相关性原则为不同类型的计算机用户制定不同的等级防护策略，从而形成统一的安全策略管理。根据计算机用户的监测日志进行全面统一的日志审计，生成企业风险管理的数据报表。按照“应急响应-知识查询-问题排除-知识库修复”的操作流程不断丰富应急响应知识库，为全面管理计算机用户提供理论支撑和实践经验。

4.2 分权分级的管理模式

避免因集中权限而增加系统管理威胁，我们采用分权的管理员管理模式。管理员可以划分为：系统管理员、系统操作员、系统审计员和安全官，每种管理员的管理权限可根据用户的实际需要进行自定义。同时为了增强系统数据的安全性，我们对管理员的管理范围进行划分，即：一个系统可以有多个系统操作员，每个操作员的管理范围都不一样的。基于角色的分级分权管理使不同角色的管理员权限分离，各司其职，加强了系统的安全性。

4.3 方便灵活的安全策略

对终端用户的安全策略进行统一管理，根据不同的用户状态执行不同的安全策略，支持策略模板和策略集的定义与应用，支持群组管理与群组策略的下发。策略的灵活管理满足了在线用户、离线用户和笔记本出差用户的使用，满足大规模部署和群组策略的集中管理，在最大限度范围内保证了终端用户的安全和简化了系统的管理。

4.4 终端安全风险量化管理

按照保密规定的“等级防护”指导方针，将终端系统的告警事件划分为不同级别的风险等级，

目前支持五个等级的风险自定义，根据告警事件的统计结果，生成不同等级风险的数据报表，实现了风险的量化管理。

4.5 周全详细的系统报表

根据计算机用户所产生的日志信息，形成多种类型的统计报表。按照多个事件类型的查询条件形成交叉的统计报表。支持日志信息的关联查询，形成数据的关联报表，根据数据关联的查询结果可以查找出关键数据的变化轨迹。支持多样化的日志查询条件和过滤条件，便于管理人员进行详细的日志分析。支持策略统计分析。提供灵活详细的统计报表，可输出为 EXCEL、WORD、HTML 等多种格式的分析报表以及根据统计数据生成柱状图和饼图。

4.6 丰富的应急响应知识库

按照“保护—监测—响应”循环的工作模式，动态调整安全防护策略、更新应急响应知识库，为管理员应急响应提供完备的技术参考方案。

4.7 完善的插件式系统架构

系统采用插件工作模式，动态装载各功能模块。一方面是在系统变更安全策略时，能够动态加载或者卸载功能模块，从而减少对系统资源（如：内存、CPU 等）的占用。另一个方面为了使第三方组件不受系统开发环境的限制，系统采用 ATL 与 COM 技术，为与第三方软件的结合提供完善的接口支持。

4.8 方便快捷的安装、卸载和升级

系统安装方便快捷，支持 AD 域同步，用户自由注册，客户端支持 MSI 安装，实现快速部署。用户注册灵活方便，支持管理员预置与硬件 KEY 相结合的工作模式。系统升级方便，既支持在线自动升级和客户端主动检查更新，又支持离线的本地升级包升级。客户端代理程序既支持离线本地卸载，也支持在线远程卸载。提供远程客户端代理程序的故障诊断与恢复功能，实时监测客户端代理活动状况并形成代理活动状况统计报表。

4.9 多级部署支持

系统支持无限制的多级服务器部署，下级服务器注册到上级服务器后，可以定期收集下级服务器的各类统计报表以及实时警报信息，实现大规模的分布式监控，集中管理模式。

附件一：

名 词 解 释

UEM8.0：中软统一终端安全管理系统 8.0 的英文简称，英文全称是：CSS United End-point System management 8.0，简称为 UEM8.0。

Windows 系统日志：是指 Windows 操作系统本身纪录的日志,主要有三类：应用程序、系统、安全；向系统所发送的日志的类型分为：信息、警告、错误、成功审计、审计失败。

第二块网卡：除去与服务器通信的网卡之外的所有其他网卡，我们都统称为第二块网卡。

软件黑名单：非法软件的关键字列表。给客户端应用软件开放策略时，可附加一份黑名单，黑名单中列出的软件将被禁止安装和使用。

软件白名单：合法软件的关键字列表，给客户端应用软件禁止策略时，可附加一份白名单，只有白名单中列出的软件才可安装和使用。

软件基线：是软件安装的一个标准，规定客户端只能安装基线列表中的列出的软件，多了或少了都将报警。

MAC 地址：MAC 地址也叫物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。IP 地址与 MAC 地址在计算机里都是以二进制表示的，IP 地址是 32 位的，而 MAC 地址则是 48 位的，如：08:00:20:0A:8C:6D 就是一个 MAC 地址。只要你不去更改自己的 MAC 地址，那么你的 MAC 地址在世界上是唯一。

日志上传：是指将客户端生成的操作日志上传到服务器，服务器把上传的日志信息分类保存到数据库中，用户可以在控制台的统计审计分析中查看。

时间同步：客户端本地时间与服务器本地时间保持一致。可以在系统参数中设置时间同步的最小误差和频率。

心跳信号：客户端向服务器定时发送的连接信号，如果服务器在规定的时间段内收不到客户端发来的连接信号，则判定客户端离线。

MSI 类型：软件分发包中的主执行文件，是 Microsoft Windows Installer 类型的文件。

静默安装：静默安装表示软件包在后台执行安装，不需与用户交互。

交互安装：软件分发安装类型是交互安装，表示分发软件包时安装程序会弹出安装界面，用户可根据交互安装界面提示进行安装。

最大连接数：指系统能建立的 TCP 连接的最大数目。

最大并发连接数：在单位时间内系统能创建 TCP 连接的最大数目。

在线基本策略（默认策略）：安全管理系统客户端用户的策略，当用户与服务器连接时，启用该策略。

该策略通过安全管理系统控制台设置与下发。

离线策略：安全管理系统客户端的策略，当用户与服务器断开时，启用该策略。该策略通过安全管理系统控制台设置与下发。（通常离线策略应相当严格，以保护客户端主机的安全。）

时间策略：安全管理系统客户端的策略，用户在设定的时间范围内，与服务器连接时的策略。该策略通过安全管理系统控制台设置与下发。通过设置时间策略，可以方便的限制安全管理系统客户端用户在不同时间段的权限，例如，办公时间段内设置为允许使用打印机，而非办公时间段则设置为禁止使用打印机的策略。

WSUS：Windows Server Update Service 即微软的补丁服务器。通过使用 Windows Server 更新服务 (WSUS)，管理员可以快速而可靠地将 Windows 操作系统和应用程序及时更新，修复系统漏洞，获取最新功能。

可信终端：安装了可信移动存储系统客户端的主机称为可信终端。没有安装可信移动存储系统客户端的主机称为普通终端。

普通移动存储介质：未经可信移动存储管理系统授权的移动存储介质，称为普通移动存储介质，简称普通磁盘。

可信移动存储介质：经过可信移动存储管理系统授权的移动存储介质，包括 USB 设备、软盘等移动存储设备，简称可信磁盘。依据授权类型的不同，可以将可信移动存储介质分为支持商旅模式和不支持商旅模式两类。支持商旅模式的可信移动存储介质有两种状态：可信状态和商旅状态；不支持商旅模式的可信移动存储器永远处于可信状态。处于商旅状态的可信磁盘允许在普通终端自由使用，用于在可信终端与普通终端之间进行数据的交换。

商旅移动存储介质：处于商旅状态的可信移动存储介质，称为商旅移动存储介质。该介质在可信终端上只能读取该介质上的内容，不可以往该介质中写入任何数据。在普通终端上正常加载后，可以进行读写操作。

激活：将移动存储介质由可信状态转换为商旅状态的过程，称为激活。反之，将商旅状态转换为可信状态的过程，称之为反激活。

计算机密级标识：为涉密计算机设定的安全级别，安全级别包括普通、秘密、机密和绝密。

移动存储介质密级标识：在对移动存储介质进行授权的过程中，会给其设定一定的安全级别，用以说明该介质的涉密安全程度。涉密介质的安全级别包括普通、秘密、机密和绝密。

锁定：可信移动存储介质在违反规定使用时的一种处理方式，被锁定的可信移动存储介质将被限制使用，需解锁后方可在安全工作域内使用。

自毁：可信移动存储介质在违反规定使用时的一种处理方式，被自毁的可信移动存储介质上的数据将被随机数所填充，存储在该介质上的文件数据将不可被恢复。

域帐户：域帐户是指域服务器中的帐户，使用域帐户可以登录到该帐户设定范围内的任意计算机。

同步域帐户：同步域帐户是指当 UEM 服务器设置为跟域服务器同步时，UEM 服务器首先获取域服务器“Active Directory”中的由用户建立的组织单位和用户帐号，并对其进行监控，即每当这些组织单位和用户帐号改变时，UEM 服务器中的组织结构也会发生相应的改变。

网络接入认证：UEM 的网络接入认证是指 802.1x 协议认证。其基于 Client/Server 的访问控制和认证协议。它可以限制未经授权的用户或设备通过接入端口访问网络。在认证通过之前，802.1x 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

策略集：策略集是指针对特定范围对象（比如某一小组的人员、具有某一身份的用户等），预先定义的一套安全策略（如失泄密控制策略、主机安全策略等）。该策略集作为一个对象，可供管理员随时查看、修改、添加和删除。

单项策略：一个大策略集中的某一项小策略，比如失泄密策略中的打印控制策略、HTTP 控制策略等。在 UEM 中，单项策略必须是能在一个具体策略设置界面编辑完成的。

群组：具有某一类相同属性的人员或者计算机的集合，用于对人员或计算机进行逻辑上的分组。

群组管理：对于群组进行增、删、改等操作，增减群组内的人员和计算机，为群组设置相应的安全策略，这些操作统称为群组管理。

群组策略：关联到群组的一组安全策略（如失泄密控制策略、主机安全策略等），当人员或者计算机添加到某个群组中时，将会自动应用该群组的安全策略。

安全文件加解密：一套非透明的、主动的文件加解密系统；在部署了 UEM 客户端的机器上，用户通过文件加密功能选项，主动进行文件的加解密操作（比如通过资源管理器中的右键菜单“安全文件加解密”或者拖拽文件到“我的加密文件夹”等）。该系统产生的加密文件以.wsd 后缀结尾，文件图标表现为左侧带一把小锁的形式，不同于加密前文件的图标。

安全文档管理系统：一套基于 Windows 文件系统内核的、透明的文件加解密系统（通常简称为安全文档）。当用户使用由管理员设定的某类进程（称之为加密进程）编辑文件的时候，会自动将文件数据加密存储到磁盘上；当用户使用加密进程打开该文件的时候，能够在后台自动解密文件数据；文件数据的加解密操作均在操作系统的内核完成，用户感觉不到加解密过程的存在。该系统所产生的加密文件保留了原有的文件后缀，文件的图标表现为在原有文件的图标基础上，在右下方附加了一把黄色的小锁。

加密进程：在安全文档管理系统中，由管理员设定的一类能够自动对文件数据进行加解密处理的进程；当用户使用这类进程编辑并保存文件时，能够自动将数据加密存储在磁盘上；同时，在用户使用这类进程打开被加密文件时，能够自动将数据解密。

写权限打开文件：为了保障文件的安全，Windows 操作系统对一个文件提供了多种访问控制权限，如读权限（可以读取文件数据）、写权限（可以将新的数据添加到文件中）、删除权限（可以删除文件）、执行权限（如运行 EXE 程序）等。当用户使用一个应用程序打开一个文件的时候，操作系统会要求该应用程序申请访问该文件的权限；只有应用程序申请了某个权限，应用程序才有资格进行相

应的操作（比如，只有申请了删除权限，应用程序才有资格删除该文件）。写权限打开文件就是说应用程序在打开文件的时候，会申请对该文件的写操作权限。一般情况下，应用程序在打开一个文件的时候，只会申请读的权限。当用户真正编辑并要求保存的时候，才会重新申请写权限。

预加密文件类型：加密进程在以写权限打开明文文件的时候，会在打开之前先对指定类型的文件进行加密处理，这种加密处理叫做预加密，指定的文件类型即为预加密文件类型。

无效备份文件：在安全文档管理系统中，某一个备份文件所对应的原始文档不存在（被删除或者移到其他路径下），称这样的备份文件为无效备份文件；

自动备份文件：在安全文档管理系统中，依据设定的时间点，系统自动对该时间点之前用户修改过的加密文件实施备份，这个过程称为自动备份文件。

手动备份文件：用户通过 UEM 系统客户端托盘区菜单主动发起的，对用户修改过的加密文件进行备份操作的过程，这个过程称为手动备份文件。

审批管理：在安全文档管理系统中，企业内的敏感文件会被强制加密。为了能将被加密的文件带出使用，需要向系统管理员提出申请，并经具有相应权限的审批员审核同意后，方可解密文件并带出。从提交申请，到审批员审核，再到加密文件的解密，这个过程称为审批管理。

在线审批：用户将审批请求和文件发送给服务器，由服务器完成审批逻辑的处理，自动交给具有审批权限的用户进行审批的方式；

离线审批：用户将要审批的文件制作成审批包，通过网络或 U 盘等移动介质拷贝到具有审批权限的用户机器上完成审批的过程；

UEM 的安全模式：当安装 UEM 客户端的机器不满足终端安全检查条件要求（如 Windows XP 系统未安装 SP3 补丁、未安装杀毒软件等）时，UEM 客户端会将该机器设置为安全模式；当计算机被设置为安全模式后，该计算机将只能访问 UEM 服务器和其它被指定的机器(安全服务器)，而不能与其他机器通讯。

安全服务器：一个单位内部，供终端计算机进行安全升级时访问的服务器，如防病毒软件服务器、补丁更新服务器等。部署了 UEM 客户端的计算机因安全检查被设置为安全模式后，该计算机将只能访问控制台指定的安全服务器列表中的计算机。

基于密级标识的文档安全系统：英文名称 Tag-based File Protection System，缩写为 TBFPS。

可信工作域：客户所在的组织机构内部署了 UEM 环境的计算机集合。

保密性级别：用于标记主体（用户）或客体（文件）的安全等级，在本文档中简称**密级**。

密级文件：已经由密级文件管理员设置了密级的电子文件。

密级文件管理员：具有密级文件管理权限的客户端用户。

密级文件附加属性: 包括文件名、密级、产生时间、生命周期、文件来源、应用范围等。

密级文件带出：密级文件通过某种途径传播到可信工作域之外。

密级文件交流：密级文件所有者通过审批机制，将带有密级标识的文件发送给安全工作域内其他用户使用。

文件操作：包括创建、读取、写入、删除、重命名、拷贝、剪切、粘贴、销毁等操作。

文件分类：从文件是否加密角度，将文件分为非加密文件、普通加密文件（无密级标识的加密文件）、密级文件（带密级标识的加密文件）。

密级文件**生命周期**：密级文件的创建操作是密级文件生命周期的开始，密级文件被销毁后，密级文件的生命周期结束。在密级文件创建到销毁期间，可对此密级文件进行修改，带出等操作。

在线审批：用户通过 UEM 系统提供的电子审批管理机制，发出申请给密级文件管理员，管理员通过系统提供的界面对申请进行审批，并通过系统自动将审批结果反馈给用户，这个过程，我们称之为在线审批。

离线审批：UEM 系统中安全文档模块中提供的审批功能，此功能不依赖于用户的在线状态，用户将审批的文件制作成审批包，通过网络或移动存储介质途径将此审批包发给审批员，审批员执行审批后，再通过网络或移动存储介质途径将审批结果发回用户，此过程我们称之为离线审批。