arctera™

From Classification to Compliance

Microsoft Purview information protection labels enhanced by Arctera Insight Information Governance.

Solution Overview | November 2025

Summary

In a time when data breaches are expensive and frequent, effective data management has become essential. This white paper outlines a comprehensive approach to data protection by combining the capabilities of Arctera Insight Information Governance with the sensitivity labels of Microsoft Purview. This partnership offers businesses:

- A streamlined approach to accurate data classification and security compliance
- Enhanced data protection measures powered by a sophisticated, unified labeling mechanism

By harnessing Arctera, organizations can enhance the effectiveness of Microsoft Purview's labeling, leading to improved data security and compliance management.

Importance of Data Classification and Labeling

Effective data management is anchored in the fundamental practice of classifying and labeling data appropriately. Microsoft Purview's sensitivity labels are essential tools that empower organizations to categorize their data, marking the information based on its level of sensitivity. These categorizations are critical; they dictate how data is handled, shared, and secured, ensuring that sensitive information receives the necessary safeguards.

Incorrect labeling or failure to label data can lead to serious compliance breaches or security oversights. An example of the risk posed by mislabeling or not labeling data is non-compliance with regulations such as GDPR or HIPAA. For instance, if personal data is not labeled as *Confidential*, it might not receive the required level of encryption or access control, leading to potential data breaches and heavy fines.

This approach is crucial to safeguard data and ensure compliance with strict data protection rules. It requires consistent attention from the moment data is created until it is securely disposed of.

Arctera Insight Information Governance streamlines data management with its robust classification engine, enhancing the accuracy and consistency of data categorization. This advanced classification capability enables precise, ongoing adjustments to data labels, ensuring they remain aligned with evolving organizational needs and regulatory standards.

By integrating Arctera with Microsoft Purview's labeling system, organizations are equipped to manage their data with greater efficacy, maintaining a strong stance on data security and regulatory compliance.

Empowering Label Management with Arctera

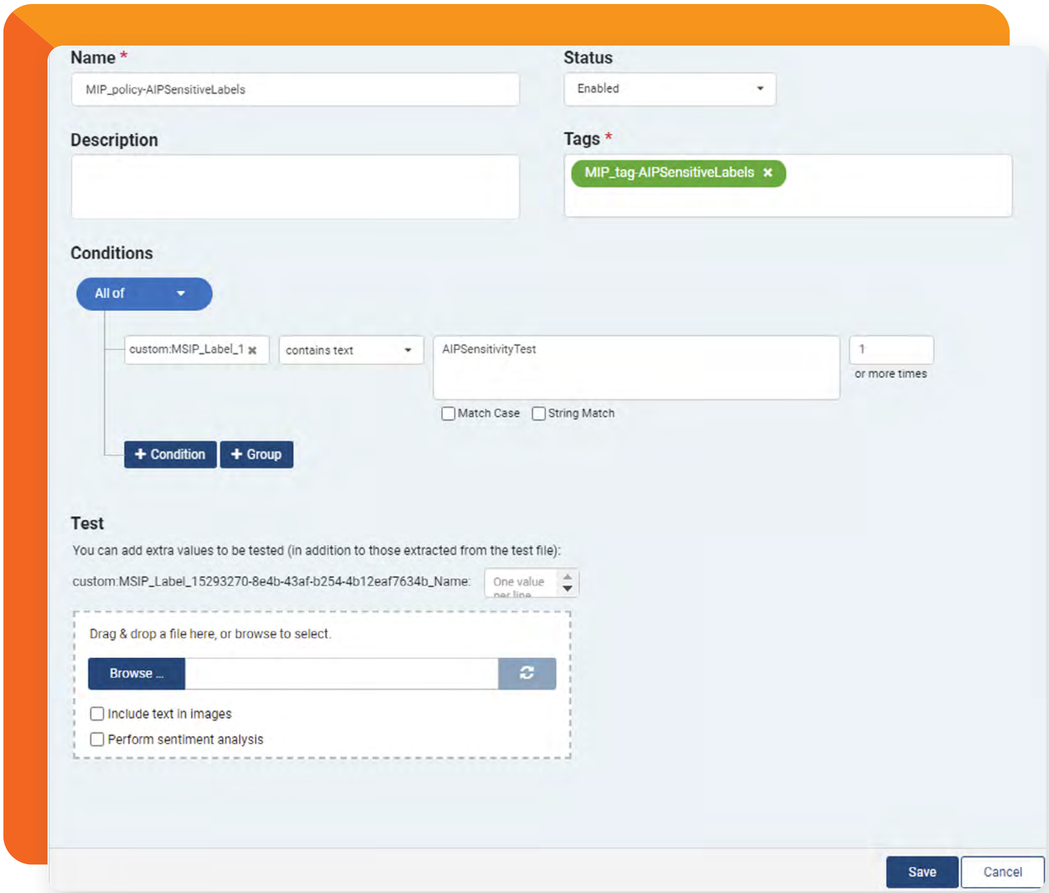
The Arctera Insight Platform brings advanced data insight and analytics to the forefront of data governance, empowering organizations to manage and protect sensitive information with precision. By enhancing Microsoft Purview Information Protection (MPIP), Arctera Insight enables customers to fully leverage MPIP's sensitivity labels across their data environments.

Label Detection and Insights

Arctera scans the enterprise's data landscape, identifying and documenting existing MPIP labels. It provides comprehensive visibility across data repositories, recognizing sensitive documents and ensuring they are properly managed.

Responsive Label Modification

Built on a powerful classification engine, Arctera Insight enables efficient adjustments to MPIP labels. Policies are designed to identify and respond to shifts in data classification, continuously updating labels to match the latest data sensitivity levels.



Name *: MIP_policy-AIPSensitiveLabels

Status: Enabled

Description:

Tags *: MIP_tag-AIPSensitiveLabels

Conditions

All of

custom:MSIP_Label_1 | contains text | AIPSensitivityTest | 1 or more times

□ Match Case □ String Match

Test

You can add extra values to be tested (in addition to those extracted from the test file):

custom:MSIP_Label_15293270-8e4b-43af-b254-4b12eaf7634b_Name: One value per line

Drag & drop a file here, or browse to select.

□ Include text in images

□ Perform sentiment analysis

Figure 1. Configuring policies using the Arctera Insight Platform's classification engine for MPIP labels.

Strategic Label Application

Arctera enables proactive labeling of documents. It identifies files and their MPIP labels, enabling the labeling of unlabeled content and the correction of mislabeled data including those on CIFS devices. This action fortifies the organization's data security strategy, particularly for shared storage systems where sensitive data might otherwise remain unprotected.

Correcting labeling errors — including non-classification and misclassification — is paramount to uphold security standards and achieve regulatory compliance.

Automated Reclassification and Remediation

The true power of Arctera lies in its automated reclassification capabilities. Users can easily set up rules within the system to auto-classify documents according to their content. With a simple setup process, sensitive files that are initially unclassified or misclassified can be detected and labeled correctly, without manual intervention.

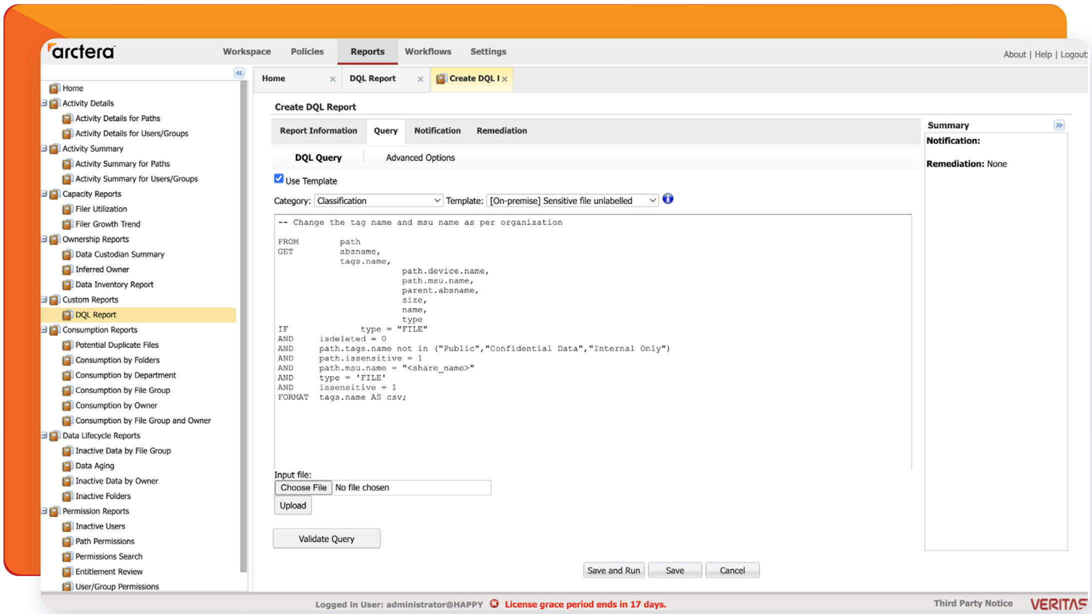
To simplify the application of MPIP labels across your data estate, Arctera provides a powerful automation tool: the Data Query Language (DQL) report. Follow this step-by-step guide to create a DQL report that automates MPIP label application for your sensitive files:

Step 1: Initiate DQL Report Creation

From the dashboard, navigate to the Custom Reports section and select DQL Report. This area allows for the creation and management of custom reports based on specific criteria.

Step 2: Configure Report Parameters

Within the *Create DQL Report* interface, direct your attention to the *Query* tab. Here you can utilize templates for various data classification scenarios. For instance, select *Classification* from *Category,* and a template such as *[On-premise] Sensitive file unlabeled* to target sensitive documents that lack MPIP labels.



Create DQL Report

☑ Use Template

Category: Classification Template: [On-premise] Sensitive file unlabelled

```
-- Change the tag name and msu name as per organization

FROM       path
GET        absname,
           tags.name,
                       path.device.name,
                       path.msu.name,
                       parent.absname,
                       size,
                       name,
                       type
IF              type = "FILE"
AND     isdeleted = 0
AND     path.tags.name not in ("Public","Confidential Data","Internal Only")
AND     path.issensitive = 1
AND     path.msu.name = "<share_name>"
AND     type = 'FILE'
AND     issensitive = 1
FORMAT  tags.name AS csv;
```

Input file: No file chosen

Summary

Notification:

Remediation: None

Logged in User: administrator@HAPPY License grace period ends in 17 days.

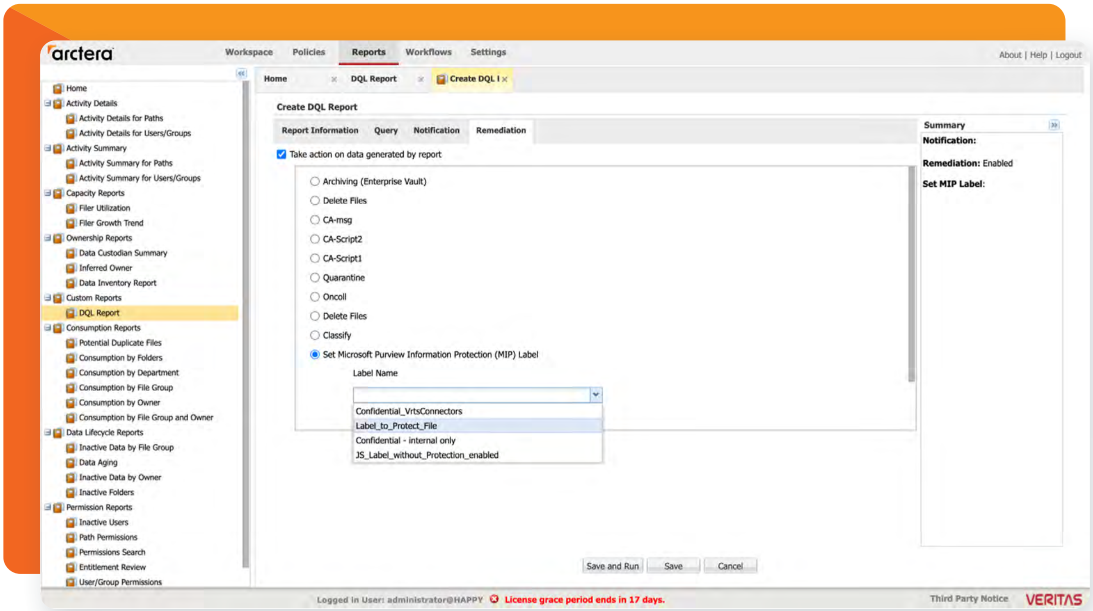
Figure 2. Creating a DQL report to automate MPIP labels application

Step 3: Customize Query for Your Environment

Modify the query parameters to suit your organization's unique environment. Adjust the *path.tags.name and path.msu.name* to match the specific labels and shares relevant to your data governance framework.

Step 4: Set Up Remediation Actions

Switch to the *Remediation* tab. Choose the *Set Microsoft Purview Information Protection (MPIP) Label* action. From the dropdown, select the appropriate label that aligns with the sensitivity of the content being targeted by the report.



Create DQL Report

☑ Take action on data generated by report

○ Archiving (Enterprise Vault)
○ Delete Files
○ CA-msg
○ CA-Script2
○ CA-Script1
○ Quarantine
○ Oncoll
○ Delete Files
○ Classify
● Set Microsoft Purview Information Protection (MIP) Label

Label Name

- Confidential_VrtsConnectors
- Label_to_Protect_File
- Confidential - internal only
- JS_Label_without_Protection_enabled

Summary

Notification:

Remediation: Enabled

Set MIP Label:

Logged in User: administrator@HAPPY License grace period ends in 17 days.

Figure 3. Creating a DQL report to automate MPIP labels application

Step 5: Justification and Execution

Before executing the report, provide a justification for the remediation action. This step is crucial for auditing and compliance purposes. Once complete, save your settings and run the report.

As the report executes, it will automatically apply the chosen MPIP label to all files that meet the criteria specified in the DQL query. This automated labeling ensures a consistent and compliant data protection stance across your organization's digital assets.

Arctera can apply MPIP labels to Microsoft Office documents and PDF files, syncing with label configurations in a customer's Office 365 environment. While it primarily operates with real-time synchronization in internet-connected environments, it can also manage labels in isolated settings. In these cases, labels can be pre-fetched and used within the solution, ensuring data classification and protection remain effective regardless of connectivity. This flexibility makes Arctera Insight adaptable to diverse operational needs, seamlessly integrating with Azure Compliance Center for up-to-date label management.

Automated Security Actions Through Label Management

The integration with MPIP labels goes beyond simple label management; it activates a security framework that adapts to changes in data classification. This dynamic approach is essential for effective remediation, ensuring that as data is reclassified—whether due to policy updates or evolving content—security measures are promptly and automatically adjusted.

Proactive Protection Measures

In data security, proactive measures are essential to safeguarding sensitive information. The integration with MPIP labels supports this approach, allowing updates to a document's sensitivity level to trigger enhanced protection measures. When a label is elevated to a higher sensitivity, it initiates a series of preemptive actions to secure the document, such as adjusting access permissions and applying additional security protocols. These actions are customized to align with the new sensitivity level, ensuring each piece of data receives the precise protection it requires. This approach strengthens data defenses against potential threats and supports compliance with evolving regulatory standards, fostering a robust and adaptive security posture.

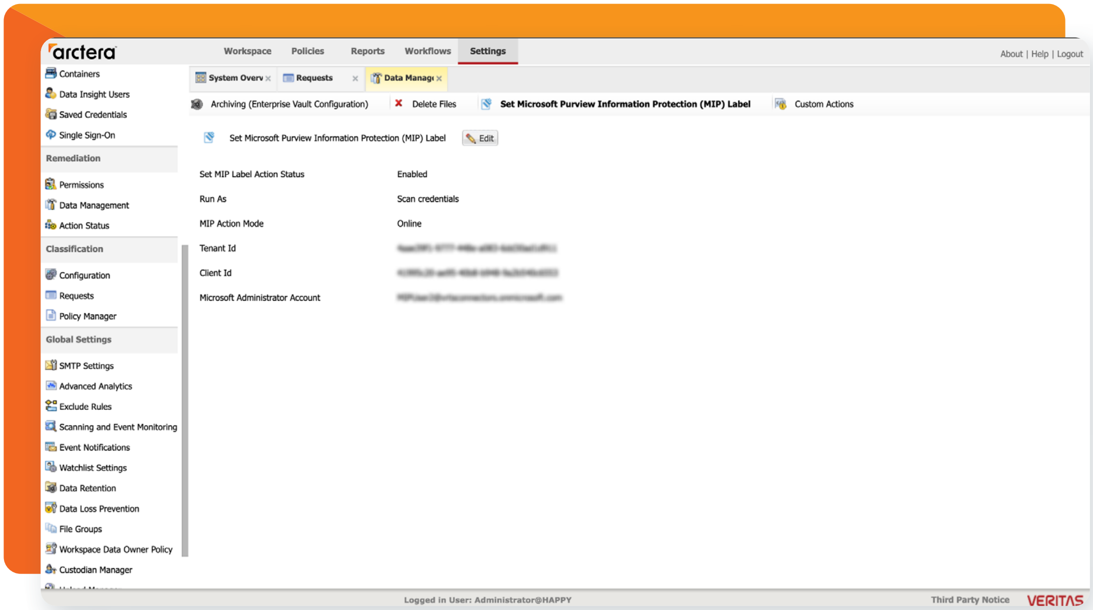
Encryption as a First Line of Defense

Label governance plays a key role in document security, activating Microsoft Purview's security measures when a document's sensitivity is updated. When an MPIP label is adjusted, Purview may apply encryption to the document, ensuring that only users with the appropriate decryption key can access it. This encryption enhances document security, guarding against unauthorized access.

Watermarking for Traceability and Deterrence

Through MPIP label management, sensitive documents can be watermarked to ensure traceability and discourage unauthorized distribution. Label updates prompt Microsoft Purview to apply watermarks, which identify document origin and help deter unauthorized sharing.

Throughout this process, users benefit from an intuitive interface for on-demand label adjustments, reinforced by role-based access controls to uphold security and compliance integrity.



Set Microsoft Purview Information Protection (MIP) Label

Set MIP Label Action Status	Enabled
Run As	Scan credentials
MIP Action Mode	Online
Tenant Id	[redacted]
Client Id	[redacted]
Microsoft Administrator Account	[redacted]

Figure 4. Setting an MPIP label in Arctera Insight Information Governance.

By incorporating these actions into data governance systems, Arctera Insight Information Governance helps organizations quickly address security vulnerabilities. Now, organizations can take a proactive approach to remediation, making it a crucial element of their overall data security strategy.

Conclusion

We have explored how Arctera Insight Information Governance integrates with MPIP labels to transform data governance and security. This combination of Arctera Insight's advanced classification and MPIP's strong labeling framework offers a complete solution for modern data protection. It enables organizations to automate the classification and protection of sensitive data, simplify compliance efforts, and enhance their security measures.

In conclusion, organizations looking to improve their data governance strategies will find a valuable partner in Arctera and MPIP integration. Contact us to discover how this integration can enhance your data management practices and support your security goals.

About Arctera

Arctera, a business unit of Cloud Software Group, is the leading global provider of compliance and governance solutions that enable firms to unleash game-changing technologies into their organizations while minimizing risk. Created in 2024 from Veritas Technologies, Arctera helps the biggest companies in the world monitor and control exactly how their information is being accessed, used and shared. The Arctera Insight Platform is able to capture data from over 130+ different content sources, and more than 280 AI policies help firms streamline compliance and adapt to evolving regulations.

arctera™

Learn more: arctera.com

Connect:

Contact: press@arctera.com