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 license do I need for AIP scanner?

A. AIP scanner requires P2 license, like any other automatic classification feature.

Q. What users should be licensed for AIP scanner?

A. Any active user that authors (creates) a content in scanned repositories should be licensed with P2 license. Users that just consume files from these repositories don’t need a license. Users that created content in scanner repositories in the past but are no longer part of the company (deleted or disabled users) don’t need to be licensed.

Q. If the scanner is configured to apply default labels to files in a repository, does it require AIP P2/EMS E5 licenses?

A. If the scanner applies default labels to files in repositories, AIP P1/EMS E3 license is sufficient.

Q. A company has 50k users with 25k on AIP P1/EMS E3 and 25K on AIP P2/EMS E5 licenses. They want to leverage the scanner but have one repository for all users. How will licensing work?

A. all active users that create content in the scanned repository need a AIP P2/EMS E5 license. Users just consuming content from this repository don't need a license.

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

A. Any action that applies automatically applies labels to files based on conditions requires AIP P2/EMS E5 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. Yes, but 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 a period of time. It is therefore recommended to retain the author's name as the owner of documents being scanned.