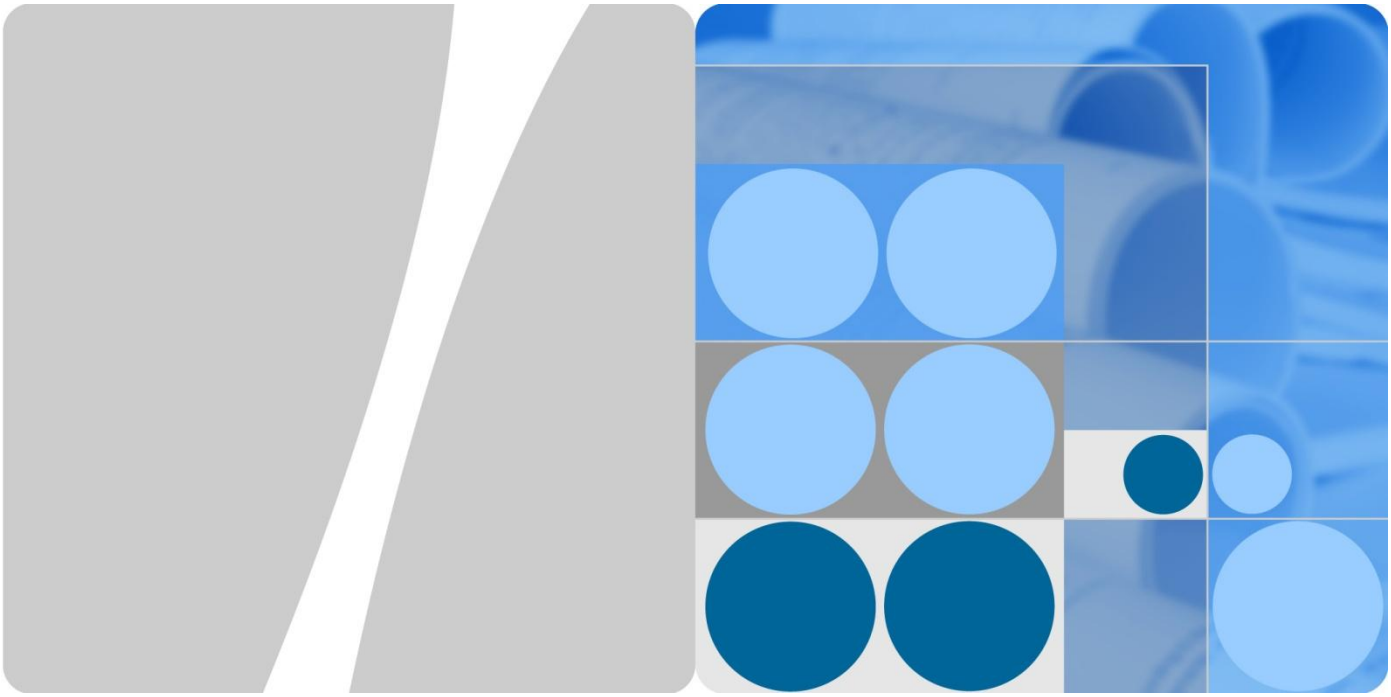

华为 DSM 文档安全管理系统
FAQ

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

1 前 言

摘要

文档安全管理（DSM, Document Security Management）系统是对机密电子文档进行加密和权限控制、防止主动泄密的一款成熟产品。通过对企业的重要文档进行加密和实时权限控制，可为企业提供安全授权下的机密信息共享机制，使信息所有者能够定义信息的访问者、访问方式和时间等，并记录文档操作日志。有效控制因不受权限限制的阅读、修改、分发文件导致的信息泄密。

缩略语清单

缩略语	英文全名	中文解释
AD	Active Directory	微软活动目录
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
DSM	Document Security Management	文档安全管理
DMC	DSM Management Center	文档安全管理系统管理中心
DS	DSM Server	文档安全管理服务器
DC	DSM Client	文档安全管理客户端

2 FAQ

功能方面的问题

Q:DSM 的主要功能有哪些？

答复：

DSM 系统的主要功能包括文档权限管理、日志审计、用户管理三大功能。

Q:DSM 支持的文档格式有哪些？

答复：

支持 Microsoft Office Word、Excel、PowerPoint 2003/2007 中英文版，支持的权限包括只读、编辑（修改）、复制、打印、再授权、离线阅读、完全控制；支持 Adobe Reader 7.0、8.0、9.0 中英文版，支持的权限包括只读、离线阅读、完全控制。

文件扩展名为：.doc、.xls、.ppt；docx、.xlsx、.pptx；pdf

Q:为什么 DSM 系统只支持特定类型的文档？

答复：

DSM 系统对安全文档做细粒度的权限控制时，需要相对应的文档编辑工具进行控制，所以支持的文件类型受限。

Q:DSM 系统如何控制安全文档打印次数？

答复：

在打印文件的时候记录已用过的打印次数。如果已经用完了打印次数，将不允许打印。详细解释：如果设置了打印次数，在每次客户端打印文档时客户端都会向服务器发送打印请求，如果服务器发现打印次数大于 0，那么给客户端返回可以打印，并且把数据库的打印次数较少 1，客户端收到打印请求成功后允许打印。

Q:离线时，DSM 系统是如何控制文档的时间？

答复：

离线文档的时间控制根据用户电脑的时间进行控制。为防止用户通过修改本地时间规避安全文档的时间控制，在用户改时间绕过检测上面做了必要控制。

Q:水印在技术上是如何实现的？是否依赖于格式的。是否能对所有格式进行支持。

答复：

依赖格式。不能支持所有的格式。在向打印机发送打印指令时，DSM 客户端将会截获此指令，然后便对此次打印任务设置水印格式，那么打印时使用的水印就是 DSM 客户端所设置的水印格式。目前 DSM 客户端只对 office word、excel、ppt 和 Acrobat Reader 软件的打印指令进行拦截并设置水印格式。

Q:若现网已经部署有 AD，那么与现有 AD 结合进行项目实施的方法和步骤？

答复：

DSM 系统会从 AD 同步用户和部门。用户认证的时候，如果用户已经登录了域，则不需要再输入用户名及密码。否则可以输入用户名和密码进行认证。

详细解释：

DSM 系统利用 Kerberos 协议与 AD 域控制器交互，对用户进行身份认证。AD 认证使用的是 Kerberos 协议。部署步骤是先部署 AD 域，然后在 AD 域上面设置一个用于提供对外认证的辅助帐号，DSM 客户端使用 Kerberos 协议到 AD 域控制器上面认证通过后，将会获取到一个认证后的票证，把此票证发送到服务器，服务器再使用此 token 通过辅助帐号到域控制器对此票证进行校验，校验通过就认为用户认证通过。

Q:文档发送给外部客户、供应商或合作伙伴时，怎么实现文档安全共享？

答复：

可为外部用户设置临时帐号，外部用户只需通过 VPN 或 Internet 与公司内部的 DSM 服务器连接，即可实现文档安全共享（外部用户需要安装 DSM 客户端）。

Q:DSM 是否同时支持全盘加密？

答复：

不支持。DSM 核心为权限控制，用户可实现基于账号来实现权限的颗粒度控制，如只读、读写、完全控制等。用户可根据文档的密级来加密文档，而全盘加密将无法支持细化的权限控制以及文档密级。

Q:员工出现部门调动时，原有文档权限是否可以直接继承？

答复：

若 DSM 系统与 AD/ED 进行联动时，DSM 系统会定时同步用户信息，当人员调动（从一个部门转移到另外一个部门）时，调动员工的 AD/ED 帐号所在部门发生变化，DSM 系统上也会相应的进行同步，此时员工原有的文档权限可以直接继承。

若使用 DSM 自带的用户管理，目前暂不支持，在下一个版本将实现该功能。

Q:如何实现快速授权？

答复：

客户端申请文档权限时，通过邮件通知审批人，审批人登陆 Web 管理界面处理权限请求，当申请流程完成后申请人邮件通知。

Q:客户端支持哪些操作系统？

答复：

客户端支持的操作系统包括：中英文 Windows xp sp1/sp2 32 位；中英文 Windows Vista Home Basic/Ultimate 32 位。

Q:客户端系统用户环境是否支持普通用户？

答复：

支持，客户端支持普通用户登陆环境。

Q:文档权限是否支持通过 Web 管理页面进行统一管理？

答复：

支持。

1、普通用户登录 DSM 服务器 Web 界面按月份查询自己制作的以及自己有分发权限或完全控制的文档，查询条件支持文件名、摘要、文档类型、时间范围。文件名和摘要支持模糊查询，支持按时间、文件名进行排序。如果用户具有完全控制权限或者分发权限，那么用户可以对文档权限进行修改。不可以在 web 界面获取到文件的内容。

2、文档管理员登陆 DSM 服务器 Web 界面可以管理的相应部门的全部文档，支持部门、文件名、文档类型、摘要、时间范围。文件名和摘要支持模糊查询。支持按时间、文件名进行排序。对于查询出来的文档，可以修改文档的权限。不可以在 web 界面获取到文件的内容。

Q:若分布式部署，是否支持用户漫游功能？

答复：

支持，同一个系统中一个服务器的用户可以接入非本地服务器进行打开文档和制作文档等操作。

Q:DSM 系统提供哪些审计日志？

答复：

DSM 系统提供丰富的审计日志信息，包括文档操作日志（包含在线和离线）、管理员操作日志。

Q:DSM 系统是否支持对外开发接口？

答复：

支持，DSM 系统提供对外 API 接口供其他第三方系统，进行文档加密、设置初始权限、修改权限、还原文档、申请文档权限、修改文档所属部门。

Q:所有加密文档的密钥及权限都存储在数据库中，单个文档的信息有多大，DSM 单台服务器可支持 20000 终端，那么平均每天产生如 20000*5 份加密文档，数据库存储信息总共多大？

答复：

每个文档大概占用 1K 的大小，如果每个文档 5 条权限，每条权限占用 0.2k 空间，那么每天产生的数据库存储空间为：

（1K＋0.2K × 5）×20000×5 ＝ 200000K ＝ 200M

每月产生的数据库存储空间为：

200M×30=6000M=6G

Q:文档加密信息存储在数据库中,数据库 1/O 瓶颈怎么解决，对服务器内存和硬盘有何特殊要求？

答复：

如果用 32 位的操作系统，最多只能上到 4G 内存，要使用超过 4G 的内存，就同时需要打开 windows 的 AWE 功能，打开这个选项将会导致内存寻址速度变慢，不过对于需要很大内存的程序（例如具有大量数据的 sqlserver），还是会比较明显的提高速度的。

服务器的硬盘无特殊要求，因为磁盘 IO 不是系统瓶颈，因为绝大部分东西都在内存里面操作。

Q:加密 100M、1G、10G 等不同等级大小文档的时间？

答复：

暂时不支持超过 200M 的文档加密，建议是不要超过 50M 的。

Q:文档的摘要的作用是什么？

答复：

DSM 提供摘要，是用来标识文档和搜索文档的。

安全方面的问题

Q:客户端和服务器之间的加密采用的是 SSL，而 SSL 是需要公钥证书的，目前是怎么管理公钥证书的。

答复：

客户端与服务器端的 SSL 通讯仅用于提供保密通信隧道，没有使用 SSL 实现服务器和客户端之间的相互认证，因此对服务端使用的证书没有进行严格的有效性验证，所使用的证书也是在服务器上配置的固定的证书/公钥对. 客户端和服务器之间的相互认证是通过在 SSL 隧道上传输的自定义协议实现，传输内容也不含客户端身份认证密码信息，因此不会对系统的安全性构成严重威胁。

DSM 新的版本已经规划完善 SSL 公钥证书的管理机制，可以将客户自有的 CA 生成的服务器证书配置到服务端，同时增加客户端对服务器端 SSL 公钥证书的合法性进行验证机制，防止服务器端被非法中间体冒充。

Q:为减少文档明文暴露时间，能否在新建文档时，弹出对话框，问是否需要加密文档，如果是加密文档，则对文档进行全程的保护？而不是文档明文存在以后，再右键加密。

答复：

对于文档的加密，DSM 当前实现的手段是当文档编辑完成后，由文档管理员或作者选取文档后右键手动进行加密，这种方式也是业界内通用的方式。Microsoft RMS 和 EMC IRM 也不能实现自动创建新的加密文档这一功能.

Q:客户端应采取措施，防止被卸载，并在被卸载时，能够终止相关的应用程序。

答复：

在 DSM 系统里，客户端程序主要的功能是当打开加密文档时，由客户端程序向服务器端请求当前用户对该文档的操作权限信息，当客户端程序被卸载后，客户端就无法请求文档权限，用户就无法通过任何手段打开加密文档，文档的安全性可以充分的保障，已经完全符合安全要求。因此，不建议对客户端程序进行防卸载保护。

Q:如果接收者在无法接触内网的情况下，获得加密文档，如何实现离线功能。

答复：

在 DSM 系统里，文档的加密信息都存储在 DSM 服务器，客户端打开加密文档必须向服务器端请求文档加密权限信息，因此要求客户端可以与服务器端通讯。对于离线状态下打开加密文档的场景，需要终端在联网的状态下至少打开该加密文档一次，此后才能在离线状态下也能打开文档。对于此场景，管理员可配置离线状态下打开文档的次数和有效时间，保证文档离线状态下的安全性。

后续 DSM 系统考虑增强其离线功能，即通过与 USB Key 绑定，配置离线策略，实现终端离线情况下的文档安全管理。

Q:DSM 系统是如何调用相关程序打开安全文档的？

答复:

DSM 系统目前已经是通过 Windows 系统根据最初的后缀名调用相关程序实现。当前近支持 word、excel、ppt、pdf 等几种文件类型。

Q:DSM 系统是否支持灾备？

答复：

DSM 系统最重要的信息是存储在 SQL Server 2005 数据库里的用户信息、文档权限信息和文档操作日志，对于此部分，可以通过 SQL Server 2005 数据库的备份功能实现数据备份以及远程灾备。管理员的维护工作只涉及当前系统瘫痪后，手动启用备份。

Q:DSM 系统是否支持在加密时设定加密期限，一旦超出期限自动解密为明文？

答复：

从文档的安全性考虑，不建议机密文档的自动解密功能。

Q:DSM 系统是否对内存进行保护？防止黑客通过内存获取明文。

答复：

DSM 系统对于打开后的加密文档的处理是基于 Office 程序本身的机制，实验室测试的结果表明，Office 程序对于打开后的文档的部分内容是以明文的形式存储在内存中，其它同类产品（包括微软的 RMS）也无法对此进行控制。建议通过其他手段（如 TSM 系统的员工行为管理）禁止终端运行黑客程序读取内存来辅助实现。

Q:授权离线阅读的文档，密钥与权限信息保存在指定客户机，是否存在安全风险？

答复：

离线文档的密钥与权限信息都用 AES 加密后保存于客户机，AES 的加密密钥跟用户名和用户密码、本地机器信息相关，难以破解。

Q:拥有离线文档操作权限的用户，如果具备对文档的更改或复制权限，可以将文档复制重新创建文档，获得对文档的永久操作权限。DSM 如何考虑控制？

回复:

用户只有拥有复制权限和完全控制权限才能复制文档内容另存为新的文档，拥有更改权限不能另存。可根据业务需求进行控制,如果是机密性高的文档可以不授予复制权限.

Q: DSM 的加密密钥集中存储在服务器中，是否对加密密钥采取了保护？

答复：

加密密钥经过加密保存于数据库中，确保密钥安全。