Data Loss Prevention (DLP)

Guidance for NetDocuments

Prepared by OTB Consulting
Client Advisory Services

CONFIDENTIAL — PREPARED FOR CLIENT USE

Contents

Who Benefits from DLP? 3
Core Functionality of DLP 3
Key Components of DLP 3
Actions Governed by DLP 3
DLP Rule Reference 4
Recommendations 5
Getting Started 5
Governance 5

Who Benefits from DLP?

Data Loss Prevention (DLP) is especially valuable for organizations that require advanced security measures exceeding the foundational V-E-S-A or N permissions available in the standard NetDocuments platform. It is commonly adopted by larger firms or highly regulated institutions where the protection of sensitive information is critical.

The DLP module in NetDocuments identifies and blocks unauthorized attempts — whether intentional or accidental — to move confidential data outside the secure environment. It accomplishes this by classifying content according to sensitivity levels and enforcing preventative measures accordingly.

Core Functionality of DLP

DLP introduces proactive, action-based document controls that supplement traditional role-based access permissions. These controls include restrictions on:

- Downloading or printing documents
- External sharing or echoing/syncing files
- Modifying user access permissions
- Opening documents in external applications (e.g., Office Online)
- Creating secure links or moving documents outside their designated locations

Key Components of DLP

- **Classifiers:** Used to assign sensitivity levels to documents, either manually or automatically. Common default categories include Highly Confidential, Confidential, and Restricted. Organizations can customize these classifiers to align with internal data governance policies.
- **Prioritization:** Administrators can rank classifiers to indicate the relative sensitivity of information. Higher-priority classifications take precedence when multiple classifiers apply.
- **Policies:** Predefined rules that govern which actions users can perform on documents. Policies may be associated with classifiers or implemented independently, and can be tailored to organizational needs by enabling or disabling specific controls.
- **Granular Control Levels:** DLP rules can be applied at multiple levels — cabinet, profile, or even individual document — offering flexibility and precision in data protection strategies.

Actions Governed by DLP

NetDocuments' DLP module can regulate or block the following activities:

- Emailing documents directly from the platform
- Sharing via CollabSpaces
- Internal duplication or copying of documents
- Creation and distribution of secure links
- Downloading files to local systems
- Syncing via ndSync
- Making explicit access control changes
- Moving documents between folders or containers

- Opening files using web-based editing tools
- Printing content directly from the platform
- Sending documents to DocuSign
- Adding documents to a Set
- Interacting with documents via AI assistants

DLP Rule Reference

The table below lists each available DLP rule and the action it restricts. These rules can be applied individually or in combination when building a classifier or policy.

Rule	Description
Attach Document	Prohibit attaching the document to an email from the NetDocuments Platform
CollabSpaces	Prohibit adding the document to a CollabSpace
Copy Document	Prohibit ability to copy the document inside the NetDocuments Platform
Deliver Secure Link	Prohibit Secure Links to the document from being generated or sent
Download Document	Prohibit using the download action to take a document out of the NetDocuments Platform
Echoing	Prohibit echoing the document
Modify Access	Prohibit allowing explicit (user-initiated) ACL changes to the document
Move Document from Container	Prohibit the ability to move the document from its parent container
ndSync	Prohibit syncing the document using ndSync
Office Online	Prohibit opening the document in Office Online
Print Document	Prohibit ability to print the document from the NetDocuments Platform
Send to DocuSign	Prohibit ability to send the document to DocuSign from the NetDocuments Platform
SetBuilder	Prohibit adding the document to a set
AI Assistant	Prohibit documents from being interacted with via AI assistants

> **Tip**
> Start narrow. A small set of well-defined classifiers is easier for staff to apply correctly and for administrators to audit than a broad, complex taxonomy.

Recommendations

Getting Started

- Start with a small set of high-value classifiers (e.g., Highly Confidential, Confidential) rather than a broad taxonomy — expand only as adoption matures.
- Apply DLP rules at the cabinet or profile level wherever possible; reserve document-level overrides for exceptions.
- Prioritize classifiers explicitly so behavior is predictable when a document could match more than one.

Governance

- Review classifier assignments and rule sets periodically as regulatory or client requirements change.
- Document the business justification for each policy so future administrators understand why a control exists.
- Coordinate DLP policy changes with IT and Records/Risk stakeholders before deployment to production cabinets.

OTB Consulting
Email: Lindsay@otb-consulting.com
Web: www.otb-consulting.com