People today are keenly concerned about data security. In enterprises, confidential data is saved in electronic documents that can be disseminated through various methods. How to guarantee the confidentiality and integrity of confidential information? Especially in an open network environment, confidential data can easily be disclosed by employees through the network, or stolen by hackers. This may lead to unforeseen consequences such as illegal access and distribution of customer data, financial statements, product specifications and other sensitive documents that ultimately damage the corporation’s reputation and business.

DSM system is a powerful yet easy-to-use document permission management software. DSM provides a mechanism that allows authors to share confidential information without relinquishing control. It enables information owners to actively determine who can access information, as well as how and when it can be used, and to record all actions. In addition, wherever the document is forwarded, either internally or externally (such as to partners and customers), access permission is always attached to the information enabling continuous control of the document permission. This effectively avoids damages and costs associated with the loss of sensitive information. In addition, high stability, reliability and scalability mean the software can be easily integrated with current systems.

Product Features

Strong encryption keeps documents secure
- Makes use of 128-bit AES transparent encryption technology based on IFS, which speeds up encryption and decryption and ensures high reliability and security.
- The keys are kept separate from contents. Keys and permissions are stored on the server; encrypted contents are stored with the client; furthermore, contents are always encrypted. The server does not exchange contents with the client. The secure connection set up through HTTPS transmits only IDs, keys and permissions ensuring a high level of security within the system.
- Encryption and decryption processes are forcibly transparent to users. The processes are easy to use, without any key management. Users do not need to change usage habits.

Dynamic access control continuously protects documents
- Access permission is always attached to the information wherever it is stored or transmitted. The persistent control mechanism for document permissions is implemented. Document owners can dynamically change or withdraw user permissions. Permission information is sent to the DSM server in real time and permission immediately takes effect, thus dynamically controlling the access permission of users.
- Only authorized users can access confidential documents, hence documents are continuously protected wherever they are stored or transmitted.
- Document recipients can apply for access permission through
emails. When a document owner receives a request for permission, granting permission to the user is as easy as clicking the authorization link.

Perfect permission controls

- Read-only, modify, copy, and full control.
- Distribution—allows users to determine whether document recipients can be authorized his or her permissions to others again.
- Print—allows printing of hard copies (supports dynamic watermarking: setting watermarking fields, including time, user information, and IP address; defining watermark format).
- Offline usage—allows safe use of document offline.
- Permission validity period—allows users to use the document in the validity period. The document expires automatically after validity period.
- Periodic time control—allows users to access the document at a specified time.
- Limit times of print/read-only—allows users to print and read the document for specified times.

Group policy and policy template to implement unified management of document permissions

- Global group policy: System administrator can log in to the management center to define the global group policy, and set the access permission of the group. In this way, all document permissions on the system can be managed in a unified manner.
- Local system group policy: System administrator can log in to the DSM server to define the local system group policy, and set the access permission of the group. In this way, all document permissions on the local system can be managed in a unified manner.
- Client policy template: During authorization, the user can save the current permission to a file as a template, facilitating repeat applications.

Various document formats to fulfill different requirements

- MS Office 2003 (SP3 or later), 2007
- Adobe Reader 7.0, 8.0, and 9.0

Integration with Directory and Authentication infrastructure

- Synchronizing user accounts and groups with Microsoft Active Directory and Novell eDirectory.
- Cross-system authorization and user roaming allows for document sharing anytime, anywhere. The secondary server user is allowed to grant the document permission to another server user or group in the same system. The user can access the remote server, then access and encrypt documents.

Comprehensive log audit

- Creating operation logs to track all actions including creating, reading, modifying, and printing documents.
- Keeping track of all offline documents and recording logs.

High reliability, scalability and performance

- Highly reliable: two-node cluster hot backup of database. The server supports load balancing. Moreover, key backup and recovery is provided.
- Highly scalable: provides API interfaces for third-party applications to encrypt documents, and set and modify permissions to meet the requirements of enterprises on application encryption and authorization such as Lotus Notes.
- The system supports centralized networking of a single system set; it also supports distributive networking of several sets of systems. It supports easy implementation and deployment.

Intuitive user interfaces to reduce administrative efforts

- Makes it easy for clients to encrypt documents and authorize users, including encrypting a single document or directly encrypting a folder.
- Users can also use Web UI to encrypt documents and authorize users. If the user receives requests from other users, the user can log in to the Web UI to authorize or deny permission.
Application Scenarios

- DMC: DSM center
- DS: DSM server
- DC: DSM client

DMC System administrator

Core network

Province A

DMC
DS1
DC

Province B

DMC
DS2
DC
Product Specifications

The DSM system consists of a DSM server, a DSM management center, and a DSM client.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSM server</td>
<td>Software processes requests from terminal users, authorizes and authenticates document users, encrypts and decrypts documents, and audits logs. Document permissions and keys are stored and managed in a unified manner.</td>
</tr>
<tr>
<td>DSM management center</td>
<td>Software, the primary layer of the DSM, is the server managing the entire system. It controls access of secondary servers. The DSM management center provides the following functions: synchronizing users, user management, alarm management, server management, and policy management.</td>
</tr>
<tr>
<td>DSM client</td>
<td>Software encrypts the client documents, controls document permissions, and also offers offline reading and document recovery.</td>
</tr>
</tbody>
</table>