Azure Information Protection

ENSURE PERSISTENT CLASSIFICATION AND PROTECTION OF YOUR DATA

Data Protection in Office 365

Office online services provide data protection (encryption + authentication + use rights) capabilities, which use Azure Information Protection. However, not all Office 365 subscriptions include the protection feature provided by Azure Information Protection. For information on which Office 365 subscriptions include protection, refer to the table below.

Subscription	Includes Protection
Office 365 Business Essentials	No[1]
Office 365 Business Premium	No[1]
Office 365 Enterprise E1	No[1]
Office 365 Education A1	Yes
Office 365 Enterprise E3	Yes
Office 365 Education A3	Yes
Office 365 Government G3	Yes
Office 365 Developer E3	No
Office 365 Enterprise E4	Yes
Office 365 Education A4	Yes
Office 365 Government G4	Yes
Office 365 Enterprise E5	Yes
Office 365 Education A5	Yes
Office 365 Enterprise F1	No[1]
SharePoint Plan 1	No[1]
SharePoint Plan 2	No[1]

Exchange Online Plan 1	No[1]
Exchange Online Plan 2	No[1]

[1] Azure Information Protection is not included but can be purchased as a separate add-on and will enable the supported Information Rights Management (IRM) features. Some Azure Information Protection features require a subscription to Office 365 Pro Plus, which is not included with Office 365 Business Essentials, Office 365 Business Premium, Office 365 Enterprise E1, Office 365 Education, or Office 365 Enterprise F1.

Key features available for O365 subscriptions with data protection

- Users can create and consume protected content by using Windows clients and Office applications
- Users can create and consume protected content by using mobile devices
- Integration with Exchange Online, SharePoint Online, and OneDrive for Business
- Integration with Exchange Server 2013/Exchange Server 2010 and SharePoint Server 2013/SharePoint Server 2010 on-premises via the AIP connector. Note for Office 365 Message Encryption customers must route mail through Exchange Online.
- Administrators can create departmental templates
- Organizations can create and manage their own tenant key in a hardware security module (the Bring Your Own Key solution)
- Support for non-Office file formats: Text and image files are natively protected; other files are generically protected
- Protection SDK for all platforms: Windows, Windows Phone, iOS, Mac OSX, and Android

Licensing FAQs for Azure Information Protection scanner

Q. What licensing is required to use the AIP scanner?

A. The AIP scanner requires Azure Information Protection Premium Plan 1 to use the tool in the default Reporting only mode. Applying automatic classification, labeling and/or protection to discovered files with the scanner requires Azure Information Protection Premium Plan 2.

Q. Which users should be licensed for AIP scanner?

A. An Azure Information Protection premium license, at the level noted above based on the capabilities in the tool you are using, is required for all internal users of all scanned file repositories. As is standard with Azure Information Protection premium licensing, additional licensing is not required for external users who are accessing protected files or

for users who previously protected files but are no longer users in the tenant, such as users who have left your organization

Q. If the scanner is configured to apply default labels to files in a repository, is an Azure Information Protection Plan 2 License required?

A. Yes, changing the scanner from reporting only mode to apply classification labels requires an Azure Information Protection Plan 2 license.

Q. A company has 50,000 users with 25,000 on Azure Information Protection Plan 1/EMS E3 and 25,000 on Azure Information Protection Plan 2/EMS E5 licenses. They want to leverage the scanner but have one repository for all users. How will licensing work?

A. An Azure Information Protection premium license, at the level noted above based on the capabilities in the tool you are using, is required for all internal users of all scanned file repositories. As is standard with Azure Information Protection premium licensing, additional licensing is not required for external users who are accessing protected files or for users who previously protected files but are no longer users in the tenant, such as users who have left your organization.

In the example above, to use the AIP scanner in reporting only mode would not require any additional licensing, as all users are licensed for at least Azure Information Protection Plan 1. Using the scanner to apply classification, labeling and/or protection would require that all 50,000 internal users have an Azure Information Protection Plan 2 license.

Q. If I use Set-AIPFileClassificaion cmdlet and apply automatic labeling to files based on defined conditions, what license do I need?

A. This cmdlet is currently the technical mechanism for changing the scanner from reporting only mode to enabling it to apply classification, labels and/or protection and therefore requires that all internal users of all scanned file repositories have an Azure Information Protection Plan 2 license.

Q. If a service account is set as the owner of files in a repository scanned by the scanner, does it require only 1 license for that account?

A. If a service account is set as owner of files, several high value features such as document tracking and revocation will not work. You will also see discrepancies in logging, auditing and some other workflows over time. It is therefore recommended to retain the author's name as the owner of documents being scanned.