

UNIFIED DRIVES AND DOCUMENT MANAGEMENT

Your documents are everywhere. That means they are **nowhere.**

Esii DDMS brings all your enterprise documents into a single, access-controlled storage infrastructure like NAS drive, AWS S3 buckets, Microsoft Azure Blob, and Windows file server.

Every file is governed, every access is logged and every share carries an expiry. Your compliance team will not have to ask twice.

● NAS • AWS S3 • Azure Blob • Windows File Server

● Role-Based Access Control

● Upload • Download • Delete

● Time-Limited Secure Sharing

● Full Audit Trail

● File Analytics

THE PROBLEM

Enterprise documents are scattered across NAS drives, windows file server, cloud storage, and personal folders. Nobody knows where the data is, who has access to it, or which version is current.

01 There is no single, authoritative platform for all your critical business documents.

Contracts, policies, approvals and reports are distributed across on-premise NAS drives, windows file servers, cloud storage buckets, and personal folders. When an auditor asks for a specific version of a document, your team has to search multiple systems and is still not certain which one is current or who last changed it.

02 Sharing a document externally means losing control of it permanently.

A document shared via email remains in the recipient's inbox indefinitely, long after the contract has expired or the relationship has ended. There is no mechanism to revoke access or confirm that the document has not been forwarded to other parties.

03 There is no record of who accessed which document and when.

Compliance audits for ISO, CMMi or internal governance require evidence of controlled document access. Without a system that captures every read, download and edit event, your team is producing these records manually, which takes time and introduces errors.

04 The two answers every IT Head and CISO needs immediately

Where is the data? Who has permission to access it? Without a single governance layer across all storage sources, these questions require manual investigation across multiple systems. For regulated organisations, the inability to answer quickly is itself a compliance risk.

05 Duplicate files, orphaned data and ungoverned storage are consuming infrastructure you are already paying for.

Without visibility across NAS, windows file server, AWS S3 and Azure Blob, organisations cannot identify which data is duplicated, which files have not been accessed in years or which storage is growing without ownership. Storage and backup infrastructure spend increases while the underlying data problem remains invisible.

06 Enterprise knowledge is locked inside folder hierarchy and hard to identify.

Contracts, SOPs, financial reports and engineering drawings contain critical information. Without intelligent search, employees recreate documents that already exist and miss precedents that could have saved hours. The knowledge is there but difficult to navigate.

07 Your existing document storage may already be creating DPDP liability.

The Personal Data Protection Act requires organisations to know where personal information is stored, who has access to it, whether consent was obtained and whether it can be erased on demand. Without a governance layer across all storage, most organisations cannot answer any of these questions firmly.

Unified View

Across all your storage sources

Links That Expire

Controlled external sharing

Full Audit Trail

Every access event logged

Governed File Operations

Upload, download and delete with full traceability

WHAT ESII DDMS DOES

ESii DDMS connects to your existing storage infrastructure and provides the unified access, governance and control that NAS drives, S3 buckets and Azure Blob containers cannot deliver alone.

Unified Storage Connectivity

ESii DDMS connects directly to your existing NAS, Windows File Server, AWS S3 and Azure Blob storage. Your files remain where they are. ESii DDMS provides the unified file explorer, governance layer and access controls that sit above them. No migration required.

Real-Time Document Monitoring

Every file and folder action across your connected storage is tracked as it happens. Edits, downloads and views trigger real-time notifications, so administrators always know what is happening to a document, not just who last touched it.

Secure External Sharing

External parties receive a time-limited, secure link to a specific document, regardless of which storage source it lives on. The link carries an expiry time that you configure. Once the link expires, access ends automatically without any manual revocation required.

Granular Role-Based Access

Permissions are configured at the folder and file level. Each user or department sees only what they are authorised to see. Access policies are enforced by the platform, not by individual file-sharing habits.

Governed Upload, Download and Delete

Every file operation is governed from the moment it is initiated. Uploads are authenticated and stored securely on your infrastructure. Downloads are logged against the user who requested them. Deletions move files to a controlled recycle bin before permanent removal. No file enters or leaves the system without a traceable event in the audit log.

File Analytics and Storage Intelligence (in Active Development, available in future shipped features)

Administrators will have complete visibility into how storage is being used utilized in context to duplicate files, access permission inconsistencies, data type distribution and compliance exposure. Decisions on access, archiving and governance are based on evidence, not on assumption.

Compliance Discovery (in Active Development, available in future shipped features)

ESii DDMS identifies personal information stored across your NAS, Windows File Server, S3 and Azure infrastructure, maps and discovers current access permissions against that data, as per India's DPDP Act guidelines, and generates the evidence your compliance team needs for audit readiness.

HOW IT WORKS

Documents are stored, governed and shared through a four-step process that keeps your team in control at every stage.

1

ESii DDMS connects to your existing storage infrastructure

Administrators configure connections to your on-premise NAS, AWS S3 buckets or Azure Blob containers. Your files remain in their current location. ESii DDMS provides the unified file explorer, access controls and governance layer above them. No data migration required.

2

Access permissions are applied at folder and file level

Administrators define role-based access policies. These permissions determine who can upload, view, download, delete or share the file. Any change to a permission is written to the audit log immediately.

3

External sharing is done through a time-limited, expiring secure link

When a document needs to be shared outside the organisation, the user generates a secure link with a configured expiry window. The recipient can access the document during that window. When the time expires, the link becomes inactive with no further action required.

4

Every action such as upload, access, download and deletion is captured in the audit log

The system records every action against every document: who uploaded it, who viewed it, when it was downloaded, when it was deleted, who made a change and which version was current at that point. Details are generated and monitored from the admin dashboard.

KEY FEATURES

Designed for enterprises that need document governance without the complexity of a full-scale ECM system.

Multi-Source Storage Connectivity

ESii DDMS connects to on-premise NAS, Windows File Server, AWS S3 and Azure Blob Storage from a single administration console. Your existing infrastructure investments are preserved. ESii DDMS provides the enterprise governance capabilities above them.

Role-Based Access Control

Granular access policies at folder and file level. Each role sees only what it is authorised for. Permissions are enforced by the platform, not by trust.

Time-Limited Secure Link Sharing

Secure, expiring links for external sharing. Access ends when the sharing period specified by the user expires.

Version Control and History

Every document version is preserved. Any previous version can be retrieved at any time, with a full record of who made which change.

Document Monitoring

Administrators and authorised users monitor document activity across all connected storage. Notifications surface on file and folder access events like Edit, Download, View through email and in the system notification panel.

Compliance-Ready Audit Logs

Every upload, read, download, deletion and share is logged. Dashboard reports are available for internal governance reviews without manual data collection.

File Analytics and Storage Insights (in Active Development, available in future shipped features)

Administrators see storage consumption, duplicate files, permission inconsistencies and data type distribution across all connected sources. PI data discovery identifies personal information across your storage infrastructure and flags DPDP compliance gaps before they become violations.

AI-Powered Document Agent (in Active Development, available in future shipped features)

Esii DDMS is built to integrate with Esii's own AI engine. Upcoming capabilities include semantic search, auto-classification and intelligent document summarisation and creation on your existing connected storage sources.

Enterprise Administration

Platform administrators manage users, groups, storage connectors, access policies and system health from a single console. Backup orchestration, archive policies and operational monitoring are centrally configured and reviewed from the same administration interface.

Offline Ready (in Active Development, available in future shipped features)

Files accessed in the last 15 days are cached locally. If internet connectivity is lost, users can continue to access and work on recent documents. Changes sync automatically when connectivity is restored.

WHERE ESII DDMS MAKES THE BIGGEST DIFFERENCE

Organisations with distributed storage, regulated documents and complex access requirements gain the most from ESii DDMS.

LEGAL AND COMPLIANCE

Contracts and policy documents with controlled access and a complete version trail

Legal teams can maintain all executed contracts in DDMS with access limited to authorised personnel. Every change to a contract document is versioned and logged. When the audit team requires evidence of controlled document management, the system generates the report directly.

FINANCE AND ACCOUNTS

Financial reports shared with external auditors through expiring, secure links

Rather than emailing financial statements as attachments, the finance team generates a time-limited SAS link to the specific document in DDMS. The auditor accesses the document during the permitted window. The access event is logged. The link expires automatically after the review period.

OPERATIONS AND QUALITY

SOPs and process documents managed as a living library with access by role

Standard operating procedures, quality manuals and process guidelines are maintained in DDMS with access configured by department and role. When an SOP is updated, the previous version is preserved in history. All team members work from the same current version at all times.

HUMAN RESOURCES

Employee documents stored with department-level isolation and compliance logging

HR documents including appointment letters, appraisal records and policy acknowledgements are stored in DDMS with access restricted to HR personnel and relevant managers. Compliance records showing who accessed each employee's documents are available at any time for internal or external review.

IT AND INFRASTRUCTURE

IT teams connect ESii DDMS to existing NAS servers, Windows File Server, S3 buckets and Azure Blob containers without migrating a single file. Access policies, audit logs and file analytics are managed from one administration console across all connected sources. Existing infrastructure investments are preserved and extended.

CONNECTED STORAGE SOURCES AND INTEGRATIONS

STORAGE

On-Premise NAS

Microsoft Azure Blob Storage

Amazon AWS S3

Windows File Server

Google Cloud Storage

IDENTITY AND ACCESS

Microsoft Entra ID (Azure AD)

Google Workspace

Local Authentication (DB Based)

GOVERNANCE

Role-Based Access Control Policy Engine

Group-Based Permissions

Full Audit Engine

Personal Identifiable Information Data Discovery

Permission Audit

PRODUCT EDITIONS / A-LA-CARTE

Esii DDMS is available as individual modules or as a complete enterprise suite. Organisations can start with File Explorer and Analytics and expand to full DDMS with DPDP Compliance, AI and Enterprise Administration as requirements grow.

See DDMS running in your environment.

ESII DDMS deploys on your infrastructure in days, not weeks. No migration. No disruption. No replacement of what already works.

[Book a Demo →](#)

esii.in
info@esii.in
A PC Solutions IP Brand
New Delhi, India