

The Microsoft Purview Information Protection client is a Windows-based tool designed to help organizations classify, label, and protect sensitive data consistently across locations. It is the successor to the Azure Information Protection (AIP) unified labeling client and offers advanced capabilities for maintaining data security and compliance.

Key Features

- **Sensitivity Labeling:** Users can apply sensitivity labels to files and emails that enforce protection settings like encryption, access control, and visual markings. These labels stay with the data wherever it travels.
- **File Explorer Integration:** Allows users to right-click and label files directly within Windows File Explorer for quick classification.
- **PowerShell Module:** Provides command-line tools that administrators can use to automate labeling, configure policy settings, and operate the Information Protection scanner.
- **Information Protection Scanner:** Scans on-premises data repositories such as file shares and SharePoint libraries to find, label, and protect sensitive information.
- **Viewer for Protected Files:** Includes a viewer app that allows users to open and read encrypted or labeled files to ensure they remain accessible.

Deployment and Compatibility

The client works on supported Windows Clients and Windows Servers. It requires .NET Framework 4.7.2 or newer and Windows PowerShell 4.0 or later. It can be deployed using an .exe or .msi installer, with options for silent installation and customization through registry settings.

Characteristic	Description
Sensitivity Labeling	Apply labels to enforce protection
File Explorer Integration	Label files directly within Explorer
PowerShell Module	Automate labeling and configure policies
Information Protection Scanner	Scan repositories to protect data
Viewer for Protected Files	Open and read encrypted files