

# Microsoft Information Protection Integration via Sensitivity Label Management

Integrated with Microsoft Information Protection and Azure Information Protection, this feature is designed to address the need for scanning sensitivity labels within files located on home shares, SMB shares, and other data repositories. This feature empowers security administrators, compliance officers, and organizations to efficiently identify, manage, and enforce sensitivity labels on their data, ensuring adherence to data security, governance, and regulatory mandates across hybrid clouds at enterprise-class scale.

## Problem Statement

In today's data-driven and highly regulated business environment, organizations face a complex array of challenges related to sensitive data management and compliance:

- **Data Protection Regulations:** Governmental regulations and industry-specific compliance standards, such as GDPR, HIPAA, or CCPA, require organizations to maintain stringent data protection measures. Failure to comply with these regulations can result in severe financial penalties and damage to an organization's reputation.
- **Data Proliferation:** The exponential growth of data within organizations, often spread across various repositories, makes it increasingly challenging to identify, classify, and protect sensitive information effectively.
- **Data Migration Challenges:** Organizations frequently need to migrate data from one location to another, whether due to infrastructure changes, cloud adoption, or data center consolidations. During these migrations, maintaining the security and sensitivity labels of data can be highly complex, and errors can lead to data exposure or non-compliance.
- **Manual Labeling Processes:** Many organizations rely on manual processes for labeling sensitive data, which are time-consuming, error-prone, and inconsistent. Manual labeling not only increases operational overhead but also introduces the risk of data misclassification.
- **Data Security Concerns:** Failing to protect sensitive data adequately can result in data breaches, financial losses, and damage to an organization's reputation, affecting customer trust and stakeholder confidence.
- **Inefficient Compliance Reporting:** Reporting on data protection compliance can be arduous, especially when sensitive data is spread across multiple repositories. Manual reporting processes can lead to delays, inaccuracies, and increased compliance risks.

## Solution Overview

The Sensitivity Label Management functionality provides comprehensive solutions to these challenges through its key features:

### Key Features:

- **Sensitivity Label Management:** The software allows integration with Microsoft Information Protection and Azure Information Protection via Sensitivity Label Management. It scans files on various data repositories, including home shares and SMB shares, to identify whether they have sensitivity labels assigned.
- **Labeling Metrics:** The functionality provides metrics, such as the number of files without sensitivity labels, offering insights into the current state of label adoption within the organization.
- **Report Generation:** Users can generate detailed reports and datasets based on the scan results. These reports serve as a foundation for making decisions about applying sensitivity labels to files prior to migration to OneDrive or other destinations.
- **Automated Label Assignment:** The system automates the assignment of appropriate sensitivity labels to each file, ensuring consistency and accuracy in data protection. This eliminates the need for manual labeling by users.
- **Data Protection Compliance:** Organizations can use the software to maintain compliance with data protection regulations. Sensitivity labels help categorize and protect data based on its level of sensitivity and importance, reducing the risk of data breaches and regulatory violations.
- **Analytics Reports:** The system allows the generation of analytics reports, indicating which files have or do not have sensitivity labels and specifying the assigned label. These reports provide a comprehensive view of the organization's data protection status.
- **API Integration:** An API is provided for programmatic access to sensitivity label assignment. This allows organizations to automate label application processes and integrate them into existing workflows.

### Business Value:

- **Enhanced Data Protection:** The functionality ensures that all files are appropriately labeled with sensitivity labels, improving data protection by aligning data security measures with data sensitivity and importance.
- **Compliance Assurance:** By automating sensitivity label assignment and offering compliance-oriented reporting, organizations can confidently meet data protection regulations, reducing the risk of non-compliance and associated penalties.
- **Efficient Data Management:** Users can efficiently manage their data by automating the sensitivity label assignment process. This reduces manual workload, minimizes errors, and ensures consistent data protection practices.
- **Streamlined Migration:** Users can make informed decisions about labeling files before migration to OneDrive or other destinations, streamlining the migration process and ensuring that sensitive data retains its protection during and after migration.
- **API Flexibility:** The API integration allows for flexibility in sensitivity label assignment, enabling organizations to tailor label applications to their specific needs and workflows.

## Conclusion

The Sensitivity Label Management functionality offers a robust solution to the complex and pressing challenges organizations face in today's data-driven and highly regulated environment. By addressing the need for efficient sensitivity label management within files located on various data repositories, this feature provides a comprehensive suite of tools to enhance data protection, streamline compliance efforts, and optimize sensitive data migration.

Your journey toward efficient data management and migration begins here. For more information or to explore how these enhancements can benefit your organization, book a demo at <https://www.datadynamicsinc.com/request-a-demo/>.

You can also sign up for a data assessment at <https://www.datadynamicsinc.com/data-assessment/>

Data Dynamics is a leading provider of enterprise data management solutions, helping organizations structure their unstructured data with their Unified Unstructured Data Management Platform. The platform encompasses four modules- Data Analytics, Mobility, Security, and Compliance. Proven in over 300 organizations, including 28 Fortune 100, the Platform uses a blend of automation, AI, ML, and blockchain technologies and scales to meet the requirements of global enterprise workloads.

With Data Dynamics, enterprise customers can eliminate the use of individual point solutions with siloed data views. Instead, they can utilize a single software platform to structure their unstructured data, unlock data-driven insights, secure data, ensure compliance and governance and drive cloud data management. Ultimately, the company's vision is to help enterprises achieve data democratization so that users, no matter their technical background, can instantly access, understand, and derive maximum insights from unstructured data sprawls.



Visit Website

Book a Demo

Contact Us

© 2023 Data Dynamics. The trademarks Data Dynamics, StorageX, Insight AnalytiX, ControlX, Universal Data Engine, UDE, Insight Analytics, Manage Your Data, Champion of Data, and Dynamic File Management are the registered or unregistered trademarks of Data Dynamics, Inc. All other trademarks are the property of their respective owners.