



Make Practice a Priority


With this book, you get resources like Practice Questions, Exam Tips, Flashcards, and more. These can be unlocked immediately after purchasing your own copy using the unique sign-up code provided in the book.


 Practice Resources SHARE FEEDBACK


DASHBOARD





MS-900 Exam Guide Third Edition
Gain the required knowledge and problem-solving skills to pass the MS-900 exam

 Practice Questions


 Flashcards

 Chapter Review Questions

 Exam Tips

 Ask a question


BACK TO THE BOOK



Microsoft 365 Certified Fundamentals MS-900 Exam Guide - Third Edition
Aaron Guilmette, Yura Lee, Marcos Zanre

Practice Questions

These will help you simulate the exam environment. Use the timed practice questions on the platform to develop a habit of thinking quickly under pressure.

 Practice Resources SHARE FEEDBACK ▾

Question 7 of 20 ⌚ Time Left 0 hr 28 mins 54 secs END QUIZ

☐ Predictable Microsoft licensing costs

☐ Increased service scalability in the cloud

☐ Increased Exchange Server Client Access License (CAL) costs

☐ Increased Windows Server Client Access License (CAL) costs


☐ Decreased service scalability in the cloud


☐ Decreased on-premises infrastructure footprint

PREVIOUS NEXT SKIP QUESTION

Chapter Review Questions and Benchmark Scores

At the end of each chapter, you'll find links to chapter review questions. These are designed to help you consolidate your learning from a chapter before moving on to the next one. Each chapter has a benchmark score, aim to match that score or beat it before picking up the next chapter.

 Practice Resources

[SHARE FEEDBACK](#) 

DASHBOARD > CHAPTER 1

Describe the Different Types of Cloud Services Available

Summary

This chapter explained the core concepts of cloud computing. Cloud computing allows you to access data — either personal or business — from any device, including your phone, tablet, or computer. You looked at the benefits of storing information this way and linked these benefits to a variety of popular use cases.

You also learned the differences between various types of cloud computing concepts, such as software as a service, platform as a service, and infrastructure as a service. While Microsoft has services that fit into all of those computing categories, the core focus for the MS-900 exam will be the Microsoft 365 SaaS offering.


Finally, you learned some of the core differences between the various Office 365 and Microsoft 365 services.

In the next chapter, you will continue exploring basic cloud architecture concepts with a discussion on the different types of clouds, including public and private clouds, as well as the advantages and use cases of each.

Chapter Review Questions

The Microsoft 365 Certified Fundamentals MS-900 Exam Guide – Third Edition by Aaron Guilmette, Yura Lee, Marcos Zanne


[Select Quiz](#)


Quiz 1 [SHOW QUIZ DETAILS](#) 

[START](#)

Flashcards

Use interactive flashcards to memorize key concepts.

 Practice Resources

[SHARE FEEDBACK](#) 

DASHBOARD > FLASHCARDS SET 1

Flashcards stack 1

Flashcards memorized so far: 1

Flashcards not memorized yet: 9

☐ Mark as memorized


Is Microsoft 365 an example of SaaS, IaaS, or PaaS?

[PREVIOUS](#) [NEXT](#)

2/9

Exam Tips

Use the exam tips on the platform to gain insights that can help you enhance your preparation strategy and maximize your chances of success.

 Practice Resources SHARE FEEDBACK

DASHBOARD > EXAM TIPS

Be sure you understand security concepts (4/10)

- Nearly a third of the exam revolves around security—from multi-factor authentication to Conditional Access and data loss prevention.
- Navigate to Secure Score (<https://aka.ms/securescore>) and review the recommended actions for your tenant. Secure Score is a great tool to improve your organization's security posture and highlights all the common configuration options that you should set.

← PREVIOUS NEXT → ☐ Mark as Helpful (0 users found this tip helpful)

Comments

Add your comment

Ask a Question

If you have any doubts, you can reach out to us via the platform. We will try our best to resolve any questions. Responses to any questions you ask will be posted in the “Resolved Questions” section of the website so that others can benefit from my answers as well. If you find any issues with the platform, the book, or any of the practice materials, you can click the **Share Feedback** button from any page and reach out to us. If you have any suggestions for improvement, you can share those as well.

Note

This section is exclusive to the sample copy and is not a part of the book. It is written for those who are looking to buy the book but have some questions regarding how the free online content works and how to make the most out of it.

About the MS-900 Exam

Microsoft 365 Fundamentals (MS-900) is a crucial certification in the field of cloud computing and productivity. This globally recognized credential validates your expertise, giving you a competitive edge and boosting your career prospects in the IT industry. Achieving MS-900 certification is pivotal for success, showcasing your proficiency in implementing Microsoft 365 services. This qualification is invaluable, establishing instant credibility in interactions with stakeholders, regulators, and customers.

The MS-900 exam focuses on the basic concepts and interdependencies between these services. This book will help you understand the basics of identity and authentication in Microsoft Entra ID (formerly Azure Active Directory) as well as ways to secure the identity platform. This book will also help you understand the core services of the Microsoft 365 platform and how personal and team productivity solutions can enhance work.

Who This Book Is For

Microsoft 365 Certified Fundamentals MS-900 Exam Guide, Third Edition, is targeted at Microsoft 365 service administrators and cloud technologists who want to prove their knowledge by passing this updated MS-900 certification exam. The qualified exam candidate should be able to demonstrate foundational knowledge of cloud concepts and the Microsoft 365 suite. Mastering the concepts tested in this exam provides a solid stepping stone to other, more advanced Microsoft certifications. You can learn more about this exam at <https://learn.microsoft.com/en-us/credentials/certifications/exams/ms-900/>.

What This Book Covers

This book is aligned with the revised syllabus of *MS-900: Microsoft 365 Fundamentals* and encompasses the following topics:

Chapter 1, Describe the Different Types of Cloud Services Available, begins by explaining the foundational cloud computing concepts and the benefits that customers can expect to take advantage of.

Chapter 2, Describe the Benefits and Considerations for Using Cloud, Hybrid, or On-Premises Services, expands your knowledge into areas such as public versus private clouds, as well as how hybrid and flexible work has changed the landscape.

Chapter 3, Describe the Productivity Solutions of Microsoft 365, explains the basics of what makes up the Microsoft 365 suite.

Chapter 4, Describe the Collaborative Solutions of Microsoft 365, goes beyond the individual productivity components of Microsoft 365 and introduces team collaborative features.

Chapter 5, Describe Endpoint Modernization, Management Concepts, and Deployment Options in Microsoft 365, provides a look at deployment and management options for Windows 10 and Windows 11 and introductions to Azure Virtual Desktop and Windows 365.

Chapter 6, Describe the Analytics Capabilities of Microsoft 365, introduces the new features of Viva Insights (formerly My Analytics), as well as core usage and the reporting functions of Microsoft 365.

Chapter 7, Describe Zero Trust Principles for Microsoft 365, explores the six pillars of the zero trust framework and how each is used to contribute to an organization's security posture.

Chapter 8, Understand Identity and Access Management Solutions, discusses identity concepts such as using Entra ID (formerly Azure Active Directory) in cloud and hybrid scenarios. This chapter also explores security features such as Conditional Access and multi-factor authentication.

Chapter 9, Describe the Threat Protection Solutions of Microsoft 365, introduces the Microsoft 365 Defender suite, which protects identity, messaging, apps, and endpoints. In addition, this chapter details the value and capability of Secure Score and automation in threat management.

Chapter 10, Describe the Trust, Privacy, Risk, and Compliance Solutions of Microsoft 365, explores the key features of compliance, governance, and data protection in Microsoft 365, including sensitivity labels, Privacy privacy management, auditing, eDiscovery, and retention policies.

Chapter 11, Identify Microsoft 365 Pricing and Billing Management Options, provides an overview of purchasing and billing scenarios for Microsoft 365 services.

Chapter 12, Identify Licensing Options Available in Microsoft 365, discusses the concepts of base and add-on licensing as well as methods for managing and assigning licenses.

Chapter 13, Identify Support Options for Microsoft 365 Services, introduces the process for obtaining support as well as the different included and add-on support options available.

To Get the Most Out of This Book

The Microsoft 365 platform is best experienced with either a laptop or desktop computer running a modern operating system, such as Windows 10 or later or macOS 10.12 or later. Additionally, modern browsers such as Microsoft Edge or a current version of Chrome, Safari, or Firefox are necessary for the Office 365 portal user interface to render properly. Older versions of Microsoft Internet Explorer may not work correctly.

An Office 365 tenant will also be required to follow along with some of the configuration examples. You can sign up for a trial tenant (no credit card required) at <https://www.microsoft.com/en-us/microsoft-365/business/compare-more-office-365-for-business-plans>. Some configuration options will require an Azure AD (Entra ID) Premium subscription, which you can obtain as part of a Microsoft 365 trial or by activating an Azure AD (Entra ID) Premium trial within the Azure portal (<https://portal.azure.com>) once you have obtained a trial Office 365 tenant.

Some examples may require various tools, such as the SharePoint Online Management Shell (<https://www.microsoft.com/en-us/download/details.aspx?id=35588>), the Microsoft Teams module (<https://www.powershellgallery.com/packages/MicrosoftTeams/>), or the Office Deployment Tool (<https://www.microsoft.com/en-us/download/details.aspx?id=49117>).

7

Describe Zero Trust Principles for Microsoft 365

Data security and compliance with regulatory acts are important for every organization. It is crucial to be mindful of how data is stored and transmitted for every organization, and whether it complies with the following:

- **Privacy legislation:** The European Union's **General Data Protection Regulation (GDPR)** or the United States' **Health Insurance Portability and Accountability Act (HIPAA)**
- **Financial regulations:** The **Sarbanes-Oxley (SOX) Act**
- **Industry compliance:** The **Payment Card Industry Data Security Standard (PCI DSS)**

With the rise of cybersecurity breaches and attacks, there is an urgent need to understand the proper configurations of the available services and features. Cloud services have changed the way organizations deploy technology and secure data.

A clear understanding of Microsoft 365's out-of-the-box security features and services is the key to successfully deploying cloud services.

You will explore security concepts that map to the following exam topics:

- Describe the zero-trust model
- Describe Microsoft **Granular Delegated Admin Privileges (GDAP)** principles

By the end of this chapter, you will have a clear understanding of how zero trust principles can help organizations remain secure.

Describe the Zero-Trust Model

Traditional **Information Technology (IT)** security measures have relied primarily on treating the corporate infrastructure as a boundary—everything inside the local network is safe, while anything outside the firewall is a threat.

However, the proliferation of mobile devices, hybrid work, and **Bring-Your-Own-Device (BYOD)** scenarios has allowed organizational data to be freely transported beyond the corporate network boundary. Firewalls in an office setting are not effective when the data you are trying to protect is on a tablet computer that was left at a restaurant or on the subway.

With that in mind, Microsoft (and the tech industry as a whole) has pivoted from the traditional security perimeter defense perspective to a model called **zero trust**.

Zero trust is based on the concept of minimizing an organization's risk footprint by interrogating the security of everything that attempts to access data or services. The zero-trust model treats all new requests as if they are from an untrusted actor until proven otherwise. In other words, *never trust, always verify*.

Zero Trust Principles

The zero-trust model is based on the following principles:

- Explicit verification
- Least-privilege access
- Assume breach

Read on to find out about each of these principles.

Explicit Verification

Explicit verification means evaluating the authentication and authorization requests. The possible evaluation criteria include user identity, the network location from which the access requests originate, the health or compliance of a device, service, or workload configuration, classification of the requested data, or other characteristics that may present themselves during the verification process.

Least-Privilege Access

The concept of **least-privilege access** focuses on reducing the standing rights and permissions that a user or device has to access a resource. For example, if an account with a high level of permission is compromised, then everything that the account is authorized to access is at risk. To limit the risk or exposure (sometimes referred to as the **blast radius**), it's important to ensure that identities and devices only have the minimum number of rights and permissions necessary.

Least privilege can be combined with technologies that offer programmatic, just-in-time, and just-enough access. That way, users or administrators can request additional rights or privileges for a defined period in order to perform specific activities.

Assume Breach

This final piece of the zero-trust model stresses that the design of the network, security, and other access controls should treat every attempt as hostile. As an administrator or architect approaching security with this design philosophy, you may choose to segment your network and application resources, require specific device or network configurations, and ensure that devices and identities pass multiple stages of verification. Once identities and devices are verified, data should be encrypted to safeguard against over-the-air or other methods of snooping on traffic, and sensors should be deployed to detect anomalous activity and isolate risky devices.

Now that you are aware of the zero-trust model and its principles, the next section will look at areas (or pillars) a zero-trust defense strategy should protect.

Zero Trust Pillars

Organizational assets can generally be broken into six categories (or pillars, as Microsoft refers to them):

- Identity
- Endpoints
- Apps
- Data
- Infrastructure
- Network

Over the next few sections, you will explore each of these areas and explore ways to reduce surface attack areas and improve organizational security.

Identity

Cloud services pose new security and access challenges. Traditionally, users have done the following:

- Only access the organization's resources inside the organization's network perimeter
- Only access the organization's services that are hosted on the organization's hardware

With cloud services, enterprise mobility, BYOD objectives, and the consumerization of IT, organizations cannot depend on the traditional way of security and access. Users are now accessing a variety of services from a multitude of vendors from both company-owned and personal devices. **Identity** is the new security perimeter for companies since it is the ultimate key to access.

From a cloud service perspective, identity defines the users, the permissions they have, and what they can do with those permissions. With that defined, organizations need to plan how to protect users wherever they may be.

Role Management

Permissions allow organizations to provide certain individuals with elevated access so that they can perform specific operations in the service. A common strategy that is shared across different Microsoft 365 admin centers is **Role-Based Access Control (RBAC)**. RBAC will allow—under the minimum level of permissions needed—users (categorized by roles) to execute their tasks and only their tasks. Utilizing roles is a key way to employ a least-privilege access model.

Microsoft 365 has a granular permissions model that allows organizations to have multiple administrators whose administrative abilities are scoped to certain groups of tasks. Some of the roles that are available in Microsoft 365 are outlined here:

- **Billing admin:** This role makes purchases, manages subscriptions and service requests, and monitors the health service.
- **Global admin:** This role is the most permissive role with the rights to access and modify all configurations in all the admin centers. It can also reset the passwords of all users and add and manage domains.
- **Exchange admin:** With full access to the **Exchange Online (EXO)** admin center, this role manages Microsoft 365 groups and service requests, and monitors service health.
- **Group admin:** The role creates and manages groups, including group naming and expiration policies.
- **Helpdesk admin:** This role can reset passwords for non-admin users, help users sign out, manage service requests, and monitor service health. The helpdesk admin can force users to sign out. Users with this role can only reset passwords for users that do not have other directory roles (except the Directory reader, Guest inviter, Helpdesk admin, Message center reader, and Reports reader roles).
- **License admin:** This role can assign and remove user licenses and usage locations.
- **Message center privacy reader:** This role grants permission to view the message center posts (including posts about data privacy), as well as view domains, groups, and subscriptions.
- **Office Apps admin:** Users with this role can use the **Cloud Policy service** to create and manage cloud-based policies for Microsoft 365 apps, create and manage service requests, monitor service health information, and manage the **What's New** content for Microsoft 365 apps.

- **Password admin:** This role resets passwords for all non-administrative users.
- **Power Platform admin:** The Power Platform admin can manage the admin features for Power Apps and **Data Loss Prevention (DLP)**. This role can also create and manage service requests as well as monitor service health information.
- **Reports reader:** The reader accesses the reports dashboard, Power BI adoption content packs, sign-in reports, and the Microsoft Graph reporting **Application Programming Interface (API)**.
- **Global reader:** Users in this role can read settings and administrative information across Microsoft 365 services but cannot take management actions. Global reader is the read-only counterpart to Global admin.
- **Service Support admin:** The Service Support admin can open and manage service requests, view message center posts, and monitor service health messages.
- **SharePoint admin:** This role has full access to the **SharePoint Online (SPO)** admin center, manages Microsoft 365 groups and service requests, and monitors service health.
- **Teams administrator:** This role has full access to the Teams admin center, manages Microsoft 365 groups and service requests, and monitors service health.
- **Teams communications administrator:** This role assigns telephone numbers, creates and manages voice and meeting policies, and reads call analytics.
- **Teams device administrator:** This role configures and manages devices used for Microsoft Teams services, such as Teams Rooms, Teams displays, and phones.
- **User admin:** This role resets user passwords, manages users and groups, manages service requests, and monitors service health.

Note

While it's not important to know all of the roles for the MS-900 exam, it's important to be familiar with a few core roles (such as Global admin, Billing admin, User admin, Helpdesk admin, Password admin, and License admin) and the overall concepts of role-based administration. You can find a more complete list at <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>.

To assign a role to a user in the Microsoft 365 admin center, an administrator with proper permissions can edit a user’s properties and assign an administrator role under **Manage admin roles**, as shown in *Figure 7.1*:

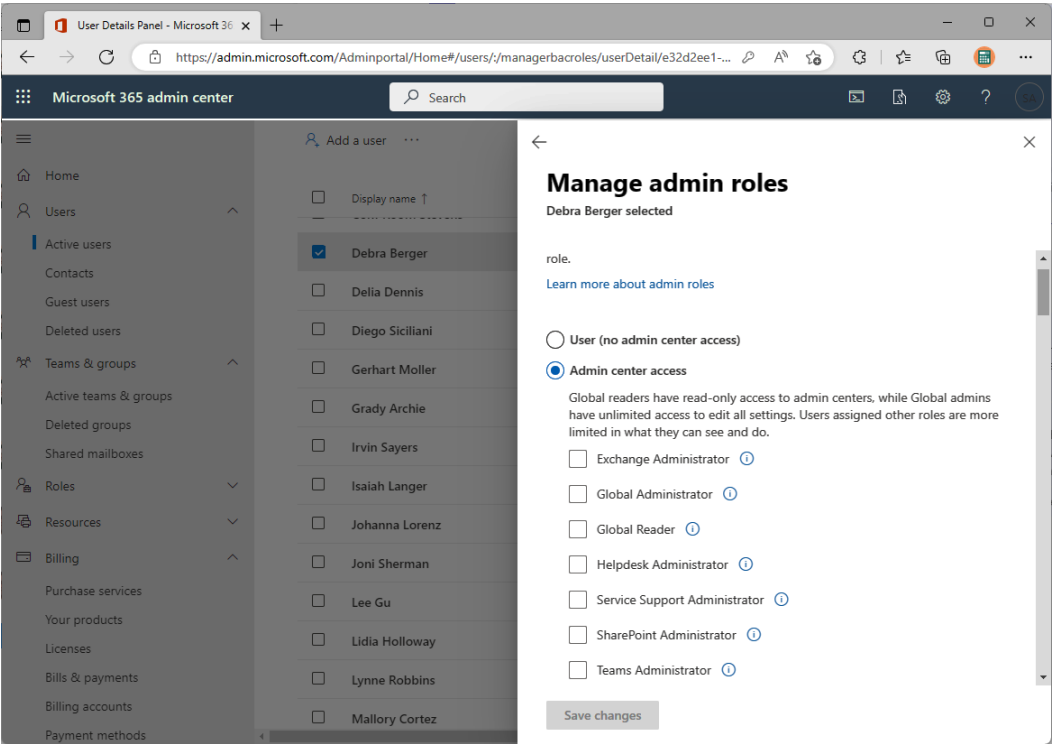


Figure 7.1 – Assigning an admin role

Additionally, more granular roles can be assigned in the **Azure Active Directory (AAD) Roles and administrators** blade, which is available in the Azure portal (<https://aad.portal.azure.com>), as shown in *Figure 7.2*:

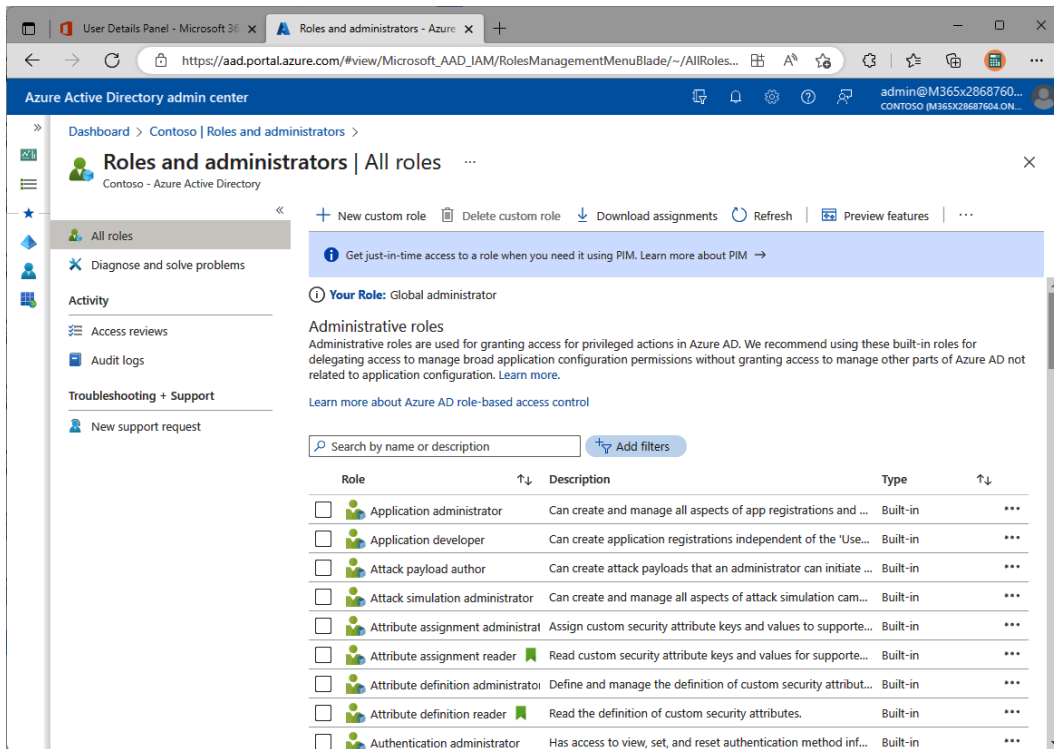


Figure 7.2 – AAD Roles and administrators blade

As part of a least-privilege access model, organizations can also use **Privileged Identity Management (PIM)**. PIM allows designated users to be granted elevated permissions for a period of time and is configured with a series of workflows to ensure proper approval is granted before assigning the role permissions. With this feature, organizations can significantly limit the number of fully privileged accounts in their environment, reducing their attack surface.

AAD PIM is configured through the Azure portal (navigate to <https://portal.azure.com> and search for Privileged Identity), as shown in *Figure 7.3*:

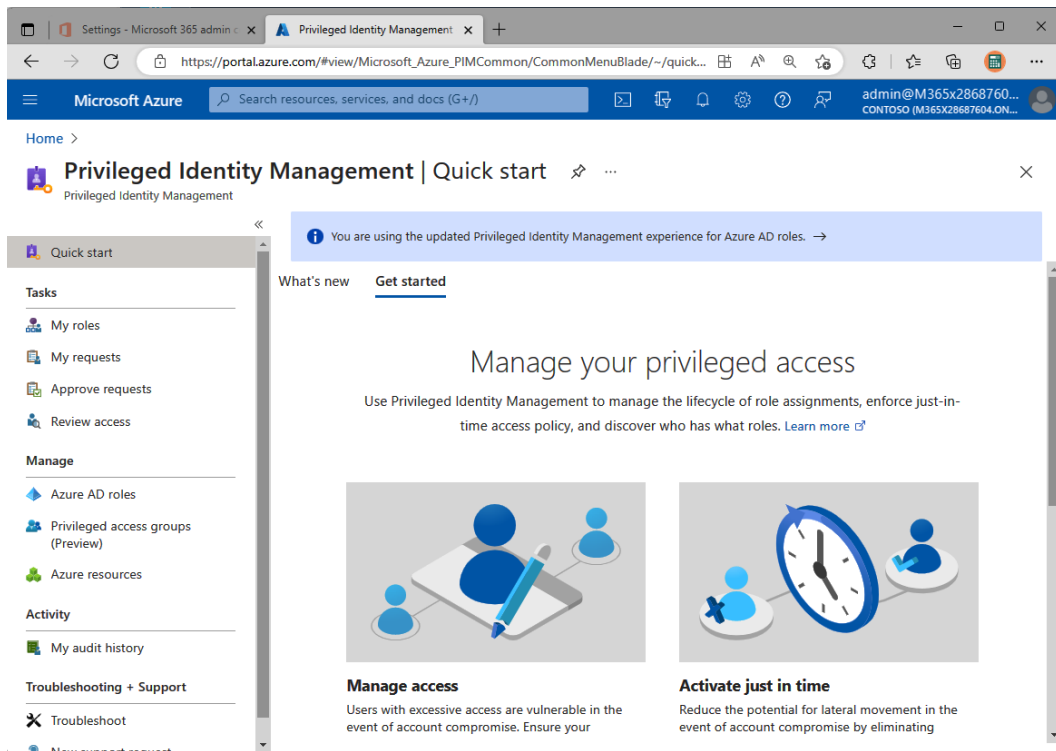


Figure 7.3 – Privileged Identity Management

Organizations should follow best practices when considering their permission, role, and administration strategies. Some recommendations include the following:

- Have no more than four and no less than two global admins.
- Whenever possible, assign the **least permissive** role to administrators.
- Require **Multi-Factor Authentication (MFA)** from all admins and end users.

You will read more about recommendations later in this chapter.

Audit Logs

Successful operations and governance strategies rely partially on being able to audit actions taken in the service. Adhering to zero trust principles means that all activities performed in the tenant are available for review.

Microsoft 365 allows administrators to review activities that are performed either by users or administrators through the audit logs. Audit logs are available in the Microsoft Purview compliance portal (formerly known as the Microsoft 365 compliance center) and are located at <https://compliance.microsoft.com/auditlogsearch>.

Some audited actions include the following:

- File and page operations
- Sharing and access request activities
- Exchange mailbox activity
- User administration activity
- Role administration activity
- eDiscovery tasks
- Microsoft Teams operations
- Exchange admin operations

Previously, audit logging was disabled by default. In new organizations, Microsoft has automatically enabled it; however, it can still be disabled manually via an administrator.

Audited activities

For a complete list of all currently audited activities, please check out the following documentation: <https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>.

In your position as administrator, you should check and ensure that auditing is turned on. Administrators can enable this by opening the Microsoft Purview compliance portal and clicking on **Start recording user and admin activity**, as shown in *Figure 7.4*:

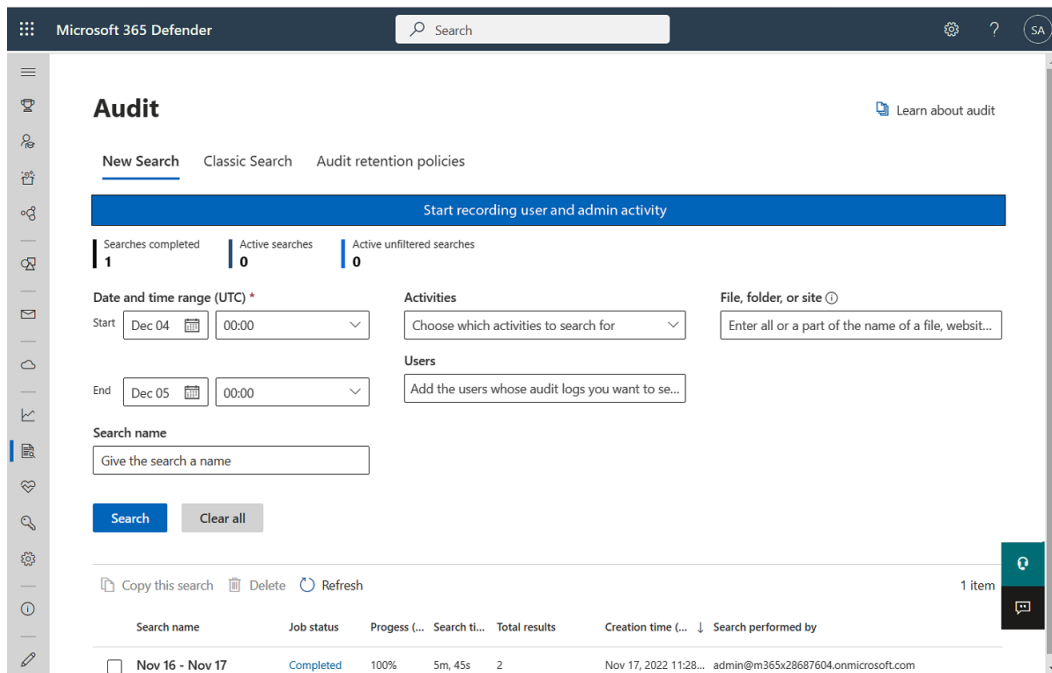


Figure 7.4 – Enabling auditing

When viewing audit logs, administrators can filter them according to the following options:

- Activities
- Start date
- End date
- Users
- File, folder, or site

Currently, Microsoft 365 audit logs are retained in the service for 90 days for users with a **Microsoft 365 Enterprise E3** license, or one year for users with a **Microsoft 365 Enterprise E5** license. If an organization wants to retain data for a longer period, it will need to plan and deploy a solution to capture that data, such as Azure Sentinel, Log Analytics, or an on-premises **Security Information and Event Management (SIEM)** product. This can be accomplished through PowerShell or with the Office 365 Management Activity API.

To export a list of audit log entries, an administrator can open the audited data and select individual entries to view and export. You can also download all of the entries by clicking **Export** and then selecting **Download all results**, as shown in *Figure 7.5*:

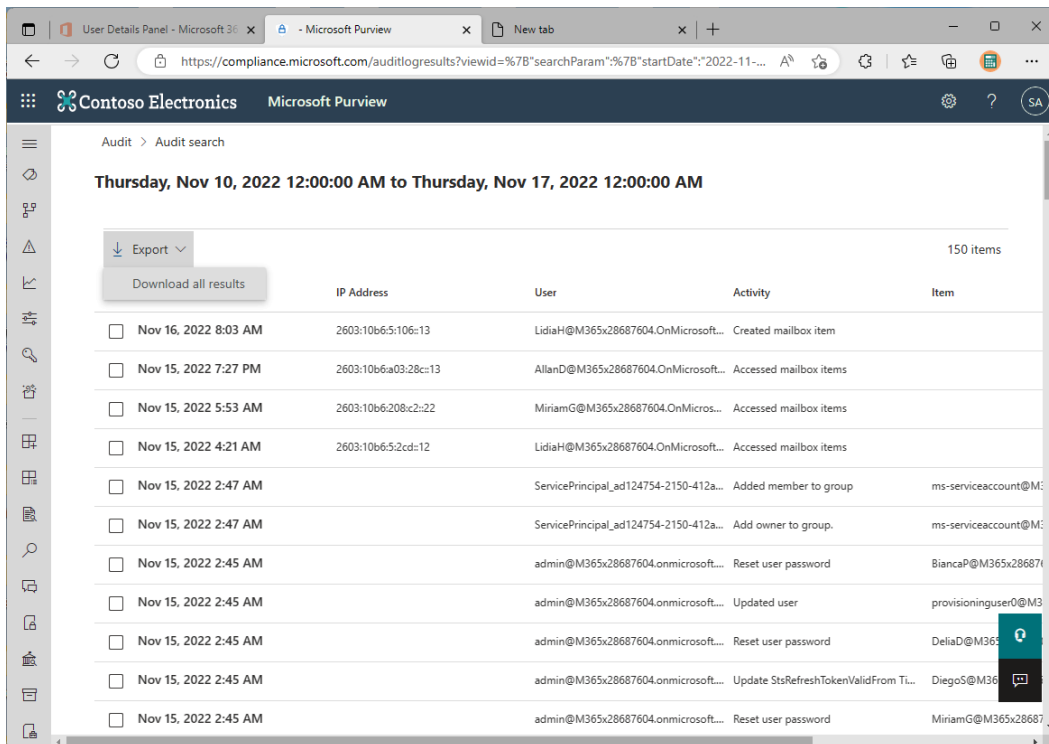


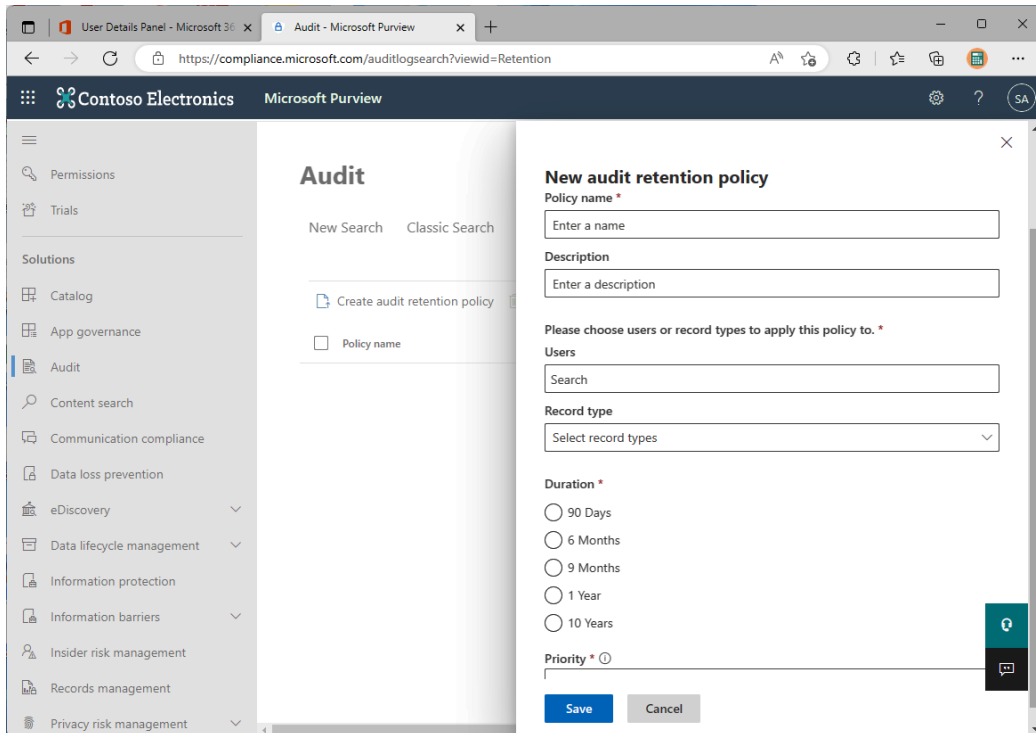
Figure 7.5 – Exporting audit search results to a CSV file

A report will be made available to the administrator in **Comma-Separated Values (CSV)** format. Next, you will review the features of audit retention policies.

Audit Retention Policies

As mentioned in the previous section, audit logs have a default retention period: users with E3 licenses are enabled for 90-day retention, and users with E5 licenses are enabled for up to a year's retention.

With the **Microsoft Purview compliance center**, you can create retention policies to govern how long the audit data will be preserved. In addition to the default policy terms, you can purchase and apply Microsoft 365 Advanced Compliance licenses for 10 years of additional audit log retention. Audit retention policies are scoped to users and record types, as shown in *Figure 7.6*:



The screenshot shows the Microsoft Purview interface for creating a new audit retention policy. The browser address bar shows the URL: <https://compliance.microsoft.com/auditlogsearch?viewid=Retention>. The left sidebar lists various solutions, with 'Audit' selected. The main content area is titled 'Audit' and includes options for 'New Search' and 'Classic Search'. Below this, there is a 'Create audit retention policy' button and a 'Policy name' input field. The right-hand panel is titled 'New audit retention policy' and contains the following fields:

- Policy name ***: A text input field with the placeholder 'Enter a name'.
- Description**: A text input field with the placeholder 'Enter a description'.
- Please choose users or record types to apply this policy to. ***: A section with two sub-sections:
 - Users**: A text input field with the placeholder 'Search'.
 - Record type**: A dropdown menu with the placeholder 'Select record types'.
- Duration ***: A group of radio buttons with the following options: 90 Days, 6 Months, 9 Months, 1 Year, and 10 Years.
- Priority ***: A dropdown menu with a help icon.

At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 7.6 – Audit retention policy

A tenant can have up to 50 audit retention policies.

Alerts

As an administrator, a common scenario for you is to alert an operations team whenever a specific activity occurs. The following are examples:

- Notifying a user who shared a document externally
- Blocking unauthorized administrators
- Blocking a potentially compromised account that is performing a suspicious activity

To do that, you can leverage **activity alerts**, which allow you to create rules based on conditions. Sample conditions might be files being shared externally, a DLP policy match, modifying the permissions of a SharePoint site, and so on.

Whenever a user does anything that meets an alert's conditions, an email will be sent to the recipient configured in the alert, notifying them about the flagged activity. *Figure 7.7* shows an example of a notification email:

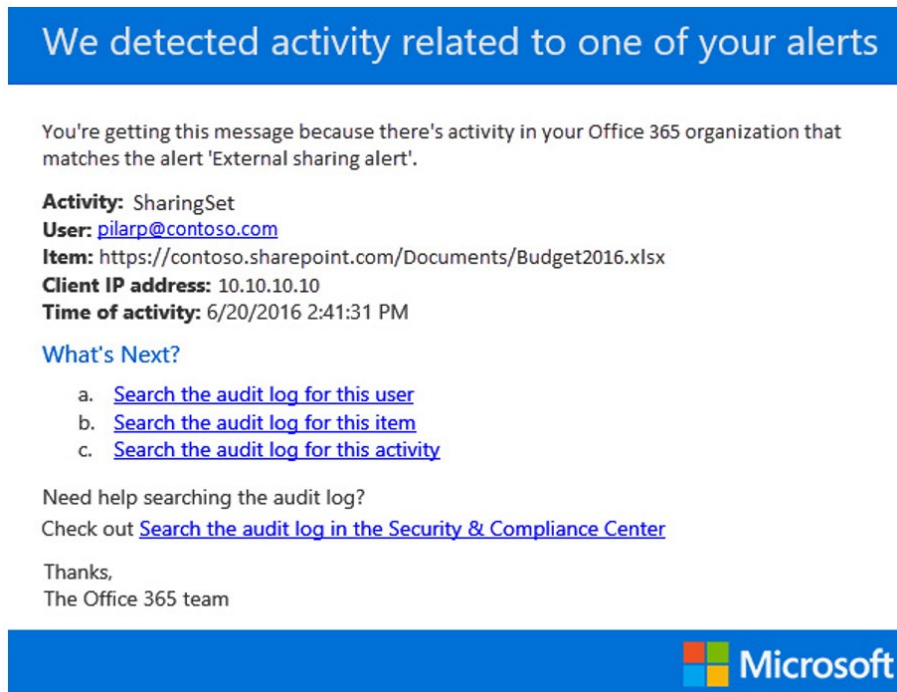


Figure 7.7 – An activity alert email triggered from a user-specific action

From here, you can open the audit log search in the Microsoft Purview compliance center to review and investigate the user activities. Administrators can automate activities that will be executed whenever a set of actions occur. To accomplish this, they can leverage **Microsoft Defender for Cloud Apps (MDA)**, formerly known as **Microsoft Cloud App Security**. MDA allows administrators to create policies to perform the following actions:

- Suspend a user
- Require a user to sign in again
- Notify a user

Note

MDA policies, including activity, file, and anomaly detection, are out of the scope of this exam. You can learn more about MDA here: <https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps>.

For example, say a user triggers a specific activity alert that warrants that the user be suspended. Instead of you (the administrator) being notified of an anomaly via email, launching a portal, navigating to the alert logs, and then performing the suspension manually, MDA can execute a workflow to automatically take the required action.

Alerts that were triggered are reviewed in the MDA portal (<https://portal.cloudappsecurity.com>) so that you, as an administrator, can act where appropriate (see *Figure 7.8*):

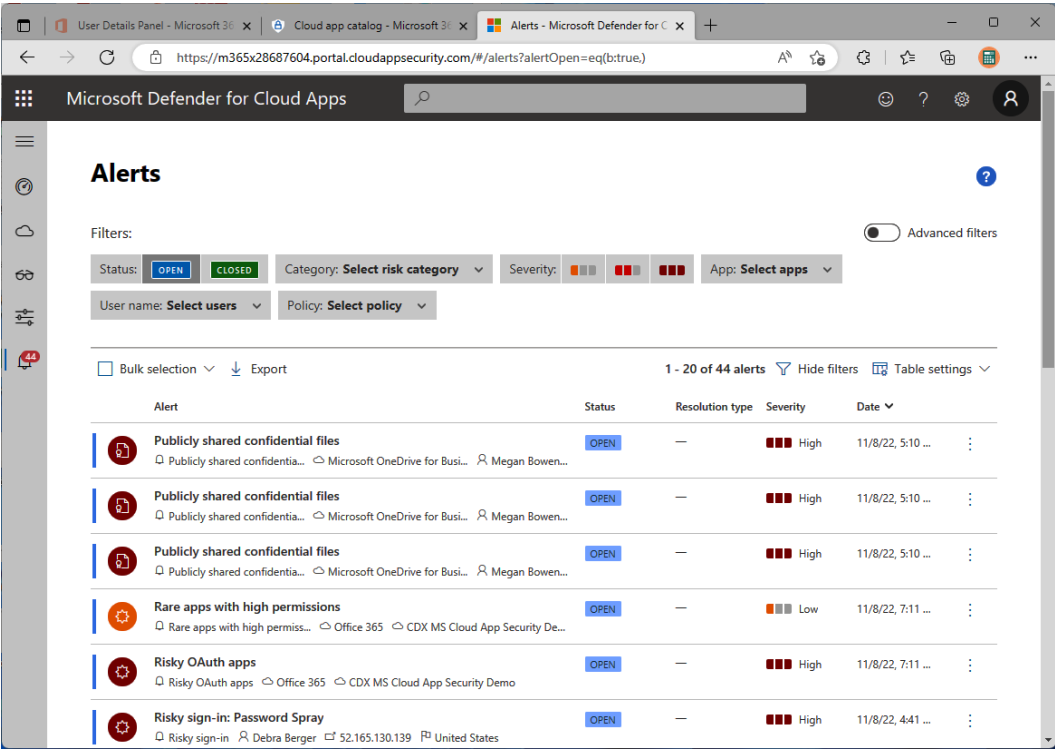


Figure 7.8 – MDA alerts

There are multiple ways to filter the results, such as by resolution status, category, and severity. Administrators can also export the results to a CSV.

Credential Management

Credentials confirm a user's identity during the sign-in process. Besides a password, AAD supports different types of authentication challenges, such as MFA with certificates, security keys, and one-time passcodes. AAD already includes a password policy that is adjusted to fit a company's requirements. Using Azure AD Connect to configure hybrid identity, administrators can synchronize password requirements from an on-premises AD as well. An organization may also be interested in a **Self-Service Password Reset (SSPR)** for its end users.

From a zero-trust perspective, you want to ensure that credentials are being used appropriately. Credentials shouldn't be stored in text files or embedded in applications.

Password Policy

A password policy can define a password's minimum length, when and if the password expires, and the password strength. The password expiration policy, located in the Microsoft 365 admin center under **Settings | Org settings | Security & privacy**, as shown in *Figure 7.9*, determines the **days before passwords expire** and **days before a user is notified about expiration settings**:

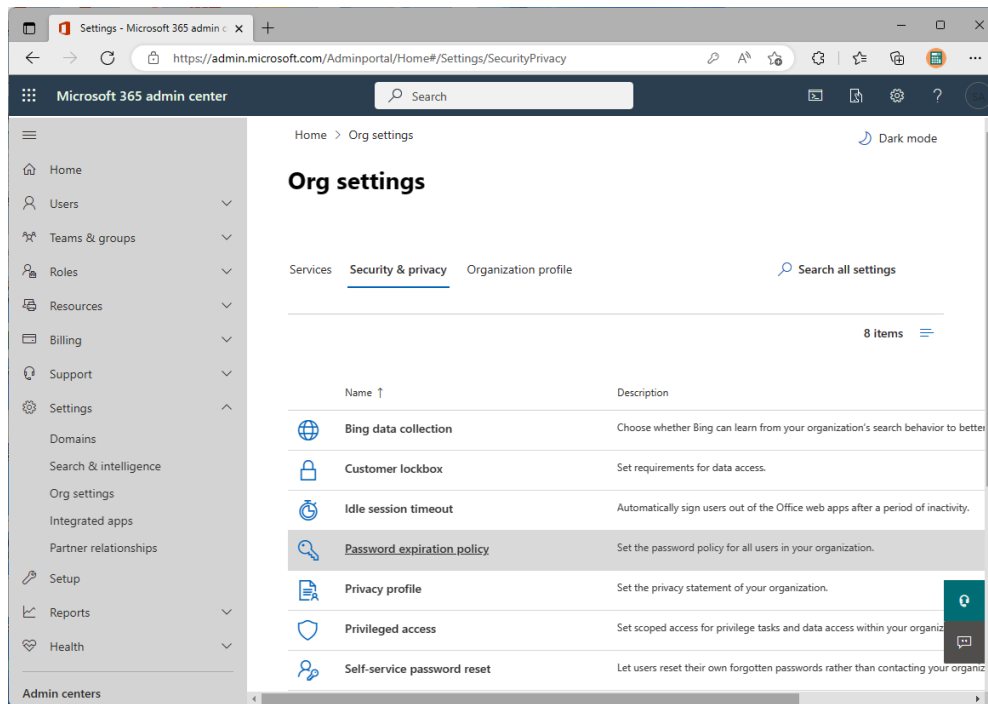


Figure 7.9 – Password expiration policy

The number of days before a password expires can range from 14 to 730, and the number of days before a user is notified can range from 1 to 30.

When an organization decides to sync user passwords from an on-premises AD to AAD using **AAD Connect**, the following existing on-premises password policies will govern the cloud requirements:

- Length
- History
- Expiration time
- Complexity

Setting a simple password policy can help reduce user confusion and helpdesk support tickets within an organization.

Self-Service Password Reset

Another common request from organizations regarding credential management is to allow users to reset their passwords without needing to open a support ticket. AAD provides a feature called SSPR that allows users to confirm their identities and reset their passwords.

The AAD SSPR confirmation is validated based on a combination of the following methods:

- Mobile phone
- Office phone
- Security questions
- Email

In addition, if configured, passwords that have been reset in AAD can be written back to a local AD using AAD Connect. You can check the status of SSPR in the Azure portal by performing the following steps:

1. Open `https://portal.azure.com`.
2. Click on **Azure Active Directory**.
3. Choose **Password reset**. The **Password reset** page is displayed, as shown in *Figure 7.10*:

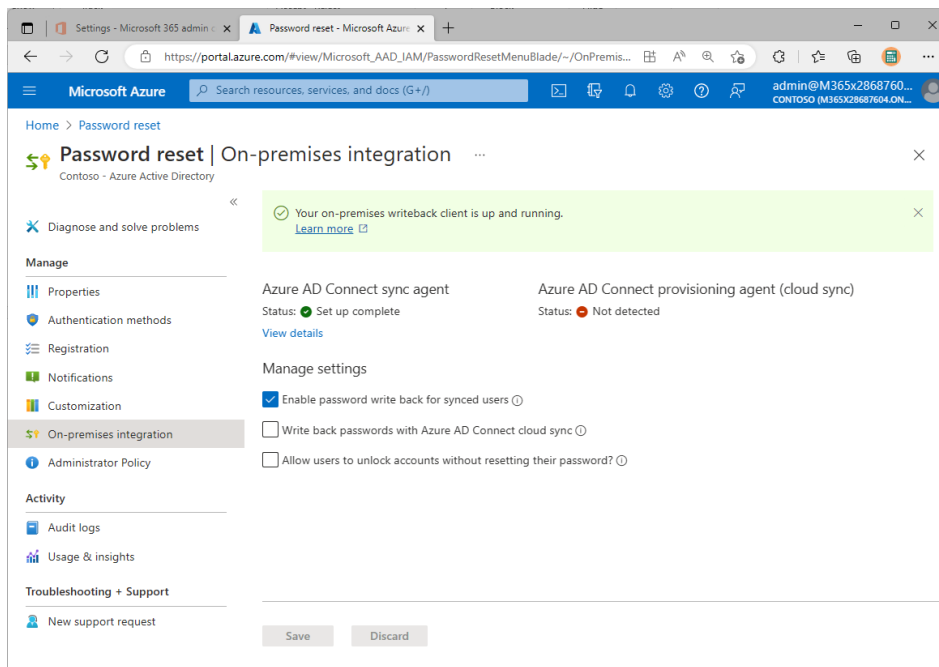


Figure 7.10 – Azure SSPR

Note

You can read more on Azure password management and policies at <https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations>.

Password writeback, configured through AAD Connect, is recommended to ensure users maintain the same password on-premises that they do in AAD.

Next, you will explore zero-trust security and compliance concepts for endpoints within an organization.

Endpoints

Endpoints play an important role throughout the entire Microsoft 365 security conversation. Microsoft 365 allows services to be accessed from a myriad of clients and device types, such as web, desktop, and mobile devices. As an administrator, you should plan which devices users will be allowed to access Microsoft 365 services from, whether devices will be managed, and which protection controls, such as Windows 10 security features, are configured on those devices.

From a zero-trust perspective, it's important to verify that the devices accessing data are allowed and accessing it under the correct circumstances.

You will explore the following concepts for devices:

- Device access
- Device management
- Device protection

Device Access

Managing **device access** for Microsoft 365 is the key to ensuring that only known devices can access the service or store company data. Two main strategies are used to control device access for Microsoft 365:

- **Network restriction:** Microsoft 365 services can only be accessed from authorized network locations. For example, managed devices reside inside the organization's perimeter. This scenario is enforced in the service during the authentication and authorization phase, where users identify themselves and their locations before being granted access to services.
- **Conditional Access:** Services can only be accessed when conditions, such as group membership, device compliance, network region, or MFA, are satisfied.

A network restriction can be implemented with one or more of the following four features:

- **Conditional Access:** As mentioned previously, Conditional Access interrogates devices accessing the service for their IP address information and then grants or denies access based on that (among other conditions). Microsoft recommends configuring Conditional Access as the best way to manage device and application access.
- **AD Federation Services (AD FS) claims rules:** In an identity federation scenario, **claims** are information about users that is exchanged between different **Identity Providers (IdPs)**, such as between a local AD and AAD. In this case, claims rules allow administrators to configure conditions that must be satisfied to enable authorization. Organizations frequently use AD FS claims rules to limit access to services based on IP addresses.

AD FS claims rules for Microsoft 365 services do not work effectively for geofencing purposes. In most Microsoft 365 application scenarios, users attempting to access the Microsoft 365 service from their device are redirected to the on-premises environment. The result is that the client IP address presented to AD FS is from the Microsoft 365 service and not the originating client device.

- **Exchange Online client access rules:** Administrators can configure conditions to authorize access to EXO services. Among the services that administrators can configure EXO client access rules for are the **Exchange Admin Center (EAC)**, PowerShell, Exchange ActiveSync, and **Exchange Web Services (EWS)**.
- **OneDrive for Business (ODFB) and SharePoint Online device access:** Administrators can configure the network users who are authorized to access OneDrive and SharePoint content. This setting also applies to external users and administrator access, so it is recommended to think things through before the settings are rolled out for users. It affects all services that use SharePoint (such as OneDrive, SPO, and Microsoft Teams). Misconfiguring the allowed networks will prevent users from accessing the service. This issue will require a phone call to Microsoft Support.

Figure 7.11 shows the device access control configuration options in the SharePoint admin center:

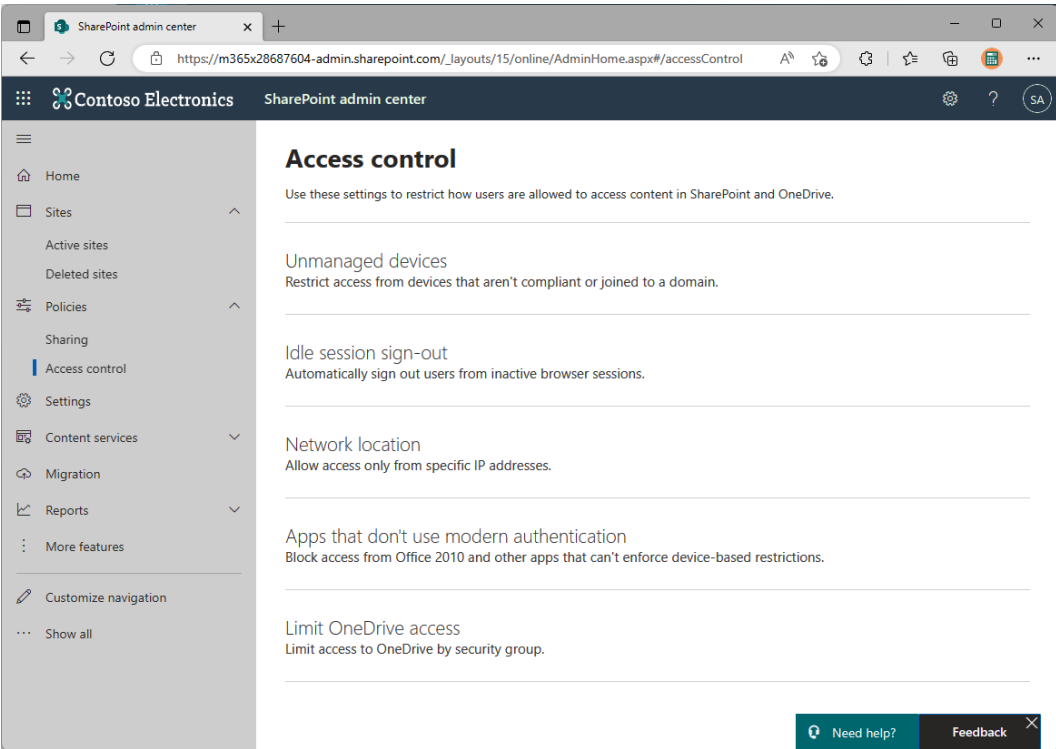


Figure 7.11 – Device access controls in the SharePoint admin center

Conditional Access provides the most granular control for defining conditions, restrictions, and other actions. The most flexible (and preferred) approach for controlling authorized locations is to create Conditional Access policies. Figure 7.12 shows the high-level components and an operational overview of a Conditional Access policy:

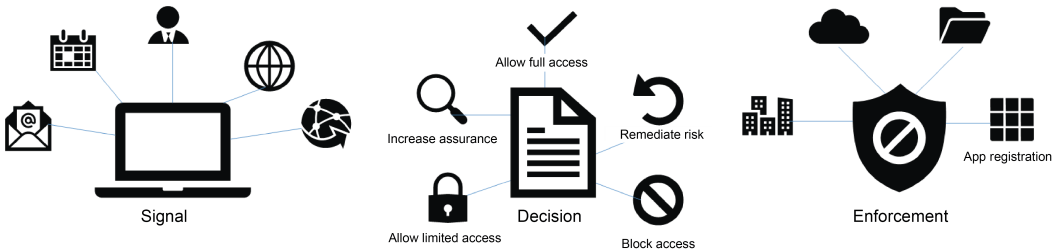


Figure 7.12 – Conditional Access overview

The core conditions for building a Conditional Access policy are set out as follows:

- Users and groups
- Sign-in risk
- Device platform
- Location
- Client apps
- Device state

Following validation, administrators can configure actions such as the following:

- Blocking access
- Granting access, but requiring MFA
- Granting access, but requiring a device to be compliant with Intune requirements
- Enforcing limited session usage, such as preventing users from opening SharePoint documents locally

As part of testing a Conditional Access policy, administrators can simulate a set of conditions, such as user and location, to understand which policy should be set up and what would happen as a result of this policy being implemented.

In the next section, you'll look into device management.

Device Management

Microsoft 365 allows administrators to manage devices that are used to connect to services. Administrators can enforce features and stipulations, such as requiring a password to unlock a device, ensuring that the device is not rooted or jailbroken, and selectively wiping company data from the device. The following two services are used to manage devices:

- **Intune:** Intune offers the ability to manage device certificates, Wi-Fi, **Virtual Private Networks (VPNs)**, and email profiles, deploy apps to users, manage app protection as well as device compliance, prevent jailbroken/rooted devices from accessing corporate resources, define password policies, and disable cameras. Intune is managed through the **Microsoft Endpoint Manager (MEM)** admin center (<https://endpoint.microsoft.com>).
- **Mobile Device Management (MDM) for Office 365:** MDM for Office 365 provides a subset of Intune features, such as preventing the connection of jailbroken or rooted devices, disabling cameras, and defining a password policy.

Table 7.1 lists the main differences between MDM for Office and Intune capabilities:

Feature	Intune	MDM for Office 365
Where devices are managed	In the Intune management portal	In the security and compliance center
Supported devices	iOS, macOS, Android, and Windows devices	iOS, Android, and Windows devices
Main capabilities	<ul style="list-style-type: none">• Requiring a password• Defining a number of sign-in failures before the device is wiped, password expiration, jailbreak or rooted detection, and corporate wipe• Pushing certificates to devices for Wi-Fi networks or VPNs• Viewing reports on compliant devices• Pushing applications to devices	<ul style="list-style-type: none">• Requiring a password• Defining a number of sign-in failures before the device is wiped, password expiration, jailbreak or rooted detection, and corporate wipe

Table 7.1 – Device management

In addition to MDM scenarios, Intune provides **Mobile Application Management (MAM)** capabilities, allowing controls to be applied to specific applications, such as the following:

- Requiring a **Personal Identification Number (PIN)** to open the app
- Encrypting corporate app data
- Data wipe (full device or selective data wipe)
- Blocking copy and paste between corporate and personal applications

Organizations that already have an MDM solution to manage corporate devices can still use Intune to manage applications with MAM.

Note

You can find more information on MAM at <https://docs.microsoft.com/en-us/intune/apps/app-protection-policy>.

Device Protection

Windows 10 and Windows 11 devices include several security features that administrators should consider during their device planning phase. In order to secure devices, you'll want to evaluate both built-in technologies as well as components from the full Microsoft Defender suite.

To fully protect devices, consider the following components:

- **Microsoft Defender antivirus:** Formerly known as Windows Defender Antivirus, Microsoft Defender antivirus anti-malware can protect Windows 10 and Windows Server computers.
- **Microsoft Defender for Identity:** Formerly known as Microsoft Azure Advanced Threat Protection, **Microsoft Defender for Identity (MDI)** protects against threats leveraging behavioral sensors, security analytics across different Microsoft services, and **Threat Intelligence (TI)** by Microsoft hunters and security teams.
- **Microsoft Defender Application Guard:** Formerly known as Windows Defender Application Guard, Microsoft Defender Application Guard isolates untrusted sites that are opened in an isolated Hyper-V-enabled container, separate from the host operating system.
- **Windows Hello for Business:** This component replaces passwords with strong **Two-Factor Authentication (2FA)** on PCs and mobile devices using a device-specific PIN or biometric credentials that can't be captured or replayed on other devices.
- **Credential Guard:** This component is responsible for isolating secrets that are used throughout the machine to prevent unauthorized access.
- **Windows Defender Application Control:** This component allows only authorized applications to run on users' machines.
- **BitLocker:** This is a whole-disk encryption, integrated with a device's trusted computing module or Trusted Platform Module chip and the Windows 10 operating system.
- **Windows Information Protection (WIP):** Previously known as **Enterprise Data Protection (EDP)**, WIP protects against data leakage separating personal and corporate data.
- **Microsoft Defender for Endpoint (MDE):** In addition to advanced antivirus capabilities, MDE can also apply corporate restrictions such as locking down USB devices and providing URL filtering. MDE can also protect Windows 7, Windows 8.1, Windows Server, and macOS.

Note

You can find more information on MDE at <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint>. You can read about the Windows security features at <https://learn.microsoft.com/en-us/windows/security/>.

You should plan on implementing some level of endpoint device protection and compliance checks as part of a zero-trust policy.

Apps

Applications provide both a method for individuals to accomplish tasks as well as an avenue for attackers. A zero-trust deployment model for applications includes the following:

- **Application visibility:** Gaining visibility into how applications are used in your environment is critical to understanding how your users are conforming to your governance policies. Modern application platforms provide APIs that determine how users interact with the applications. MDA interrogates a wide range of application platforms and extracts usage data. MDA can also be used to audit applications for general compliance with your organization's policies and risk tolerance.
- **Managing shadow IT:** Discovering shadow IT in your organization is the first step toward guiding your users toward supported solutions. Shadow IT presents multiple avenues for compromise. For example, users not only bypass your governance policies but they may even raise additional risks by downloading applications that have malware or allow data to be intercepted by third parties.
- **Managing application access policies:** You can use Microsoft Defender for Cloud Apps to determine whether applications are performing risky behaviors (such as downloading or uploading data abnormally) and then apply security policies such as suspending accounts, quarantining files, or applying sensitivity labels for encryption.

Using a cloud access security broker such as Microsoft Defender for Applications can help mitigate risks presented by both managed and unmanaged applications in your organization.

Data

Content authoring, storage, and sharing are the key components of every organization's collaboration strategy. Data is typically viewed as the organization's most important managed asset. When applying the principles of zero trust, it's important to understand how the data is being created, stored, accessed, protected, and transmitted throughout the environment and then enact appropriate controls so that behavior complies with the organizational policy.

Here, administrators need to implement policies to determine the following:

- Where will users be able to store files?
- How and where will users be able to access files?
- How can the files be shared inside and, if enabled, outside the organization?
- How long will documents be retained for?
- How can auditors find out who accessed or deleted a document or find documents that contain specific information?
- How can documents be classified and protected?

You will now explore the following data concepts in depth:

- Document storage
- Sharing
- Auditing
- Retention
- eDiscovery
- Classification and protection

Document Storage

Although documents can be accessed from almost all the services of the suite, Microsoft 365 has three primary interfaces (listed next) where users can store, share, and collaborate on files:

- **ODFB:** Personal documents
- **SPO sites:** Team, group, or department documents
- **Teams:** Team, group, or department documents

The underlying storage component for all these interfaces is SPO. Documents stored in SPO (or any service that leverages SharePoint) are automatically indexed, support custom metadata, have versioning enabled, and can be synchronized between desktop and mobile devices. All locations are automatically covered under the organization's security and compliance requirements.

Table 7.2 depicts the main differences between ODFB, SPO, and Teams for document storage:

Feature	ODFB	SPO or Teams
Storage space	Per user and varies according to the plan, ranging from 2 Gigabytes (GB) to unlimited storage. An administrator can increase the limit up to 5 Terabytes (TB) of storage, but beyond that would require a service ticket up to 25 TB. Beyond 25 TB would require more storage.	Per tenant. Every user license will add to the tenant pooled storage, and administrators will be able to decide if sites will have a manually set amount of storage or if the site storage will be consumed automatically out of the tenant pooled storage.
Ownership	Per user. Each user is accountable for managing what to do with the files in their personal storage.	Per group or user. It is a good practice to assign SharePoint site permissions to a security group or Microsoft 365 Group, rather than individual users, but it is up to each user with the appropriate permissions to decide how to manage the storage space.
Teams integration	Yes. Users can access their personal storage inside the Files left-rail icon in Microsoft Teams. In addition, inside individual or group chat conversations, files that have been shared are automatically uploaded to the OneDrive site of the user sharing the file.	Yes. Each Team automatically has a SharePoint site, which is where the Team's channel files are stored and can be accessed or edited by users.
Sync client	Yes. Users can synchronize and access a local copy of their personal ODFB with the sync client.	Yes. Users can decide which SPO libraries they will choose to synchronize locally, and they can have more than one library synced at the same time. Users can also decide which folders of these libraries will be synced.
Mobile client	Yes (ODFB mobile app)	Yes (SharePoint, and Teams mobile apps)

Feature	ODFB	SPO or Teams
File storage limit (at the time of writing)	250 GB	250 GB
Sharing	Managed by the user, who is the owner of the personal storage. Global sharing controls can be configured by administrators to prevent external sharing.	Managed by the SharePoint site, which includes its members, owners, and visitors. If a site is connected to a Microsoft Teams team, user permissions to access files are managed inside Teams itself. In addition, users with appropriate permissions can also choose to share individual files or folders, without sharing the entire site. Global sharing controls can be configured by administrators to prevent external sharing.
Audit logs	Yes. Auditors can review sharing and file activities on OneDrive.	Yes. Auditors can review sharing and file activities on SPO sites.

Table 7.2 – Storage locations, features, and capabilities of ODFB, SPO, and Teams

Sharing

Among the benefits of storing documents in OneDrive, SharePoint, or Teams is the ability to share files without needing to send a copy to each recipient. Efficient file sharing is also important because it allows organizations to manage access to content. Documents sent as email attachments may be outside the management or oversight of security, compliance, or business administrators. When shared inside the framework of ODFB, SharePoint, or Teams, files are kept in place and are configured so that users cannot send them to another party.

Sharing End User Controls

Sharing can be done by almost all clients. Supported clients include the following:

- Mobile app
- Web client
- Desktop sync client
- Outlook client
- Teams web, desktop, and mobile app

Outlook sharing is particularly interesting because it allows users to attach files to email messages as **cloud attachments**, thus automatically sharing those files out of their OneDrive personal storage. End users can even configure the permissions the recipients can have for these files, as shown in *Figure 7.13*:

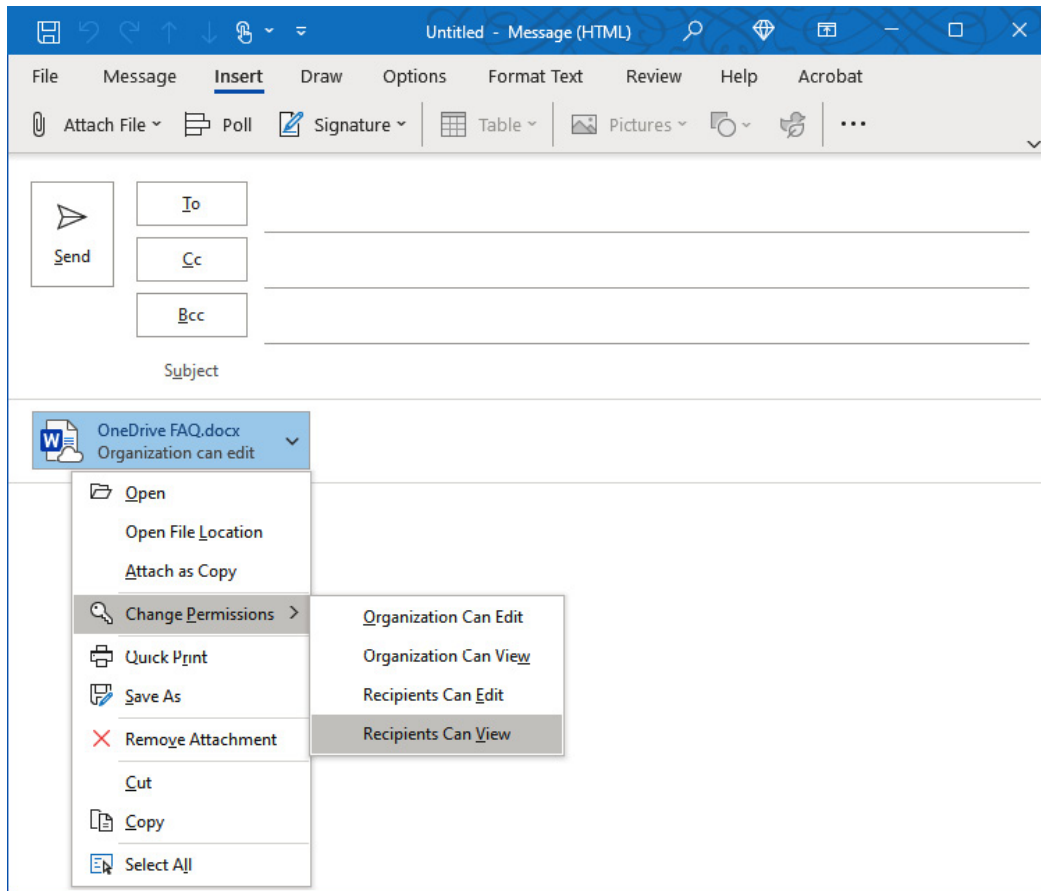


Figure 7.13 – Managing attachment permissions in Outlook

In addition, owners or users with the appropriate permissions can review and even revoke permissions that have been assigned to others at any time through the SharePoint or OneDrive user interface by performing the following steps:

4. Select the file.
5. Click on **Details**.
6. Choose **Manage access**. An example of managing permissions is shown in *Figure 7.14*:

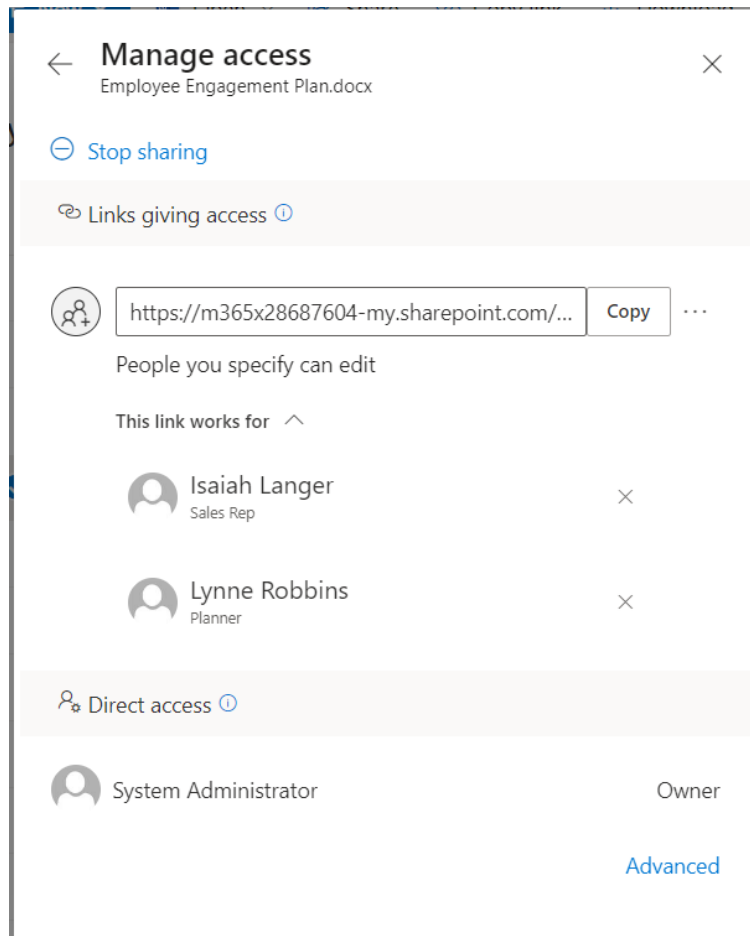


Figure 7.14 – OneDrive permissions management

If you click **Stop sharing**, the link to the document becomes invalid to external users. External users, as discussed previously, are users that are outside the boundary of the tenant.

Sharing Admin Controls

As an administrator, you can govern how sharing will be configured for the organization under the following categories:

- **Anyone:** Users can create links to files that can be shared with others without requiring any type of authentication.
- **New and existing external users:** Users can invite existing or external users who aren't enrolled in their organization directory.

- **Existing external users:** Users can only invite external users who have already accepted an invitation.
- **Only users in your organization:** Users can invite internal users only. This means files can't be shared with external users.

OneDrive, SharePoint site administrators, and Teams owners can invite internal and external users (if the overall tenant settings are configured to allow it). However, if needed, organizations can leverage a *Guest inviter* role, granting non-administrators the ability to invite guests.

Note

Organizations can also restrict which domains users can share with. By defining allow or block lists, administrators can allow or prohibit sharing with specific domains.

While many settings can be configured globally, exceptions can still be made for groups of individuals. Sharing controls can be modified to give different levels of permissiveness between SharePoint (which also governs Teams) and OneDrive, though the OneDrive setting may never be more permissive than the overall SharePoint setting.

Sharing controls are managed in the SharePoint admin center under **Policies > Sharing**, as shown in Figure 7.15:

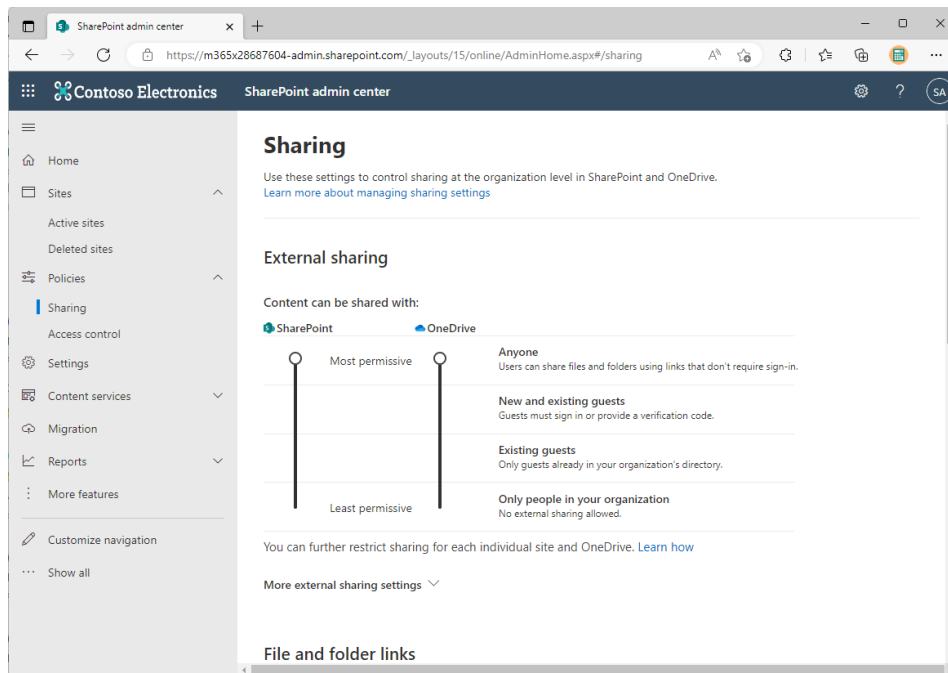


Figure 7.15 – SharePoint and OneDrive sharing different levels of controls

Several best practices can be utilized to protect an organization while allowing guests to collaborate with it. Among them are the following:

- Defining group and team classifications (such as *Internal Only*, *Confidential*, and so on) and limiting which groups are eligible for guest access
- Defining authentication requirements for guests, such as MFA
- Forcing guests to accept terms of use
- Frequently reviewing guest access to ensure that only allowed users are guests (such as with **access reviews**)
- Defining client access requirements for guests
- Frequently reviewing activities in the audit log search

Security, compliance, and governance conversations should include a proposed strategy for guest access.

Note

You can gather more information on configuring guest access for Microsoft Teams at <https://learn.microsoft.com/en-us/microsoftteams/guest-access>.

Auditing

Auditing determines which actions were executed by which identity, and the time those actions were performed. As described earlier, Microsoft 365 allows administrators to audit actions that are performed in the service regarding file sharing and collaboration, syncing, deletion, and access. A comprehensive zero-trust policy will ensure that auditing data is captured for security analysis purposes.

The main auditing activities for files are as follows:

- Accessed file
- Copied file
- Deleted file
- Deleted file from the recycle bin
- Deleted file from the second stage recycle bin
- Downloaded file
- Moved file
- Uploaded file

In addition, sharing is also part of the audited log activities. The main sharing audited activities are listed as follows:

- Created access request
- Created a company-shareable link
- Created a sharing invitation
- Shared a file, folder, or site
- Used a company-shareable link
- Withdrew sharing invitation

A view of the audited sharing activities on the **Audit** screen inside the Microsoft Purview compliance center located at <https://compliance.microsoft.com/auditlogsearch> can be seen in Figure 7.16:

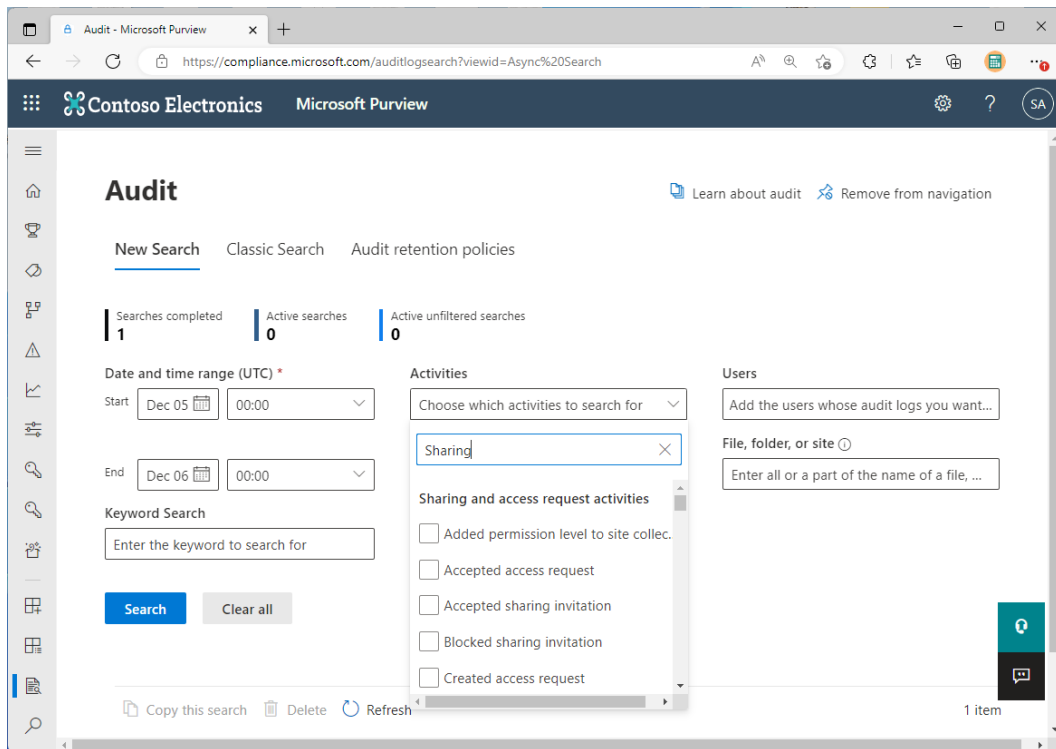


Figure 7.16 – Audit activities

As mentioned earlier, administrators should leverage audit logs, along with activity alerts and **Cloud App Security (CAS)** policies, to learn which actions are being taken by users and administrators regarding files and sharing inside their organization.

Classification and Protection

Microsoft 365 allows users and administrators to classify and protect documents (stored in OneDrive, SharePoint, or locally) as well as email messages, using the **Azure Information Protection (AIP)** service. AIP is part of Microsoft Purview Information Protection (formerly **Microsoft Information Protection (MIP)**).

From a zero-trust perspective, classification is important because it can be used to influence policy (both organizational policy and technology policy) to restrict access to data based on business needs.

Administrators can create classification labels and configure the actions available to users of the label. For example, a label can be configured to allow or deny the ability to take screenshots, copy content, or print it. Labels can be used to prevent users from modifying the recipients of a message or forwarding it to others. Once the labels have been configured and published, users can apply them to protect documents, files, and emails.

Administrators can also audit and control how classification and encryption technologies are used across the organization. Content is classified using the following methods:

- Outlook
- Office applications such as Word or Excel
- EXO transport rules, which modify specific message properties throughout its transport
- Security and compliance center DLP rules
- Windows Explorer using the AIP unified labeling client

After classification has been applied, the email message or document will display its tag, and users—if authorized to open the file—will be able to review which actions they are allowed to take on that information (*Figure 7.17*):

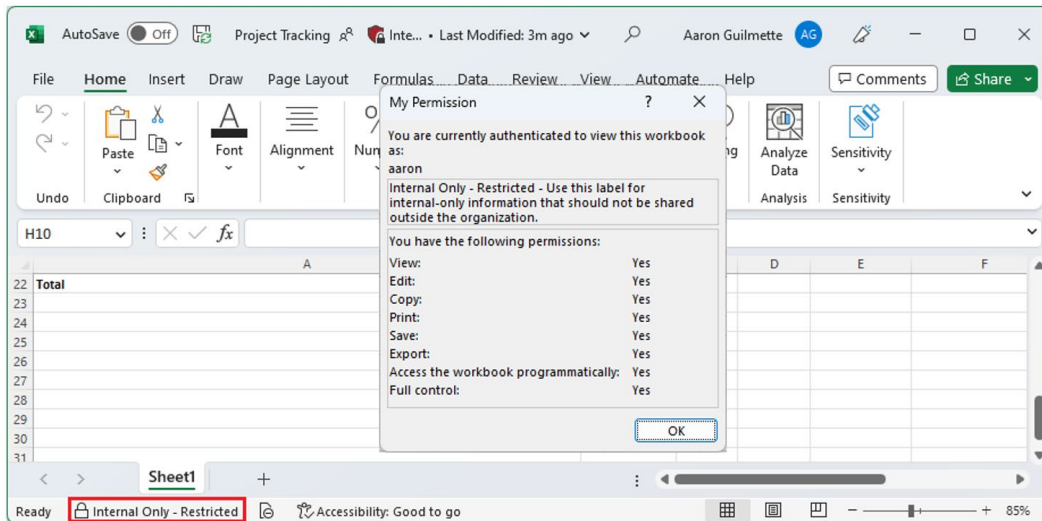


Figure 7.17 – Classification label

AIP is part of both Microsoft 365 E3 and Microsoft 365 E5. In Microsoft 365 E3, users must perform data classification manually. With Microsoft 365 E5, administrators can configure classification so that it happens automatically, such as when an application detects sensitive content such as credit cards or social security numbers.

Infrastructure

Applying zero trust principles to your infrastructure means that, as an administrator, you need to take a holistic view of everything that interacts with your organization's data, including servers, cloud infrastructure and platforms, and development environments.

You can use a tool such as **Microsoft Defender for Cloud**, which is a **Cloud Security Posture Management (CSPM)** and **Cloud Workload Protection Platform (CWPP)**, to evaluate your cloud workloads and platforms as well as look for anomalous patterns in potential unknown risks to ensure that your organization is protected from known and unknown security risks.

Further Reading

For more information on Microsoft Defender for Cloud, see <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>.

The next section will describe the security and compliance concepts for networking.

Network

Microsoft 365 services are generally accessed over the public internet. You will review the ways by which users will access the Microsoft 365 service, and how data will flow to and be stored in the service.

From a zero-trust perspective, it is important to identify all the points on your network that you can secure as well as identify the tools that are used to help protect identity, devices, and data as it moves from point to point.

When considering Microsoft 365 in terms of networking, administrators need to grasp the following concepts:

- Connectivity
- Encryption
- Performance

Connectivity

As a cloud service, Microsoft 365 components are not available on the internal network. From the perspective of a network administrator, you must allow internal users to access the internet endpoints for the Microsoft 365 service, which may mean configuring existing appliances such as firewalls and proxy devices.

Endpoints, such as **Internet Protocol (IP)** addresses or **Uniform Resource Locators (URLs)**, are classified into three categories:

- **Optimize:** This category is required for connectivity to services and represents over 75% of the consumed bandwidth.
- **Allow:** This category is required for connectivity, but not as sensitive to latency as **Optimize** endpoints.
- **Default:** These are endpoints that are treated as normal internet traffic.

Organizations should plan for network best practices when planning their Microsoft 365 deployment. Some of the recommended practices are as follows:

- Differentiating Microsoft 365 traffic from normal internet traffic
- Egressing network connections locally so that users will be routed as quickly as possible to the Microsoft network
- Bypassing proxies to reduce the amount of time needed for data to arrive at Office 365 services

Microsoft 365 administrators and network administrators should work together to plan a network connectivity strategy. To help plan effectively, Microsoft provides a web service for obtaining the IP addresses and URLs that are used in the service.

Note

You can find more information about the Office 365 IP address and URL web service at <https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-ip-web-service>.

Microsoft typically recommends bypassing proxy devices for network traffic destined for Microsoft 365.

Encryption

Encryption, a critical part of the zero-trust strategy, is a mechanism that protects information from unauthorized access. Data stored or transmitted in clear text can potentially be intercepted or modified by bad actors. Encryption can help protect against both unauthorized access and data alteration.

Microsoft 365 implements several encryption technologies across the platform. Encryption is enforced for data in two core states:

- **At rest:** In this state, data is stored in the service. This includes files and documents uploaded to OneDrive, SharePoint, and Teams, as well as email content. Data at rest is protected by BitLocker, **Distributed Key Manager (DKM)**, and Customer Key for Microsoft 365. Depending on the service, data may also be stored in blob storage, with each chunk being encrypted using the **key store**.
- **In transit:** This state refers to data that is transferred between clients and services, as well as between different endpoints within the service and data centers. Data in transit is protected via **Transport Layer Security (TLS)** and **IP Security (IPsec)**. TLS is typically used to secure application-layer traffic between clients and services, while IPsec secures the underlying physical or logical networking connections.

In addition to the built-in encryption technologies, customers can also apply unique content encryption to files and email messages using the AIP client. Not only does AIP provide data classification services (as described earlier), but it can also be used to encrypt content at the file or document level.

Organizations in highly regulated industries may be required to control the encryption keys that are used in the service. To accomplish this, organizations may use the **Customer Key** service, which allows them to manage the key life cycle and encrypt data in the following services:

- EXO, including Skype for Business Online and Microsoft Teams data stored in user mailboxes
- Files stored in OneDrive and SPO

Setting up the Customer Key service requires additional Azure services, such as **Key Vault**, and further considerations are out of the scope of this book.

Note

You can learn about Customer Key at <https://learn.microsoft.com/en-us/microsoft-365/compliance/customer-key-overview>.

Performance

Since Microsoft 365 is a cloud service, organizations should follow the best practices during the network planning phase. Customers should ensure that adequate network capacity and redundancy are available so that users have consistent and reliable connectivity to the service. Network performance planning should consider the following:

- How to make sure that the correct ports, IP addresses, and URLs are allowed for Microsoft 365 services
- How to reduce the latency between users and the Microsoft 365 network
- How to prepare the customer network so that it supports additional internet traffic
- How to plan Microsoft 365 features so that they use a local cache whenever possible

As described previously, Microsoft provides a list of URLs and IP addresses that are used by its services. Organizations should use this data to configure their networking and edge devices. Depending on the security requirements and configurations, the network team should be prepared to update edge device configurations in the event that Microsoft adds or removes endpoints and services.

To reduce the amount of latency, organizations should consider Microsoft 365 network best practices, such as bypassing proxies and local network egress (as opposed to backhauled connections to a central office), so that information arrives at the Microsoft 365 network through the shortest path.

To help measure the latency, organizations can use tools such as **PsPing** or **tracert** against Microsoft 365 service endpoints, such as the following:

- `outlook.office365.com`
- `<tenant>.sharepoint.com`
- `portal.microsoftonline.com`

There are also calculators and tools available to help measure latency, such as the Network Onboarding tool and the Network Assessment Tool, which help organizations determine where improvements are necessary (see *Figure 7.18*):

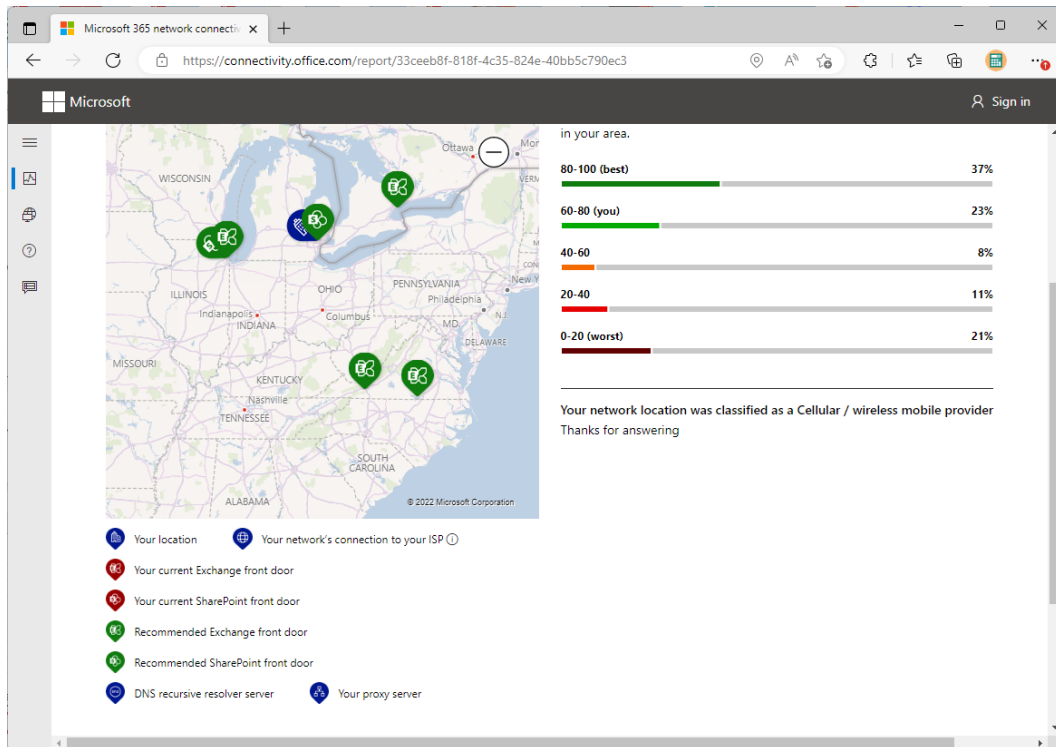


Figure 7.18 – Network Onboarding tool

Note

You can learn more about the Network Onboarding tool at <https://techcommunity.microsoft.com/t5/Office-365-Networking/Updated-Office-365-Network-Onboarding-Tool-POC-with-new-network/m-p/711130>.

Also, to prepare the network for additional Office 365 traffic, organizations that are currently deployed with on-premises systems should plan to accommodate the network traffic that is necessary to communicate with Microsoft 365 services. Another planning tool, known as **Network Planner for Microsoft Teams** (available in the Teams admin center at <https://admin.teams.microsoft.com>), estimates how much traffic the Teams workload will contribute to their overall internet bandwidth. *Figure 7.19* depicts the Network Planner for Microsoft Teams:

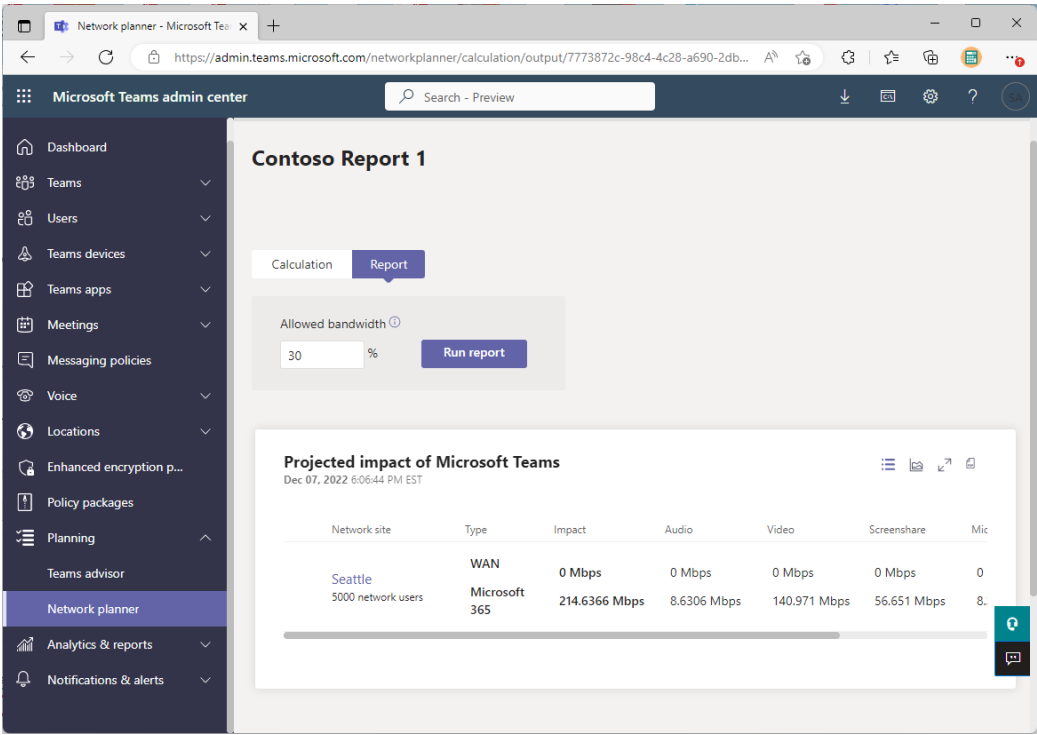


Figure 7.19 – Network Planner for Microsoft Teams to deduce the traffic in a Teams workload

Organizations that deploy services such as Microsoft Teams for phone systems, audio conferencing, and video or Microsoft Stream for video may also want to consider deploying **Quality of Service (QoS)**, which allows them to prioritize some types of network traffic over others to provide better real-time communication experiences.

Figure 7.20 shows an example of an organization using QoS to shape its traffic:

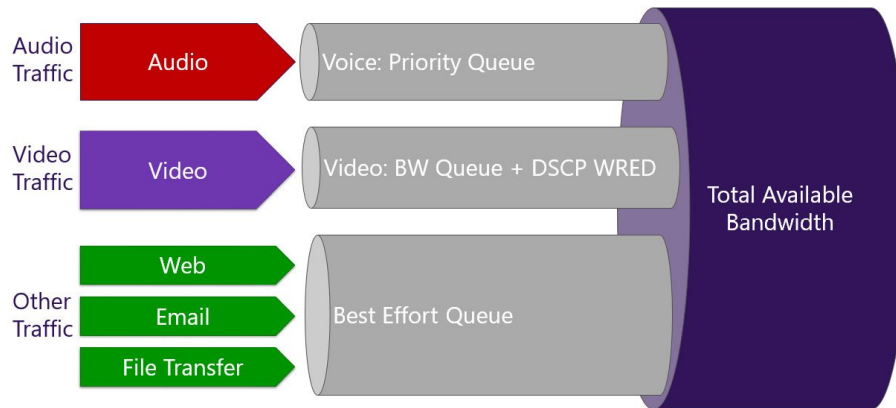


Figure 7.20 – QoS example

In addition to network traffic, companies should be aware of the features available in the service's applications and clients that can help reduce the amount of internet traffic needed. Some of these features are listed as follows:

- **Outlook cache:** This stores a local copy of the user's email data that can be used offline.
- **OneDrive sync client:** This can keep a local copy of both a user's personal OneDrive storage and their selected SPO libraries.
- **Microsoft 365 apps binaries and servicing updates:** As discussed in *Chapter 5, Describe Endpoint Modernization, Management Concepts, and Deployment Options in Microsoft 365*, there are a number of ways to cache local content for installation update distribution.

Network planning is an ongoing task that requires, among other things, the engagement and commitment of both the networking and Microsoft 365 administrative teams to ensure the optimal **User Experience (UX)**.

Finally, you will cover security and compliance concepts for devices.

Describe Microsoft Granular Delegated Admin Privileges (GDAP) Principles

Zero trust principles such as least privilege don't just apply to your organization. In the context of service providers, it's important to make sure that they are also following secure administration practices.

This is where **Granular Delegated Admin Privileges (GDAP)** comes into play.

GDAP's capabilities empower partners to exercise precise control over access to their clients' workloads, thereby enhancing security measures and addressing potential concerns. This not only enables partners to offer a broader range of services to clients uncomfortable with granting global administrator access but also helps organizations with regulatory requirements necessitating a least-privileged approach be compliant.

GDAP serves as an integral security feature aligned with the zero-trust cybersecurity framework. It empowers partners to configure highly specific and time-bound access to their clients' workloads, whether in production or sandbox environments. Crucially, this least-privileged access must be explicitly granted by clients to their respective partners.

GDAP facilitates the seamless segregation of partners' access on a per-customer basis. In this arrangement, partners no longer possess default access to all client tenants across Azure subscriptions via admin agents. Instead, partners managing Azure operations are integrated into a distinct security group. This group, in turn, is a member of the Admin agent group and provides owner-level RBAC across all Azure subscriptions associated with that specific customer.

As the roles are granted and managed by the customer, they can also be revoked or terminated at the customer's discretion—further helping secure the customer organization against threats posed by **standing** (permanently granted) high-level access.

Summary

Microsoft 365 was built with security features in mind. Administrators should take some time to review the wide range of features and controls that are available to them for delegating and administering the security aspects of tenants.

In this chapter, you learned about the overall principles of zero-trust security and its concepts and controls, including managing identity, endpoints, apps, data, infrastructure, and networking. In addition, you grasped ways to manage access to resources through credentials, network perimeter controls, and Conditional Access, as well as using encryption as a layer to protect against unauthorized access or data modification.

In the next chapter, you will cover identity protection and management.