Microsoft

Microsoft 365 Tenant-Level Services
Licensing Guidance

Contents

Overview 1
Azure Active Directory Identity Protection 2
Azure Advanced Threat Protection 2
Azure Information Protection 3
Office 365 Advanced Threat Protection 3
Office 365 Cloud App Security 4
Microsoft Cloud App Security 4
Office 365 Advanced Data Governance 5
Office 365 Advanced eDiscovery 6
Office 365 Customer Key 6
Office 365 Customer Lockbox 7
Privileged Access Management in Office 365 8
Data Loss Prevention for Exchange Online, SharePoint Online, and OneDrive for Business 8
Data Loss Prevention for Teams chat and channel conversations 9
Information barriers 9
Advanced Message Encryption 10

Overview

For the purposes of this guide, a tenant-level service is an online service that when purchased for any user on the tenant (standalone or as part of Office/Microsoft 365 plans) is activated in part or in full for all users on the tenant. While in these cases some unlicensed users may be able to access the service technically, a license is required for any user that you intend to benefit from the service.

Note: Some tenant services currently do not have the capability to limit benefits to specific users, over time those capabilities will be included in the services. Efforts should be taken to limit the service benefits to licensed users to avoid disruption to your organization when targeting capabilities are employed.

Microsoft

Azure Active Directory Identity Protection

Azure Active Directory Identity Protection (AADIP) is a feature of the Azure Active Directory Premium P2 that enables you to detect potential vulnerabilities affecting your organization's identities, configure automated responses to detected suspicious actions that are related to your organization's identities and investigate suspicious incidents and take appropriate action to resolve them.

Who is entitled to the service?

Licensed users of Enterprise Mobility + Security E5, Microsoft 365 E5, Microsoft 365 E5 Security, and Azure Active Directory Premium Plan 2 are entitled to receive the benefit of AADIP.

How is a user benefiting from the service?

SecOps analysts and security professionals benefit from having consolidated views of flagged users and risk events based on machine learning algorithms. End users benefit from the automatic protection provided through risk-based Conditional Access and the improved security posture provided by acting on vulnerabilities.

How is the service provisioned/deployed?

By default, AADIP features are enabled at the tenant-level for all users within the tenant. For information on configuring AADIP, refer to https://docs.microsoft.com/azure/active-directory/identity-protection/enable

How can the service be applied to only users in the tenant that are licensed for the service?

Admins can scope AADIP by assigning risk policies that define the level for password resets and allowing access for licensed users only. Follow the instructions here for scoping AADIP deployments: Configure the sign-in risk policy

Azure Advanced Threat Protection

Azure Advanced Threat Protection (Azure ATP) is a cloud service that helps protect your enterprise hybrid environments from multiple types of advanced targeted cyber-attacks and insider threats.

Who is entitled to the service?

Licensed users of Enterprise Mobility + Security E5, Microsoft 365 E5, Microsoft 365 E5 Security, and Azure Advanced Threat Protection for Users are entitled to receive the benefit of Azure ATP.

How is a user benefiting from the service?

SecOp analysts and security professionals benefit from Azure ATP's ability to detect and investigate advanced threats, compromised identities, and malicious insider actions. and protect your enterprise hybrid environment. End users benefit by having their data monitored by Azure ATP.

How is the service provisioned/deployed?

By default, Azure ATP features are enabled at the tenant-level for all users within the tenant. For information on configuring Azure ATP, refer to https://docs.microsoft.com/azure-advanced-threat-protection/install-atp-step1

How can the service be applied to only users in the tenant that are licensed for the service?

Microsoft does not commit to providing threat detection capabilities for users who are not licensed. Over time license checks or targeted tooling will be added to Azure ATP to ensure Azure ATP functionality is applicable to licensed users only.

Microsoft

Azure Information Protection

Azure Information Protection (AIP) helps an organization discover, classify, label and protect its sensitive documents and emails. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.

Who is entitled to the service?

Licensed users of Microsoft 365 F1, Microsoft 365 E3, and AIP Plan 1 are entitled to receive the benefit of AIP Plan 1. Microsoft 365 E5, Microsoft 365 E5 Compliance, and AIP Plan 2 licensed users are entitled to receive the benefit of AIP Plan 2.

How is a user benefiting from the service?

Users classifying, labeling or protecting documents or emails benefit from Azure Information Protection capabilities. The Azure Information Protection scanner feature automatically classifies, labels and protects files that reside in on-premises file repositories.

How is the service provisioned/deployed?

By default, Azure Information Protection features are enabled at the tenant-level for all users within the tenant. For information on configuring Azure Information Protection policies for licensed users, refer to https://docs.microsoft.com/azure/information-protection/activate-service

How can the service be applied to only users in the tenant that are licensed for the service?

Azure Information Protection feature policies (save for the scanner feature) can be scoped to specific groups or users; registries can be edited to prevent unlicensed users from running Azure Information Protection classification or labeling features. Follow the instructions here for scoping Azure Information Protection deployments: Configuring the Azure Information Protection policy

For the Azure Information Protection scanner feature, Microsoft does not commit to providing file classification, labelling or protection capabilities to user who are not licensed. Over time license checks or targeted tooling will be added to Azure Information Protection to ensure the scanner feature is assignable to licensed users.

Office 365 Advanced Threat Protection

Microsoft Office 365 Advanced Threat Protection (ATP) helps protect your organization against sophisticated attacks such as phishing and zero-day malware. It also provides actionable insights by correlating signals from a broad range of data to help identify, prioritize, and provide recommendations on how to address potential threats.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Security, Microsoft 365 Business, and Office 365 ATP Plans 1 and 2 are entitled to receive the benefit of ATP.

How is a user benefiting from the service?

ATP benefits a user when the service is used to protect that user from sophisticated attacks such as phishing and zero-day malware. Please see here for the full list of services provided in Plan 1 and Plan 2.

Microsoft

How is the service provisioned/deployed?
By default, ATP features are enabled at the tenant-level for all users within the tenant. For information on configuring ATP policies for licensed users, refer to https://docs.microsoft.com/office365/securitycompliance/office-365-atp.

How can the service be applied to only users in the tenant that are licensed for the service?
To scope ATP, follow the Safe Links and Safe Attachments deployment policies

- Safe Links can be configured only for licensed users as described here: Safe Links Policies
- Safe Attachments can be configured only for licensed users as described here: Safe Attachments Policies

Office 365 Cloud App Security

Office 365 Cloud App Security (OCAS) is a subset of Microsoft Cloud App Security, with features limited to Office 365 and without additional security for 3rd party cloud apps and IaaS services.

It gives customers visibility into their productivity cloud apps and services, provides sophisticated analytics to identify and combat cyberthreats, and enables you to control how your data travels – across Office 365.

For a comparison of features visit: https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-o365

Who is entitled to the service?
Licensed users of Office 365 E5.

For more information, please refer to the Microsoft Cloud App Security licensing guide at www.aka.ms/mcaslicensing

How is a user benefiting from the service?
Office 365 Cloud App Security benefits a user by discovering Shadow IT, providing threat protection across Office 365, and the ability to control which apps have permissions to Office 365 data.

How is the service provisioned/deployed?
By default, Office 365 Cloud App Security features are enabled at the tenant-level for all users within the tenant.

For information on configuring the service, refer to: https://docs.microsoft.com/Office365/SecurityCompliance/turn-on-office-365-cas.

How can the service be applied to only users in the tenant that are licensed for the service?
Office 365 Cloud App Security deployments can be scoped by Office 365 administrators to enforce how certain apps are accessed and limit user groups monitored by Office 365 Cloud App Security as described here: Scoped Deployment.

Microsoft Cloud App Security

Microsoft Cloud App Security (MCAS) is a Cloud Access Security Broker (CASB) solution that gives customers visibility into their cloud apps and services, provides sophisticated analytics to identify and combat cyberthreats and enables you to control how your data travels – across any cloud app.

Microsoft

Who is entitled to the service?

Licensed users of Microsoft Cloud App Security standalone, EMS E5, M365 E5 and M365 E5 Security are entitled to receive the benefits of Microsoft Cloud App Security.

Azure AD P1 licensed users are entitled to leverage the Discovery capabilities in Microsoft Cloud App Security.

To be able to leverage Conditional Access App Control capabilities in Microsoft Cloud App Security, users additionally require to be licensed for Azure Active Directory P1, which is included in EMS E3, EMS E5, M365 E3, M365 E5, and M365 E5 Security.

For automatic labelling, users are required to be licensed for Azure Information Protection P2, which is included in EMS E5, M365 E5, and M365 E5 Compliance.

For more information, please refer to the Microsoft Cloud App Security licensing guide at www.aka.ms/mcaslicensing

How is a user benefiting from the service?

Microsoft Cloud App Security benefits a user by discovering and assessing Shadow IT in the organization, providing threat protection across 1st and 3rd party cloud apps, and the ability to protect information wherever it travels across 1st and 3rd party cloud apps.

How is the service provisioned/deployed?

By default, Microsoft Cloud App Security features are enabled at the tenant-level for all users within the tenant.

For information on configuring Microsoft Cloud App Security policies for licensed users, refer to: https://docs.microsoft.com/cloud-app-security/what-is-cloud-app-security

How can the service be applied to only users in the tenant that are licensed for the service?

Microsoft Cloud App Security deployments can be limited to licensed users by using the scoped deployment capabilities in the service described here: https://docs.microsoft.com/en-us/cloud-app-security/scoped-deployment.

Office 365 Advanced Data Governance

Office 365 Advanced Data Governance (ADG) helps organizations meet information governance requirements with policies to enable retention and deletion. ADG provides the ability to auto-label content based on sensitive information type and apply governance policies to that content.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and Office 365 Advanced Compliance are entitled to receive the benefit of ADG.

How is a user benefiting from the service?

Users benefit from ADG's ability to apply labels to specific data to uphold specific policies, including ability to automatically label content as a record, and manage the full records process from declaration to disposal.

Microsoft

How is the service provisioned/deployed?

By default, ADG features are enabled at the tenant-level for all users within the tenant. For information on configuring ADG to apply auto-labeling and policies licensed users, refer to https://docs.microsoft.com/office365/securitycompliance/labels

How can the service be applied to only users in the tenant that are licensed for the service?

ADG retention policies may be applied to licensed users only through automatic classification to the locations (i.e. team sites, group sites, etc.). Follow the instructions here to apply ADG retention policies: Applying Retention Policies.

Office 365 Advanced eDiscovery

Office 365 Advanced eDiscovery provides investigation and eDiscovery solutions for IT and Legal departments within corporations to identify, collect, preserve, reduce and review content related to an investigation or litigation prior to export out of the Office 365 system.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and Office 365 Advanced Compliance are entitled to receive the benefit of Advanced eDiscovery.

How is a user benefiting from the service?

Users benefit from Advanced eDiscovery when their content is put on hold content as part of a litigation or investigation.

How is the service provisioned/deployed?

By default, Advanced eDiscovery features are enabled at the tenant-level for all users within the tenant when assigning eDiscovery permissions in the Security and Compliance center.

How can the service be applied to only users in the tenant that are licensed for the service?

Organizations can manage Advanced eDiscovery on a per user basis and add users to an Advanced eDiscovery case, as well as provide users with edit access to the shared locations through eDiscovery permissions. To apply Advanced eDiscovery permissions to licensed users only, follow the instructions here: Assign eDiscovery Permissions.

Office 365 Customer Key

With Office 365 Customer Key, you control your organization's encryption keys and then configure Office 365 to use them to encrypt your data at rest in Microsoft's data centers. In other words, Customer Key allows customers to add a layer of encryption that belongs to them, with their keys. Data at rest includes data from Exchange Online and Skype for Business that is stored in mailboxes and files that are stored in SharePoint Online and OneDrive for Business.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and Office 365 Advanced Compliance are entitled to receive the benefit of Office 365 Customer Key. Additionally, customers must also have a subscription for Azure Key Vault to get the full benefit of Office 365 Customer Key.

How is a user benefiting from the service?

Users benefit from Office 365 Customer Key by having their data encrypted at rest at the application layer using encryption keys that are provided, controlled and managed by the customer organization.

Microsoft

How is the service provisioned/deployed?

Office 365 Customer Key encryption keys can be enabled for all data stored in Exchange Online and Skype for Business mailboxes and SharePoint Online and OneDrive for Business files. For information on configuring Office 365 Customer Key to encrypt your data at rest, refer to: Controlling Your Data Using Customer Key

How can the service be applied to only users in the tenant that are licensed for the service?

To assign encryption keys to data within an Office 365 and/or Microsoft 365 tenant for licensed users only, follow the Office 365 Customer Key encryption keys deployment policies:

- For SharePoint Online, files on one or more sites can be encrypted using Customer Key as described here: Setting up Customer Key for SharePoint Online and OneDrive for Business.
- For Exchange Online and Skype for Business Online, mailboxes can be encrypted using Customer Key as described here: Setting up Customer Key for Exchange Online and Skype for Business

Office 365 Customer Lockbox

Customer Lockbox provides an additional layer of control by offering customers the ability to give explicit access authorization for service operations. By demonstrating that procedures are in place for explicit data access authorization, Customer Lockbox may also help customers meet certain compliance obligations such as HIPAA and FEDRAMP.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and the Office 365 Advanced Compliance are entitled to receive the benefit of Customer Lockbox.

How is a user benefiting from the service?

Users benefit from Customer Lockbox's ability to ensure that no one at Microsoft can access their content to perform a service operation without the customer's explicit approval. Customer Lockbox brings the customer into the approval workflow for requests to access their content. Occasionally, Microsoft engineers are involved during the support process to troubleshoot and fix customer reported issues. In most cases, issues are fixed through extensive telemetry and debugging tools that Microsoft has in place for its services. However, there may be cases that require a Microsoft engineer to access customer content to determine the root cause and fix the issue. Customer Lockbox requires the engineer to request access from the customer as a final step in the approval workflow. This gives organizations the option to approve or deny these requests, which gives them direct control of whether a Microsoft engineer can access the organizations' end user data.

How is the service provisioned/deployed?

An Office 365 administrator can turn on Customer Lockbox controls in the Microsoft 365 admin center as described at https://docs.microsoft.com/Office365/Admin/manage/customer-lockbox-requests. When Customer Lockbox is turned on, Microsoft is required to obtain an organization's approval prior to accessing any of their content.

How can the service be applied to only users in the tenant that are licensed for the service?

Microsoft does not commit to providing Customer Lockbox access control approval requests for the users who are not licensed. Over time license checks or targeted tooling will be added to Customer Lockbox to ensure Customer Lockbox is assignable to licensed users.

Microsoft

Privileged Access Management in Office 365

Privileged access management in Office 365 (PAM) provides granular access control over privileged admin tasks in Office 365. After enabling privileged access management, users will need to request just-in-time access to complete elevated and privileged tasks through an approval workflow that is highly scoped and time-bound.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and Office 365 Advanced Compliance are entitled to receive the benefit of PAM.

How is a user benefiting from the service?

Enabling PAM will allow your organization to operate with zero standing privileges. Users benefit from the added layer of defense against vulnerabilities arising from standing administrative access that can provide unfettered access to their data.

How is the service provisioned/deployed?

By default, PAM features are enabled at the tenant-level for all users within the tenant. For information on configuring PAM policies, refer to https://docs.microsoft.com/office365/securitycompliance/privileged-access-management-configuration

How can the service be applied to only users in the tenant that are licensed for the service?

Customers can manage PAM on a per user basis through approver group and access policies, which may be applied to licensed users only, as described here: Privileged Access Management in Office 365.

Data Loss Prevention for Exchange Online, SharePoint Online, and OneDrive for Business

With Data Loss Prevention (DLP) for Exchange Online, SharePoint Online, and OneDrive for Business, organizations can identify, monitor, and automatically protect sensitive information across emails and files (including files stored in Microsoft Teams file repositories).

Who is entitled to the service?

Licensed users of Office 365 E3, Microsoft 365 E3, and Office 365 Data Loss Prevention are entitled to receive the benefits of DLP for Exchange Online, SharePoint Online, and OneDrive for Business.

How is a user benefiting from the service?

A user is benefiting from DLP for Exchange Online, SharePoint Online, and OneDrive for Business when their emails and files are being inspected for sensitive information, as configured in the organization's DLP policy.

How is the service provisioned/deployed?

By default, Exchange Online emails, SharePoint sites, and OneDrive accounts are "enabled Locations (workloads)" for these DLP features for all users within the tenant. For additional information about using DLP policies, refer to https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies.

How can the service be applied to only users in the tenant that are licensed for the service?

Admins can customize locations (workloads), included users, and excluded users in the Office 365 Security & Compliance Center, under **Data loss prevention** > **Locations**.

Microsoft

Data Loss Prevention for Teams chat and channel conversations

With Data Loss Prevention (DLP) for Teams chat and channel conversations, organizations can block messages in chats and channel conversations that contains sensitive information, such as financial information, PII, health-related info or other confidential information.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and Office 365 Advanced Compliance are entitled to receive the benefit of DLP for Teams chat and channel conversations.

How is a user benefiting from the service?

The sender benefits by having sensitive information in their outgoing chat and channel conversation messages inspected for sensitive information, as configured in the organization's DLP policy.

How is the service provisioned/deployed?

By default, Teams chat and channel conversations are an "enabled Location (workload)" for these DLP features for all users within the tenant. For additional information about using DLP policies, refer to https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies.

How can the service be applied to only users in the tenant that are licensed for the service?

Admins can customize locations (workloads), included users, and excluded users in the Office 365 Security & Compliance Center, under **Data loss prevention** > **Locations**.

Information barriers

Information barriers are policies that an admin can configure to prevent individuals or groups from communicating with each other. This is useful if, for example, one department is handling information that shouldn't be shared with other departments or a group needs to be prevented from communicating with any outside contacts. Information barrier policies also prevent lookups and discovery. This means that if you attempt to communicate with someone you should not be communicating with, you will not find that user in the people picker.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and Office 365 Advanced Compliance are entitled to receive the benefit of information barriers.

Microsoft

How is a user benefiting from the service?

A user is benefitting from the advanced compliance capabilities of information barriers when that user is restricted from communicating with others. For example:

Scenario:	Who is benefitting and therefore requires a license?
Two groups (Group 1 and Group 2) cannot communicate with each other (i.e., Group 1 users are restricted from communicating with Group 2 users, and Group 2 users are restricted from communicating with Group 1 users.	Users in both Group 1 and Group 2
Users in Group 1 are restricted from communicating with the rest of the company.	Users in Group 1 only
The rest of the company is restricted from communicating with Group 1.	All users except those in Group 1
Group 1 users are restricted from communicating with Group 2 users, but Group 2 users can communicate with Group 1 users.	Users in Group 1 only

How is the service provisioned/deployed?

Admins create and manage information barriers policies via PowerShell cmdlets in the Security & Compliance Center. Admins must be assigned the Microsoft 365 Enterprise Global Administrator, Office 365 Global Administrator or Compliance Administrator role to establish an information barrier policy. By default, these policies apply to all users on the tenant. For more information about information barriers, refer to https://docs.microsoft.com/en-us/MicrosoftTeams/information-barriers-in-teams.

How can the service be applied to only users in the tenant that are licensed for the service?

Admins can customize locations (workloads), included users, and excluded users in the Office 365 Security & Compliance Center. For example, if all their users are licensed for Office 365 E3, and none are licensed for Office 365 Advanced Compliance/E5, they could avoid creating any information barriers policies for their organization. For more information about information barriers, refer to Information barriers in Microsoft Teams preview.

Advanced Message Encryption

Advanced Message Encryption in Office 365 helps customers meet compliance obligations that require more flexible controls over external recipients and their access to encrypted emails. With Advanced Message Encryption in Office 365, admins can control sensitive emails shared outside the organization with automatic policies that can detect sensitive information types (e.g. PII, Financial or Health IDs) or keywords to enhance protection by applying custom email templates and expiring access through a secure web portal to encrypted emails. Additionally, admins can further control encrypted emails accessed externally through a secure web portal by revoking access at any time.

Who is entitled to the service?

Licensed users of Office 365 E5, Microsoft 365 E5, Microsoft 365 E5 Compliance, and Office 365 Advanced Compliance are entitled to receive the benefit of Advanced Message Encryption.

Microsoft

How is a user benefiting from the service?

The sender of a message is benefiting from the added control over sensitive emails provided by Advanced Message Encryption.

How is the service provisioned/deployed?

Admins create and manage Office 365 Advanced Message Encryption policies in the Exchange Admin Center under mail flow rules. By default, these rules apply to all users on the tenant. For more information about setting up new Office 365 Message Encryption capabilities, refer to https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-new-message-encryption-capabilities

How can the service be applied to only users in the tenant that are licensed for the service?

Admins can avoid applying mail flow rules for Advanced Message Encryption that apply to unlicensed users. For more information about defining mail flow rules, refer to https://docs.microsoft.com/en-us/office365/securitycompliance/define-mail-flow-rules-to-encrypt-email.