MICROSOFT 365 CERTIFICATION

MS-102

Microsoft 365 Administrator Expert

The Complete Study & Reference Guide

From Tenant Setup to Zero Trust Security

Identity • Devices • Exchange • Teams • SharePoint • Compliance • Automation

200+ Pages • Hands-On Labs • PowerShell • Real-World Scenarios

Audience: System Administrators · Cloud Engineers · IT Support · Working Professionals

Purpose: First-Attempt Pass · Job Interview Preparation · Production Administration

Includes: Step-by-step labs · GUI navigation · PowerShell · Exam tips · 30-day study plan

How to Use This Guide

Welcome to the most comprehensive MS-102 Microsoft 365 Administrator study and reference guide ever assembled into a single document. This guide was built to serve three audiences simultaneously: **certification candidates** preparing for the MS-102 exam, **working administrators** who need a practical reference, and **job seekers** preparing for interviews in Microsoft 365 roles.

What's Inside

This guide covers **every objective domain** in the official MS-102 blueprint, organized into 10 logical sections. Each section is built using the same repeatable structure so you always know where to find what you need:

- **Introduction & Why This Matters** — beginner-friendly conceptual framing
- **Key Concepts & Architecture** — deep technical explanation
- **Portal Navigation Paths** — exact GUI clicks
- **Step-by-Step Configuration** — copy-and-paste-ready procedures
- **PowerShell Commands** — automation and scripting
- **Real-World Scenarios** — how enterprises actually deploy this
- **Best Practices & Security Considerations** — production-grade recommendations
- **Common Errors and Troubleshooting** — the things that go wrong
- **Interview Questions and Answers** — what hiring managers ask
- **Exam-Focused Notes** — what Microsoft specifically tests
- **Hands-On Labs** — practice exercises with a free trial tenant
- **Summary & Quick Recap** — for last-minute revision

How to Study

RECOMMENDED APPROACH

The MS-102 is a broad exam covering identity, devices, productivity, security, and compliance. The best preparation combines reading, lab work, and practice questions.

1. **First pass (read-through):** read each section end-to-end without trying to memorize.
2. **Second pass (hands-on):** sign up for a free Microsoft 365 developer tenant at `developer.microsoft.com/microsoft-365/dev-program` and perform every lab.
3. **Third pass (deep dive):** focus on weak areas — security, Intune, and compliance are heavily tested.
4. **Fourth pass (rapid revision):** use the cheat sheets and last-minute revision notes at the end.

Exam Snapshot

Detail	Value
Exam Code	MS-102
Certification	Microsoft 365 Certified: Administrator Expert
Prerequisites	One of MS-700, MS-203, MS-500, or MD-102 (Associate-level cert)
Duration	~120 minutes
Question count	40–60 questions (mix of MCQ, drag-drop, case studies, hot-area)
Passing score	700 / 1000
Languages	English, Japanese, Chinese, Korean, German, French, Spanish, Portuguese (Brazil)
Cost (USD)	$165 (varies by region)
Validity	1 year (free annual renewal via Microsoft Learn)

Skills Measured

Domain	Weight
Deploy and manage a Microsoft 365 tenant	25–30%
Implement and manage identity and access in Microsoft Entra ID	25–30%
Manage security and threats by using Microsoft Defender XDR	20–25%
Manage compliance by using Microsoft Purview	15–20%

EXAM TIP

Microsoft updates exam objectives roughly every 6–9 months. Before sitting the exam, **always** download the current skills outline from `learn.microsoft.com/credentials/certifications/exams/ms-102/` and compare it against this guide's coverage.

Lab Environment Setup

You can complete every lab in this guide using a **Microsoft 365 Developer Tenant**, which is free, comes with 25 licensed users, and includes E5 features (Defender, Purview, Intune, Power BI). Sign up at:

> 📍 https://developer.microsoft.com/microsoft-365/dev-program

Required tools to install on your management workstation:

- PowerShell 7+ (cross-platform, recommended over Windows PowerShell 5.1)
- Microsoft Graph PowerShell SDK (`Install-Module Microsoft.Graph`)
- Exchange Online Management module (`Install-Module ExchangeOnlineManagement`)
- Microsoft Teams module (`Install-Module MicrosoftTeams`)
- SharePoint Online module (`Install-Module Microsoft.Online.SharePoint.PowerShell`)
- Modern web browser (Edge or Chrome) with multiple profiles for admin/user testing

Table of Contents

Section 3 — Device Management (Intune)

Section 4 — Exchange Online Administration

Section 5 — Microsoft Teams Administration

Section 6 — SharePoint Online & OneDrive

Section 7 — Security & Threat Protection

SECTION 1

01

Microsoft 365 Tenant Management

The foundation of every Microsoft 365 environment. Learn how tenants, subscriptions, identities, and DNS records come together to form a cloud workspace.

Architecture · Subscriptions · Entra ID · Tenant Setup · Custom Domains · DNS
Admin Center · Branding · Apps Deployment · Service Health · Billing · Hybrid Identity

1.1 Microsoft 365 Architecture Overview

Introduction

Microsoft 365 is a **cloud-based productivity and security suite** that bundles together a portfolio of services hosted by Microsoft in its global Azure data centers. It is not a single product — it is a federation of dozens of services (Exchange Online, SharePoint Online, Teams, Intune, Defender, Purview, Power Platform, and many more), all stitched together by a shared identity system called **Microsoft Entra ID** (formerly Azure Active Directory).

When an organization "moves to Microsoft 365," they receive a logical container called a **tenant**. A tenant is an isolated instance of Microsoft 365 dedicated to one organization, identified by a unique **initial domain name** in the format `yourcompany.onmicrosoft.com`. All of the organization's users, data, mailboxes, sites, devices, and policies live inside that tenant.

Why This Topic Is Important

Understanding the architecture is non-negotiable for an MS-102 administrator because **everything else rests on it**. Where does a user account actually live? Where are emails stored? How does a mobile device know to apply a compliance policy? Which service is responsible for blocking a phishing email? Knowing the answers prevents the most common failure mode in cloud administration: blaming the wrong service for a problem.

In real organizations, architectural understanding directly translates to faster troubleshooting and better design decisions. An administrator who knows that "Teams chat lives in Exchange Online mailboxes and meeting recordings live in OneDrive" can diagnose a problem in minutes instead of hours.

Key Concepts

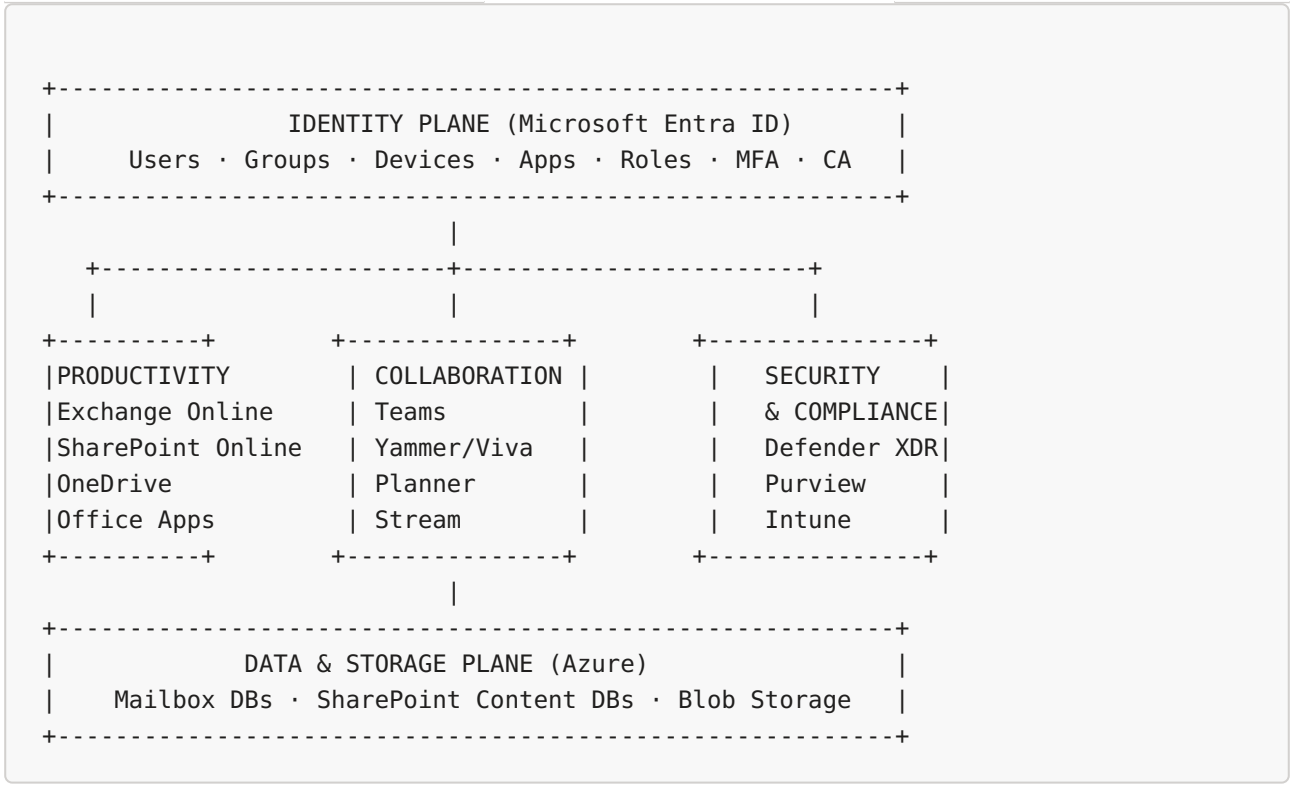
The Microsoft 365 Tenant

A **tenant** is the top-level container for an organization's resources. It is created when someone signs up for a Microsoft 365 subscription. Every tenant has:

- **A unique Tenant ID** (a GUID like `1a2b3c4d-5e6f-7890-abcd-ef1234567890`).
- **A primary initial domain** (`contoso.onmicrosoft.com`) that cannot be removed.
- **One or more verified custom domains** (`contoso.com`, `contoso.co.uk`, etc.).
- **A home region** (e.g., North America, EMEA, APAC) that determines where data is stored at rest.
- **One or more subscriptions** that grant access to services and licenses to users.

The Service Plane

Inside a tenant, Microsoft 365 services are organized into several logical "planes" that work together:



Entra ID — The Identity Foundation

Microsoft Entra ID is the cloud directory that holds all identities used by Microsoft 365 services. It replaces and extends the on-premises Active Directory Domain Services (AD DS) for cloud workloads. Every user, group, device, and application that interacts with Microsoft 365 has a corresponding object in Entra ID.

Concept	On-Premises AD	Microsoft Entra ID
Protocol	LDAP, Kerberos, NTLM	HTTPS, OAuth 2.0, OpenID Connect, SAML
Structure	Forest → Domain → OU	Tenant → Administrative Units
Group Policy	GPO	Intune configuration profiles
Trust Direction	Forest trusts	Cross-tenant access settings, B2B
Authentication	Domain controller	Cloud authentication (or hybrid via Entra Connect)

Multi-Tenancy

Microsoft 365 is multi-tenant — many customers' tenants share the same physical infrastructure but are **logically isolated**. Microsoft enforces strict boundaries: data, identities, and configurations in one tenant cannot be accessed by another tenant unless an administrator explicitly enables cross-tenant collaboration (B2B guest access, cross-tenant access settings, etc.).

Global Service Architecture

Microsoft 365 runs in geographically distributed regions called **geos**. When you create a tenant you select a country/region, which maps to a geo. Microsoft promises that **data at rest** stays within that geo for core workloads (Exchange, SharePoint, OneDrive, Teams). Some services are global (Entra ID, parts of compliance), which is why some compliance frameworks require additional configuration to stay regional.

Geo	Includes Countries
North America	United States, Canada
Europe	EU member states, UK, Switzerland, Norway
Asia Pacific	Japan, Australia, India, Korea, Singapore, etc.
South America	Brazil, Chile, etc.
Middle East & Africa	UAE, South Africa, Qatar
Sovereign Clouds	US Government (GCC, GCC High, DoD), China (operated by 21Vianet), Germany (legacy)

Architecture / Workflow — How a User Sign-In Works

To illustrate how the components interact, consider what happens when Sarah at Contoso opens Outlook and checks her email:

1. Outlook contacts `autodiscover.contoso.com` via DNS.
2. DNS returns a CNAME pointing to `autodiscover.outlook.com`.
3. Outlook hits Exchange Online's autodiscover endpoint, which redirects to Entra ID for authentication.
4. Entra ID prompts for credentials. Sarah enters her UPN `sarah@contoso.com` and password.
5. Entra ID checks the password (cloud-only) or forwards to her on-prem domain controller (hybrid).
6. If authenticated, Conditional Access policies are evaluated (device compliant? trusted location? MFA required?).
7. If policies pass, Entra ID issues an **access token** (JWT) for Exchange Online.
8. Outlook presents that token to Exchange Online and starts syncing mail.

Every step matters for an administrator: DNS misconfigurations break autodiscover, expired or revoked tokens force re-sign-in, Conditional Access blocks unmanaged devices, and so on.

Microsoft Portal Navigation

Microsoft 365 administration is distributed across multiple admin portals. Knowing which portal does what is essential.

Portal	URL	Purpose
Microsoft 365 Admin Center	admin.microsoft.com	Users, groups, billing, service health
Microsoft Entra Admin Center	entra.microsoft.com	Identity, MFA, Conditional Access, roles
Microsoft Intune Admin Center	intune.microsoft.com	Devices, apps, compliance, Autopilot
Exchange Admin Center	admin.exchange.microsoft.com	Mailboxes, mail flow, transport rules
SharePoint Admin Center	admin.microsoft.com/sharepoint	Sites, sharing, storage, hub sites
Teams Admin Center	admin.teams.microsoft.com	Teams policies, voice, meetings, apps
Microsoft Defender Portal	security.microsoft.com	Threat investigation, Defender XDR
Microsoft Purview Portal	purview.microsoft.com	Compliance, DLP, retention, eDiscovery
Microsoft 365 Apps Admin Center	config.office.com	Office app deployment policies

EXAM TIP

The MS-102 frequently asks "which portal is used to do X?" Memorize this table cold. A classic trap: "where do you create a mailbox?" The correct answer is Microsoft 365 Admin Center (where you license a user) — Exchange Admin Center only manages an existing mailbox.

Real-World Scenarios

SCENARIO: MULTI-GEO AT A MULTINATIONAL

Contoso Ltd is a global manufacturer with offices in Germany, Japan, and the US. Their GDPR officer mandates that EU employees' mailboxes stay in EU data centers, while their HR systems require US storage. The administrator deploys **Microsoft 365 Multi-Geo**, configures preferred data locations on each user, and uses sensitivity labels to prevent cross-region data transfer. This requires both architectural understanding (which workloads honor multi-geo) and compliance knowledge (labels enforce the residency).

SCENARIO: MIGRATING FROM GOOGLE WORKSPACE

A 500-user company is moving from Google Workspace to Microsoft 365. The admin signs up for a Business Standard subscription, verifies their custom domain (after temporarily delaying MX cutover), uses the Exchange Online migration tool to copy mailboxes from Gmail, deploys Outlook via Microsoft 365 Apps, and finally cuts over DNS to redirect mail to Exchange Online. Architecture knowledge dictates the safe order: identity → mail → DNS → applications.

Best Practices

ADMINISTRATOR BEST PRACTICES

- **Never use a "real" user account as the global admin.** Create dedicated cloud-only accounts with names like `gadmin.john@contoso.onmicrosoft.com` protected with MFA and Privileged Identity Management.
- **Keep at least two emergency-access ("break-glass") accounts** excluded from Conditional Access, with extremely long random passwords stored in a physical safe.
- **Tag your tenant in admin portals with the company name** and a contact email so technical-support tickets route correctly.
- **Document the tenant ID and primary domain** in your IT runbook — recovery procedures may require them.
- **Choose the right tenant region during creation** — it cannot be easily changed afterward.

Security Considerations

SECURITY NOTES

- The initial domain (`*.onmicrosoft.com`) is publicly enumerable — attackers can guess at tenant existence. Always use a custom domain for user UPNs.
- Global Administrators can do anything in the tenant — limit the count to 2–4 persons maximum.
- Enable **Security Defaults** on day one if you do not yet have Conditional Access; this enforces MFA on all users.
- Review tenant-level settings every quarter using a tool like **Microsoft Secure Score**.

Interview Questions and Answers

COMMON INTERVIEW QUESTIONS

Q1. What is a Microsoft 365 tenant and how is it different from a subscription?

A tenant is the logical Entra ID container for an organization; a subscription is a commercial agreement that grants licenses to services within that tenant. One tenant can have many subscriptions (e.g., Microsoft 365 E3 + Power BI Premium + Azure).

Q2. What is the difference between Microsoft 365 and Office 365?

Office 365 is a subset focusing on productivity apps (Exchange, SharePoint, Teams, Office apps). Microsoft 365 includes Office 365 plus Windows licensing, Intune (Enterprise Mobility + Security), and Defender XDR. Microsoft 365 = Office 365 + Windows + EMS.

Q3. Can you move a Microsoft 365 tenant between regions?

For most workloads, no — the home region is set at creation. Microsoft does offer a limited "tenant move" service for qualifying customers, but it is rarely done. The recommended approach is to plan the right region from the start.

Q4. What is the relationship between Azure AD and Microsoft Entra ID?

They are the same product. Microsoft renamed Azure AD to Microsoft Entra ID in 2023. APIs, PowerShell modules, and most documentation still mention "Azure AD" interchangeably.

Q5. How does Microsoft 365 ensure tenant isolation in a multi-tenant cloud?

Through logical partitioning at every layer: each request includes a tenant ID, services validate it against tokens issued by Entra ID, and data stores (mailboxes, sites, files) tag every record with a tenant identifier. Network isolation, encryption keys, and access policies further enforce boundaries.

Exam-Focused Notes

HIGH-YIELD EXAM POINTS

- A tenant has **one and only one initial onmicrosoft.com domain** that cannot be deleted.
- Microsoft 365 = Office 365 + Windows + EMS (Intune + Entra ID P1/P2).
- The tenant region determines data residency for Exchange, SharePoint, OneDrive, Teams.
- Multi-Geo is a paid add-on that enables per-user data residency override.
- You can have multiple custom domains but only **one default** domain at a time.
- Tenant ID and Tenant Name (primary onmicrosoft.com) are both important identifiers for support and PowerShell.

Hands-On Lab: Inspect Your Tenant

LAB 1.1 — DISCOVER YOUR TENANT IDENTITY

1. Sign in to `admin.microsoft.com` as a Global Administrator.
2. Click **Settings → Org settings → Organization profile**. Note the *Name*, *Default domain*, and *Tenant ID*.
3. Click **Setup → Domains**. List the primary domain (always ends in `.onmicrosoft.com`) and any custom domains.
4. Open **PowerShell 7** and run:

```
PS> Connect-MgGraph -Scopes "Organization.Read.All"
PS> Get-MgOrganization | Select-Object DisplayName, Id, VerifiedDomains
```

5. Compare the PowerShell output to the GUI — they should match exactly.
6. Document the values in a notebook; you will reference them in later labs.

Summary

Section 1.1 Recap

- Microsoft 365 is a federation of services unified by Microsoft Entra ID.
- A tenant is the per-organization container; a subscription grants license to services within it.
- Administration is split across multiple specialized portals.
- Region and initial domain are chosen at tenant creation and largely immutable.
- Identity is the foundation — get it right, and everything else follows.

1.2 Microsoft 365 Subscriptions and Licensing

Introduction

A **subscription** is a commercial agreement with Microsoft that grants your tenant access to a defined bundle of services for a defined number of users over a defined time. A **license** is what you assign to an individual user (or group, via group-based licensing) to give them access to the features of that subscription.

Think of it this way: a subscription is the bucket of seats you bought; a license is the seat you assigned to a person.

Why This Topic Is Important

Licensing is the second-largest line item in most IT budgets (after salaries) and one of the most common reasons IT admins are audited. Over-licensing wastes thousands of dollars per month. Under-licensing causes feature outages — a user with the wrong license suddenly cannot use Defender, or their mailbox stops working. Microsoft also requires that every **active** service or feature have a valid license; using an unlicensed feature violates the agreement.

Key Concepts

Subscription Families

Family	Target Audience	User Cap
Business	Small & midsize organizations	Up to 300 users
Enterprise	Large organizations	Unlimited
Frontline (F)	Frontline workers (retail, manufacturing, healthcare)	Per-user, often combined with Enterprise
Education (A)	Schools and universities	Unlimited (per institution)
Government (G)	Public sector — GCC, GCC High, DoD	Sovereign cloud
Apps for Business / Enterprise	Office apps only, no Exchange/SharePoint	Varies

Common Enterprise SKUs Compared

Feature	M365 E3	M365 E5	Business Premium
Office Apps (Word, Excel, etc.)	✔	✔	✔
Exchange Online (50 GB / 100 GB)	50 GB	100 GB	50 GB
SharePoint + OneDrive (1 TB)	✔	✔	✔
Teams	✔	✔	✔
Intune MDM & MAM	✔	✔	✔
Entra ID P1	✔	✔ (P2)	✔ (P1)
Entra ID P2 (PIM, Identity Protection)	✘	✔	✘
Defender for Office 365 Plan 1	✘	✔ (Plan 2)	✔ (Plan 1)
Defender for Endpoint P2	✘	✔	✘
Defender for Identity	✘	✔	✘
Purview eDiscovery (Premium)	✘	✔	✘
Purview Insider Risk	✘	✔	✘
Power BI Pro	✘	✔	✘
Windows 11 Enterprise	✔	✔	✔
User cap	Unlimited	Unlimited	300

Add-On Subscriptions

Beyond the core bundles, customers often add:

- **Microsoft 365 E5 Compliance** — adds Purview Premium to an E3 base.
- **Microsoft 365 E5 Security** — adds Defender XDR (full) to an E3 base.
- **Teams Phone** — adds PSTN calling.
- **Audio Conferencing** — adds dial-in conference numbers.
- **Microsoft 365 Copilot** — generative AI across Office apps (separate per-user license).
- **Power BI Pro / Premium** — business analytics.
- **Visio Plan 1/2**, **Project Plan 1/3/5**.

Microsoft Portal Navigation

> 📍 Microsoft 365 Admin Center → Billing → Your products

> 📍 Microsoft 365 Admin Center → Billing → Licenses

> 📍 Microsoft 365 Admin Center → Users → Active users → (select user) → Licenses and apps

Step-by-Step: Assign a License to a User

1. Go to `admin.microsoft.com` as a Global Administrator or License Administrator.
2. Navigate to **Users → Active users**.
3. Click the user's display name to open the user pane.
4. Click the **Licenses and apps** tab.
5. Select the desired license SKU (for example, "Microsoft 365 E3").
6. Optionally toggle off individual service plans the user should not have (e.g., turn off "Yammer" for compliance).
7. Confirm the user's **Usage location** (a 2-letter country code) is set — required for licensing.
8. Click **Save changes**.
9. The user can sign in to `office.com` immediately; full provisioning of mailboxes/sites can take 5–15 minutes.

PowerShell Commands

License management is one of the most common PowerShell scenarios because the GUI does not scale.

List Available SKUs

```
PS> Connect-MgGraph -Scopes "Organization.Read.All","User.ReadWrite.All"
PS> Get-MgSubscribedSku | Select-Object SkuPartNumber, ConsumedUnits,
@{N='Available';E={$_.PrepaidUnits.Enabled - $_.ConsumedUnits}}
```

Assign a License via Graph PowerShell

```
# Get the SKU ID for Microsoft 365 E3
PS> $sku = Get-MgSubscribedSku -All | Where-Object SkuPartNumber -eq "SPE_E3"

# Set Usage Location (required) and assign the license
PS> Update-MgUser -UserId "sarah@contoso.com" -UsageLocation "US"
PS> Set-MgUserLicense -UserId "sarah@contoso.com" `
        -AddLicenses @(@{SkuId = $sku.SkuId}) `
        -RemoveLicenses @()
```

Bulk-Assign Licenses to All Users in a Group

```
# Group-based licensing - the modern, recommended approach
PS> $group = Get-MgGroup -Filter "displayName eq 'Sales-Department'"
PS> $sku   = Get-MgSubscribedSku -All | Where SkuPartNumber -eq "SPE_E3"
PS> Set-MgGroupLicense -GroupId $group.Id `
        -AddLicenses @(@{SkuId = $sku.SkuId}) `
        -RemoveLicenses @()
```

Find Unlicensed Users

```
PS> Get-MgUser -All -Property DisplayName,UserPrincipalName,AssignedLicenses |
        Where-Object { $_.AssignedLicenses.Count -eq 0 } |
        Select-Object DisplayName, UserPrincipalName
```

Real-World Scenarios

SCENARIO: RIGHT-SIZING LICENSES TO SAVE COST

An IT director at a 2,000-employee company runs the "Microsoft 365 usage analytics" Power BI template and discovers that 600 of the company's E5 users have not opened Teams or used Defender features in 90 days. Working with HR, they downgrade those 600 users to E3 and assign E5 only to roles that need the security features. Annual savings: ~$700,000.

SCENARIO: MIXED LICENSING FOR FRONTLINE WORKERS

A retail chain has 300 corporate users on E3 and 5,000 store associates who need only Teams and a small mailbox. The admin assigns **Microsoft 365 F3** to frontline workers (a fraction of the E3 cost), with shared device sign-in for store kiosks. The architecture works because Entra ID can host both license types in the same tenant.

Best Practices

LICENSING BEST PRACTICES

- **Use group-based licensing** — assign licenses to security groups, not individual users. New hires get the right license automatically when added to the group.
- **Always set Usage Location first** or license assignment fails silently.
- **Review consumed-vs-available quarterly**. Surrender unused subscriptions before renewal.
- **Use Azure cost management + license reports** together for true TCO.
- **Document license assignment rules** — which job titles get E3 vs E5 vs F3 — to avoid drift.

Common Errors and Troubleshooting

Error	Cause	Resolution
"Subscription has expired"	Credit card declined or grace period ended	Billing → Payment methods; renew or update card
"User missing Usage Location"	Required attribute not set	Update-MgUser -UsageLocation "US"
"License assignment failed: conflict"	Two licenses include the same service plan (e.g., two Exchange Online)	Remove duplicate service plans or pick one parent SKU
"Group-based license not applied"	User missing usage location, or licensing processing delay	Wait 10–15 min; or run Reprocess on group license
"Office apps say activation failed"	License removed or expired	Verify user still has license; sign out and back in

Interview Questions and Answers

INTERVIEW Q&A

Q. What is the difference between Microsoft 365 E3 and E5?

E5 adds advanced security (Defender XDR full stack, including Defender for Identity and Defender for Office 365 P2), advanced compliance (Purview eDiscovery Premium, Insider Risk, Communication Compliance), Entra ID P2 (PIM, Identity Protection), Power BI Pro, and Teams Phone with conferencing.

Q. What is group-based licensing and why use it?

Licenses are assigned to a security group; all members automatically inherit them. Members removed from the group lose the license. This eliminates manual per-user assignment and ensures consistency for HR-driven user lifecycle management.

Q. A user is licensed but cannot open Office apps. What do you check?

(1) Usage Location set; (2) license is "enabled" and not disabled at service-plan level; (3) shared-computer

activation conflict if on a shared device; (4) sign out and re-activate via Office.com; (5) tenant Office app config (config.office.com).

Q. How do you remove a license from 200 users at once?
Use group-based licensing — remove users from the licensing group, or use a CSV-driven PowerShell script with `Set-MgUserLicense -RemoveLicenses`.

Exam-Focused Notes

HIGH-YIELD EXAM POINTS

- Usage Location is mandatory for any licensed user.
- Group-based licensing requires Entra ID P1+ (included in M365 E3/E5/Business Premium).
- Business plans cap at 300 users — exceeding this requires Enterprise.
- F (Frontline) plans cannot host shared mailboxes as the primary mailbox owner.
- E5 Security and E5 Compliance are add-ons; they require an E3 base or equivalent.

Hands-On Lab

LAB 1.2 — GROUP-BASED LICENSING

1. In Microsoft 365 Admin Center, create a security group named `LIC-M365-E3-Users`.
2. Navigate to **Billing → Licenses → select Microsoft 365 E3 → Assign licenses**, then assign to the group.
3. Add 3 test users to the group.
4. Verify (after ~5 minutes) that each user inherited the license — visible on the user's Licenses tab.
5. Remove one user from the group; verify the license is reclaimed within 10 minutes.
6. Run `Get-MgGroupLicense -GroupId <id>` in PowerShell to confirm group-level licensing.

Summary

Section 1.2 Recap

- Subscriptions are commercial contracts; licenses are user-level grants.
- Business caps at 300 users; Enterprise is unlimited.
- E3 = productivity + base security/management; E5 adds advanced security, compliance, BI, voice.
- Group-based licensing scales license management to thousands of users.
- Usage Location is always required.

1.3 Microsoft Entra ID Overview

Introduction

Microsoft Entra ID (formerly Azure Active Directory or Azure AD) is the cloud-based identity and access management (IAM) service that underpins every Microsoft 365 tenant. Every user, group, device, application, role assignment, sign-in attempt, and authentication policy ultimately lives in Entra ID.

If you came from on-premises Active Directory, Entra ID will feel familiar but fundamentally different. AD DS is a directory service for the corporate network: it relies on Kerberos and LDAP, requires line-of-sight to domain controllers, and authenticates Windows-joined PCs. Entra ID is a directory service for the internet: it relies on HTTPS-based protocols (OAuth 2.0, OpenID Connect, SAML), authenticates any device from anywhere, and is designed to integrate with thousands of SaaS applications.

Why This Topic Is Important

Microsoft Entra ID is the single most important component of Microsoft 365. Lose access to it and you lose access to *everything*: email, files, Teams, devices. Misconfigure it, and you expose the entire organization to credential theft. The MS-102 exam dedicates 25–30% of questions to identity management, and real-world security incidents almost always involve identity compromise.

Key Concepts

Identity Object Types

Object	Description	Example
User	A person who can sign in	sarah@contoso.com
Guest User	External identity invited from another tenant or consumer account	partner_contoso.com#EXT#@contoso.onmicrosoft.com
Group	A collection of users/devices/groups for permissions or licensing	Sales-Department
Device	A registered, joined, or hybrid-joined device	SARAH-LAPTOP01
Application	A registered cloud app integrated with Entra ID	Salesforce, custom app
Service Principal	The local identity of an application in a tenant	SAP HR integration
Managed Identity	Auto-managed service principal for Azure resources	VM with managed identity
Administrative Unit	A sub-scope of the tenant for delegated admin	"Europe-Region-AU"

Entra ID Editions (Licenses)

Edition	Included Features	Bundled With
Free	Basic identity, security defaults, B2B guest	Any Microsoft 365 tenant
Microsoft 365 Apps	Free features + SSO for ~10 SaaS apps	Microsoft 365 Apps for Business
P1	Conditional Access, SSPR with writeback, dynamic groups, group-based licensing, hybrid identities, custom branding	M365 E3, Business Premium
P2	P1 + Identity Protection (risk policies), Privileged Identity Management (PIM), Access Reviews, Entitlement Management	M365 E5
Entra Suite	P2 + Verified ID, Internet Access, Private Access, Permissions Management	Separate add-on

Authentication Protocols

Protocol	Used By	Notes
OAuth 2.0	Modern apps, REST APIs, Microsoft Graph	Access & refresh tokens, scoped permissions
OpenID Connect (OIDC)	Sign-in for web/mobile apps	Built on OAuth 2.0; adds identity tokens (JWT)
SAML 2.0	Legacy SaaS apps, single sign-on	XML-based assertions; common in enterprise SaaS
WS-Federation	Older Microsoft apps	Largely replaced by OIDC
FIDO2 / WebAuthn	Passwordless	Hardware security keys, Windows Hello

Tokens

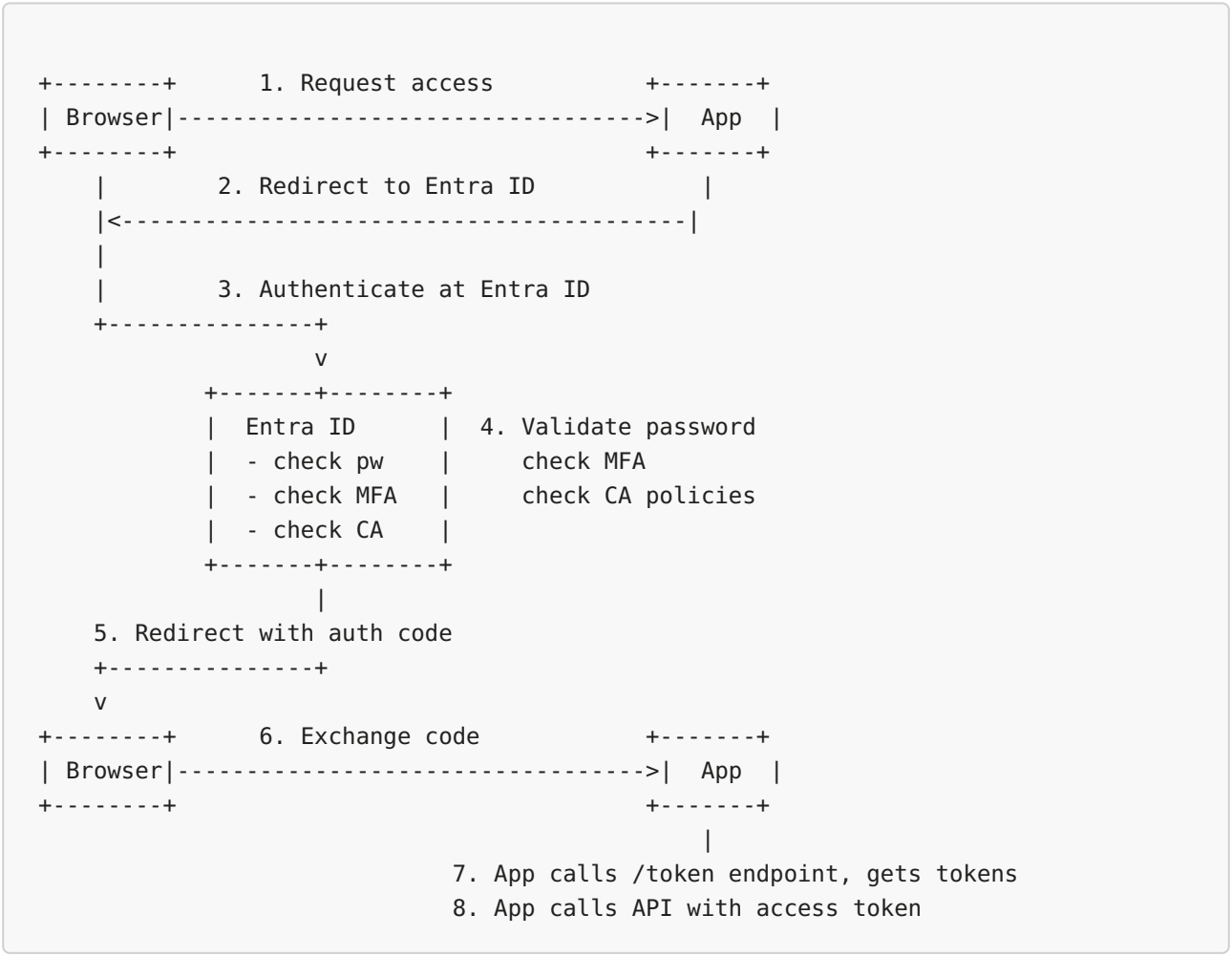
Entra ID issues two main token types:

- **ID token** — proves who you are; consumed by the client application.
- **Access token** — grants permission to call a resource (e.g., Microsoft Graph, Exchange Online); consumed by the API.
- **Refresh token** — long-lived secret used to obtain new access tokens without re-prompting the user.

Default lifetimes (configurable via Conditional Access session controls):

- Access token: 60–90 minutes
- Refresh token: up to 90 days (with sliding renewal)
- Session token (browser): governed by the browser and CA policy

Architecture / Workflow — How OIDC Sign-In Works



Microsoft Portal Navigation

📍 Microsoft Entra Admin Center → Identity → Overview

📍 Microsoft Entra Admin Center → Identity → Users → All users

📍 Microsoft Entra Admin Center → Identity → Groups → All groups

📍 Microsoft Entra Admin Center → Identity → Devices → All devices

📍 Microsoft Entra Admin Center → Identity → Applications → Enterprise applications

📍 Microsoft Entra Admin Center → Identity → Roles & admins → Roles & administrators

📍 Microsoft Entra Admin Center → Protection → Conditional Access

📍 Microsoft Entra Admin Center → Monitoring & health → Sign-in logs

Step-by-Step: Tour Your Entra ID Tenant

1. Sign in to `entra.microsoft.com` as a Global Administrator.
2. On the **Overview** blade, record:
    - Tenant name
    - Tenant ID
    - Primary domain
    - License (Free / P1 / P2)
3. Click **Users** — note the count.
4. Click **Groups** — note Security, Microsoft 365, mail-enabled, distribution.
5. Click **Devices** — note any registered devices.
6. Click **Enterprise applications** — note pre-installed Microsoft and Microsoft Graph apps.
7. Click **Sign-in logs** — review your own recent sign-ins. This is the most useful day-to-day troubleshooting tool.

PowerShell Commands

```
# Connect with the right scopes
PS> Connect-MgGraph -Scopes "Directory.Read.All","User.Read.All","Group.Read.All"

# Tenant info
PS> Get-MgOrganization | Format-List DisplayName, Id, City, Country, VerifiedDomains

# Count of users, groups, devices
PS> (Get-MgUser   -All).Count
PS> (Get-MgGroup  -All).Count
PS> (Get-MgDevice -All).Count

# Recently created users
PS> Get-MgUser -All -Property DisplayName,CreatedDateTime |
        Sort-Object CreatedDateTime -Descending |
        Select-Object -First 10 DisplayName, CreatedDateTime
```

Real-World Scenarios

SCENARIO: M&A IDENTITY CONSOLIDATION

Contoso acquires Fabrikam. Both have Microsoft 365 tenants. The IT team uses Entra ID B2B to add Fabrikam users as guests in Contoso while planning a tenant-to-tenant migration over 6 months. During the transition, cross-tenant access settings, sensitivity labels, and Conditional Access policies maintain security while users from both companies collaborate seamlessly.

Best Practices

ENTRA ID BEST PRACTICES

- Enable **Security Defaults** immediately (free tier) — or implement equivalent Conditional Access in P1+.
- Use **cloud-only break-glass accounts** with FIDO2 keys; exclude from CA policies.
- Move admin assignments into **PIM (P2)** — eligible, not active, with approval and time limits.
- Standardize UPN to match primary SMTP (e.g., `first.last@contoso.com`) for usability.
- Audit sign-in logs weekly for impossible-travel and risk events.

Security Considerations

ENTRA ID SECURITY NOTES

- Identity is the new perimeter — protect it more aggressively than the network.
- Phishing-resistant MFA (FIDO2, Windows Hello) is the gold standard; SMS is the worst MFA option.
- Service principal credentials (client secrets) are often stolen — prefer managed identities or certificates.
- Enable Identity Protection (P2) to automatically remediate compromised accounts.

Interview Questions and Answers

INTERVIEW Q&A

Q. What is the difference between Active Directory and Microsoft Entra ID?
AD DS is on-prem, LDAP/Kerberos-based, designed for Windows networks. Entra ID is cloud, HTTP-based (OAuth/OIDC/SAML), designed for SaaS and modern apps. They can coexist via Entra Connect (hybrid).

Q. Which Entra ID edition do you need for Conditional Access?
P1 minimum. P2 adds risk-based policies (Identity Protection).

Q. What is a Service Principal?
The local identity an application uses to access tenant resources. When you register an app, you get an Application object (global) and a Service Principal (per tenant). The SP gets the role assignments and permissions.

Q. What is the difference between a token and a session cookie?
A token is a signed credential proving identity or granting API access. A session cookie is a browser-side artifact letting a web app remember you. Browsers carry session cookies; APIs carry tokens.

Exam-Focused Notes

HIGH-YIELD EXAM POINTS

- Free tier includes Security Defaults; Conditional Access requires P1.
- Privileged Identity Management (PIM) and Identity Protection require P2.

- Guest users have UPNs in the format `upn_externaltenant.com#EXT#@yourtenant.onmicrosoft.com`.
- Object types: User, Group, Device, App, Service Principal, Managed Identity.
- UPN must match a verified domain to enable sign-in with that suffix.

Hands-On Lab

LAB 1.3 — EXPLORE ENTRA ID

1. In Entra Admin Center, locate your tenant's **P1/P2 license status**.
2. Click your own profile → Authentication methods. Note registered methods.
3. Navigate to Sign-in logs → filter for "Last 24 hours". Review user, app, status, IP, location.
4. Open Audit logs and review activities of category "User Management".
5. From PowerShell:

```
PS> Get-MgAuditLogSignIn -Top 5 | Select-Object UserDisplayName,
AppDisplayName, Status
```

Summary

Section 1.3 Recap

- Entra ID is the cloud directory powering Microsoft 365.
- Free, P1, P2 editions unlock progressively more features.
- Authentication uses modern protocols: OAuth, OIDC, SAML.
- Identity is the new security perimeter.

1.4 Tenant Creation and Setup

Introduction

Creating a Microsoft 365 tenant is a one-time decision that shapes your organization's cloud identity for years. The choices made during sign-up — region, primary domain, billing email — are partially immutable. This section walks through the process carefully.

Why This Topic Is Important

A poorly planned tenant creation can lead to permanent friction: an organization in Germany discovers their data sits in a US region; a startup picks a misspelled initial domain that follows them forever; an admin signs up under their personal Microsoft account, losing control when they leave the company.

Key Concepts

Tenant Creation Options

Method	Use Case
Sign up for trial	Quick start; 30-day trial of any SKU
Microsoft 365 Developer Program	Free perpetual sandbox tenant with E5 features and 25 demo users
Buy from microsoft.com	Standard commercial purchase
Buy from a Cloud Solution Provider (CSP)	Volume discount; CSP is billing/support contact
Enterprise Agreement (EA)	Large enterprises with negotiated terms via Microsoft account team

What Cannot Be Changed Later

- **Tenant region/geo** (without Microsoft-assisted move)
- **The `.onmicrosoft.com` primary domain prefix** (you can add new ones, but the original cannot be deleted)
- **Tenant type** (commercial vs sovereign cloud)

Step-by-Step: Create a New Tenant

1. Browse to `microsoft.com/microsoft-365/business/microsoft-365-business-standard` (or any other SKU).

2. Click **Try free for 1 month**.
3. Sign in with a work or school email (do *not* use a personal hotmail/outlook.com account for production).
4. If you have no work email, the wizard asks for personal details — provide them carefully.
5. Enter your **company name**, country (selects region), and language.
6. Choose your **initial domain prefix**: `yourcompanyname.onmicrosoft.com`. *Pick carefully — it cannot be removed.*
7. Create the **first Global Admin** account (e.g., `admin@yourcompanyname.onmicrosoft.com`).
8. Provide a strong password (16+ characters, mix of types).
9. Add a recovery phone number.
10. Complete payment setup (a credit card is required even for trial; you won't be charged until the trial ends).
11. The tenant is provisioned within 1–2 minutes; you are redirected to `admin.microsoft.com`.

Step-by-Step: Initial Configuration

Once your tenant exists, perform these first-day tasks:

1. **Verify global admin recovery info.** Settings → Org settings → Security & privacy → confirm recovery email and phone.
2. **Set the tenant time zone and language.** Settings → Org settings → Organization profile.
3. **Update the org profile** (logo, address) — appears on sign-in screens, invoices.
4. **Create a second Global Admin** as redundancy.
5. **Create two break-glass accounts** (e.g., `break.glass.01`, `break.glass.02`) with extremely long random passwords, FIDO2 keys, stored physically.
6. **Enable Security Defaults** (Entra Admin Center → Identity → Overview → Properties → Manage Security Defaults).
7. **Add your custom domain** (next section).

PowerShell Commands

```
# Once tenant exists, connect and verify
PS> Connect-MgGraph -Scopes "Organization.Read.All","Domain.ReadWrite.All"
PS> Get-MgOrganization | Select-Object DisplayName, Id, CountryLetterCode,
PreferredLanguage
PS> Get-MgDomain | Select-Object Id, IsVerified, IsDefault, IsInitial
```

Real-World Scenarios

SCENARIO: STARTUP FOUNDER TRAP

A founder signs up for Microsoft 365 with their personal Hotmail address as the billing contact, naming the tenant `cool-startup-2024`. Two years later, the company is acquired by a Fortune 500. The acquirer cannot

easily change the initial domain, and the founder's personal Hotmail is still the only billing contact. The fix is painful — they migrate to a new, clean tenant.

Best Practices

- **Always sign up under a corporate domain identity**, not a personal Microsoft account.
- **Plan the initial domain prefix** — short, professional, no version numbers or years.
- **Pick the correct country** first time — this controls data residency.
- **Document credentials in an enterprise vault** (Azure Key Vault, CyberArk).

Common Errors and Troubleshooting

Problem	Fix
"Email already associated with another tenant"	Use a different email or contact Microsoft Support to disassociate
"Country not supported"	Some countries lack commercial Microsoft 365; use a global region (EU, US)
"Cannot remove initial domain"	This is by design — only add additional domains, set one as default

Interview Questions and Answers

Q. Can a tenant be moved between Microsoft 365 regions?
For most workloads, no — region is set at creation. Microsoft offers a limited "tenant move" service for qualifying customers, but it's rarely done in practice. Plan correctly the first time.

Q. What is a "break-glass" account?
A highly secured emergency-access account excluded from Conditional Access policies and used only when normal admin access is broken (e.g., MFA service outage). Typically two such accounts exist, with credentials in a physical safe.

Exam-Focused Notes

- The initial onmicrosoft.com domain is created at tenant provisioning and cannot be removed.
- Region/geo is set at creation; affects Exchange/SharePoint data residency.
- Always create redundant Global Admins on day one.

Hands-On Lab

LAB 1.4 — CREATE A DEVELOPER TENANT

1. Browse to `developer.microsoft.com/microsoft-365/dev-program`.
2. Sign up using your Microsoft account.
3. Select **Instant sandbox** (E5 with 25 demo users) or **Configurable sandbox** (clean E5 tenant).
4. Choose region, admin name, password, and primary domain prefix.
5. Wait 1–2 minutes for provisioning.
6. Sign in to `admin.microsoft.com` and explore.

Summary

- Tenant creation locks in region and initial domain — choose carefully.
- Always create at least two Global Admins and two break-glass accounts.
- Enable Security Defaults immediately for free baseline protection.

1.5 Custom Domain Configuration & DNS

Introduction

Every Microsoft 365 tenant starts with an `onmicrosoft.com` address that no one wants on their business cards. The first task for any new administrator is to **add their custom domain** (`contoso.com`) so that user emails, login names, and SharePoint URLs reflect the company brand.

Custom domain configuration is half identity, half DNS. You must prove ownership by adding TXT records, and then publish service-specific records (MX, CNAME, SRV, SPF) so that mail flow and other workloads work correctly.

Why This Topic Is Important

Mis-configured DNS is the #1 cause of mail flow problems in Microsoft 365. An MX record pointed at the wrong host means inbound email vanishes. A missing SPF record means recipients mark your email as spam. The MS-102 exam tests DNS record knowledge heavily.

Key Concepts

Domain States

State	Meaning
Unverified	Added to tenant but ownership not yet proven
Verified	TXT record found; you can now create users with this UPN suffix
Activated	Service records (MX, CNAME, SRV) deployed; mail flow and other services live
Default	The domain used as the default UPN suffix for new users
Federated	Authenticated via on-prem AD FS (legacy, rarely used today)

DNS Records You Will Touch

Record	Purpose	Example Value
TXT (verification)	Prove domain ownership	`MS=ms12345678`
MX	Receive inbound email	`contoso-com.mail.protection.outlook.com` (priority 0)
TXT (SPF)	Authorize Microsoft 365 to send mail for your domain	`v=spf1 include:spf.protection.outlook.com -all`
CNAME (autodiscover)	Outlook client auto-config	`autodiscover.outlook.com`
CNAME (lyncdiscover)	Teams / Skype client discovery (legacy)	`webdir.online.lync.com`
CNAME (sip)	Teams SIP federation	`sipdir.online.lync.com`
SRV _sip._tls	Teams SIP discovery	`sipdir.online.lync.com:443`
SRV _sipfederationtls._tcp	Teams federation	`sipfed.online.lync.com:5061`
CNAME (enterpriseregistration)	Hybrid device registration	`enterpriseregistration.windows.net`
CNAME (enterpriseenrollment)	Hybrid Intune enrollment	`enterpriseenrollment.manage.microsoft.com`
TXT (DKIM)	Email signing	Two CNAMEs for selectors
TXT (DMARC)	Email policy	`v=DMARC1; p=quarantine; rua=mailto:...`

Microsoft Portal Navigation

> 📍 Microsoft 365 Admin Center → Settings → Domains

> 📍 Microsoft 365 Admin Center → Settings → Domains → Add domain

Step-by-Step: Add and Verify a Custom Domain

1. Sign in to `admin.microsoft.com` as a Global Administrator.

2. Go to **Settings → Domains → Add domain**.
3. Enter your domain (e.g., `contoso.com`) and click **Use this domain**.
4. Microsoft generates a unique TXT verification value: `MS=ms87654321`.
5. Log in to your DNS registrar (GoDaddy, Cloudflare, Route53, etc.) and add the TXT record at the root (@).
6. Wait 5–30 minutes for DNS propagation.
7. Return to the wizard and click **Verify**. The domain moves to "Verified".
8. The wizard offers to add service records automatically. If your DNS host is supported (GoDaddy, Cloudflare, etc.), Microsoft can do this via API. Otherwise, copy the list and add them manually.
9. Once service records are live, the domain moves to "Active".
10. Optionally, set this domain as **default**.

PowerShell Commands

```
PS> Connect-MgGraph -Scopes "Domain.ReadWrite.All"

# Add a domain
PS> New-MgDomain -Id "contoso.com"

# Get the verification record
PS> Get-MgDomainVerificationDnsRecord -DomainId "contoso.com"

# After publishing the TXT, verify
PS> Confirm-MgDomain -DomainId "contoso.com"

# List all domains and status
PS> Get-MgDomain | Select-Object Id, IsVerified, IsDefault, AuthenticationType

# Set as default domain
PS> Update-MgDomain -DomainId "contoso.com" -IsDefault:$true
```

Real-World Scenarios

SCENARIO: PHASED MIGRATION WITH SUBDOMAIN

A company migrating from Google Workspace to Microsoft 365 wants zero email downtime. They add `contoso.com` to Microsoft but keep the MX record on Google. They create users with UPNs like `sarah@contoso.com` (works for sign-in immediately) but route mail temporarily to `sarah@m365.contoso.com` (a subdomain MX'd to Microsoft) while Google still holds primary mail. After all mailboxes are migrated, the team flips the MX cutover during a weekend window.

Best Practices

- Use a DNS provider that **supports API integration** with Microsoft 365 (GoDaddy, Cloudflare, Route53) — it removes manual error.
- **Add SPF carefully**. Only one SPF record per domain. Combine all senders in one record.
- **Enable DKIM** immediately after domain activation (Defender → Email & collaboration → Policies → DKIM).
- **Publish DMARC in monitor mode first** (`p=none`) to gather data before enforcing.
- Document all DNS records in a runbook in case of registrar lockout.

Security Considerations

- DNS hijacking is a real attack — protect your registrar account with hardware MFA.
- Missing SPF makes your domain trivially spoofable. **Always** publish SPF with `-all` (hard fail) once you know all legitimate senders.
- DKIM ensures recipient mail servers can verify your messages weren't modified in transit.
- DMARC tells receivers what to do with unauthenticated mail and provides aggregate reports.

Common Errors and Troubleshooting

Error	Likely Cause	Fix
"Verification record not found"	DNS hasn't propagated, wrong record location, typo	Wait, use nslookup/dig to verify, re-check
"Domain already used by another tenant"	Domain attached to a different M365 tenant	Use Microsoft support to release; or use a different domain
"MX record conflict"	Multiple MX records prevent mail delivery	Remove old MX; set Microsoft's MX to lowest priority
Outlook autodiscover fails	Missing/incorrect autodiscover CNAME	Add `autodiscover` CNAME → `autodiscover.outlook.com`
"Cannot delete domain"	Users, groups, or shared mailboxes still use this UPN	Reassign affected objects to another verified domain first

Interview Questions and Answers

Q. What DNS records are needed for Exchange Online?

MX (for inbound mail), TXT/SPF (to authorize Microsoft as sender), autodiscover CNAME (for Outlook auto-config), DKIM (recommended), DMARC (recommended).

Q. How would you migrate a custom domain from an old M365 tenant to a new one?
You cannot have the same custom domain in two tenants simultaneously. Steps: (1) prepare new tenant with custom domain still in old tenant; (2) reassign users/groups/mailboxes in old tenant off the custom domain (back to `onmicrosoft.com`); (3) remove domain from old tenant; (4) add and verify in new tenant; (5) update DNS records to new tenant's targets.

Q. Why is SPF a single record but DKIM/DMARC can be multiple TXT entries?
RFC 7208 states each domain may publish only one SPF record. DKIM uses multiple records on selector subdomains (`selector1._domainkey`). DMARC has one record at `_dmarc.domain`.

Exam-Focused Notes

- Verification is always a TXT record at the root.
- MX record format: `<tenant>.mail.protection.outlook.com` where tenant is your domain with dashes replacing dots (contoso-com).
- Outlook autodiscover: CNAME named `autodiscover` pointing to `autodiscover.outlook.com`.
- Teams SIP records are optional for cloud-only deployments but recommended for federation.
- A verified domain must be reassigned away from all objects before deletion.

Hands-On Lab

LAB 1.5 — ADD A DOMAIN TO YOUR DEV TENANT

1. Use a domain you own (or a cheap throwaway from Namecheap).
2. In M365 Admin Center → Domains → Add domain.
3. Copy the TXT verification value.
4. Add it to your DNS registrar at the root.
5. Verify, then publish service records.
6. Update one of your dev tenant users to use the new domain as their UPN.
7. Sign in with the new UPN to confirm it works.

Summary

- A custom domain is verified by adding a TXT record, then activated with service-specific records.
- MX, autodiscover CNAME, SPF, DKIM, and DMARC are the most important records.
- Only one SPF per domain; DKIM and DMARC live on selector subdomains.
- A domain cannot be deleted if any object still uses its UPN suffix.

1.6 Microsoft 365 Admin Center

Introduction

The **Microsoft 365 Admin Center** at `admin.microsoft.com` is the front door of M365 administration. It is intentionally designed for less-technical IT admins — guided wizards, simplified workflows, "common tasks" dashboards. Behind the scenes it calls the same Microsoft Graph APIs that the specialist portals and PowerShell use.

Why This Topic Is Important

Most day-to-day admin tasks (user creation, license assignment, password reset, billing) start in this portal. Understanding its layout reduces troubleshooting time. Many MS-102 exam questions reference exact navigation paths within this portal.

Key Concepts

Admin Roles That Can Access the Portal

Role	Access Level
Global Administrator	Full access; can do anything
User Administrator	Users, groups, password reset
License Administrator	License assignment only
Billing Administrator	Purchases, payment, invoices
Service Support Administrator	Read service health, file tickets
Helpdesk Administrator	Reset non-admin passwords
Reports Reader	View usage reports

Admin Center Layout

- **Home** — dashboard with cards for users, billing, service health, training.
- **Users** — active users, guest users, contacts, deleted users.
- **Teams & groups** — Microsoft 365 groups, distribution lists, security groups.
- **Roles** — admin roles and assignments (forwards to Entra).
- **Resources** — sites, rooms, equipment.

- **Billing** — products, licenses, bills, payments.
- **Support** — open service requests.
- **Settings** — org settings, domains, search & intelligence, partner relationships.
- **Setup** — guided setup wizards.
- **Reports** — usage analytics.
- **Health** — service health and message center.
- **Admin centers** — quick links to specialist portals (Exchange, Teams, SharePoint, Intune, Entra, Defender, Purview).

Microsoft Portal Navigation

> 📍 https://admin.microsoft.com

Step-by-Step: Personalize the Admin Center

1. Click the gear icon (top right) → **Customize navigation**.
2. Pin frequently-used items, hide unused ones.
3. Switch to **Dashboard view** or **Compact list view** for users.
4. Enable **Targeted release** (Org settings → Release preferences) to test preview features.

PowerShell Commands

The admin center does not expose its own PowerShell; you use Graph PowerShell, Exchange Online PowerShell, etc., to script equivalent tasks.

```
# Open the admin center programmatically
PS> Start-Process "https://admin.microsoft.com"

# Connect to Graph for equivalent operations
PS> Connect-MgGraph -Scopes "User.ReadWrite.All","Group.ReadWrite.All"
```

Real-World Scenarios

Scenario: The HR director needs to see the list of all licensed users at the end of each month for cost allocation. The IT admin grants her the **Reports Reader** role; she now signs into `admin.microsoft.com`, navigates to **Billing → Licenses**, exports CSV, and self-serves without bothering IT.

Best Practices

- **Use least privilege:** assign Helpdesk Admin to first-line support, not Global Admin.

- **Enable Targeted Release** on a small pilot group; this lets IT see new features before the org gets them.
- **Pin Message Center** so service announcements are visible.
- **Customize navigation** per role — many items are noise for license admins.

Common Errors and Troubleshooting

Issue	Cause	Fix
Cannot see admin center after assigning admin role	Role activation pending or browser cached old token	Sign out / sign back in; in PIM (P2) activate the role
Some panels show "Insufficient permissions"	Role doesn't cover that area (e.g., Helpdesk admin opening billing)	Assign appropriate role or contact higher-privilege admin
Service health page is empty	You're viewing personal scope, not org scope	Switch view; or check Microsoft 365 status page externally

Interview Questions and Answers

Q. Where do you reset a user password from?
Microsoft 365 Admin Center → Users → Active users → select user → Reset password. (Also possible in Entra Admin Center; both work.)

Q. Which role can reset other users' passwords but not admin passwords?
Helpdesk Administrator can reset passwords for non-admin users only.

Q. How do you enable a preview feature for testing?
Org settings → Release preferences → Targeted release for selected users.

Exam-Focused Notes

- Helpdesk Admin can reset only non-privileged user passwords.
- User Admin can create/delete users and reset non-admin passwords.
- License Admin can assign licenses but not create users.
- "Targeted release" is enabled in Org settings, not in Microsoft 365 Apps.

Hands-On Lab

LAB 1.6 — ADMIN CENTER TOUR

1. Sign in to admin.microsoft.com.
2. Find Tenant ID under Settings → Org settings → Organization profile.
3. Customize navigation: pin "Reports" and "Health".

4. Open Health → Service health and review any current advisories.
5. Open Setup and skim available guided wizards.
6. Use the "Admin centers" left-rail to launch Entra Admin Center.

Summary

- The M365 Admin Center is the primary GUI for day-to-day admin tasks.
- Specialized portals (Exchange, Teams, SharePoint, Entra, Intune, Defender, Purview) handle deeper configuration.
- Use least-privilege admin roles; Global Admin is for emergencies only.

1.7 Organizational Settings & Company Profile

Introduction

Organizational settings define how your Microsoft 365 tenant behaves for all users — display language, time zone, password policy expiration, release preferences, and external sharing defaults. These settings impact every user in the tenant and should be reviewed during initial setup and quarterly thereafter.

Why This Topic Is Important

A tenant configured with the wrong time zone will deliver calendar invites at the wrong time for an entire country. A tenant left on default password expiration will force every user to change passwords every 90 days even though current Microsoft guidance recommends "never expire" (with MFA enforced). One poorly-configured setting can cause organization-wide problems.

Key Concepts

Setting	What It Does	Where Configured
Organization Profile	Name, address, phone, technical contact, default language	Admin Center → Settings → Org settings → Organization profile
Release Preferences	Standard (everyone gets features on GA), Targeted (selected users get early), or Targeted for entire org	Org settings → Organization profile → Release preferences
Privacy Profile	Privacy statement URL shown to users	Org settings → Organization profile → Privacy profile
Password Expiration	Default 90 days, recommended "never" with MFA	Org settings → Security & privacy → Password expiration policy
Sharing Settings	Global toggles for guest, external, anonymous sharing	Org settings → Security & privacy → Sharing
Customer Lockbox	Requires admin approval for Microsoft engineers to access tenant data	Org settings → Security & privacy → Customer lockbox

Microsoft Portal Navigation

> 📍 Microsoft 365 Admin Center → `Settings` → `Org settings`

You will see three tabs: Services, Security & privacy, and Organization profile. Each contains dozens of granular settings — review them all once.

Step-by-Step Configuration

Setting the Organization Profile

1. Go to Admin Center → Settings → Org settings → Organization profile.
2. Click "Organization information".
3. Fill in: Name (displayed on receipts), Address (used for tax calculation), Phone, Technical contact (alerts go here), Preferred language.
4. Click Save.

Configuring Release Preferences

Targeted release lets you preview upcoming features 1–3 months before general availability — ideal for power users and IT staff:

1. Org settings → Organization profile → Release preferences.

2. Choose: Standard release (default), Targeted release for entire organization, or Targeted release for selected users.
3. If "selected users," add IT pilots and power users.
4. Save.

Best Practice
Always enable Targeted Release for IT/Help Desk staff. This way you see and break new features before users experience them on a Monday morning support call.

Password Expiration Policy

1. Org settings → Security & privacy → Password expiration policy.
2. Check "Set passwords to never expire (recommended)" or set days between password changes (1–730).
3. Save.

Security Note
NIST SP 800-63B and Microsoft both now recommend against periodic password expiration when MFA is in place. Forced rotation causes users to pick weaker, more predictable passwords. Enforce: long passphrases + MFA + banned password list + risk-based authentication.

PowerShell Commands

```
# Connect to Microsoft Graph
Connect-MgGraph -Scopes "Organization.ReadWrite.All"

# Get organization profile
Get-MgOrganization | Select-Object DisplayName,Street,City,Country,PreferredLanguage

# Get password expiration policy via domain (legacy MSOnline)
Connect-MsolService
Get-MsolPasswordPolicy -DomainName contoso.com
Set-MsolPasswordPolicy -DomainName contoso.com -ValidityPeriod 2147483647 -
NotificationDays 30
# 2147483647 days = practically "never expires"
```

Real-World Scenarios

Scenario: Multi-region company

A company headquartered in Karachi opens offices in Dubai and London. Each region needs locally-appropriate calendar defaults. Solution: keep tenant-wide language in English; let each user set their own region/time zone in Outlook Web (OWA → Settings → Language and time zone). Calendar invites then render correctly per attendee.

Common Errors and Troubleshooting

Problem	Cause	Solution
User can't change password	SSPR not enabled or password policy too restrictive	Enable SSPR in Entra ID; verify password policy
Settings changes don't appear	Caching in Admin Center	Hard refresh (Ctrl+F5); sign out and back in
Wrong time zone on meetings	User's personal Outlook time zone is wrong	OWA Settings → Calendar → set time zone

Interview Questions and Answers

Q: Why does Microsoft recommend disabling password expiration?

A: Forced periodic rotation leads to weaker passwords (predictable patterns like "Spring2026!"). With MFA enforced, password strength matters more than rotation. NIST SP 800-63B also recommends this approach.

Q: What is Customer Lockbox?

A: A control that requires explicit admin approval before Microsoft support engineers can access tenant data (such as during a support ticket). It provides an audit trail and protects against insider threats from the cloud provider itself.

Exam-Focused Notes

- Release preferences: Standard vs Targeted (entire org or specific users).
- Customer Lockbox is a Microsoft 365 E5 / dedicated SKU feature.
- Default password policy: 8 chars min, 90-day expiry (changeable).
- Setting password to "never expire" requires MFA per Microsoft guidance.

Summary

Section 1.7 Summary

- Organizational settings live under Admin Center → Settings → Org settings.
- Three tabs: Services, Security & privacy, Organization profile.
- Configure release preferences to pilot new features.
- Disable forced password expiration; require MFA instead.
- Enable Customer Lockbox in regulated environments.

1.8 Company Branding

Introduction

Microsoft Entra ID company branding lets you customize the sign-in experience users see when they authenticate to Microsoft 365, your own apps registered in Entra, and other federated services. A consistent visual identity helps users distinguish legitimate sign-in pages from phishing pages (a major security benefit beyond mere aesthetics).

Why This Topic Is Important

Phishing pages mimicking Microsoft sign-in are the #1 corporate credential theft vector. When users see a sign-in page with the corporate logo, custom background, and tagline they recognize, they're trained to be suspicious of generic-looking Microsoft pages — making credential harvesting harder.

Key Concepts

Element	What It Customizes	Asset Requirements
Background image	Behind the sign-in box	1920×1080 PNG/JPG, < 300 KB
Banner logo	Top-left of sign-in pages and Office 365 portal	280×60 PNG (transparent), < 10 KB
Square logo (light/dark)	App tiles, MFA prompts	240×240 PNG, < 50 KB
Sign-in page text	Username hint, helpful info	1024 chars max
Username hint	Suggests format like "alias@contoso.com"	64 chars max
Layout	Header, footer, hide self-service password reset, etc.	Toggle-based

Microsoft Portal Navigation

> 📍 Microsoft Entra Admin Center → `User experiences` → `Company branding`

(Older path: Entra ID → User experiences → Company branding.)

Step-by-Step Configuration

Customize Default Branding

1. Sign in to entra.microsoft.com as Global Admin or Organizational Branding Administrator.

2. Navigate to User experiences → Company branding.
3. Click "Customize" next to Default sign-in experience.
4. Upload background image (1920×1080 recommended).
5. Upload banner logo (280×60 PNG with transparent background).
6. Upload square logo for app tiles.
7. Enter sign-in page text (e.g., "For technical support, call extension 1234").
8. Enter username hint text (e.g., "yourname@contoso.com").
9. Configure footer with terms of use URL and privacy statement URL.
10. Review and Create.

Configure Language-Specific Branding

For multinational companies, configure different branding per browser language:

1. From the Company branding blade, click "Add language."
2. Select language (e.g., Spanish, French, German).
3. Repeat upload process with localized assets and translated text.
4. Browser language preference determines which set users see.

Best Practice
Use a distinctive background image — not a generic stock photo. The point is to be recognizable, not aesthetic. A photo of your office or a custom illustration helps users identify legitimate sign-in pages.

Real-World Scenarios

Scenario: Anti-phishing reinforcement

Contoso Bank conducted an internal phishing simulation. 18% of users clicked. After branding the sign-in experience with a distinctive blue background showing the bank's logo with the slogan "Always check for the blue background before entering credentials," and pairing this with awareness training, the next simulation showed only 4% click rate. The branding was a memorable visual anchor for the training message.

Security Considerations

- Branding helps users spot fake sign-in pages but is not a complete defense.
- Combine with MFA, Conditional Access, and user training.
- Use HTTPS-only image URLs; never link to assets from unverified hosts.
- Keep branding role (Organizational Branding Administrator) separate from Global Admin.

Common Errors and Troubleshooting

Issue	Resolution
Image too large	Compress (TinyPNG, ImageOptim) below the size limit
Changes not visible	Wait up to 1 hour; clear browser cache; open InPrivate window
Custom branding shows only after login	The sign-in URL must include tenant context (login.microsoftonline.com/contoso.com or use email domain hint)
"Show option to remain signed in" missing	Toggle in the Layout section of branding settings

Interview Questions and Answers

Q: How does company branding improve security?

A: By providing a consistent visual identity (custom logo, background, text), users become trained to recognize legitimate sign-in pages. This makes phishing pages that mimic generic Microsoft sign-in more obviously suspicious.

Q: Where do users see Entra ID company branding?

A: On login.microsoftonline.com when they specify the tenant (via email domain), Office.com portal headers, multi-factor authentication prompts, and any app federated to Entra ID.

Exam-Focused Notes

- Branding is configured in Entra Admin Center, not the M365 Admin Center.
- You can have multiple language-specific branding sets plus one default.
- Required role: Global Admin OR Organizational Branding Administrator.
- Branding does NOT customize the Outlook desktop client UI — only web sign-in.
- Free tier supports default branding; some advanced options need Entra ID P1/P2.

Lab 1.8 — Apply Company Branding

1. Sign in to Entra Admin Center as Global Admin.
2. Navigate to User experiences → Company branding.
3. Click Customize next to Default sign-in experience.
4. Download a free 1920×1080 background image (Unsplash, Pexels).
5. Create a 280×60 PNG banner logo using Canva or PowerPoint.
6. Upload both files; add sign-in page text "Welcome to Contoso. Need help? Call IT at x1234."
7. Save and wait 60 minutes.

8. Open InPrivate browser and go to login.microsoftonline.com → enter user@contoso.com.
9. Verify branding appears.

Summary

Section 1.8 Summary

- Branding customizes the Entra ID sign-in experience for users.
- Configure via Entra Admin Center → User experiences → Company branding.
- Add language-specific variants for multinational deployments.
- Helps users distinguish real sign-in from phishing.
- Requires Global Admin or Organizational Branding Administrator role.

1.9 Microsoft 365 Apps Deployment

Introduction

Microsoft 365 Apps for Enterprise (formerly Office 365 ProPlus, formerly Microsoft Office) is the desktop client suite: Word, Excel, PowerPoint, Outlook, OneNote, Teams (legacy), Access, Publisher. As an M365 admin, you control how these apps are installed, updated, and configured for thousands of devices.

Why This Topic Is Important

Bad deployment decisions cause real pain: users on different Office versions can't open each other's files, security patches are months behind, the wrong update channel breaks a critical Excel macro. Good deployment design ensures consistency, security, and predictability across the organization.

Key Concepts

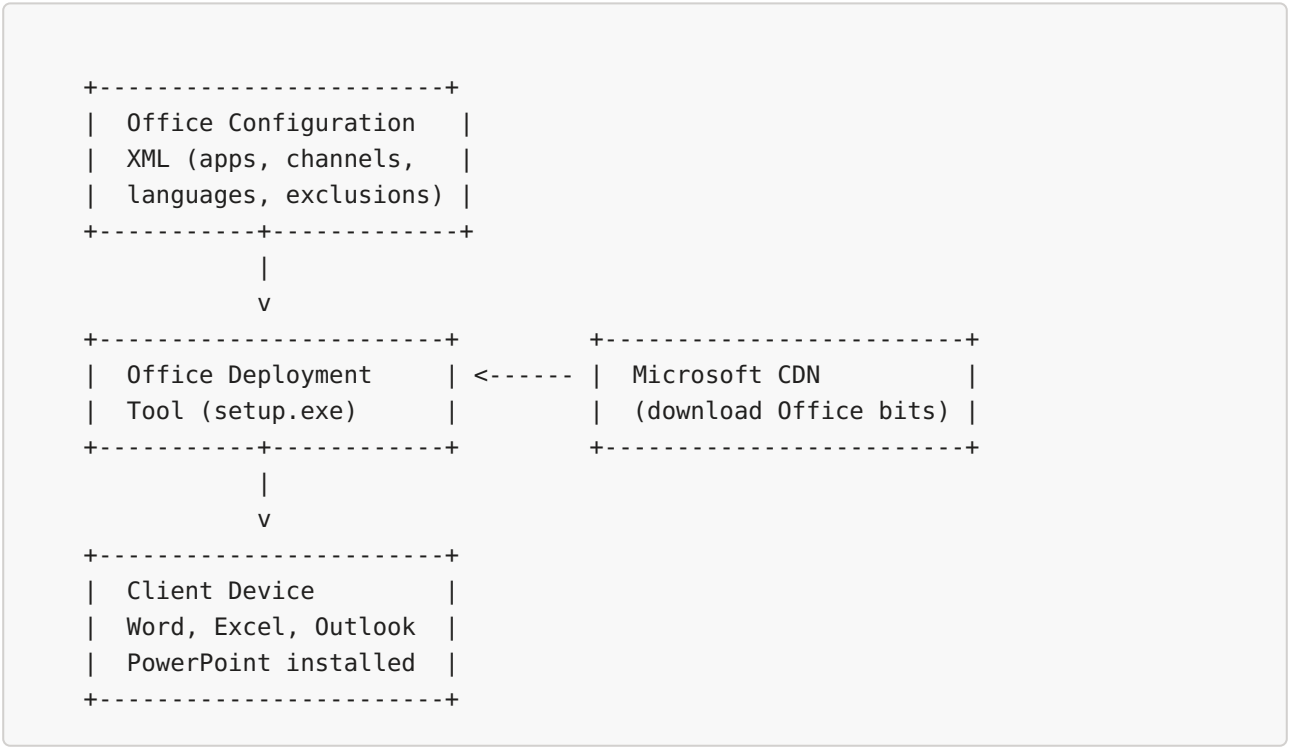
Update Channels

Channel	Release Cadence	Use Case
Current Channel	New features as released (~monthly)	Most users — get latest features
Monthly Enterprise Channel	Once monthly (predictable Patch Tuesday)	Enterprises wanting predictability
Semi-Annual Enterprise Channel	Every 6 months (Jan, Jul)	Heavily-tested environments, line-of-business apps
Semi-Annual Enterprise (Preview)	2 months before Semi-Annual GA	Pilot ring before semi-annual GA
Beta Channel	Pre-release, frequent	Insiders testing pre-release features

Deployment Methods

Method	How It Works	Best For
User-driven from portal	User signs into office.com → Install Office	BYOD, small business, remote users
Office Deployment Tool (ODT)	Script-driven install using XML config	IT admins, scripted deployments
Configuration Manager (MEMCM/SCCM)	On-prem deployment + updates	Large enterprises with existing CM
Microsoft Intune	Cloud-managed deployment to MDM-joined devices	Modern workplace
Apps for Business via M365 Admin	Pre-defined templates	SMB with simple needs

Architecture / Workflow



Microsoft Portal Navigation

📍 M365 Admin Center → `Setup` → `Deploy software updates`

📍 Microsoft Intune Admin Center → `Apps` → `Windows` → `+ Add` → `Microsoft 365 Apps`

Step-by-Step: Deploy via Office Deployment Tool (ODT)

1. Download ODT

Go to aka.ms/ODT, run the installer to extract setup.exe + sample XMLs.

2. Build Configuration XML

```
<Configuration>
  <Add OfficeClientEdition="64" Channel="MonthlyEnterprise">
    <Product ID="O365ProPlusRetail">
      <Language ID="en-us"/>
      <ExcludeApp ID="Groove"/>
      <ExcludeApp ID="Lync"/>
      <ExcludeApp ID="Bing"/>
    </Product>
  </Add>
  <Updates Enabled="TRUE" Channel="MonthlyEnterprise"/>
  <Display Level="None" AcceptEULA="TRUE"/>
  <Property Name="AUTOACTIVATE" Value="1"/>
  <Property Name="SharedComputerLicensing" Value="0"/>
</Configuration>
```

3. Download Office Bits

```
setup.exe /download configuration.xml
```

This downloads ~3 GB of Office files to the current folder.

4. Install

```
setup.exe /configure configuration.xml
```

5. Verify

Open Word → File → Account. Confirm version, channel, and licensing.

Step-by-Step: Deploy via Intune

1. Intune Admin Center → Apps → Windows → + Add → Microsoft 365 Apps.
2. Choose "Configuration designer" (GUI) or "XML data" (paste your ODT XML).
3. App suite: select Word, Excel, PowerPoint, Outlook, OneNote, OneDrive, Teams; exclude apps not needed (Access, Publisher).
4. Architecture: 64-bit (recommended for modern hardware).
5. Update channel: Monthly Enterprise.
6. Languages: English + any required.
7. Assign to a device or user group.
8. Click Create. Apps deploy automatically to Intune-managed devices.

Shared Computer Activation (SCA)

For shared devices (kiosks, hot-desks, RDP/VDI), enable SCA so multiple users can sign into Office on the same machine:

```
<Property Name="SharedComputerLicensing" Value="1"/>
```

- License token cached for ~30 days, refreshed on each sign-in.
- Required for Azure Virtual Desktop, Windows 365, and shared workstations.
- Each user must have an M365 Apps license assigned.

PowerShell Commands

```
# Check installed Office channel and version via registry
Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Office\ClickToRun\Configuration" |
    Select-Object UpdateChannel, VersionToReport, Platform

# Trigger Office update
& "C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe" /
update user

# Force update to a specific version
& "C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe" `
   /update user updatetoversion=16.0.16924.20000
```

Real-World Scenarios

Scenario: Critical Excel macro breaks after update

A finance team's macro stopped working after Office updated. Root cause: a deprecated Excel function. Solution: move the finance team to Semi-Annual Enterprise Channel (delays updates 6 months) while IT validates each update. Once tested, finance moves back to Monthly Enterprise.

Scenario: VDI deployment

An Azure Virtual Desktop pool runs 50 concurrent users. Each user signs in and out. Setting `SharedComputerLicensing = 1` prevents license token errors. Without SCA, only one user at a time can activate Office.

Best Practices

- Standardize on 64-bit Office unless you have add-ins that require 32-bit.
- Use Monthly Enterprise Channel as default — predictable monthly updates.
- Pilot Current Channel with IT before rolling out.

- Enable Shared Computer Activation only on VDI/RDS, not regular desktops.
- Exclude unused apps to save disk and reduce attack surface (Groove, Lync, OneDrive Groove are legacy).
- Keep Office Cloud Policy Service in mind for per-user policy targeting.

Common Errors and Troubleshooting

Error	Cause	Resolution
"Could not activate"	No license, network blocks activation endpoints	Verify license assignment; check firewall rules for *.officeapps.live.com
"Sorry, we ran into a problem"	Corrupt install	Run Office repair (Control Panel → Programs → Office → Change → Online Repair)
Mixed 32/64-bit conflict	Trying to install different bitness over existing	Uninstall first; use SaRA (Support and Recovery Assistant)
Outlook prompts repeatedly	Modern auth disabled or stale cached creds	Verify modern auth enabled in EXO; clear Credential Manager
Updates not applying	Group Policy blocks updates	Verify `Enable Automatic Updates` GPO is enabled

Interview Questions and Answers

Q: Compare Current Channel and Monthly Enterprise Channel.

A: Current Channel releases new features as soon as they ship (unpredictable timing). Monthly Enterprise Channel collects features and releases them on a predictable second-Tuesday cadence. Most enterprises pick Monthly Enterprise for IT predictability.

Q: When do you use Shared Computer Activation?

A: On shared devices: Azure Virtual Desktop, Windows 365 Cloud PCs, Remote Desktop Services hosts, kiosks. Each user signing in gets their own license token cached locally.

Q: What is the Office Deployment Tool?

A: A free command-line utility from Microsoft (setup.exe) that downloads and installs Microsoft 365 Apps using an XML configuration file. Used for unattended, scripted, or customized deployments.

Exam-Focused Notes

- 5 channels: Current, Monthly Enterprise, Semi-Annual Enterprise (+ Preview), Beta.
- Default channel changed multiple times — currently Current Channel for most new tenants.
- SCA is per-machine and requires explicit XML enablement.

- Office 365 Apps license is required even on shared devices (per-user).
- You can deploy from M365 Admin → Setup, Intune, SCCM, or ODT.

Lab 1.9 — Deploy Office via ODT

1. Download ODT from aka.ms/ODT to a test VM.
2. Extract and modify the included configuration.xml: set Channel="MonthlyEnterprise", exclude Access & Publisher.
3. Run `setup.exe /download configuration.xml` (waits while downloading).
4. Run `setup.exe /configure configuration.xml`.
5. Open Word → File → Account → verify channel and licensing.
6. Confirm Word and Excel installed but Access did not (per your exclusion).

Summary

Section 1.9 Summary

- Microsoft 365 Apps = Word/Excel/PowerPoint/Outlook/OneNote desktop suite.
- Five update channels — pick Monthly Enterprise for most enterprises.
- Deploy via M365 portal (user-driven), ODT (scripted), SCCM (on-prem), or Intune (cloud).
- Enable Shared Computer Activation for VDI / RDS.
- Exclude unused apps to reduce footprint.

1.10 Service Health Monitoring

Introduction

Microsoft 365 Service Health provides real-time visibility into the status of all Microsoft cloud services your tenant consumes — Exchange Online, Teams, SharePoint, OneDrive, Entra ID, Intune, and more. Service Health distinguishes between Microsoft-side incidents (their fault) and tenant-specific issues (yours).

Why This Topic Is Important

When users complain "Outlook is broken," the first question is: is it just us, or is Microsoft having an outage? Service Health answers this in seconds. Without it, IT wastes hours investigating problems Microsoft is already aware of and fixing.

Key Concepts

Health Statuses

Status	Meaning
Healthy	Service is fully operational
Advisory	Minor degradation, most users unaffected
Service degradation	Significant slowdown or limited functionality
Service interruption	Major outage, service unusable for many users
Restoring service	Microsoft has identified cause and is rolling out fix
Extended recovery	Fixed for new connections, residual impact for some
Investigating	Issue identified but cause unknown
Service restored	Resolved; post-incident report (PIR) may follow
False positive	Initial signal wasn't a real issue
Post-incident report published	Microsoft has issued detailed root-cause analysis

Incident IDs

Every issue has a unique ID with prefix:

- **EX** = Exchange Online
- **SP** = SharePoint Online
- **OD** = OneDrive
- **TM** = Teams
- **MO** = Microsoft 365 suite
- **OP** = Office Portal
- **DZ** = Identity (Entra)
- **IN** = Intune

Microsoft Portal Navigation

> 📍 M365 Admin Center → `Health` → `Service health`

Step-by-Step: Monitor Service Health

1. Sign in to admin.microsoft.com as Global Reader, Service Support Admin, or higher.
2. Click Health → Service health.
3. Review the dashboard: active issues sorted by severity.
4. Click any issue to see details: affected workload, scope (your tenant or global), timeline, root cause (when known).
5. Click "Get help" to open a support ticket if needed.
6. Pin the Service Health dashboard to your Admin Center home.

Configure Service Health Notifications

1. Service health → Preferences (top right).
2. Enable email notifications.
3. Add up to 2 email addresses (distribution lists allowed).
4. Select severity levels: incidents only, or incidents + advisories.
5. Select which services trigger notifications.
6. Save.

Best Practice
Subscribe your NOC distribution list and your helpdesk leads. Have helpdesk display the Service Health dashboard on a shared screen so they see incidents before users call.

Message Center vs Service Health

Feature	Message Center	Service Health
What it tells you	Upcoming changes (new features, retirements, security)	Current incidents and degradations
Timeline	Days to months in advance	Real-time
Source	Microsoft Roadmap	Microsoft service monitoring
Use case	Plan changes ahead	React to outages now

PowerShell / Graph API

```
# Connect to Microsoft Graph
Connect-MgGraph -Scopes "ServiceHealth.Read.All"

# Get all current service health issues
Get-MgServiceAnnouncementIssue -All |
    Select-Object Id, Title, Service, Status, StartDateTime |
    Format-Table

# Get only active issues
Get-MgServiceAnnouncementIssue -All |
    Where-Object { $_.IsResolved -eq $false }

# Get message center messages
Get-MgServiceAnnouncementMessage -All |
    Select-Object Id, Title, Category, StartDateTime |
    Sort-Object StartDateTime -Descending |
    Select-Object -First 20
```

Real-World Scenarios

Scenario: Global Teams outage

On a Monday morning, helpdesk calls spike. Service Health shows incident TM123456 — Teams chat impaired in EMEA region. Helpdesk posts a banner on the company intranet. Support tickets drop by 80% because users see the announcement. Microsoft resolves in 2 hours; helpdesk removes the banner.

Best Practices

- Configure email notifications to a monitoring inbox.
- Train helpdesk to check Service Health BEFORE investigating user complaints.
- Use the Service Health Status Reporter Power BI template for management dashboards.
- Maintain an "outage communication" playbook with template messages.
- Integrate with monitoring (Azure Monitor, ServiceNow, Datadog) via Graph API or Office 365 Communications API.

Common Errors and Troubleshooting

Issue	Resolution
"You don't have permission to view service health"	Need at least Service Support Administrator, Global Reader, or higher role
Not seeing email notifications	Verify preferences saved; check spam folder; sender is mc-noreply@microsoft.com
"No active issues" but users report problems	Issue may be tenant-specific; open support ticket; verify from Microsoft 365 status Twitter (@MSFT365Status)

Interview Questions and Answers

Q: What's the difference between Message Center and Service Health?

A: Message Center announces planned changes (new features, deprecations, security alerts) — often days to months ahead. Service Health reports current operational issues (outages, degradations) in real time. Both live under Admin Center → Health.

Q: What admin role is required to view Service Health?

A: Global Reader (view-only), Service Support Administrator (can open tickets), or higher roles like Global Admin. Use least privilege — Service Support Admin is typical for helpdesk.

Exam-Focused Notes

- Service Health vs Message Center is a common exam question.
- Incident prefixes (EX, TM, SP, OD, DZ) identify affected workloads.
- Notifications go to up to 2 email addresses (use DLs for more).
- Service Health Status Reporter is a Power BI template — useful for execs.
- Graph API endpoints: `/admin/serviceAnnouncement/issues` and `/messages`.

Lab 1.10 — Service Health Setup

1. Sign in to admin.microsoft.com.
2. Navigate to Health → Service health.
3. Click Preferences → enable email notifications.
4. Add helpdesk@contoso.com and select all severity levels for Exchange + Teams.
5. Save.
6. Pin Service Health to home: click ⋯ → Pin.

7. Open PowerShell, run the Graph cmdlets above to enumerate active issues.

Summary

Section 1.10 Summary

- Service Health = real-time outage and degradation reporting.
- Message Center = upcoming changes and announcements.
- Configure email notifications to monitoring inbox.
- Use Graph API for programmatic integration.
- Role: Service Support Administrator (least privilege).

1.11 Microsoft 365 Reporting

Introduction

Microsoft 365 reports tell you who is using what, how much, and where adoption is strong or weak. Reports cover Exchange (email volume, mailbox usage), Teams (active users, meetings, calls), SharePoint & OneDrive (storage, sharing), Yammer, Forms, Stream, and licensing.

Why This Topic Is Important

Reports drive evidence-based IT decisions: license optimization (don't pay for Teams users who never log in), security monitoring (sudden spike in external sharing), adoption planning (which department needs Teams training). Without reports, you fly blind.

Key Concepts

Report Categories

Category	Reports
Usage	Active users, app usage, email activity, Teams activity, SharePoint activity, OneDrive activity, Yammer activity
Productivity Score	Composite metric measuring digital habits and tech experiences
Security & Compliance	DLP matches, label usage, threat detections, audit log searches
Adoption	License utilization, training recommendations
Service-specific	Inside Exchange / Teams / SharePoint admin centers

Report Retention

- Default usage reports: 7, 30, 90, or 180 days lookback.
- Audit log: 90 days standard, 1 year with E5, 10 years with E5 + Audit Premium add-on.
- Reports anonymize user identifiers by default (configurable).

Microsoft Portal Navigation

> 📍 M365 Admin Center → `Reports` → `Usage`

> 📍 Defender Portal → `Reports` (security reports)

> 📍 Purview Portal → `Reports` (compliance reports)

Step-by-Step: Run Usage Reports

1. Sign in to admin.microsoft.com.
2. Reports → Usage.
3. Select a workload (e.g., Microsoft Teams).
4. Choose date range: 7/30/90/180 days.
5. Review charts: active users, user activity, device usage.
6. Click "View more" for granular per-user data.
7. Export to CSV for further analysis.

Disable Anonymization

By default, reports show users as "User1, User2, ..." to protect privacy. To see actual usernames:

1. Admin Center → Settings → Org settings → Reports.
2. Uncheck "Display concealed user, group, and site names in all reports."
3. Save.

Privacy Note
Disabling anonymization may violate GDPR or local privacy law in some jurisdictions. Consult legal/compliance before disabling. EU customers should usually keep anonymization on except during targeted investigations.

PowerShell & Graph Reporting API

```
# Connect
Connect-MgGraph -Scopes "Reports.Read.All"

# Email activity - last 30 days
Get-MgReportEmailActivityUserDetail -Period D30 -OutFile email_activity.csv

# Teams user activity
Get-MgReportTeamUserActivityUserDetail -Period D30 -OutFile teams_activity.csv

# OneDrive usage
Get-MgReportOneDriveUsageAccountDetail -Period D30 -OutFile onedrive.csv

# SharePoint site usage
Get-MgReportSharePointSiteUsageDetail -Period D30 -OutFile sharepoint.csv

# Active users across the suite
Get-MgReportOffice365ActiveUserDetail -Period D30 -OutFile active_users.csv
```

Power BI Adoption Content Pack

Microsoft provides a free Power BI template app called "Microsoft 365 Usage Analytics" that builds rich dashboards over your usage data:

1. In M365 Admin Center → Reports → Usage → click "Get Power BI."
2. Enable the data feed (one-time).
3. Sign in to Power BI service.
4. Install "Microsoft 365 Usage Analytics" template app.
5. Connect to your tenant ID.
6. Dashboards refresh daily.

Real-World Scenarios

Scenario: License optimization

An E5 tenant has 500 licenses costing $57/user/month = $342k/year. Reports show 80 users haven't signed in for 90+ days. Downgrade those to E1 ($10/user/month) saving $45k/year. The CFO loves you.

Scenario: Teams adoption

After Teams rollout, management asks "is anyone using it?" The Teams Usage report shows 60% active users in Sales but only 15% in Operations. IT designs targeted training for Operations. Within 60 days, Operations climbs to 75% active users.

Best Practices

- Schedule monthly review of usage reports.
- Identify zero-activity licensed users — reclaim or downgrade.
- Track adoption per department to focus training.
- Combine usage data with HR data (department, location) for executive dashboards.
- Keep anonymization on unless you have a legitimate investigation need.
- Use Graph API for automated, scheduled exports to a data warehouse.

Common Errors and Troubleshooting

Issue	Resolution
Reports show "loading" forever	Allow up to 48 hours after tenant creation for first data; refresh after
Per-user names hidden	Anonymization is on; disable in Org settings → Reports if permitted
"No data available"	Tenant may be too new; or service not licensed; or user has Reports Reader role missing
CSV export missing columns	Permissions issue; ensure Reports Reader or Global Reader role

Interview Questions and Answers

Q: How do you find unused Microsoft 365 licenses?

A: Run the Office 365 Active Users report (or use `Get-MgReportOffice365ActiveUserDetail`) for 90+ days. Filter for users with no activity across all workloads, then cross-reference with license assignments to identify candidates for downgrade or removal.

Q: How long does Microsoft retain usage reports?

A: Lookback windows of 7, 30, 90, and 180 days in the admin center. Beyond that, you must export and store data yourself, or use Power BI Usage Analytics which retains 12+ months in the dataset.

Exam-Focused Notes

- Anonymization is ON by default — exam loves this question.
- Reports Reader is the least-privilege role for viewing.
- Power BI Usage Analytics is FREE for M365 tenants.
- Date ranges: 7/30/90/180 days.
- Use Graph API `/reports/` endpoints for automation.

Lab 1.11 — Generate Usage Reports

1. Admin Center → Reports → Usage.
2. Open "Email activity" — 30-day view.
3. Export CSV; open in Excel.
4. Open PowerShell, install Microsoft.Graph module if needed.
5. Run: `Connect-MgGraph -Scopes "Reports.Read.All"`
6. Run: `Get-MgReportEmailActivityUserDetail -Period D30 -OutFile email.csv`
7. Compare with GUI export.

Summary

Section 1.11 Summary

- Usage reports under Admin Center → Reports → Usage.
- Anonymization on by default — toggle in Org settings → Reports.
- 7/30/90/180 day windows.
- Use Graph API for automation; Power BI for dashboards.
- Drives license optimization, adoption planning, security monitoring.

1.12 Billing and Subscription Management

Introduction

Billing in Microsoft 365 covers subscription purchases, license assignment, invoices, payment methods, cost centers, billing notifications, and renewals. Most M365 admins won't be billing admins, but understanding the model is essential — license problems are the #1 cause of "user can't access" tickets.

Why This Topic Is Important

Subscriptions silently expire and disable users. Trial licenses convert to paid (or get deleted with data). Annual commitments lock you in. Mid-year SKU changes are penalized. Misunderstanding billing causes both unexpected costs and unexpected outages.

Key Concepts

Subscription Types

Type	Commitment	Best For
Monthly	Pay each month, no commitment	Variable headcount, short-term needs (higher per-user cost)
Annual (Pay monthly)	1-year commitment, pay each month	Stable headcount, want monthly cash flow
Annual (Pay yearly)	1-year commitment, pay upfront	Lowest per-user cost, willing to commit cash
Three-year (CSP)	3-year commitment via partner	Mature deployments, deep discounts

License States

State	Meaning	Duration
Active	License paid, users functioning	—
Expired	Past expiration, users still function	30 days
Disabled	Users blocked from signing in	Days 31–90
Deprovisioned	Tenant data being deleted	Days 91–180
Removed	All data deleted	Day 180+

Warning
After 90 days, mailbox and OneDrive data are progressively deleted. Recovery requires opening a support ticket BEFORE day 180. After day 180 data is generally unrecoverable.

Microsoft Portal Navigation

📍 M365 Admin Center → `Billing` → `Your products`

> 📍 Billing → `Bills & payments`

> 📍 Billing → `Billing accounts` (for multi-account orgs)

Step-by-Step: Purchase Additional Licenses

1. Admin Center → Billing → Your products.
2. Find subscription → click "+ Buy licenses."
3. Enter quantity → review price.
4. Confirm. New licenses immediately available to assign.

Step-by-Step: Remove Licenses

1. Billing → Your products → subscription → "Remove licenses."
2. Enter new (lower) total.
3. Note: removing licenses while users have them assigned will unassign first.
4. Pro-rated credit on next bill if annual commitment, none if monthly.

Step-by-Step: Change Payment Method

1. Billing → Bills & payments → Payment methods.
2. + Add a payment method (credit card, bank account, or invoice for enterprise).
3. Mark default.
4. For enterprises: contact Microsoft to switch to invoice billing (NET 30 typically).

Cost Centers and Billing Account Hierarchy

For multi-entity organizations:

- **Billing account** — the legal entity that pays.
- **Billing profile** — invoice / payment method per business unit.
- **Invoice section** — show different costs on the same invoice.

PowerShell Commands

```
# Connect
Connect-MgGraph -Scopes "Organization.Read.All", "Directory.Read.All"

# List all subscriptions in tenant
Get-MgSubscribedSku |
    Select-Object SkuPartNumber,
@{Name="Total";Expression={$_.PrepaidUnits.Enabled}}, ConsumedUnits

# Check expiration / status
Get-MgSubscribedSku | Select-Object SkuPartNumber, CapabilityStatus, ConsumedUnits

# MSCommerce module for purchase decisions (insider only)
# Most billing actions are GUI-only - no full PowerShell parity
```

Real-World Scenarios

Scenario: Trial expires, users locked out

An admin signed up for an E5 trial 30 days ago and forgot. On day 31, all users lose access to Defender features and Power BI Pro. To recover: convert the trial to paid (1-click in Admin Center → Billing → Trials), OR cancel and the tenant remains on the lower SKU. Data is preserved.

Scenario: Annual renewal coming up

A 200-user E3 annual subscription auto-renews in 14 days. The CFO wants to reduce to 175 because of layoffs. The renewal page shows the new commit (175 × E3 annual). Confirm before the auto-renew date or risk paying for 200 again.

Best Practices

- Set billing notifications to a shared finance + IT mailbox.
- Review subscriptions quarterly for over-licensing.
- Don't let trials silently convert — calendar-block 25 days after trial start.
- Use Group-Based Licensing to ensure licenses follow employees.
- Reconcile license counts with HR onboarding/offboarding monthly.
- Document subscription end-dates centrally (Excel or ServiceNow CMDB).

Common Errors and Troubleshooting

Issue	Resolution
"You don't have enough licenses"	Buy more or unassign from unused users
License assigned but features missing	Verify sub-services enabled within the license; replication can take 1–6 hours
Card declined	Update payment method; review with bank; check international transaction limits
Subscription expired unexpectedly	Check Billing → Bills & payments for failed payment; reactivate within 90 days
"You can't reduce licenses below assigned"	Unassign first, then reduce

Interview Questions and Answers

Q: What happens to user data after a subscription expires?

A: Days 1–30 (Expired): users continue working. Days 31–90 (Disabled): users blocked from signing in. Days 91–180 (Deprovisioned): tenant data progressively deleted. After 180 days: data unrecoverable.

Q: What's the difference between billing account, billing profile, and invoice section?

A: Billing account = legal entity paying Microsoft. Billing profile = invoice / payment method within an account. Invoice section = line-item grouping on a single invoice (departments, cost centers).

Exam-Focused Notes

- 30/90/180 day timeline after subscription expiry is exam-critical.
- Annual commitment = lower per-user price.
- You cannot reduce licenses below assigned count — unassign first.
- Trial → Paid conversion preserves all data and settings.
- Billing admin role: Billing Administrator (least privilege for billing tasks).

Lab 1.12 — Billing & Subscriptions

1. Admin Center → Billing → Your products. Note current subscriptions and seat counts.
2. Billing → Bills & payments → review last 3 invoices.
3. Billing → Billing notifications → add finance@contoso.com.
4. Run `Get-MgSubscribedSku` in PowerShell. Compare to GUI.

5. Calculate: if your tenant has X E3 + Y E5 at current prices, what's the monthly cost?

Summary

Section 1.12 Summary

- Subscriptions: monthly, annual (monthly pay), annual (yearly pay), 3-year CSP.
- After expiry: 30 days expired → 60 days disabled → 90 days deprovisioned → 180 days deleted.
- Billing portal manages subscriptions, payments, invoices.
- Use Group-Based Licensing for HR-driven assignment.
- Review subscriptions quarterly to control cost.

1.13 Hybrid Identity Overview

Introduction

Hybrid identity is the architecture where an on-premises Active Directory Domain Services (AD DS) coexists with Microsoft Entra ID, with user accounts and credentials synchronized between them. Most enterprises with existing on-prem AD adopt hybrid identity rather than starting fresh in the cloud.

Why This Topic Is Important

Few large organizations are 100% cloud-native. Hybrid identity lets users use the same username and password for on-prem file servers, line-of-business apps, AND Microsoft 365. Done well, users don't notice the transition. Done poorly, users have multiple passwords and complain endlessly.

Key Concepts

Identity Models

Model	Description	When Used
Cloud-only	Users exist only in Entra ID. No on-prem AD.	Startups, SMBs, fully cloud-native
Synchronized identity	On-prem AD users sync to Entra; password hashes also sync (PHS)	Most enterprises — simplest hybrid
Federated identity	AD FS or third-party IdP authenticates; Entra trusts the federation	Strict compliance, custom auth, smart cards
Pass-Through Authentication (PTA)	Cloud auth pings on-prem AD in real time	Don't want password hashes in cloud, but no AD FS infrastructure

Sign-In Methods

Method	How It Works	Pros	Cons
Password Hash Sync (PHS)	Hash-of-hash sent to Entra; auth happens in cloud	Simplest, no on-prem dependency for auth, supports leaked-credentials protection	Password hash (one-way) stored in cloud
Pass-Through Authentication (PTA)	Cloud sends auth request to on-prem agent which validates against AD	No hashes in cloud, real-time enforcement of on-prem policies	Requires agents online; latency
Federation (AD FS)	Entra redirects user to on-prem AD FS for authentication	Full control, smart card / cert auth	Complex infra, single point of failure
Seamless SSO	Add-on to PHS or PTA; transparent Kerberos auth on domain-joined machines	No prompts at all on domain devices	Domain-joined only

Architecture / Workflow — PHS Sign-In

```
[User] ----credentials---> [Browser/Outlook] -----> [login.microsoftonline.com]
                                                              |
                                                              | (validates hash)
                                                              v
                                                      [Entra ID auth]
                                                              |
                                                              v
                                                    [Issue token to app]

Meanwhile, on-premises:
[On-prem AD] <--every 2 min sync-- [Entra Connect Sync server]
                                              |
                                              v hash-of-hash
                                     [Entra ID directory]
```

Microsoft Portal Navigation

📍 Entra Admin Center → `Identity` → `Hybrid management` → `Entra Connect`

Choosing the Right Model

Requirement	Recommended Method
Simplest, fewest moving parts	PHS + Seamless SSO
Don't store password hashes in cloud	PTA + Seamless SSO
Smart card or PKI authentication	Federation (AD FS or third-party)
Multi-factor enforced on-prem	PTA or Federation
Auditable on-prem auth events	PTA or Federation
Cloud-only authentication	Move away from federation; use PHS

Microsoft Recommendation

Microsoft now recommends PHS + Seamless SSO for the vast majority of organizations. Federation is being deprecated in favour of cloud-native authentication for resilience and security (e.g., during AD FS outages, PHS-based tenants keep working).

Real-World Scenarios

Scenario: AD FS outage

A company federated to on-prem AD FS. The AD FS server crashes at 9 AM Monday. All Microsoft 365 access stops — users can't read email, attend Teams meetings, or open files. Recovery takes 4 hours. Lesson: Federation = SPOF. Migrating to PHS would have avoided this entirely.

Scenario: Acquisition

Contoso acquires Fabrikam. Fabrikam has its own AD forest. Solution: extend Entra Connect to sync both forests into the single Contoso tenant; users keep working with their existing AD passwords until consolidation.

Security Considerations

- PHS stores a hash-of-hash — not the password — in Entra. Microsoft cannot derive the original password.
- PHS enables Entra ID Protection's "leaked credentials" detection (compares against credentials found in breaches).
- Federation places auth on your on-prem AD FS — protect this with MFA, lockout, and high availability.
- Seamless SSO requires the AZUREADSSOACC computer account; rotate its kerberos key every 30 days.

Common Errors and Troubleshooting

Issue	Resolution
"User not found" in cloud	Verify object synced; check UPN matches a verified domain
UPN suffix not routable	Add UPN suffix in AD; verify domain in Entra; bulk-update users
Password change on prem not reflecting in cloud	Force sync: `Start-ADSyncSyncCycle -PolicyType Delta`
Federation outage	Convert to managed authentication: `Set-MsolDomainAuthentication -DomainName contoso.com -Authentication Managed`

Interview Questions and Answers

Q: What are the three sign-in methods in hybrid identity?

A: (1) Password Hash Sync (PHS) — hash-of-hash to cloud, cloud auth; (2) Pass-Through Authentication (PTA) — agent validates against on-prem AD in real time; (3) Federation — AD FS or third-party IdP handles auth, Entra trusts it.

Q: Why does Microsoft recommend PHS over Federation?

A: PHS removes the on-prem authentication infrastructure as a single point of failure. If on-prem AD goes down, cloud authentication continues. PHS also enables Entra ID Protection's leaked-credential detection.

Exam-Focused Notes

- PHS = hash-of-hash (one-way), syncs every 2 minutes.
- PTA = real-time, requires at least one agent (HA = 3+).
- Federation = AD FS or third-party; complex; being deprecated.
- Seamless SSO = transparent Kerberos auth on domain-joined Windows.
- Default sync cycle = 30 minutes; can be triggered manually.

Summary

Section 1.13 Summary

- Hybrid identity = on-prem AD + Entra ID, kept in sync.
- Three sign-in methods: PHS, PTA, Federation.
- Microsoft recommends PHS + Seamless SSO for most.
- Federation requires AD FS — complex and SPOF.
- Sync interval default 30 min; password write-back optional with Entra ID P1.

1.14 Microsoft Entra Connect Overview

Introduction

Microsoft Entra Connect (formerly Azure AD Connect, formerly DirSync) is the synchronization engine that copies user, group, and contact objects from on-premises Active Directory to Microsoft Entra ID. It runs as a Windows Service on a domain-joined server and is the heart of hybrid identity.

Why This Topic Is Important

Entra Connect is the bridge that lets on-prem AD users access Microsoft 365 seamlessly. A broken sync means new hires can't log in, password changes don't replicate, and group membership is stale. Every M365 admin in a hybrid environment must understand at least the basics.

Versions: Entra Connect vs Entra Cloud Sync

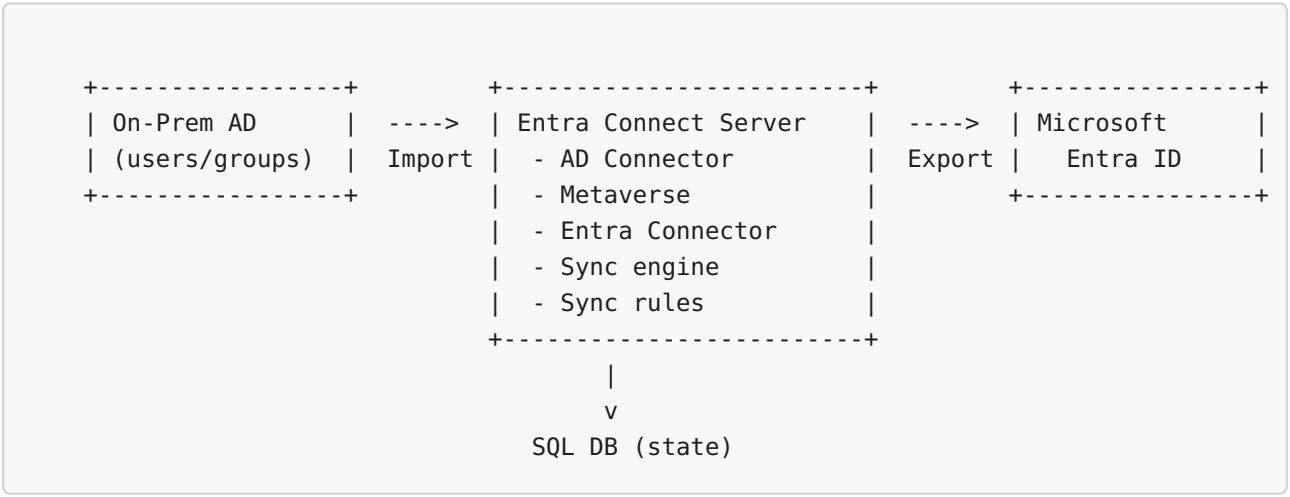
Feature	Entra Connect Sync	Entra Cloud Sync
Installation	Windows server (on-prem)	Lightweight agent (on-prem)
Sync engine location	On-prem	Cloud
Customization	Extensive (sync rules, attribute flow)	Limited (basic mapping)
Multi-forest	Yes (single agent)	Yes (one agent per forest)
Hash sync, PTA	Yes	Yes
Group write-back	Yes	Limited
Sync interval	30 min default	2 min
Recommendation	Complex environments	Simple environments, modern deployments

Note
Microsoft is gradually pushing customers toward Cloud Sync for new deployments. Existing Entra Connect deployments continue to be supported.

Key Components

Component	Purpose
Sync Engine	The Windows service that orchestrates sync cycles
Connectors	One per directory (AD, Entra ID); pulls and pushes data
Metaverse	Internal in-memory holding space joining objects across directories
Sync rules	How attributes flow and which objects are in scope
Connector spaces	Staging area per connector before metaverse
SQL Server	Backs the sync engine (LocalDB by default, full SQL for larger orgs)

Architecture / Workflow



Sync Steps (each cycle)

1. **Import** — read changes from each source (AD, Entra)
2. **Synchronization** — apply rules, populate metaverse, calculate exports
3. **Export** — push changes outbound to each target

Filtering — Choosing What Syncs

Filter Type	How It Works
Domain-based	Sync only specific AD domains in a forest
OU-based	Sync only specific Organizational Units
Group-based	Sync only members of a specific AD group
Attribute-based	Custom: e.g., sync only if extensionAttribute1 = "M365User"

Best Practice

Always start with OU-based filtering for first deployment — sync a pilot OU first to validate before expanding.

Step-by-Step: Install Entra Connect

1. Prepare Windows Server 2019/2022, domain-joined, 4 GB RAM minimum, 70 GB disk.
2. Sign in as Domain Admin to the future Entra Connect server.
3. Download Entra Connect from aka.ms/AzureADConnect.
4. Run AzureADConnect.msi; agree to license.
5. Choose "Express settings" (PHS + SSO) for simple deployments, or "Customize" for advanced.

6. Enter Global Admin credentials for Entra ID.
7. Enter Enterprise Admin credentials for on-prem AD.
8. Optionally configure OU filtering.
9. Optionally enable Seamless SSO and password write-back (P1 license).
10. Click Install — initial sync starts.
11. Monitor via Synchronization Service Manager (miisclient.exe).

PowerShell Commands

```
# Import the Entra Connect module
Import-Module ADSync

# Force a delta sync
Start-ADSyncSyncCycle -PolicyType Delta

# Force a full initial sync
Start-ADSyncSyncCycle -PolicyType Initial

# Get the current scheduler config
Get-ADSyncScheduler

# Disable scheduled sync (for maintenance)
Set-ADSyncScheduler -SyncCycleEnabled $false

# Re-enable
Set-ADSyncScheduler -SyncCycleEnabled $true

# Check connector status
Get-ADSyncConnector | Select-Object Name, Type, Identifier

# From Entra side
Connect-MgGraph -Scopes "Directory.Read.All"
Get-MgDirectoryObject -DirectoryObjectId <userId>
```

Monitoring Sync Health

Entra Connect Health provides cloud-based monitoring of sync, AD FS, and AD DS infrastructure:

1. Entra Admin Center → Identity → Hybrid management → Entra Connect → Entra Connect Health.
2. Install the Health agent on the Entra Connect server.
3. Dashboards show sync errors, last sync time, attribute conflicts.
4. Configure email alerts for failures.

Warning
Entra Connect Health requires Entra ID P1 or higher for the synced users. Without P1, you can install the agent but won't see all the metrics.

Real-World Scenarios

Scenario: Disabled user still has access

An employee is fired. HR disables their AD account at 5 PM. At 6 PM the employee can still read corporate email via Outlook Mobile. Cause: Entra Connect last synced at 4:55 PM, next sync at 5:25 PM. Solution: Force sync immediately with `Start-ADSyncSyncCycle -PolicyType Delta`. For terminations, also revoke Entra ID sessions and tokens.

Scenario: Sync stops working

Monday morning: helpdesk reports new hires aren't appearing in M365. Investigation: Entra Connect service stopped on the server. Restart service (`Start-Service ADSync`) and run delta sync. Add a watchdog: monitoring tool that alerts when ADSync service is not Running.

Best Practices

- Deploy Entra Connect on a dedicated server, not a domain controller.
- Install staging mode server as backup (read-only second copy).
- Use full SQL Server for > 100,000 objects.
- Monitor sync health via Entra Connect Health.
- Keep Entra Connect updated — Microsoft releases patches monthly.
- Document customizations (sync rules, attribute mappings) — they survive upgrades but knowing them matters.
- Backup the configuration: `Export-AdSyncConfiguration`.

Common Errors and Troubleshooting

Error	Cause	Solution
"Object cannot be exported - QuarantinedAttributeValueMustBeUnique"	Duplicate UPN or proxyAddress	Resolve duplicate in on-prem AD
"InvalidSoftMatch"	UPN clash with existing cloud-only user	Remove or rename cloud user
"FederatedDomainChangeError"	Domain federation change misaligned	Use `Convert-MsolFederatedUser`
Sync taking hours	Initial sync with large directory	Patience; consider SQL Server upgrade
Sync errors in dashboard	Bad data on prem	Use IdFix tool to find and fix data errors before sync

Interview Questions and Answers

Q: What's the difference between Entra Connect Sync and Entra Cloud Sync?

A: Entra Connect Sync runs the sync engine on-prem, supports complex customizations, single agent for multi-forest. Cloud Sync runs the sync engine in the cloud, requires only a lightweight agent on-prem, simpler config, less customization. Microsoft recommends Cloud Sync for new, simple deployments.

Q: What is staging mode?

A: A read-only secondary Entra Connect server that performs all sync operations except export. Use it as a hot standby — if primary fails, promote staging to active. Also useful for testing config changes before they take effect.

Q: How often does sync run?

A: Default 30 minutes for Entra Connect, 2 minutes for Cloud Sync. Can be triggered manually with `Start-ADSyncSyncCycle -PolicyType Delta`. Password hash sync happens every 2 minutes regardless.

Exam-Focused Notes

- Default sync = 30 min; password hash sync = 2 min.
- Cloud Sync default sync = 2 min.
- One active Entra Connect per tenant + multiple staging mode servers.
- Required ports: 443 outbound from server to Microsoft endpoints.
- IdFix tool fixes UPN / proxyAddress issues before first sync.

- Hard match = ImmutableID; soft match = UPN/Mail.

Lab 1.14 — Entra Connect Operations

1. If lab AD available: install Entra Connect on a Windows Server VM.
2. Choose Express settings, sync a test OU only.
3. Wait for first sync; verify users appear in Entra Admin Center.
4. Make a change in AD (add a user); run `Start-ADSyncSyncCycle -PolicyType Delta`.
5. Verify new user appears within 2-3 minutes.
6. Open Synchronization Service Manager (miisclient.exe); view connector run history.
7. Install Entra Connect Health agent; verify dashboards.

Summary

Section 1.14 Summary

- Entra Connect = sync engine between on-prem AD and Entra ID.
- Two flavours: Entra Connect Sync (on-prem engine) and Cloud Sync (cloud engine, lightweight agent).
- Default sync 30 min (Connect) / 2 min (Cloud Sync); password hash sync 2 min.
- Filter by OU, domain, group, or attribute.
- Use staging mode for HA / testing.
- Monitor with Entra Connect Health.

Section 1 — Wrap-Up: Tenant Management Mastery

Section 1 Key Takeaways

Section 1 Synthesis

- **Architecture:** M365 = bundle of services (EXO + SPO + ODB + Teams + Entra + Intune + Purview + Defender) tied to a single Entra ID tenant.
- **Licensing:** SKUs (E1/E3/E5/F1/F3, A1/A3/A5, etc.) bundle service plans; assign to users or groups.
- **Tenant:** created once at tenant signup; you cannot rename .onmicrosoft.com.
- **Custom domain:** add via DNS TXT/MX/CNAME verification, then assign as user UPN suffix.
- **Admin Center:** central hub with specialized portals for each workload.
- **Branding:** customize sign-in for security and identity.
- **Apps:** deploy via ODT, Intune, SCCM; pick the right update channel.
- **Health:** Service Health (now) and Message Center (future).
- **Reports:** usage, security, compliance — drive optimization.

- **Billing:** 30/90/180-day timeline after expiry; review quarterly.
- **Hybrid:** PHS, PTA, Federation — pick PHS + Seamless SSO by default.
- **Entra Connect:** the bridge; sync every 30 min (or 2 min for Cloud Sync).

Section 1 Mini Quiz

Quiz — 10 Questions

Q1. What is the default tenant suffix when you sign up for M365?

A: contoso.onmicrosoft.com

Q2. After subscription expiration, how many days until users are blocked from signing in?

A: 30 days (then 31-90 days disabled, 91-180 deprovisioned)

Q3. Which DNS record proves domain ownership during tenant verification?

A: TXT record with a Microsoft-provided value (or MX with MS=ms#### value)

Q4. Default Entra Connect sync interval?

A: 30 minutes (delta)

Q5. Which sign-in method does Microsoft recommend for most enterprises?

A: Password Hash Sync (PHS) + Seamless SSO

Q6. What is the difference between Service Health and Message Center?

A: Service Health = current incidents; Message Center = upcoming changes

Q7. Which update channel gets new features monthly on a predictable Patch Tuesday cadence?

A: Monthly Enterprise Channel

Q8. What's the role required to view usage reports (least privilege)?

A: Reports Reader

Q9. What happens to mailbox data 180 days after subscription expiry?

A: It's deleted and generally unrecoverable

Q10. Where do you configure Entra ID company branding?

A: Entra Admin Center → User experiences → Company branding

Section 2
02
User & Identity Management
Creating, managing, and securing user accounts and groups — the foundation of every Microsoft 365 administrative task. Identity is the new perimeter.
Exam Weight: ~25%

2.1 Create and Manage Users

Introduction

User accounts are the foundation of Microsoft 365. Every employee, contractor, service identity, and guest needs a user object in Entra ID to access services. As an M365 admin, user creation is something you'll do daily — onboarding, offboarding, name changes, role changes, password resets.

Why This Topic Is Important

User management is the most common admin task. A new hire who can't sign in on day 1 makes a bad impression. A terminated employee who can still access email is a security breach. Mastery of user lifecycle reduces helpdesk tickets and protects the organization.

Key Concepts

User Object Types

Type	Description	Source
Cloud-only user	Created and managed entirely in Entra ID	Microsoft Entra
Synchronized user	Originates in on-prem AD, synced via Entra Connect	Windows Server AD
Guest user	External user invited via B2B, identity in their home tenant	External
Service principal	Application identity, used for app-to-app calls	Application
Managed identity	Auto-managed identity for Azure resources	Azure resource

Key User Attributes

Attribute	Purpose
UserPrincipalName (UPN)	Sign-in name; format user@domain.com
DisplayName	Shown in address books and Teams
GivenName / Surname	First / last name
JobTitle, Department, Manager	HR attributes — drive dynamic groups
UsageLocation	ISO country code; required before assigning licenses
Mail	Primary email (typically = UPN)
ObjectId	Immutable GUID for the user
OnPremisesImmutableId	Anchor for synced users (typically AD objectGUID)
AccountEnabled	true/false — controls sign-in

Microsoft Portal Navigation

> 📍 Microsoft 365 Admin Center → `Users` → `Active users`

> 📍 Microsoft Entra Admin Center → `Identity` → `Users` → `All users`

Both portals manage the same underlying object. M365 Admin Center is simpler for daily tasks; Entra Admin Center exposes advanced attributes and Conditional Access context.

Step-by-Step: Create a User (GUI)

1. Sign in to admin.microsoft.com as User Administrator or higher.
2. Navigate to Users → Active users → + Add a user.
3. Enter Display name, Username (UPN), select domain.
4. Auto-generate password OR set initial password; require change on first sign-in.
5. Click Next → assign location (UsageLocation) and licenses.
6. Click Next → optionally assign role (default: User).
7. Optional profile info: Department, Office, Manager.
8. Review and Finish.
9. Email the credentials securely to the user (NEVER plain text email).

Best Practice

Use a self-service password portal or HR-driven JIT provisioning where possible. Never send passwords in plain text emails — use a secure secret-sharing tool or have the user set up SSPR immediately.

Step-by-Step: Bulk User Creation via CSV

1. Users → Active users → ⋯ → Bulk operations → Bulk add.
2. Download the CSV template.
3. Open template in Excel — required columns: Name, Username, Initial password, etc.
4. Fill in 10–10,000 users.
5. Save as CSV (UTF-8).
6. Upload back to the portal.
7. Review preview; click Verify.
8. Click Submit; wait for processing.
9. Download the results CSV — contains success/failure per row.

PowerShell Commands

```
# Connect to Microsoft Graph
Connect-MgGraph -Scopes "User.ReadWrite.All", "Directory.ReadWrite.All"

# Create a single user
$PasswordProfile = @{
    Password = "TempP@ss123!"
    ForceChangePasswordNextSignIn = $true
}

New-MgUser `
    -DisplayName "Ali Ahmed" `
    -UserPrincipalName "ali.ahmed@contoso.com" `
    -MailNickname "ali.ahmed" `
    -AccountEnabled `
    -PasswordProfile $PasswordProfile `
    -GivenName "Ali" `
    -Surname "Ahmed" `
    -JobTitle "Sales Manager" `
    -Department "Sales" `
    -UsageLocation "PK"

# Get a user
Get-MgUser -UserId "ali.ahmed@contoso.com" | Format-List

# Update a user
Update-MgUser -UserId "ali.ahmed@contoso.com" -JobTitle "Sales Director"

# Disable a user
Update-MgUser -UserId "ali.ahmed@contoso.com" -AccountEnabled:$false

# Delete a user (goes to recycle bin for 30 days)
Remove-MgUser -UserId "ali.ahmed@contoso.com"

# Bulk create from CSV
Import-Csv users.csv | ForEach-Object {
    $pwd = @{
        Password = "TempP@ss123!"
        ForceChangePasswordNextSignIn = $true
    }
    New-MgUser `
        -DisplayName $_.DisplayName `
        -UserPrincipalName $_.UPN `
        -MailNickname $_.MailNickname `
        -AccountEnabled `
        -PasswordProfile $pwd `
        -UsageLocation $_.Country
}

# Find users created in last 7 days
Get-MgUser -All -Property CreatedDateTime,DisplayName,UserPrincipalName |
    Where-Object { $_.CreatedDateTime -ge (Get-Date).AddDays(-7) }
```

Real-World Scenarios

Scenario: HR-driven onboarding

Contoso uses Workday for HR. When a new hire is approved, Workday calls a webhook that triggers a Logic App. The Logic App reads HR attributes, creates the user in Entra via Graph, assigns license group membership (which auto-assigns E3 + Teams Phone), creates a mailbox, and emails IT a confirmation. Time from HR approval to user being ready: 5 minutes. Day 1 productivity: instant.

Scenario: Offboarding (the right way)

An employee resigns. The proper sequence:

1. Block sign-in immediately (don't delete yet)
2. Revoke all active sessions: `Revoke-MgUserSignInSession`
3. Reset password to a random value
4. Convert mailbox to shared (preserves email, no license needed)
5. Move OneDrive ownership to manager
6. Remove from group memberships
7. Wipe corporate data from mobile devices
8. After 30-90 days, delete the user

Best Practices

- Standardize UPN format: `firstname.lastname@contoso.com`.
- Always set UsageLocation before assigning licenses.
- Use group-based licensing — never assign licenses to individual users.
- Document offboarding procedure in a runbook.
- Enable soft-delete (default 30 days) before hard-delete.
- Audit user creation events via Entra audit logs.
- Use Privileged Identity Management (PIM) for admin role activation.

Common Errors and Troubleshooting

Error	Cause	Solution
"UPN must use a verified domain"	Domain not added/verified in tenant	Add and verify domain first
License cannot be assigned	UsageLocation missing	Set UsageLocation country code
User created but can't sign in	AccountEnabled = false, or sign-in blocked by CA	Enable account; review CA policy What-If
"Duplicate proxyAddress"	Email collision with another user/group	Find and resolve duplicate (Get-MgUser -Filter)
Synced user changes not appearing	Sync delay or filter excluding object	Force sync: `Start-ADSyncSyncCycle`

Interview Questions and Answers

Q: Why must UsageLocation be set before assigning a license?

A: Microsoft licensing is region-specific — some services have legal restrictions (e.g., specific cryptography in certain countries). UsageLocation tells Microsoft which legal framework applies. Without it, the API refuses to assign the license.

Q: What's the difference between disabling and deleting a user?

A: Disable (AccountEnabled = false): user can't sign in, but the object and all its data remain. License still consumed. Delete: object moved to recycle bin for 30 days, can be restored. After 30 days, permanently deleted. Best practice: disable for 30–90 days, then delete.

Q: How do you restore a deleted user?

A: Within 30 days: Entra Admin Center → Users → Deleted users → select → Restore. Or PowerShell: `Restore-MgDirectoryDeletedItem`. After 30 days, permanently deleted — recovery requires support ticket and is not guaranteed.

Exam-Focused Notes

- Deleted users restorable for 30 days.
- UsageLocation required before license assignment.
- UPN must use verified domain.
- Synced users cannot be edited in cloud (changes overwritten on next sync), except for some attributes after preview features.
- Bulk CSV upload supports up to 250,000 users per operation.

Lab 2.1 — User Management

1. Create a user via GUI: alice.test@yourtenant.onmicrosoft.com.
2. Assign E3 license — observe failure if UsageLocation missing; set it, retry.
3. Sign in as alice.test in private window; force password change.
4. Run PowerShell: `Get-MgUser -UserId "alice.test@..."`.
5. Update job title via PowerShell.
6. Disable user; verify sign-in blocked.
7. Delete user; restore from deleted users.

Summary

Section 2.1 Summary

- Five user types: cloud, synced, guest, service principal, managed identity.
- Create via Admin Center GUI, bulk CSV, or PowerShell/Graph.
- UsageLocation required for licensing.
- Deleted users restorable 30 days.
- Offboarding: block sign-in → revoke sessions → reset password → convert mailbox to shared → delete after retention.

2.2 Bulk User Creation

Introduction

When you onboard 50 interns on day one, or migrate a department of 500, you don't create users one at a time. Bulk creation tools — CSV import, PowerShell scripts, HR integrations — make large-scale provisioning fast and consistent.

Methods for Bulk User Creation

Method	Best For	Effort
Admin Center CSV import	One-time bulk loads of 10–10,000 users	Low
PowerShell scripts	Repeated, scheduled, or customized creation	Medium
HR system integration	Continuous provisioning from authoritative HR data	High initial, low ongoing
Entra Cloud HR Provisioning	SaaS HR systems (Workday, SAP SuccessFactors)	Medium-High
SCIM provisioning	Apps and systems that support SCIM standard	Medium

Step-by-Step: CSV Bulk Import

1. Prepare the CSV

Required columns:

- User name (UPN)
- First name
- Last name
- Display name
- Job title
- Department
- Office number
- Office phone
- Mobile phone
- Fax
- Alternate email
- Address, City, State or Province, Zip or postal code, Country or region

2. Upload

1. Admin Center → Users → Active users → ⋯ → Bulk operations → Bulk add users.
2. Upload CSV.
3. Click Verify to validate.
4. Click Next; assign location and licenses.
5. Click Submit.
6. Download results CSV when complete.

PowerShell Bulk Script

```
# bulk_create_users.ps1

Connect-MgGraph -Scopes "User.ReadWrite.All", "Directory.ReadWrite.All"

$users = Import-Csv -Path ".\new_hires.csv"
$results = @()

foreach ($user in $users) {
    try {
        $pwd = @{
            Password = "Welcome$(Get-Random -Min 1000 -Max 9999)!"
            ForceChangePasswordNextSignIn = $true
        }

        $newUser = New-MgUser `
            -DisplayName "$($user.FirstName) $($user.LastName)" `
            -UserPrincipalName "$($user.FirstName).$
($user.LastName)@contoso.com".ToLower() `
            -MailNickname "$($user.FirstName).$($user.LastName)".ToLower() `
            -GivenName $user.FirstName `
            -Surname $user.LastName `
            -JobTitle $user.JobTitle `
            -Department $user.Department `
            -UsageLocation "PK" `
            -AccountEnabled `
            -PasswordProfile $pwd

        $results += [PSCustomObject]@{
            UPN = $newUser.UserPrincipalName
            Status = "Created"
            Password = $pwd.Password
        }
    }
    catch {
        $results += [PSCustomObject]@{
            UPN = "$($user.FirstName).$($user.LastName)@contoso.com"
            Status = "Failed: $($_.Exception.Message)"
            Password = ""
        }
    }
}

$results | Export-Csv -Path ".\results.csv" -NoTypeInformation
Write-Host "Done. $($results.Count) users processed."
```

Best Practices

- Test with a 3-row CSV before uploading thousands.
- Use unique, temporary, complex passwords per user.
- Force password change on first sign-in.
- Assign licenses via group, not individually, to scale.
- Log every creation with timestamp and admin identity.
- Encode CSV as UTF-8 with BOM for non-ASCII names.

Common Errors and Troubleshooting

Error	Cause	Fix
"Duplicate UPN"	UPN already exists	Append a number or middle initial
"Domain not verified"	UPN suffix not added to tenant	Add and verify domain
"Special characters in UPN"	UPN contains invalid chars (e.g., spaces)	Strip or replace before creation
License assignment fails partially	Insufficient licenses in tenant	Buy more before bulk upload
Encoding error on Arabic / Chinese names	CSV not UTF-8	Re-save in Excel as "CSV UTF-8"

Summary

Section 2.2 Summary

- GUI bulk import: up to 250,000 users via CSV.
- PowerShell offers more flexibility (validation, error handling, custom logic).
- For ongoing HR-driven onboarding, use Entra Cloud HR Provisioning or SCIM.
- Always test with a small sample first.

2.3 Guest Users and External Collaboration

Introduction

Guest users let external collaborators — partners, vendors, contractors, customers — access Teams, SharePoint, and other M365 resources WITHOUT requiring them to have an account in your tenant. The technology underneath is Entra ID B2B (Business-to-Business) collaboration.

Why This Topic Is Important

Modern work crosses organizational boundaries. Without guest access, partners send files through email attachments (insecure, no version control). With guests, partners join your Teams channels with native access controls and DLP applied — secure collaboration at scale.

Key Concepts

How Guest Identity Works

Aspect	Details
Home directory	Guest's actual identity lives in their home tenant (or as personal Microsoft account)
Your tenant view	Guest appears as a user with UserType = Guest, UPN like `partner_contoso.com#EXT#@yourtenant.onmicrosoft.com`
Authentication	Happens in home tenant; your tenant trusts the assertion
License	Guests don't consume licenses in your tenant for most scenarios (5:1 guest ratio per licensed user via Monthly Active Users)
MFA	Can be required by your CA policies even though identity is external

Guest vs Member

Feature	Member	Guest
Can see directory by default	Yes (limited)	Highly restricted
Can invite other guests	Yes (by default)	No (typically)
License needed	Yes	Usually no
Counts toward seat licenses	Yes	No
Access scope	Default access policies	Limited per guest settings

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Identity` → `Users` → `All users` → `+ New guest user`

> 📍 Entra Admin Center → `Identity` → `External Identities` → `External collaboration settings`

Step-by-Step: Invite a Guest

1. Entra Admin Center → Identity → Users → All users.
2. + New user → Invite external user.
3. Enter email address (partner@otherco.com).
4. Optional: display name, personal message, send invite directly.
5. Optional: assign groups or roles.
6. Click Invite.
7. Partner receives invitation email with redemption link.
8. Partner clicks → consents to terms → identity created in your tenant.

External Collaboration Settings

Control globally what guests can do:

Setting	Options
Guest user access restrictions	Same as members, Limited access, Most restrictive
Guest invite restrictions	Anyone, Members + admins, Admins only, No one
Self-service sign-up via user flows	Enabled / Disabled
Allow/block list	Allow only specific domains, OR block specific domains

Configure Allow List

1. External Identities → External collaboration settings.
2. "Collaboration restrictions" → "Allow invitations only to the specified domains."
3. Add domains: partner1.com, customer2.com.
4. Save.

PowerShell Commands

```
# Invite a guest
$invite = New-MgInvitation `
    -InvitedUserEmailAddress "partner@otherco.com" `
    -InvitedUserDisplayName "Partner Name" `
    -InviteRedirectUrl "https://myapps.microsoft.com" `
    -SendInvitationMessage:$true

# List all guests
Get-MgUser -Filter "userType eq 'Guest'" -All | Format-Table DisplayName,
UserPrincipalName

# Find stale guests (not signed in for 90 days)
$cutoff = (Get-Date).AddDays(-90)
Get-MgUser -All -Filter "userType eq 'Guest'" -Property SignInActivity, DisplayName
|
    Where-Object { $_.SignInActivity.LastSignInDateTime -lt $cutoff } |
    Select-Object DisplayName, UserPrincipalName,
        @{Name="LastSignIn";Expression={$_.SignInActivity.LastSignInDateTime}}

# Remove a guest
Remove-MgUser -UserId "partner_otherco.com#EXT#@contoso.onmicrosoft.com"
```

Real-World Scenarios

Scenario: Joint venture project

Contoso and Fabrikam form a 6-month joint venture. Solution: create a Microsoft 365 Group "JV-Project-2026" with channels in Teams. Invite Fabrikam members as guests. They access Teams chat, files in SharePoint, calendar — all natively, without VPN or duplicate accounts. When project ends, remove the group; access for all guests revoked automatically.

Scenario: Vendor portal

An auditor needs read-only access to specific SharePoint folders for 30 days. Solution: invite as guest, share specific document libraries with view-only permission, set access reviews to remove after 30 days. No need to create them in your AD or give them a license.

Best Practices

- Use access reviews to periodically validate guest membership.
- Apply Conditional Access policies to guests (MFA, device requirements).
- Restrict guest invitations to specific roles (User Admin, not all users).
- Use entitlement management for self-service guest onboarding with approval workflow.
- Audit guest activity via sign-in logs.

- Tag guests with sponsoring department for easy review.

Security Considerations

- Guests are often a security blind spot — they appear in your directory but you don't manage their devices.
- Enforce MFA for all guests via Conditional Access.
- Block legacy authentication for guests (no IMAP, POP, basic auth).
- Consider Conditional Access App Control to restrict guest data download.
- Disable self-service sign-up unless specifically needed.

Common Errors and Troubleshooting

Issue	Resolution
Guest doesn't receive invitation email	Check spam; resend via Entra; verify their email is correct
Guest can't redeem invitation	Their tenant may block external invitations; ask their admin to allow
Guest can see directory contents they shouldn't	Tighten Guest user access restrictions to "Most restrictive"
Guest sign-in blocked by CA	Review CA What-If tool; ensure guest scope intended

Interview Questions and Answers

Q: How does Entra B2B differ from creating internal accounts for partners?

A: B2B uses the partner's existing identity in their home tenant (or personal MS account). No new password to manage, no license needed in your tenant, MFA enforced by their home tenant or your CA. Internal account = duplicate identity, additional license cost, password management burden.

Q: What is the 5:1 guest licensing rule?

A: For every Entra ID P1/P2 licensed user, you can have up to 5 guest users without additional cost. Beyond that ratio, you pay for guests at the Monthly Active Users (MAU) price. Free tier has its own limits.

Exam-Focused Notes

- Guest UPN format: `partner_externaldomain.com#EXT#@yourtenant.onmicrosoft.com`.
- External collaboration settings live under Entra → External Identities.
- Cross-tenant access settings (newer) provide granular B2B controls per partner.
- Entitlement Management = approval workflow + access reviews + lifecycle for guests.
- Restrict guest invitations to least privilege.

Lab 2.3 — Guest Collaboration

1. Invite a guest (use a personal Gmail/Outlook account you control).
2. Check the invitation email; redeem the invite.
3. Add the guest to a Microsoft 365 Group.
4. Add the group to a Team; verify guest can see the Team.
5. Configure External collaboration settings to block invites to gmail.com (for testing).
6. Try to invite another Gmail user — observe block.
7. Revert setting; remove the guest.

Summary

Section 2.3 Summary

- Guests = external users with identity in their home tenant.
- Invite via Entra Admin Center, Teams, SharePoint, or M365 Group.
- Configure global behaviour via External collaboration settings.
- Apply CA policies to guests for MFA enforcement.
- Use access reviews and entitlement management for lifecycle.

2.4 Password Policies

Introduction

Password policies define what makes a password acceptable: minimum length, complexity, expiration, banned words. Microsoft Entra ID enforces a default policy on all cloud users, with additional protections like Banned Password List and Smart Lockout.

Default Entra ID Password Policy

Property	Cloud-Only Users
Minimum length	8 characters
Maximum length	256 characters
Character set	Must contain 3 of 4: lowercase, uppercase, number, symbol
Expiration	Default 90 days (configurable)
Expiration notification	14 days before
History	Last password cannot be reused
Account lockout	10 failed attempts → 1-minute lockout (Smart Lockout)

Note
For synced users, password policy is enforced on-prem AD. Cloud password policies don't override on-prem.

Password Protection Features

Global Banned Password List

Microsoft maintains a list of common passwords (Password123, Summer2024, etc.) — automatically blocked. Cannot be disabled.

Custom Banned Password List (Entra ID P1+)

Add up to 1000 custom banned terms specific to your org (company name, products, sports teams that locals might use).

Smart Lockout

Detects brute-force attempts and locks the account temporarily, even if the attacker uses different IP addresses each attempt. Distinguishes between bad actor and legitimate user.

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Protection` → `Authentication methods` → `Password protection`

Step-by-Step: Configure Custom Banned Passwords

1. Entra Admin Center → Protection → Authentication methods → Password protection.
2. Lockout threshold: 10 (default).
3. Lockout duration in seconds: 60 (default).
4. Enforce custom list: Yes.
5. Custom banned password list: add terms like "contoso", "headquartersaddress", "ceoname", "products".
6. Variations are auto-detected (contoso, c0nt0so, Contoso!).
7. Save.

Password Protection for On-Prem AD

Extend Entra Password Protection to on-prem AD:

- Install Azure AD Password Protection Proxy on member server.
- Install Azure AD Password Protection DC Agent on each DC.
- Choose Audit or Enforce mode.
- Audit: log only; Enforce: actually block bad passwords.

PowerShell

```
# Force a user to change password at next sign-in
$pwd = @{
    ForceChangePasswordNextSignIn = $true
}
Update-MgUser -UserId "user@contoso.com" -PasswordProfile $pwd

# Reset password
$pwd = @{
    Password = "TempP@ss12345!"
    ForceChangePasswordNextSignIn = $true
}
Update-MgUser -UserId "user@contoso.com" -PasswordProfile $pwd

# Set "never expires" for specific user (cloud-only)
Connect-MsolService
Set-MsolUser -UserPrincipalName "service@contoso.com" -PasswordNeverExpires $true

# Bulk: never-expire for service accounts
Get-MsolUser -All |
    Where-Object { $_.DisplayName -like "*ServiceAccount*" } |
    Set-MsolUser -PasswordNeverExpires $true
```

Real-World Scenarios

Scenario: Service account compromise

An attacker tries "P@ssw0rd123" on the service account svc-backup. Smart Lockout locks them out after 10 attempts. Without Smart Lockout, the attacker could try via different IPs and bypass simple lockouts. With it, the lockout state is shared across all login attempts to the same account.

Best Practices

- Set passwords to never expire ONLY if MFA is enforced.
- Add company-specific terms to custom banned list (organization name, addresses, product names).
- Deploy Password Protection to on-prem AD for consistency.
- Educate users: longer passphrase > complex short password.
- Combine with MFA — strong password alone is not enough.

Interview Questions and Answers

Q: Why does Microsoft recommend disabling password expiration?

A: Forced periodic rotation produces predictable patterns (Summer2024 → Autumn2024). NIST SP 800-63B research shows MFA + strong unique passphrase + breach-detection beats expiration. So with MFA enabled, eliminate expiration to reduce user friction and weak password patterns.

Q: What is Smart Lockout?

A: Entra ID feature that locks an account after 10 (default) failed sign-in attempts, even if the attempts come from different IPs. Distinguishes between attacker and legit user by tracking auth state per account, not per IP.

Exam-Focused Notes

- Default lockout: 10 attempts → 60-second lockout.
- Custom banned list: 1000 terms (Entra ID P1+).
- Global banned list is on for all tenants, can't be disabled.
- Password Protection for on-prem AD requires P1 + Proxy/DC agents.

Summary

Section 2.4 Summary

- Default: 8-char min, 90-day expiry, complexity, Smart Lockout.
- Microsoft recommends "never expire" with MFA.
- Custom banned password list blocks company-specific common terms.

- Extend Password Protection to on-prem AD.

2.5 Self-Service Password Reset (SSPR)

Introduction

SSPR lets users reset their own passwords without calling the helpdesk. Studies show password resets are 20–40% of all helpdesk calls. SSPR slashes this overhead while improving user experience. With password write-back, cloud password resets also flow back to on-prem AD.

Why This Topic Is Important

A user locked out at midnight before a deadline can't wait for helpdesk to open. SSPR provides 24/7 self-service while maintaining security through multi-factor verification.

Key Concepts

SSPR Components

Component	Purpose
Registration	Users register verification methods (phone, email, security questions, authenticator)
Reset flow	User proves identity via 1 or 2 methods to reset
Password write-back	Cloud reset flows back to on-prem AD (hybrid only)
Audit log	Records every SSPR attempt and outcome

Verification Methods

Method	Notes
Mobile app notification	Push approval via Microsoft Authenticator
Mobile app code	TOTP code from Authenticator
Mobile phone (SMS or call)	Voice or text
Office phone (call)	For desk-bound roles
Email (alternate)	Non-corporate email like personal Gmail
Security questions	Knowledge-based (3-5 questions); admin-defined

License Requirements

License	SSPR Capability
Free Entra ID	Admin password reset only
Entra ID P1	Cloud user SSPR + Password Write-back
Entra ID P2	Same as P1 + advanced
Microsoft 365 Business Premium	SSPR included

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Protection` → `Password reset`

Step-by-Step: Enable SSPR

1. Entra Admin Center → Protection → Password reset → Properties.
2. "Self service password reset enabled" → choose: None, Selected (group), or All.
3. Best practice: pilot with "Selected" group first.
4. Save.
5. Configure Authentication methods:
    - Number of methods required to reset: 2 (recommended)
    - Methods available: mobile app notification, SMS, email, security questions

6. Configure Registration:
    - "Require users to register when signing in": Yes
    - "Number of days before users are asked to reconfirm": 180
7. Configure Notifications: notify user + admin on password reset events.
8. Configure Customization: helpdesk link or phone shown on reset page.
9. Optional: Password Write-back (for hybrid) → On-premises integration → enable.

User Registration Experience

On first sign-in after SSPR is enabled, users see:

1. "More information required" prompt.
2. Register at https://aka.ms/ssprsetup.
3. Provide 2 (or required number) methods.
4. Verify each method (SMS code, email link, app scan).
5. Done — can now reset password from sign-in page.

Reset Experience

1. User goes to https://aka.ms/sspr or clicks "Forgot password" at sign-in.
2. Enters UPN + CAPTCHA.
3. Receives challenge via verification methods.
4. Verifies → sets new password meeting policy.
5. Password reset, signs in normally.

Password Write-Back

For hybrid environments, write-back syncs the cloud reset to on-prem AD:

- Requires Entra Connect installed with Password write-back option enabled.
- Requires Entra ID P1 or higher for users.
- Requires Service Account in AD with "Reset password" + "Change password" rights.
- Without write-back, hybrid users' on-prem and cloud passwords get out of sync after cloud reset.

PowerShell

```
# Get user's registered SSPR methods
Connect-MgGraph -Scopes "UserAuthenticationMethod.Read.All"

Get-MgUserAuthenticationMethod -UserId "user@contoso.com" |
    Select-Object @{Name="Type";Expression={$_.AdditionalProperties.'@odata.type'}},
Id

# Get SSPR registration status report
Get-MgReportAuthenticationMethodUserRegistrationDetail -All |
    Select-Object UserPrincipalName,
        IsSsprRegistered,
        IsSsprEnabled,
        IsSsprCapable
```

Real-World Scenarios

Scenario: After-hours password reset

An employee in Karachi locks themselves out at 11 PM on Friday. Helpdesk in London is closed. Without SSPR, they're stuck until Monday. With SSPR, they hit "Forgot password," receive SMS to mobile, set new password, back in 30 seconds.

Scenario: Helpdesk volume

Before SSPR: 400 password reset tickets/month at ~$25 each = $10,000/month or $120k/year. After SSPR: 50 tickets/month for complex issues. Savings: $90k/year + faster recovery.

Best Practices

- Require 2 methods for reset (not 1).
- Avoid security questions if possible — easy to social engineer.
- Prefer authenticator app over SMS (SMS vulnerable to SIM-swap).
- Combine with combined registration (SSPR + MFA registration in one flow).
- Pilot with IT group first; roll out gradually.
- Educate users with email + intranet article + 1-page guide.
- Monitor SSPR usage reports monthly.

Common Errors and Troubleshooting

Issue	Resolution
"You can't reset your password at this time"	User not licensed or not registered; verify license, prompt to register
Password write-back fails	Verify Entra Connect service account permissions; restart sync
User never sees registration prompt	Verify "Require to register" toggle on; check assigned group
SMS not received	Phone number wrong format (need country code); carrier blocks short codes
"Methods not approved by admin"	Method disabled in Authentication methods policy

Interview Questions and Answers

Q: What's Password Write-Back?

A: In a hybrid environment with Entra Connect, when a user resets their password in the cloud via SSPR, write-back sends the new password to on-prem AD so both stay in sync. Requires Entra Connect feature enabled + Entra ID P1+ licensing.

Q: How many verification methods should be required?

A: 2 is the secure default. 1 = phishable single-factor. 2 = multi-factor protection. Don't go above 2 unless regulatory requirement demands it; user friction outweighs security gain.

Exam-Focused Notes

- SSPR requires Entra ID P1+ for cloud users (or M365 Business Premium).
- Password Write-Back requires Entra Connect with feature enabled.
- Combined registration: users register SSPR + MFA in single experience.
- Admins always use 2 methods regardless of user policy.
- Security questions are admin-defined; not recommended due to phishability.

Lab 2.5 — SSPR End-to-End

1. Entra Admin Center → Protection → Password reset → Properties.
2. Enable for "Selected" group; create group "SSPR-Pilot" with 1 test user.
3. Configure 2 methods required, allow SMS + email + authenticator.
4. Sign in as test user; should be prompted to register.
5. Register 2 methods.

6. Sign out; click "Can't access your account" → reset password.
7. Verify successful reset and sign-in.

Summary

Section 2.5 Summary

- SSPR = users reset their own passwords without helpdesk.
- Configure under Entra → Protection → Password reset.
- Require 2 verification methods.
- Hybrid: enable password write-back via Entra Connect.
- Combined registration unifies SSPR + MFA setup.

2.6 Group Management

Introduction

Groups in Microsoft Entra ID are collections of users (and sometimes other groups) used for collaboration, access control, and licensing. Groups are central to scalable administration — assign a license, permission, or policy to a group once, and it applies to all members automatically.

Group Types Overview

Group Type	Purpose	Has Email?	Has SharePoint Site?
Security group	Access control to apps, resources	Optional (Mail-enabled)	No
Microsoft 365 Group	Collaboration: Teams, Outlook, SharePoint, Planner	Yes	Yes
Distribution list	Email distribution only (legacy)	Yes	No
Mail-enabled security group	Security + email	Yes	No
Dynamic group	Membership auto-calculated by rule	Either type	Either

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Identity` → `Groups` → `All groups`

> 📍 M365 Admin Center → `Teams & groups` → `Active teams & groups`

Step-by-Step: Create a Security Group

1. Entra Admin Center → Groups → All groups → + New group.
2. Group type: Security.
3. Group name: "Sales-Team".
4. Membership type: Assigned (manual) or Dynamic User (auto).
5. Owners: at least one (you, by default).
6. Members: add users.
7. Create.

Step-by-Step: Create a Microsoft 365 Group

1. Entra Admin Center → Groups → All groups → + New group.
2. Group type: Microsoft 365.
3. Group name + description.
4. Membership type: Assigned or Dynamic.
5. Owners + members.
6. Create — within 5 minutes:
    - Shared mailbox created
    - SharePoint site provisioned (group.sharepoint.com/sites/Sales-Team)
    - Planner board ready
    - OneNote notebook ready
    - Teams team can be added on top

PowerShell

```powershell
# Create a security group
New-MgGroup `
    -DisplayName "Sales-Team" `
    -MailEnabled:$false `
    -MailNickname "salesteam" `
    -SecurityEnabled

# Create a Microsoft 365 group
New-MgGroup `
    -DisplayName "Marketing Project Alpha" `
    -MailEnabled:$true `
    -MailNickname "marketing-alpha" `
    -SecurityEnabled:$false `
    -GroupTypes @("Unified")

# Add member
$user = Get-MgUser -UserId "ali@contoso.com"
$group = Get-MgGroup -Filter "displayName eq 'Sales-Team'"
New-MgGroupMember -GroupId $group.Id -DirectoryObjectId $user.Id

# Bulk add from CSV
$members = Import-Csv .\members.csv
foreach ($m in $members) {
    $u = Get-MgUser -UserId $m.UPN
    New-MgGroupMember -GroupId $group.Id -DirectoryObjectId $u.Id
}

# Get group members
Get-MgGroupMember -GroupId $group.Id |
    ForEach-Object { Get-MgUser -UserId $_.Id } |
    Select-Object DisplayName, UserPrincipalName

# Remove member
Remove-MgGroupMemberByRef -GroupId $group.Id -DirectoryObjectId $user.Id
```

Best Practices

- Naming convention: prefix + purpose + role (e.g., `SG-Sales-AccessFinanceApp`).
- Use M365 Groups for collaboration; Security Groups for access control.
- Assign at least 2 owners per group to avoid orphan groups.
- Use Group Naming Policy to enforce prefixes (P1+ feature).
- Set Group Expiration policy (180/365 days) to clean up stale groups.
- Block users from creating M365 groups; control via IT to avoid sprawl.

Restrict M365 Group Creation

```
# Restrict who can create M365 Groups
Connect-MgGraph -Scopes "Directory.ReadWrite.All"

# Create a security group of allowed creators
$creators = New-MgGroup `
    -DisplayName "M365-Group-Creators" `
    -MailEnabled:$false `
    -MailNickname "m365groupcreators" `
    -SecurityEnabled

# Configure the directory setting
$template = Get-MgBetaDirectorySettingTemplate |
    Where-Object { $_.DisplayName -eq "Group.Unified" }

$params = @{
    TemplateId = $template.Id
    Values = @(
        @{ Name = "EnableGroupCreation"; Value = "false" }
        @{ Name = "GroupCreationAllowedGroupId"; Value = $creators.Id }
    )
}
New-MgBetaDirectorySetting -BodyParameter $params
```

Summary

Section 2.6 Summary

- Five group types: Security, M365, Distribution, Mail-enabled Security, Dynamic.
- M365 Groups bring shared mailbox + SharePoint + Planner + Teams.
- Security Groups for access control / licensing.
- Restrict creation to specific group of IT pros.
- Use expiration and naming policy to control sprawl.

2.7 Security Groups vs Microsoft 365 Groups

Comparison Table

Feature	Security Group	Microsoft 365 Group
Primary purpose	Access control	Collaboration
Members	Users, groups, devices, contacts	Users, guests
Owners required	Optional	Required (min 1, recommend 2+)
Mail enabled	Optional (becomes mail-enabled security group)	Always (shared mailbox)
SharePoint site	No	Yes (auto-provisioned)
Teams support	No (use M365 Group)	Yes
Conditional Access targeting	Yes	Yes
License assignment	Yes	Yes
Dynamic membership	Yes	Yes
Nesting (group of groups)	Yes (security in security)	No
Visibility	Public/Private (limited concept)	Public/Private/Hidden
Sensitivity labels	No	Yes
Expiration policy	No	Yes (180/365 days)

When to Use Each

Use Security Group When:

- You need to grant access to an application or resource
- Assigning Conditional Access policies to a group of users
- Targeting an Intune compliance / configuration policy
- Group-based licensing (common pattern)
- Mail isn't needed

Use Microsoft 365 Group When:

- A team needs collaboration: shared inbox, files, Planner, Teams

- Cross-functional project
- Department-wide email + file sharing
- Yammer community
- Power BI workspace (legacy concept, now Fabric workspace)

Decision Rule
"If you want a Team, you need a Microsoft 365 Group. If you want a license assignment or app access, you want a Security Group."

Real-World Scenarios

Scenario: Mixed needs

A department wants Teams, Planner, and SharePoint (collaboration) AND needs to control access to a custom HR app (security/access). Solution: create a Microsoft 365 Group "HR-Department" for collaboration. Create a Security Group "SG-HR-AppAccess" for the HR app permissions. Nest the M365 Group as a member of the security group, OR use dynamic membership rules.

Summary

Section 2.7 Summary

- Security = access control. M365 = collaboration.
- Most organizations have both, for different reasons.
- Don't try to make Security Groups do M365 Group's job, or vice versa.
- M365 Groups get email, SharePoint, Planner, optional Teams.

2.8 Distribution Groups and Dynamic Groups

Distribution Groups

Distribution Groups (DLs) are legacy email-only groups for sending email to multiple recipients. They originate from Exchange and exist for backward compatibility.

When You'd Still Use a DL

- Pure mail distribution where no shared mailbox is needed
- Migration scenarios from on-prem Exchange
- Sending to thousands of external addresses

Microsoft Recommendation

For new collaboration scenarios, use M365 Groups. DLs lack the modern features (shared SharePoint, Teams, file collaboration). Microsoft offers automatic "Upgrade Distribution List" in EAC.

Mail-Enabled Security Groups

Hybrid between security and DL: provides both access control AND email. Useful for:

- Granting access to a SharePoint resource AND letting people email the group
- Legacy compatibility

Dynamic Groups

Dynamic groups auto-calculate membership using a rule based on user attributes. Set the rule once; membership stays current as users join, leave, or change roles.

License Requirement

Dynamic groups require Entra ID P1 for users in dynamic groups.

Membership Rule Syntax

```
# All Sales department users
(user.department -eq "Sales")

# All employees in Pakistan with a manager assigned
(user.country -eq "PK") and (user.manager -ne null)

# Specific job titles
(user.jobTitle -contains "Manager") or (user.jobTitle -contains "Director")

# Exclude disabled accounts
(user.department -eq "Engineering") and (user.accountEnabled -eq true)

# Combined with extensionAttribute
(user.extensionAttribute1 -eq "FullTime") and (user.companyName -eq "Contoso")

# Devices (separate dynamic group)
(device.deviceOSType -eq "Windows") and (device.managementType -eq "MDM")
```

Step-by-Step: Create a Dynamic Group

1. Entra Admin Center → Groups → + New group.
2. Group type: Security or Microsoft 365.
3. Membership type: **Dynamic User**.

4. Click "Add dynamic query."
5. Build rule: Property = department, Operator = Equals, Value = Sales.
6. Or click "Edit" to write directly: `(user.department -eq "Sales")`.
7. Validate Rule (top right) → enter a test UPN to confirm.
8. Save → group provisions.
9. Wait 5–15 minutes for initial population.

PowerShell

```
# Create dynamic group
New-MgGroup `
    -DisplayName "All Sales (Dynamic)" `
    -MailEnabled:$false `
    -MailNickname "all-sales-dyn" `
    -SecurityEnabled `
    -GroupTypes @("DynamicMembership") `
    -MembershipRule '(user.department -eq "Sales")' `
    -MembershipRuleProcessingState "On"
```

Real-World Scenarios

Scenario: Auto-license by department

Sales gets E5; everyone else gets E3. Create:

- Dynamic security group "Sales-Dynamic" = `(user.department -eq "Sales")`
- Apply group-based licensing: E5 → Sales-Dynamic, E3 → All Users (minus Sales-Dynamic).

When HR updates a user's department in Workday, sync to Entra → user automatically moves between groups → license updates within an hour.

Best Practices

- Test rules with the "Validate Rule" feature before saving.
- Keep rules simple; complex nested rules slow processing.
- Document each dynamic group's rule in description.
- Source attributes from authoritative HR system, not free-text user fields.
- Don't use dynamic groups for time-critical access (5–15 min lag).

Common Errors

Error	Resolution
"Dynamic group requires P1"	Assign P1 license to all users in scope
Rule processing state: "Processing error"	Bad syntax; rewrite rule
Membership not updating	Wait up to 24 hours; processing can be delayed
User missing from group	Attribute may be missing or wrong case; rules are case-sensitive on values

Summary

Section 2.8 Summary

- Distribution Groups = legacy email-only, prefer M365 Groups now.
- Mail-enabled Security Group = access control + email.
- Dynamic Groups = auto-membership via rules (P1 required).
- Use HR attributes to drive dynamic membership.
- Allow 5-30 min for membership processing.

2.9 Group-Based Licensing

Introduction

Group-based licensing assigns Microsoft 365 licenses to a group; all members automatically inherit the license. When a user joins, license assigned. When they leave, license removed. Combined with dynamic groups, you get fully automated lifecycle management.

Why It Matters

Manual per-user license assignment doesn't scale. For 10,000 users with role changes, terminations, and acquisitions, you'd spend half your week on license admin. Group-based licensing reduces this to near zero.

How It Works

1. Admin assigns license to a group.
2. Entra evaluates each member.
3. If user lacks UsageLocation, processing fails for that user (flagged).
4. Otherwise, license assigned with the service plans inherited from group.

5. Disable specific service plans for the group if you want to exclude services (e.g., disable Yammer for everyone).
6. User keeps direct + group licenses; if both, both are applied (direct + inherited).

Step-by-Step: Assign License to Group

1. Entra Admin Center → Groups → select group.
2. Licenses (left menu) → + Assignments.
3. Choose SKU (e.g., Microsoft 365 E3).
4. Optionally toggle individual service plans on/off.
5. Save.
6. Wait 5–30 minutes; all members receive license.

License Reconciliation When Multiple Groups

If a user is in 2 groups each assigning a license:

- If different SKUs: user gets both.
- If same SKU: user gets one assignment with combined service plans (most inclusive).
- Direct assignments are independent and additive.

Best Practices

- Use one group per SKU (e.g., "Lic-M365-E3", "Lic-M365-E5", "Lic-PowerBI-Pro").
- Drive group membership dynamically from HR data.
- Don't assign licenses to "All Users" — segment by job profile.
- Monitor "Licensing Errors" in the group blade and resolve weekly.
- Never mix direct + group assignment for the same SKU on the same user (confusing).

Common Errors

Error	Resolution
"Usage location not set"	Set UsageLocation on the user
"Insufficient licenses"	Purchase more or reduce group size
"Conflicting service plans"	Two SKUs include same service that doesn't allow duplicates; toggle off one
"Mutually exclusive service plans"	E.g., two Exchange plans; disable one

Summary

Section 2.9 Summary

- Group-based licensing scales license management.
- Combine with dynamic groups for full automation.
- Monitor licensing errors and resolve UsageLocation issues.
- One group per SKU = clean architecture.

2.10 Multi-Factor Authentication (MFA)

Introduction

Multi-Factor Authentication (MFA) requires users to verify their identity with two or more factors before accessing resources. Microsoft research shows MFA blocks 99.2% of automated account takeover attacks. It's the single most impactful security control you can deploy.

Why This Topic Is Important

Passwords alone are not enough. Phishing, credential stuffing, password sprays, and breach reuse mean any single password — no matter how strong — eventually leaks. MFA adds a second factor (something you have or are) that attackers cannot easily steal remotely.

Key Concepts

The Three Authentication Factors

Factor	Description	Examples
Something you **know**	Knowledge factor	Password, PIN, security questions
Something you **have**	Possession factor	Phone with Authenticator app, FIDO2 key, smart card
Something you **are**	Inherence factor	Fingerprint, face recognition, voice

MFA Deployment Options

Method	Description	Best For
Security Defaults	Tenant-wide MFA enforcement for all users, all sign-ins	Small orgs, no Entra ID P1
Per-user MFA	Legacy — enable MFA flag per user	Avoid for new deployments
Conditional Access	Granular: MFA based on user, app, location, device, risk	Enterprise (Entra ID P1+)

Best Practice
Use Conditional Access if you have Entra ID P1+. Use Security Defaults for everyone else. Avoid per-user MFA — it's legacy and lacks flexibility.

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Identity` → `Overview` → `Properties` → `Manage Security defaults`

> 📍 Entra Admin Center → `Protection` → `Conditional Access` (for granular MFA)

> 📍 Entra Admin Center → `Protection` → `Authentication methods` (configure available factors)

Step-by-Step: Enable Security Defaults

1. Entra Admin Center → Identity → Overview → Properties (tab).
2. "Manage Security defaults."
3. Toggle "Security defaults": Enabled.
4. Save.
5. Within 14 days, all users prompted to register MFA at next sign-in.
6. All admin accounts require MFA every sign-in immediately.

Step-by-Step: MFA via Conditional Access

1. Entra Admin Center → Protection → Conditional Access → + New policy.
2. Name: "Require MFA for all users".
3. Users: All users (exclude break-glass accounts).
4. Target resources: All cloud apps (exclude specific apps if needed).
5. Conditions: leave default (all locations, all platforms).

6. Grant: Require multi-factor authentication.
7. Enable policy: Report-only first (test).
8. Save.
9. Monitor for 1 week via Sign-in logs → CA report.
10. Switch to "On" once confident.

CRITICAL
ALWAYS exclude at least 2 break-glass / emergency access accounts from MFA policies. Otherwise, an MFA infrastructure failure can lock you out of the tenant permanently.

MFA Verification Methods

Method	Security Level	Notes
Microsoft Authenticator (push)	★★★★★	Recommended; phishing-resistant when number matching enabled
Authenticator OATH code (TOTP)	★★★★	Works offline; 30-second code
FIDO2 security key	★★★★★	Phishing-resistant; hardware key (Yubikey)
Windows Hello for Business	★★★★★	PIN + biometric tied to device
Certificate-based authentication	★★★★★	Smart cards, PKI
SMS	★★	Vulnerable to SIM swap; allowed but discouraged
Voice call	★★	Similar weakness to SMS
OATH hardware token	★★★★	Physical TOTP device

Number Matching (Important!)

Without number matching: user gets push notification on phone, taps "Approve." Vulnerable to MFA fatigue attacks (attacker spams approval requests until user accidentally taps yes).

With number matching: sign-in screen shows a 2-digit number; user must type that number into the Authenticator app to approve. Stops MFA fatigue. **On by default since May 2023.**

MFA Registration Status

```
# Report: users registered for MFA
Connect-MgGraph -Scopes "AuditLog.Read.All"

Get-MgReportAuthenticationMethodUserRegistrationDetail -All |
    Select-Object UserPrincipalName,
        IsMfaRegistered,
        IsMfaCapable,
        DefaultMfaMethod,
        IsSsprRegistered |
    Export-Csv mfa_registration.csv -NoTypeInformation
```

Real-World Scenarios

Scenario: MFA rollout in 2,000-user company

IT plans MFA rollout: Week 1 — communicate via email + intranet. Week 2 — enforce for IT + executives (pilot). Week 3-4 — enforce for departments in waves with helpdesk on standby. Week 5 — enforce for all users. Use Conditional Access policies with "Report-only" mode first to identify users who'd be blocked, then flip to "On". Result: 99% MFA-enrolled in 6 weeks with 5 helpdesk escalations.

Scenario: MFA fatigue attack

Attacker phished an exec's password. Tried to sign in 50 times in 5 minutes, spamming push approvals to exec's phone. Without number matching, the exec accidentally taps Approve while in a meeting. With number matching: the exec sees "Enter 73 in your app" — clearly suspicious, denies and reports.

Best Practices

- Enable Conditional Access MFA for all users (not just admins).
- Exclude 2+ break-glass accounts.
- Require MFA for risky sign-ins via Entra ID Protection.
- Disable SMS/voice if possible; require Authenticator app or FIDO2.
- Enable number matching (now default).
- Pilot first; communicate well; have helpdesk ready.
- Use "Authentication strength" policies for granular factor selection (P1+).
- Monitor MFA registration rates monthly.

Common Errors and Troubleshooting

Issue	Resolution
"Your sign-in was blocked"	Review CA policy; check sign-in log; possible legacy auth attempt
User lost phone	Admin revokes MFA methods, user re-registers from temporary access pass
"This sign-in is from an unfamiliar location"	Identity Protection risk-based prompt — verify legitimate
MFA registration link broken	https://aka.ms/mfasetup — direct user there
"Couldn't verify your identity"	Method expired (rare); re-register

Temporary Access Pass (TAP)

For new hires who don't yet have a phone, or users who lost their device, a TAP provides time-limited access:

- Admin generates an 8-digit code valid for 1-720 minutes.
- User uses it to sign in and register permanent MFA methods.
- One-time or multi-use.

```
# Issue TAP
$params = @{
    StartDateTime = "2026-01-15T08:00:00Z"
    LifetimeInMinutes = 480
    IsUsableOnce = $false
}
New-MgUserAuthenticationTemporaryAccessPassMethod `
    -UserId "newhire@contoso.com" `
    -BodyParameter $params
```

Interview Questions and Answers

Q: What is MFA fatigue, and how does Microsoft prevent it?

A: MFA fatigue is when attackers spam push approval requests hoping the user accidentally approves. Microsoft prevents it with Number Matching (user must type a number shown on the sign-in screen into the Authenticator app) and Additional Context (shows app + location).

Q: What's the difference between Security Defaults and Conditional Access for MFA?

A: Security Defaults: free, all-or-nothing, all users required to register and use MFA. Conditional Access: P1+ feature, granular (per user/app/location/risk), supports "report-only" testing, can require MFA only when needed.

Q: Why exclude break-glass accounts from MFA?

A: If MFA infrastructure fails (Microsoft outage, phone system down), all users with MFA are locked out. Break-glass accounts (cloud-only Global Admins with strong passwords, no MFA, monitored sign-in alerts) provide emergency access to fix the tenant.

Exam-Focused Notes

- Microsoft says: MFA blocks 99.2% of automated attacks.
- Security Defaults: free, enforces MFA on all admins always, prompts users to register.
- Per-user MFA: legacy; avoid.
- CA-based MFA: requires Entra ID P1+.
- Always exclude break-glass accounts.
- Number matching: on by default since May 2023.
- TAP: temporary code for new hire onboarding or recovery.

Lab 2.10 — MFA Configuration

1. Identify and exclude 2 break-glass accounts from MFA.
2. Entra Admin Center → Conditional Access → New policy.
3. Name: "Pilot - Require MFA for IT".
4. Users: IT pilot group (5 test users).
5. Apps: All cloud apps.
6. Grant: Require MFA.
7. Enable in Report-only mode first.
8. Monitor sign-in logs for 24 hours.
9. Flip to "On".
10. Have one user attempt sign-in; verify MFA prompt.
11. Generate TAP for that user, demonstrate alternative path.

Summary

Section 2.10 Summary

- MFA = 2+ factors (know, have, are).
- Deploy via Security Defaults (free) or Conditional Access (P1+).
- Authenticator + number matching is the most robust common method.
- SMS/voice are weakest — phase out.
- Always exclude break-glass accounts.
- TAP for onboarding and recovery.

2.11 Authentication Methods

Introduction

Authentication methods are the specific ways users prove their identity: passwords, Authenticator notifications, FIDO2 keys, certificates, etc. The Authentication methods policy controls which methods are enabled in your tenant and who can use them.

Authentication Methods Catalog

Method	MFA?	SSPR?	Passwordless?
Password	—	—	—
Microsoft Authenticator (push/code)	✅	✅	✅ (Phone sign-in)
FIDO2 security key	✅	—	✅
Windows Hello for Business	✅	—	✅
Certificate-based authentication	✅	—	✅
OATH hardware token	✅	✅	—
SMS	✅	✅	✅ (low-trust)
Voice call	✅	✅	—
Email	—	✅	—
Security questions	—	✅	—

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Protection` → `Authentication methods` → `Policies`

Step-by-Step: Configure Authentication Methods Policy

1. Entra Admin Center → Protection → Authentication methods.
2. Click any method (e.g., Microsoft Authenticator).
3. Toggle Enable: Yes.
4. Target: All users OR specific groups.

5. Configure method-specific settings:
    - Require number matching
    - Show application name in push
    - Show geographic location in push
6. Save.
7. Repeat for each method you want enabled.
8. Disable methods you don't want (e.g., SMS, voice).

Authentication Strength Policies (Entra ID P1+)

"Authentication strength" defines combinations of methods that satisfy a CA policy:

Built-in Strength	Methods That Satisfy
MFA	Password + (any 2nd factor)
Passwordless MFA	Authenticator push, FIDO2, Windows Hello, cert-based
Phishing-resistant MFA	FIDO2 key, Windows Hello, cert-based

Custom strengths: combine any 2+ methods, e.g., "Hardware token OR FIDO2".

Use in Conditional Access

1. CA policy → Grant → Require authentication strength.
2. Select strength (Phishing-resistant MFA).
3. Now privileged ops require FIDO2/Hello, blocking SMS-only MFA.

PowerShell

```
# Get authentication method policy
Connect-MgGraph -Scopes "Policy.Read.All"
Get-MgPolicyAuthenticationMethodPolicy

# Get specific method policy
Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration |
    Select-Object Id, State

# Update method (example: disable SMS)
Update-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration `
    -AuthenticationMethodConfigurationId "Sms" `
    -State "disabled"
```

Best Practices

- Disable SMS and voice for new tenants.
- Enable Authenticator app (push + code).
- Enable FIDO2 for high-value users (admins, finance, executives).
- Use authentication strengths to enforce phishing-resistant MFA on privileged actions.
- Phase out per-user MFA in favour of CA.

Summary

Section 2.11 Summary

- Authentication methods policy = central control of which factors are available.
- Push + number matching = baseline.
- FIDO2 / Hello = phishing-resistant tier.
- Authentication strengths let CA require specific factor combinations.

2.12 Passwordless Authentication

Introduction

Passwordless authentication eliminates the password entirely. Users sign in with biometric (face, fingerprint), PIN tied to a device, FIDO2 hardware key, or phone-based approval. No password = no phishing target.

Why Go Passwordless

- Eliminates password phishing attacks
- No password to leak in breaches
- No password reset tickets (different mechanism)
- Better UX — no typing, just tap/look
- Microsoft's strategic direction

Three Microsoft Passwordless Options

Option	How It Works	Best For
Microsoft Authenticator phone sign-in	Approve from phone with biometric or PIN; no password entered	Most users; works on any device
FIDO2 security key	Hardware key (Yubikey, Feitian); tap to sign in	Shared workstations, kiosks, high-security roles
Windows Hello for Business	Biometric/PIN tied to specific Windows device	Domain-joined Windows PCs

Step-by-Step: Enable Authenticator Phone Sign-In

1. Entra Admin Center → Protection → Authentication methods → Microsoft Authenticator.
2. Enable: Yes; Target: All users (or pilot group).
3. Authentication mode: Any (push + OATH + passwordless).
4. Save.
5. User registers Authenticator at https://mysignins.microsoft.com → Add method → Microsoft Authenticator.
6. User enables phone sign-in: open Authenticator app → tap account → Enable phone sign-in.
7. Now at sign-in: enter username → choose "Use Microsoft Authenticator app" → phone shows approval prompt with biometric.

Step-by-Step: FIDO2 Security Key

Configure Tenant

1. Authentication methods → FIDO2 security key.
2. Enable: Yes.
3. Allow self-service set up: Yes.
4. Enforce attestation: Yes (verify the key is genuine).
5. Enforce key restrictions: Yes (allow only specific AAGUIDs / brands).
6. Save.

User Registration

1. User goes to https://mysignins.microsoft.com → Security info.
2. + Add sign-in method → Security key.
3. Insert key, touch sensor.
4. Set PIN (8 chars min by default).
5. Name the key (e.g., "Work Yubikey").

6. Save.

Sign-In Experience

1. At sign-in: choose "Sign in with security key."
2. Insert key, touch sensor, enter PIN.
3. Signed in — no password ever typed.

Windows Hello for Business

Configured via Intune compliance/configuration policies or Group Policy:

- Provisioned during Windows out-of-box experience (OOBE) or post-join.
- Uses TPM-backed credentials.
- Authenticates against Entra ID with PKI.

Real-World Scenarios

Scenario: Finance team passwordless rollout

Finance handles sensitive ACH/wire data. IT issues each member a Yubikey 5C Nano. CA policy: "Finance app requires Phishing-Resistant MFA." Yubikey + PIN = phishing-resistant. Even if attacker phishes credentials, they can't replay against the FIDO2-protected app. Major bank fraud incidents prevented.

Scenario: Shared workstation

A factory has 5 shared kiosk PCs used by 50 different workers per shift. Issuing each worker a Yubikey makes shared workstations work cleanly: each worker has their own key on a lanyard, sign in by tap, get their session, sign out. No shared passwords, no posted-note credentials.

Best Practices

- Start with one user group (e.g., IT or executives).
- Provide hardware keys for users who need them.
- Enforce attestation to prevent counterfeit FIDO2 keys.
- Pair passwordless with Conditional Access "Phishing-Resistant MFA" requirement.
- Document recovery: what happens when key is lost (revoke + issue new + TAP).
- Combine with Conditional Access location/risk requirements for layered security.

Common Errors

Issue	Resolution
"Security key isn't supported"	Browser doesn't support WebAuthn; use Edge/Chrome/Firefox
"This security key is not allowed"	Attestation blocked; verify AAGUID allow-list includes that brand
Phone sign-in not appearing	User hasn't enabled phone sign-in in Authenticator app; check tenant policy
Hello not provisioned	Verify Intune policy; TPM available; Entra-joined

Interview Questions

Q: Why is passwordless authentication more secure than password + MFA?

A: Password + MFA: still has a password that can be phished or breached. Attacker steals password, social-engineers MFA, takes over. Passwordless: no password exists. The credential is hardware-bound (FIDO2 key, TPM) or biometric — not phishable, not transferable.

Q: What's WebAuthn?

A: W3C standard for passwordless web authentication. FIDO2 = WebAuthn + CTAP (Client to Authenticator Protocol). Combined: a hardware security key registers a public-private keypair with the relying party; auth involves signing a challenge with the private key. Phishing-resistant by design — the key only signs challenges from the registered origin.

Exam-Focused Notes

- Three passwordless options: Authenticator phone, FIDO2, Windows Hello.
- FIDO2 = phishing-resistant.
- Attestation = verifying the FIDO2 key is genuine.
- AAGUID = identifier per FIDO2 key model.
- Combine with CA "Authentication strength" for phishing-resistance enforcement.

Summary

Section 2.12 Summary

- Passwordless removes the phishable password.
- Three options: Authenticator app, FIDO2, Windows Hello.
- FIDO2 = highest security via WebAuthn.
- Pair with CA Authentication Strength for enforcement.

2.13 Microsoft Entra Roles

Introduction

Microsoft Entra has 100+ built-in administrative roles, each grouping specific permissions. Roles let you grant the right level of access to admins — Global Admin for everything, User Administrator for user management only, Helpdesk Administrator for password resets only.

Why This Topic Is Important

Granting Global Admin to a helpdesk tech is malpractice — one compromised credential takes down the whole tenant. Role-based access control gives least privilege: each admin gets exactly what they need, no more.

Key Concepts

Most Common Roles

Role	What They Can Do
Global Administrator	Everything. Total tenant control. Limit to 2-5 people max.
Privileged Role Administrator	Manage role assignments and CA policies
User Administrator	Create/manage users (non-admins), groups, licenses
Helpdesk Administrator	Reset passwords for non-admin users
Authentication Administrator	Reset auth methods (MFA, FIDO) for non-admin users
License Administrator	Assign and remove licenses
Exchange Administrator	Full Exchange Online management
SharePoint Administrator	Manage SharePoint Online + OneDrive
Teams Administrator	Full Teams management
Intune Administrator	Full Intune / endpoint management
Security Administrator	Defender, identity protection, audit
Security Reader	Read-only on security features
Compliance Administrator	Manage Purview compliance solutions
Global Reader	Read-only on everything (perfect for auditors)
Billing Administrator	Manage subscriptions, invoices, payment
Reports Reader	View usage reports only

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Identity` → `Roles & admins` → `All roles`

Step-by-Step: Assign a Role

1. Entra Admin Center → Roles & admins → All roles.
2. Search for role (e.g., "Helpdesk Administrator") → click.

3. + Add assignments.
4. Choose user(s) or group.
5. Assignment type:
    - Eligible (with PIM, P2 only) — user can activate when needed
    - Active — permanent assignment
6. Set duration if eligible.
7. Justification (audit trail).
8. Assign.

Just-In-Time Activation with PIM (Entra ID P2)

Privileged Identity Management (PIM) lets admins activate elevated roles on demand instead of holding them permanently:

- Eligible: user CAN activate the role.
- Active: role currently activated for them.
- Activation requires: MFA, justification, optional approval, time limit (default 8 hours).
- After expiration: automatically returned to eligible state.
- All activations are logged.

PIM Activation Flow

1. Admin needs to perform privileged task.
2. Go to https://portal.azure.com → PIM → My roles.
3. Find eligible role → Activate.
4. Provide justification, complete MFA if required.
5. Optionally wait for approver.
6. Role active for set duration.
7. Performs work; role deactivates automatically.

PowerShell

```
# List all directory roles
Connect-MgGraph -Scopes "RoleManagement.Read.Directory"
Get-MgRoleManagementDirectoryRoleDefinition |
    Select-Object DisplayName, Id, IsBuiltIn |
    Sort-Object DisplayName

# Get current role assignments for a user
$userId = (Get-MgUser -UserId "admin@contoso.com").Id

Get-MgRoleManagementDirectoryRoleAssignment -Filter "PrincipalId eq '$userId'" |
    ForEach-Object {
        $role = Get-MgRoleManagementDirectoryRoleDefinition -UnifiedRoleDefinitionId
$_.RoleDefinitionId
        [PSCustomObject]@{
            User = "admin@contoso.com"
            Role = $role.DisplayName
            Scope = $_.DirectoryScopeId
        }
    }

# Assign Helpdesk Administrator role
$role = Get-MgRoleManagementDirectoryRoleDefinition -Filter "displayName eq
'Helpdesk Administrator'"
$user = Get-MgUser -UserId "helper@contoso.com"

New-MgRoleManagementDirectoryRoleAssignment `
    -PrincipalId $user.Id `
    -RoleDefinitionId $role.Id `
    -DirectoryScopeId "/"

# Find all Global Admins
$ga = Get-MgRoleManagementDirectoryRoleDefinition -Filter "displayName eq 'Global
Administrator'"
Get-MgRoleManagementDirectoryRoleAssignment -Filter "RoleDefinitionId eq '$
($ga.Id)'" |
    ForEach-Object {
        Get-MgUser -UserId $_.PrincipalId | Select-Object DisplayName,
UserPrincipalName
    }
```

Role Best Practices

- Limit Global Admins to 2-5 people; use PIM for activation.
- Use built-in roles before custom roles.
- Apply least privilege: pick the most specific role that works.
- Audit role assignments quarterly via access reviews.

- Require MFA + phishing-resistant auth strength for privileged role activations.
- Document each role assignment with justification.
- Use cloud-only accounts for Global Admins (not synced from on-prem).
- Have 2+ break-glass Global Admins excluded from all CA policies.

Common Errors

Error	Resolution
"You don't have permission"	Need higher role or scope; check assignment
"Role assignment not in effect"	Replication lag (up to 1 hour); sign out + back in
"Cannot remove last Global Admin"	Must always have at least one
"PIM activation failed"	MFA not registered; activate MFA registration first

Interview Questions

Q: How many Global Administrators should a tenant have?

A: 2-5. Two minimum for redundancy. Five maximum to limit attack surface. Use PIM (eligible) instead of permanent assignment for daily admins.

Q: What's the difference between Eligible and Active in PIM?

A: Eligible = user has the right to activate the role on demand (default state, no privilege). Active = role is currently activated for the user (privileged state, time-limited). PIM = framework for this Just-In-Time access.

Q: What is a break-glass account?

A: Emergency access account. Cloud-only Global Admin with very strong unique password, no MFA (to avoid lockout from MFA outage), excluded from all CA policies. Used only when normal admin access fails (Microsoft outage, CA misconfiguration). Sign-in alerts monitored aggressively.

Exam-Focused Notes

- Global Admin = highest privilege. Default: 2-5 max.
- PIM requires Entra ID P2.
- Built-in roles: 100+; custom roles supported (P1+).
- Role assignment scopes: directory (root), administrative unit, or specific app.
- Break-glass: 2+ accounts excluded from CA, monitored for sign-in.

Summary

Section 2.13 Summary

- 100+ built-in Entra roles for least-privilege admin.
- Common: Global Admin, User Admin, Helpdesk Admin, Exchange/SharePoint/Teams/Intune Admins.
- PIM provides Just-In-Time activation (P2).
- Eligible vs Active assignment.
- Have 2+ break-glass cloud-only Global Admins.

2.14 Role-Based Access Control (RBAC)

Introduction

RBAC is the access-control model used throughout Microsoft 365 and Azure. The principle: assign permissions to roles, assign roles to users (or groups). This decouples "what can be done" from "who can do it."

RBAC vs ABAC

Model	Description	Use
RBAC	Roles + permissions; users get roles	Entra, Exchange, SharePoint, Teams
ABAC (Attribute-Based)	Conditions based on user/resource attributes	Azure Storage with conditions

RBAC Components Across Workloads

Workload	Built-in Roles	Custom Roles?
Entra ID	100+ roles	Yes (P1+)
Azure (resources)	Owner, Contributor, Reader, Custom	Yes
Exchange Online	15+ (RBAC role groups + management roles)	Yes
SharePoint Online	Site collection admin, Site owner, Site member	Limited
Teams	Teams Admin, Comms Admin, Comms Support	No
Intune	10+ scoped roles	Yes
Defender	Defender for Endpoint roles, MTP RBAC	Yes
Purview	Compliance Admin, eDiscovery Manager, etc.	Yes

Custom Roles in Entra ID

When built-in roles don't fit, create custom roles. Example: "Group Administrator for Sales Department" — can create/manage groups whose name starts with "Sales-".

1. Entra Admin Center → Roles & admins → All roles → + New custom role.
2. Name + description.
3. Permissions: select from catalog (e.g., microsoft.directory/groups/create).
4. Save.
5. Assign with scope: directory or specific administrative unit.

Exchange Online RBAC

Exchange has its own RBAC model — role groups (containers) made up of management roles (sets of cmdlets):

Built-in Role Group	Purpose
Organization Management	Full Exchange admin
Recipient Management	Mailbox + recipient management
Compliance Management	Litigation hold, audit, journaling
Records Management	Retention
Help Desk	Limited recipient changes
View-Only Organization Management	Read-only

Custom Exchange RBAC

1. EAC → Roles → Admin roles.
2. + Add a role group → name + permissions.
3. Add members.
4. Optionally scope: specific OUs or recipient filters.

RBAC Scopes

Scopes limit where the role applies:

Scope	Where Role Applies
Tenant (default)	Entire directory
Administrative unit	Limited subset of users/groups/devices
Application	Specific app registration
Resource (Azure)	Subscription, resource group, or resource

Best Practices

- Use groups for role assignment, not direct user assignment, where possible.
- Prefer built-in roles; custom roles only when justified.
- Apply scope (admin units, AU) to limit blast radius.
- Audit roles quarterly with Access Reviews.
- Don't over-permission service principals — apps are common attack vectors.
- Use PIM for time-bound activation of high-privilege roles.

Summary

Section 2.14 Summary

- RBAC = roles with permissions, assigned to users/groups.
- Each workload has its own RBAC model.
- Use scopes (administrative units) to limit role reach.
- Combine with PIM for time-bound activation.

2.15 Administrative Units

Introduction

Administrative Units (AUs) in Entra ID let you delegate administration over a SUBSET of users/groups/devices. Without AUs, an admin role applies tenant-wide. With AUs, you grant the same role but scope it to only the AU's members.

Why This Topic Is Important

In a multi-region, multi-business-unit organization, you don't want a regional helpdesk to reset passwords for users in OTHER regions. AUs solve this: the EMEA Helpdesk admin gets Helpdesk Administrator role scoped to the EMEA AU, can only reset EMEA users' passwords.

Key Concepts

Aspect	Details
What an AU contains	Users, groups, devices (since 2022)
Membership	Manual or dynamic (rule-based)
License required	Entra ID P1+ for users in AUs
Roles that support AU scoping	User Admin, Helpdesk Admin, Authentication Admin, Groups Admin, License Admin, etc.
Roles that DON'T support AU scoping	Global Admin, Application Admin, several specialty roles

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Identity` → `Roles & admins` → `Administrative units`

Step-by-Step: Create an Administrative Unit

1. Entra Admin Center → Roles & admins → Administrative units → + Add.
2. Name: "EMEA-Region".
3. Description: "EMEA users and groups."
4. Next → Membership type: Assigned or Dynamic.
5. If Dynamic User:
    - Rule: `(user.country -eq "DE") or (user.country -eq "FR") or (user.country -eq "PK")`
6. Next → assign roles within this AU:
    - "Helpdesk Administrator" → emea-helpdesk@contoso.com
7. Review + Create.

Scoped Role Assignment

The EMEA Helpdesk admin can now:

- Reset passwords for users in EMEA AU
- Cannot reset passwords for users in other AUs (or no AU)
- Cannot modify their own role assignments

PowerShell

```
# Create an AU
$au = New-MgDirectoryAdministrativeUnit `
    -DisplayName "EMEA-Region" `
    -Description "Users in EMEA countries"

# Add member to AU
$user = Get-MgUser -UserId "alice@contoso.com"
New-MgDirectoryAdministrativeUnitMember `
    -AdministrativeUnitId $au.Id `
    -OdataId "https://graph.microsoft.com/v1.0/users/$($user.Id)"

# Assign Helpdesk Admin role scoped to AU
$role = Get-MgRoleManagementDirectoryRoleDefinition -Filter "displayName eq
'Helpdesk Administrator'"
$admin = Get-MgUser -UserId "emea-helpdesk@contoso.com"

New-MgRoleManagementDirectoryRoleAssignment `
    -PrincipalId $admin.Id `
    -RoleDefinitionId $role.Id `
    -DirectoryScopeId "/administrativeUnits/$($au.Id)"
```

Dynamic AU Membership

Like dynamic groups, dynamic AUs auto-calculate membership based on user/device attributes:

```
# EMEA dynamic AU rule
(user.country -in ["DE", "FR", "PK", "GB"]) and (user.accountEnabled -eq true)

# Sales department AU rule (users)
(user.department -eq "Sales")

# All Windows devices AU rule
(device.deviceOSType -eq "Windows")
```

Real-World Scenarios

Scenario: Regional delegation

Contoso has 5 regional helpdesks (US, EMEA, APAC, LATAM, MEA). Each helpdesk should only manage users in their region. Solution: create 5 dynamic AUs based on user.country attribute. Assign Helpdesk Administrator role per AU. Now an APAC helpdesk tech cannot interfere with EMEA users.

Scenario: School / multi-tenant scenario

A university has 5 colleges (Arts, Engineering, Business, Medicine, Law) each wanting their own IT admin team. Solution: 5 AUs based on department. Each college's IT staff gets User Administrator role scoped to their AU. They can manage their own users/groups but not interfere with others.

Best Practices

- Use dynamic AUs for scale; manual for very small sets.
- Source AU rules from authoritative HR / OU data.
- Document each AU's purpose and rule.
- Pair with access reviews of AU-scoped role assignments.
- Combine with PIM for time-bound activation of AU-scoped roles.

Common Errors

Issue	Resolution
"Role does not support administrative unit scope"	Use a role that does — check role definition
User not appearing in dynamic AU	Verify rule syntax; wait 15-30 min
Admin sees more users than they should	Verify role is scoped to AU, not tenant
"P1 license required"	Assign P1 to users in dynamic AUs

Interview Questions

Q: What problem do Administrative Units solve?

A: Without AUs, an admin role like Helpdesk Administrator applies tenant-wide. AUs let you scope roles to a subset of users/groups/devices. Critical for regional or business-unit delegation in multinational organizations.

Q: Can Global Administrator be scoped to an AU?

A: No. Global Admin and several specialty roles cannot be AU-scoped — they're inherently tenant-wide. Use specific scoped roles (User Admin, Helpdesk Admin) for delegated admin.

Exam-Focused Notes

- AUs contain users, groups, devices.
- Membership: assigned or dynamic.
- P1 required for dynamic AU users.
- Not all roles support AU scoping.
- Best for regional/business-unit delegation.

Lab 2.15 — Administrative Units

1. Create a dynamic AU: "Country-PK" with rule `(user.country -eq "PK")`.
2. Wait for population (15 min).
3. Create a test admin user "pk-helpdesk@contoso.com".
4. Assign Helpdesk Administrator role scoped to Country-PK AU.
5. Sign in as pk-helpdesk; try to reset password for a PK user (should work) and a US user (should fail).
6. Document the experience.

Summary

Section 2.15 Summary

- AUs = sub-scopes for role assignments.
- Contain users, groups, devices.
- Dynamic or assigned membership.
- Not all roles support AU scoping.
- P1 required for dynamic AU users.
- Solves multi-region / multi-BU delegation.

2.16 Identity Synchronization

Introduction

Identity synchronization is the process of copying user accounts, groups, and contacts from on-premises Active Directory into Microsoft Entra ID, keeping them aligned through regular sync cycles. The result: a user uses the same username + password for both on-prem resources (file servers, intranet) and Microsoft 365.

Sync Engines

Engine	Where It Runs	Best For
Microsoft Entra Connect Sync	On-prem Windows server	Complex hybrid environments
Microsoft Entra Cloud Sync	Lightweight agent, sync in cloud	Simple deployments, modern recommendation

What Syncs?

Object Type	Direction	Notes
Users	AD → Entra	UPN, names, dept, manager, phone
Groups (security)	AD → Entra	Memberships sync
Distribution lists	AD → Entra	Email-enabled
Contacts	AD → Entra	Mail-enabled
Password hash	AD → Entra	If PHS enabled; every 2 min
Password write-back	Entra → AD	SSPR pushes new password back
Group write-back	Entra → AD	M365 Groups appear in AD
Device write-back	Entra → AD	For seamless Conditional Access

Sync Filtering

Filter	How	Use
Domain	Include/exclude AD domains	Multi-forest, exclude legacy domains
OU	Include/exclude OUs	Pilot, exclude service accounts, test accounts
Group	Sync only members of a specific AD group	Pilots, gradual rollout
Attribute	Custom (extensionAttribute1, msExchHideFromAddressLists)	Advanced filtering

Step-by-Step: Initial Entra Connect Setup

1. Provision Windows Server 2019/2022 (domain joined, 4+ GB RAM).
2. Sign in as Domain Admin.
3. Download Azure AD Connect from aka.ms/AzureADConnect.
4. Run installer; agree to license.
5. Choose Express settings (most defaults) OR Customize (for advanced).
6. Provide Global Admin credentials for Entra.
7. Provide Enterprise Admin credentials for AD.
8. Optionally configure OU filtering (recommended for pilot).

9. Optionally enable: Seamless SSO, Password Write-back, Group Write-back, Device Write-back.
10. Install — first sync starts.
11. Verify in Entra Admin Center → Users; objects appear.

Sync Schedule

Component	Default Interval
Object sync	30 minutes
Password hash sync	2 minutes
Pass-through auth	Real-time
Cloud Sync interval	2 minutes

Force Sync

```
# Delta sync - only changes since last sync (use most of the time)
Start-ADSyncSyncCycle -PolicyType Delta

# Full initial sync - re-evaluate everything (after rule changes)
Start-ADSyncSyncCycle -PolicyType Initial

# Check current scheduler config
Get-ADSyncScheduler

# Disable scheduled sync (for maintenance / pause)
Set-ADSyncScheduler -SyncCycleEnabled $false
# Don't forget to re-enable!
```

Soft Match vs Hard Match

When a sync object meets an existing cloud-only object with same UPN or mail, Entra Connect tries to merge them:

Match Type	How	Use
Soft match	Matches by SMTP address or UPN	First-time sync where cloud users already exist
Hard match	Matches by ImmutableId (binary representation of objectGUID)	Forest migrations, recovery scenarios

IdFix Tool

Before first sync, run the IdFix tool against your on-prem AD to find:

- UPNs with invalid characters
- Duplicate proxyAddresses
- Bad formatting in email/UPN attributes
- Display names too long

Fix these BEFORE first sync to avoid sync errors. Download from Microsoft.

Hybrid Identity Models

Model	Description	Auth Location
Password Hash Sync (PHS)	Hash-of-hash to cloud	Cloud
Pass-through Authentication (PTA)	Cloud queries on-prem AD via agent	On-prem (via agent)
Federation (AD FS)	Browser redirects to AD FS	On-prem (federation)

Choosing the Right Model

Microsoft Recommends
PHS + Seamless SSO for most organizations. It's the simplest, most resilient (works during on-prem outages), and enables Entra ID Protection features (leaked credentials detection).

PHS + Seamless SSO Flow

```
User signs in to office.com
      |
      v
Entra ID asks for credentials
      |
      v
If domain-joined PC with Seamless SSO:
    Kerberos ticket exchanged silently
      |
      v
Authenticated; no password typed
```

Migrate from Federation to PHS

```
# Use Azure AD Connect wizard to switch sign-in method
# Or PowerShell on the Entra Connect server:
Import-Module ADSync
Set-MsolDomainAuthentication -DomainName contoso.com -Authentication Managed
```

Common Sync Errors

Error	Cause	Resolution
QuarantinedAttributeValueMustBeUnique	Duplicate UPN or proxyAddress	Find duplicate in AD, fix
InvalidSoftMatch	UPN/Mail conflict with cloud-only user	Soft-delete the cloud user, then re-sync
FederatedDomainChangeError	Domain switched between Federated/Managed	Use Convert-MsolFederatedUser cmdlets
InvalidHardMatch	ImmutableID mismatch	Set ImmutableID correctly on cloud user
LargeObject	Attribute exceeds size limit	Trim attribute value on prem

Sync Monitoring

Use **Entra Connect Health**:

- Install agent on the Entra Connect server.
- Dashboards: sync status, errors, latency, AD FS health.
- Email alerts when sync fails.
- Requires Entra ID P1 (counts users in dirSync).

Real-World Scenarios

Scenario: First-time sync

A 5,000-user company runs IdFix, finds 230 issues, fixes them. Configures Entra Connect with OU filtering scoped to "OU=Pilot." Pilot OU contains 50 IT users. Syncs successfully. Validates sign-in. Expands filter to include all production OUs. Initial sync takes 4 hours; subsequent delta syncs complete in 1-2 minutes.

Scenario: Removing federation

Company has AD FS that became a SPOF. Migration plan: Update Entra Connect to PHS mode (Sign-in method change). Run sync. Convert federated domain to managed: `Set-MsolDomainAuthentication -Authentication Managed`. Decommission AD FS over 30 days after confirming all users work.

Best Practices

- Run IdFix BEFORE first sync.
- Pilot with OU filtering.
- Deploy a staging-mode Entra Connect server for HA / testing.
- Monitor with Entra Connect Health.
- Use PHS + Seamless SSO unless specific reason otherwise.
- Source authoritative HR data; sync attributes from there.
- Document sync rules and customizations.
- Don't directly edit synced object attributes in cloud — they'll be overwritten.

Interview Questions

Q: What's the difference between PHS and PTA?

A: PHS sends a one-way hash-of-hash of the password to Entra; authentication happens in cloud. PTA leaves passwords on-prem; cloud sends auth requests to on-prem agents that validate against AD in real time. PHS is simpler and more resilient; PTA appeals to orgs that don't want password material in cloud.

Q: How would you migrate from AD FS to PHS?

A: Use Entra Connect wizard to switch sign-in method to "Password Hash Sync + Seamless SSO." Verify sync. Convert federated domain: `Set-MsolDomainAuthentication -DomainName contoso.com -Authentication Managed`. Test sign-in. Decommission AD FS after grace period.

Exam-Focused Notes

- Default sync intervals: 30 min (Connect), 2 min (Cloud Sync, PHS).
- IdFix runs against on-prem AD before initial sync.
- PHS + Seamless SSO is Microsoft's recommendation.
- Hard match = ImmutableID; Soft match = UPN/SMTP.
- Staging mode = read-only secondary, hot standby.

Summary

Section 2.16 Summary

- Entra Connect (on-prem) or Cloud Sync (lightweight) syncs AD → Entra.

- 30-min default; 2-min for password hash.
- Three sign-in methods: PHS, PTA, Federation.
- PHS + SSO recommended.
- Run IdFix first; pilot with OU filtering.
- Monitor with Entra Connect Health.

2.17 Hybrid Identity (Deep Dive)

Architecture Patterns

Pattern 1: PHS + Seamless SSO (Recommended)

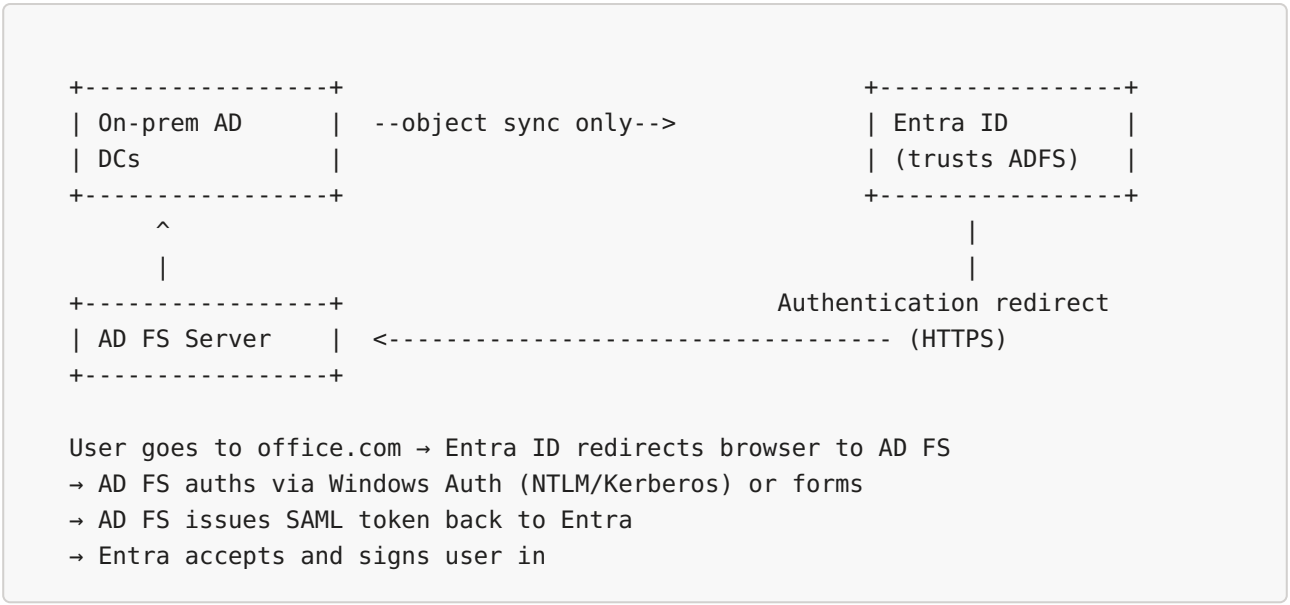
```
+-----------------+              Internet              +-----------------+
| On-prem AD      |  --hash-of-hash sync (2min)-->     | Entra ID        |
| DCs             |  --object sync (30min)-->          |                 |
+-----------------+                                    +-----------------+
      |                                                       |
      |                                                       |
      +-----------+ Same UPN/password used for both +--------+
                  |
                User signs in to office.com
                → authenticated in cloud
                → if domain-joined PC: Kerberos SSO
```

Pattern 2: PTA + Seamless SSO

```
+-----------------+                                    +-----------------+
| On-prem AD      |  --object sync only-->             | Entra ID        |
| DCs             |                                    |                 |
+-----------------+                                    +-----------------+
      ^                                                       |
      |                                                       |
      |                                                       |
+-----------------+  <--auth request (real-time)----------+
| PTA Agent       |
+-----------------+

User signs in to office.com
→ Entra ID forwards auth to on-prem PTA agent
→ Agent validates against AD
→ Returns yes/no to Entra
```

Pattern 3: AD FS Federation



Comparison: Three Hybrid Models

Aspect	PHS	PTA	Federation
Where auth happens	Cloud	On-prem (real-time)	On-prem
Password hash in cloud	Yes (one-way)	No	No
On-prem AD outage impact	Auth still works	Auth stops	Auth stops
Complexity	Low	Medium	High
Infrastructure	Entra Connect	Connect + Agents	Connect + AD FS + WAP
Smart card auth	No	No	Yes
Identity Protection (leaked credentials)	Yes	No	No
Disaster recovery	Easy	Medium	Hard

Decision Matrix

If your org needs...	Choose
Simplicity + resilience	PHS + Seamless SSO
Password hash never in cloud (regulatory)	PTA + Seamless SSO
Smart cards or X.509 certificate sign-in	Federation (or move to Entra cert-based auth)
Existing AD FS infrastructure already in place	Stay with federation OR plan migration to PHS
Cloud-only future	PHS today, plan to eliminate hybrid

Real-World Migration Story

Case: Contoso Bank, 45,000 users

Original setup: AD FS federation. Frequent AD FS issues caused multi-hour outages affecting all 45,000 users. Decision: migrate to PHS + Seamless SSO over 6 months. Phase 1: deploy Entra Connect with PHS already syncing hashes (no impact). Phase 2: switch sign-in method on a single test domain. Phase 3: validate users sign in. Phase 4: migrate remaining domains over 3 weeks. Phase 5: decommission AD FS / WAP infrastructure. Outcome: zero outages for 18 months post-migration; saved $500k/year in licensing + maintenance.

Summary

Section 2.17 Summary

- Three hybrid models: PHS (cloud auth), PTA (on-prem real-time), Federation (on-prem AD FS).
- PHS = simplest, most resilient; recommended default.
- Federation increasingly being retired in favor of PHS.
- Match the model to compliance and operational needs.

2.18 Conditional Access Policies

Introduction

Conditional Access (CA) is the heart of Entra ID's Zero Trust enforcement. CA policies evaluate every sign-in: *who is signing in, to what, from where, on what device, with what risk level?* Then they apply controls: allow, block, require MFA, require compliant device, require password change, and more.

Why This Topic Is Important

Static policies (allow all from internal network, deny all from outside) don't work in cloud reality. CA dynamically evaluates each sign-in. It's how modern orgs enforce strong auth without crippling productivity.

The CA Mental Model

WHO + WHAT + WHERE/HOW = THEN what?

WHO (Users)	WHAT (Resources)	WHERE/HOW (Conditions)	THEN (Controls)
All users Specific users Groups Guests Roles External users	All cloud apps Specific apps Microsoft 365 services User actions (register security info)	Sign-in risk User risk Device platforms Locations Client apps Device state Filter for devices	Block Require MFA Require compliant device Require Entra-joined Require app protection policy Require password change Require terms of use

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Protection` → `Conditional Access`

Recommended Baseline CA Policies

Policy	Why
1. Block legacy authentication	POP/IMAP/Basic Auth bypass MFA; block at source
2. Require MFA for all users (excl. break-glass)	99.2% of automated attacks blocked
3. Require MFA for admins (always)	Admins are high-value targets
4. Require compliant device for sensitive apps	Defense-in-depth: MFA + device posture
5. Block high-risk sign-ins	Identity Protection signals
6. Require password change for high user risk	Identity Protection signals
7. Country block (block sign-ins from countries you don't operate)	Reduce attack surface
8. Require MFA for Azure management	Cloud admin actions need MFA

Step-by-Step: Create Your First CA Policy

Block Legacy Authentication

1. Entra Admin Center → Protection → Conditional Access → + New policy.
2. Name: "CA-001 - Block Legacy Authentication".
3. Users: All users (Exclude: break-glass accounts).
4. Target resources → Cloud apps → All cloud apps.
5. Conditions → Client apps → Yes (configure). Select: Exchange ActiveSync clients, Other clients. Uncheck: Browser, Mobile apps.
6. Grant: Block access.
7. Enable policy: Report-only.
8. Save.
9. Monitor sign-in logs → CA report column for 7-14 days.
10. If no legitimate failures, switch to "On".

Require MFA for All Users

1. + New policy.
2. Name: "CA-002 - Require MFA for All Users".
3. Users: All users (Exclude: break-glass accounts).
4. Target resources → All cloud apps.
5. Conditions: (default = all).
6. Grant: Require multi-factor authentication.
7. Report-only first, then On.

Block by Country (Geo-Block)

1. Conditional Access → Named locations → + Countries location.
2. Name: "Disallowed Countries". Add countries you don't operate in.
3. Save.
4. + New CA policy: "CA-005 - Geo Block".
5. Users: All (excl break-glass).
6. Apps: All.
7. Conditions → Locations → Include: "Disallowed Countries".
8. Grant: Block access.
9. Enable.

Policy Evaluation Order

CA does NOT evaluate policies in numbered order. It evaluates ALL applicable policies for the sign-in, then:

1. If ANY policy says "Block" → blocked.
2. If grant controls have AND/OR — all required controls must be satisfied.
3. Most restrictive wins.

Report-Only Mode

Critical feature. Report-only logs what WOULD happen without enforcing. Use for:

- Testing new policies before production
- Validating policy targeting (right users, right apps)
- Finding edge cases (service accounts, legacy clients)

Activity: View under Sign-in logs → filter by CA policy.

What-If Tool

Simulate a sign-in to see which policies apply:

1. CA blade → What If.
2. Enter: user, app, IP, platform, sign-in risk, etc.
3. Click Run.
4. See: matching policies, applied controls, result.

PowerShell

```
# List all CA policies
Connect-MgGraph -Scopes "Policy.Read.All"
Get-MgIdentityConditionalAccessPolicy | Select-Object DisplayName, State

# Export policies (backup)
$policies = Get-MgIdentityConditionalAccessPolicy
$policies | ConvertTo-Json -Depth 10 | Out-File ca_backup_2026-01-15.json

# Get policy details
$policy = Get-MgIdentityConditionalAccessPolicy |
    Where-Object { $_.DisplayName -eq "CA-002 - Require MFA for All Users" }

$policy.Conditions | Format-List
$policy.GrantControls | Format-List
```

Common CA Conditions

Sign-in Risk (Identity Protection)

Real-time risk score per sign-in:

- High → block or require strong MFA
- Medium → require MFA
- Low → require MFA (optional)
- None → no action

User Risk (Identity Protection)

Aggregate risk score per user:

- High → require secure password change + MFA
- Medium → require MFA
- Low → monitor

Device Filter

Target devices with specific attributes — manufacturer, model, OS, extension attributes from Intune.

Authentication Strength

Require specific factor combinations: Phishing-Resistant MFA (FIDO2 + Windows Hello + cert).

Real-World Scenarios

Scenario: Layered CA strategy

Bank deploys 12 CA policies:

1. Block legacy auth (all users)
2. Require MFA for all users
3. Require Phishing-Resistant MFA for Global Admins
4. Block sign-ins from countries the bank doesn't operate in
5. Require compliant device for SAP, finance apps
6. Block downloads from unmanaged devices via SharePoint
7. Require Intune app protection on personal devices
8. Sign-in risk High → block + investigation
9. User risk High → password change + MFA
10. Block all guests from privileged apps
11. Require ToU on first sign-in for guests

12. Require MFA for Azure portal

Result: phishing attempts caught at the door, even when credentials leak.

Scenario: Accidental lockout

Admin creates "Require Compliant Device" CA for all users. Production breaks: developers using personal Macs without Intune are locked out. Lesson: always use Report-only mode first; have break-glass accounts; communicate changes; pilot small groups.

Best Practices

- Always exclude 2+ break-glass accounts from every CA policy.
- Use Report-only first for all new policies.
- Document each policy: purpose, owner, last review date.
- Naming convention: CA-### - Description.
- Backup CA policies regularly (PowerShell export).
- Quarterly review: do these policies still match the threat model?
- Use What-If tool when troubleshooting blocked sign-ins.
- Test critical policies in lab tenant first.
- Combine CA with Identity Protection for risk-based decisions.
- Avoid policy sprawl — fewer, well-designed policies beat many overlapping ones.

Common Errors

Issue	Resolution
"AADSTS50005: User tried to log in with legacy auth"	Block legacy auth policy worked; update client to modern auth
"AADSTS53003: Access blocked by CA policy"	Sign-in matched a block policy; review which one in sign-in logs
"AADSTS53000: Device not compliant"	Intune marks device non-compliant; user must remediate
Accidental admin lockout	Use break-glass account; remove offending policy; never test in production
Service account fails	Service accounts often hit MFA policy; exclude them with named exception (then secure them via different means — secret management, hardware key)

Interview Questions

Q: Why does Microsoft require MFA enforcement via CA over Security Defaults for enterprises?

A: Security Defaults is all-or-nothing. CA is granular: different users, apps, conditions, controls. Enterprises need: report-only mode for testing, exclusion of break-glass accounts, conditional logic. CA delivers all that with Entra ID P1+.

Q: How does Conditional Access support Zero Trust?

A: Zero Trust = "never trust, always verify." CA verifies every sign-in: identity (MFA), device (compliance), context (location, risk), application (sensitivity). Decisions are made per-sign-in, not perimeter-based. CA + Identity Protection + Intune + Defender = Microsoft Zero Trust stack.

Q: What's "report-only" mode used for?

A: Testing a CA policy before enforcement. Policy evaluates but doesn't enforce; results visible in sign-in logs. Lets admins identify users/apps that WOULD be blocked and address before flipping to "On".

Exam-Focused Notes

- CA requires Entra ID P1+ (P2 unlocks risk-based).
- CA policies are NOT evaluated in order — all applicable policies evaluated; Block wins.
- Report-only mode logs without enforcing.
- What-If simulates without affecting real sign-in.
- Always exclude break-glass accounts.
- Service accounts often need explicit exclusion + alternative protection.

Lab 2.18 — Conditional Access

1. Create break-glass account (cloud-only Global Admin); document credentials in physical safe.
2. Create CA-001 - Block Legacy Auth (Report-only).
3. Monitor for 24 hours; identify legacy clients.
4. Flip CA-001 to "On".
5. Create CA-002 - Require MFA (Report-only).
6. Use What-If: simulate a sign-in as a test user.
7. Monitor 24 hours.
8. Flip to "On".
9. Export all policies via PowerShell as backup.

Summary

Section 2.18 Summary

- CA = if/then policies that evaluate sign-ins.
- WHO + WHAT + WHERE/HOW = THEN.
- Common baseline: block legacy auth, require MFA, block high-risk.

- Use Report-only mode for safe testing.
- Use What-If for simulation.
- Always exclude break-glass accounts.
- P1 required; P2 unlocks risk-based.

2.19 Identity Protection

Introduction

Microsoft Entra ID Protection uses machine learning and signal data from billions of daily sign-ins to detect compromised identities. It flags risky sign-ins (impossible travel, anonymous IP, malware-linked IP) and risky users (leaked credentials, anomalous patterns). Then it can auto-remediate via Conditional Access.

Why This Topic Is Important

Even with MFA, attackers find ways in — token theft, MFA fatigue, business email compromise. Identity Protection adds a second layer: detect compromise after authentication and respond automatically.

License Requirements

License	Identity Protection Features
Free Entra ID	None
Entra ID P1	Risk reports (limited detail)
Entra ID P2	Full features: risk-based CA policies, all detections, investigation, PIM

Risk Detections (Sign-In Risk)

Detection	What It Catches
Anonymous IP	Sign-in from Tor / proxy network
Atypical travel / Impossible travel	Two sign-ins from far-apart locations within impossible timeframe
Malware linked IP	IP known to host malware
Suspicious browser	Anomalous browser activity
Unfamiliar sign-in properties	Combination of factors atypical for user
Admin confirmed user compromised	Admin marked user as compromised
Password spray	Account targeted in spray attack
Token issuer anomaly	Suspicious SAML token
Activity from anonymous IP via auth method	Suspicious method combination

Risk Detections (User Risk)

Detection	What It Catches
Leaked credentials	Username/password found in public breach
Entra threat intelligence	Microsoft threat intel hit
Anomalous user activity	Unusual behavior pattern

Risk Levels

Level	Confidence in Compromise
High	Strong indicator; act immediately
Medium	Possible compromise; verify
Low	Anomaly worth monitoring
None	Normal

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Protection` → `Identity Protection`

Identity Protection Reports

Report	What It Shows
Risky users	Users with active or remediated risk
Risky sign-ins	Sign-in events with risk score
Risk detections	Individual detection events
Workbook reports	Customizable Azure Monitor workbooks

Step-by-Step: Configure Risk-Based CA Policies

Sign-In Risk Policy

1. Entra Admin Center → Protection → Conditional Access → + New policy.
2. Name: "CA-008 - Sign-in Risk".
3. Users: All (excl break-glass).
4. Apps: All cloud apps.
5. Conditions → Sign-in risk → Yes; select High, Medium.
6. Grant: Require MFA (or Block for high-risk).
7. Enable.

User Risk Policy

1. + New policy → "CA-009 - User Risk".
2. Users: All (excl break-glass).
3. Apps: All cloud apps.
4. Conditions → User risk → Yes; High.
5. Grant: Require MFA AND Require password change.
6. Session: configure if needed.
7. Enable.

Investigating Risky Users

1. Identity Protection → Risky users.
2. Click a risky user → see risk history, risk events, sign-in details.
3. Actions:
    - Reset password (forces user to set new)
    - Confirm user compromised (raises risk to High)
    - Dismiss user risk (false positive)
    - Block sign-in

PowerShell

```
# Get risky users
Connect-MgGraph -Scopes "IdentityRiskyUser.ReadWrite.All"
Get-MgRiskyUser -All |
    Where-Object { $_.RiskState -eq "atRisk" } |
    Select-Object UserDisplayName, RiskLevel, RiskLastUpdatedDateTime

# Get risky sign-ins (last 7 days)
Connect-MgGraph -Scopes "IdentityRiskEvent.Read.All"
Get-MgRiskDetection -Filter "activity eq 'signin'" -Top 100 |
    Where-Object { $_.RiskLevel -in @("high", "medium") } |
    Select-Object UserPrincipalName, IpAddress, Location, RiskEventType, RiskLevel,
ActivityDateTime

# Dismiss risk on a user (false positive)
$user = Get-MgRiskyUser -Filter "userPrincipalName eq 'alice@contoso.com'"
Invoke-MgDismissRiskyUser -BodyParameter @{ userIds = @($user.Id) }

# Confirm user compromised
Invoke-MgConfirmRiskyUserCompromised -BodyParameter @{ userIds = @($user.Id) }
```

Real-World Scenarios

Scenario: Leaked credentials response

An employee re-uses their corp password on a public site that gets breached. Hours later, Identity Protection flags user risk "High" via leaked credentials detection. CA policy "CA-009 - User Risk" triggers: forces MFA + password change. User goes through SSPR; new password is unique. Attacker, who has the old leaked password, can't get in. Compromise prevented before exploitation.

Scenario: Impossible travel

User signs in from Karachi at 10:05 AM. At 10:09 AM, sign-in attempt from Brazil. Impossible travel detection fires (no commercial flight makes that route in 4 minutes). CA "CA-008 - Sign-in Risk" requires MFA — the Brazilian attacker has the password but no MFA device, sign-in fails. User's account secure.

Best Practices

- Enable both Sign-in Risk and User Risk CA policies.
- Start with Report-only to estimate scale.
- Set Sign-in Risk High → Block; Medium → MFA.
- Set User Risk High → MFA + password change.
- Investigate persistent risky users (could be compromised).
- Tune dismissal — false positives mean you're dismissing legitimate detections.
- Use Entra ID P2 to fully unlock features.
- Integrate with SIEM (Sentinel, Splunk) for correlated investigation.

Common Errors

Issue	Resolution
"User can't reset password" after user risk	SSPR not enabled — enable it for the user / org
Risk detections not firing	Need Entra ID P2; verify license assignment
Too many false positives (impossible travel)	Frequent travelers; whitelist trusted locations; tune CA exclusions
User stuck "At risk" after fix	Dismiss user risk in portal to reset status

Interview Questions

Q: What's the difference between sign-in risk and user risk?

A: Sign-in risk is per-sign-in-event: this particular login appears anomalous. User risk is aggregate: this user shows compromise indicators (leaked credentials, multiple anomalies). Different CA policies respond differently — sign-in risk often requires MFA; user risk requires password change.

Q: How does Identity Protection detect leaked credentials?

A: Microsoft monitors paste sites, dark web, and security researchers' breach feeds. When a username/password combo appears, it's checked against tenants using PHS (password hash sync). If a match, user risk raised. Hash-of-hash, so Microsoft sees only hashes, not original passwords.

Exam-Focused Notes

- Identity Protection requires Entra ID P2 for full features.
- Risk-based CA policies = automatic response to detections.
- Leaked credentials detection requires PHS enabled.
- Sign-in risk vs user risk: different scopes, different controls.
- Risk states: at risk → remediated → dismissed.

Lab 2.19 — Identity Protection

1. Verify Entra ID P2 licenses on test users.
2. Create CA "Sign-in Risk High → MFA" (Report-only).
3. Create CA "User Risk High → Password Change" (Report-only).
4. Monitor for a week.
5. Try simulating: sign in from a Tor browser to trigger Anonymous IP detection.
6. Check Risky Sign-ins report.
7. Flip policies to On.

Summary

Section 2.19 Summary

- Identity Protection = ML detection of risky sign-ins and users.
- Sign-in risk = per-event; user risk = aggregate.
- Risk-based CA policies = auto-remediation.
- Requires Entra ID P2 for full features.
- Combines with PHS for leaked-credential detection.

Section 2 — Wrap-Up

Section 2 Synthesis

Section 2 Mastery

- **Users:** create cloud-only, synced, or guest; UsageLocation required for licensing.
- **Bulk creation:** CSV up to 250k; PowerShell scripts for repeatable workflows.
- **Guests (B2B):** external collaboration without giving them a license.
- **Password Policies:** default 8-char, 90-day; "never expire" with MFA recommended.
- **SSPR:** users reset own passwords; P1+; combine with write-back for hybrid.

- **MFA:** Security Defaults (free) or CA (P1+); number matching default.
- **Auth Methods:** Authenticator (push, code), FIDO2, Windows Hello, SMS, voice.
- **Passwordless:** Authenticator phone sign-in, FIDO2, Windows Hello.
- **Entra Roles:** 100+; least privilege; Global Admin 2-5 max with PIM.
- **RBAC:** roles + permissions assigned to users/groups.
- **Administrative Units:** scope roles to subset of directory.
- **Groups:** Security (access), M365 (collaboration), Distribution (email), Dynamic (auto).
- **Group-Based Licensing:** assign once, members inherit.
- **Hybrid Identity:** PHS, PTA, Federation; PHS+SSO recommended.
- **Entra Connect:** 30-min default sync; PHS 2-min; IdFix before first sync.
- **Conditional Access:** if/then policies; Report-only first; always exclude break-glass.
- **Identity Protection:** sign-in risk and user risk; auto-remediate via CA; P2 required.

Section 2 Mini-Quiz

Quiz — 12 Questions

Q1. What attribute must be set before assigning a Microsoft 365 license?

A: UsageLocation (ISO country code)

Q2. How long are deleted users restorable?

A: 30 days

Q3. What's the recommended hybrid sign-in method?

A: Password Hash Sync + Seamless SSO

Q4. Maximum number of Global Admins (recommended)?

A: 2-5 (with at least 2 break-glass)

Q5. Why exclude break-glass accounts from MFA?

A: To preserve emergency access during MFA outages

Q6. Default Entra Connect sync interval?

A: 30 minutes (password hash sync = 2 minutes)

Q7. What license is required for dynamic groups?

A: Entra ID P1 (for users in those groups)

Q8. Which guest UPN format does Entra use?

A: partner_externaldomain.com#EXT#@yourtenant.onmicrosoft.com

Q9. What does CA "Report-only" mode do?

A: Evaluates policies without enforcing; logs would-be outcome in sign-in logs

Q10. What's the strongest MFA method?

A: Phishing-resistant: FIDO2 security key, Windows Hello, certificate-based

Q11. What license is required for risk-based Conditional Access?

A: Entra ID P2

Q12. What does PIM provide?

A: Just-in-time activation of privileged roles, requires Entra ID P2

Section 3
03
Device Management with Intune
Modern endpoint management for Windows, macOS, iOS, Android, and Linux. From enrollment to compliance to remote wipe — Intune is the cloud-native MDM/MAM platform that secures every device touching your data.
Exam Weight: ~20%

3.1 Microsoft Intune Overview

Introduction

Microsoft Intune is the cloud-based Mobile Device Management (MDM) and Mobile Application Management (MAM) service in the Microsoft 365 platform. It's part of Microsoft Intune Suite (formerly Endpoint Manager) and lets you manage endpoints — Windows PCs, Macs, iOS, Android, Linux — from a single web console.

Why This Topic Is Important

Devices are now the primary workspace — and the primary attack surface. Without device management, an organization can't enforce encryption, push updates, deploy applications consistently, or remotely wipe lost devices. Intune is the modern replacement for on-prem SCCM (which still exists for hybrid scenarios as Microsoft Configuration Manager).

Key Concepts

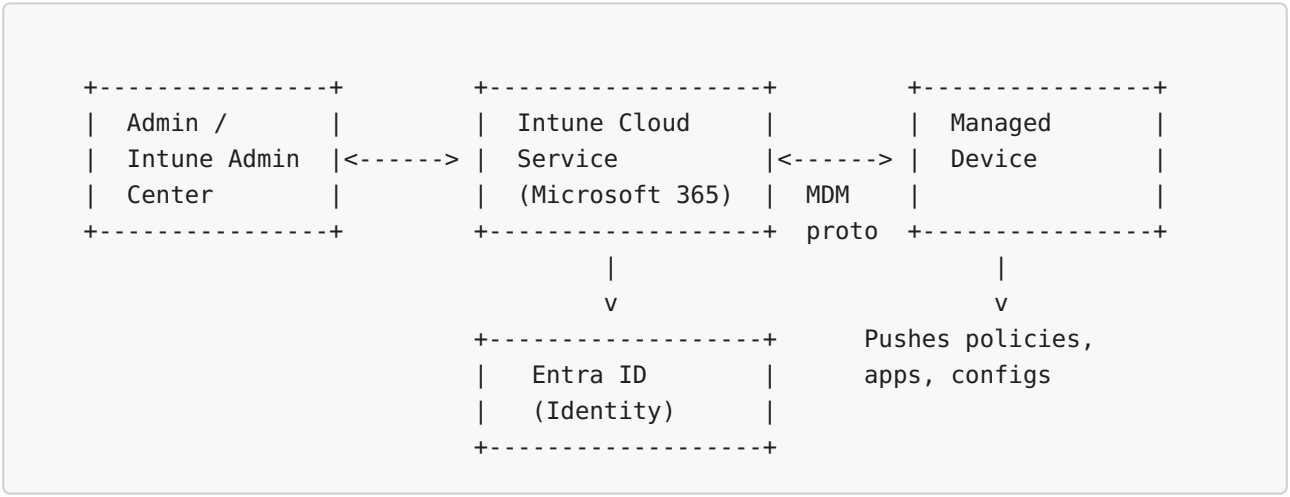
What Intune Does

Capability	Description
MDM (Mobile Device Management)	Full device control: encryption, OS updates, settings, wipe
MAM (Mobile App Management)	App-level control without enrolling device (BYOD)
App deployment	Push apps to devices (Microsoft 365, Win32, line-of-business)
Compliance	Define "healthy device" rules; enforce via Conditional Access
Configuration	Push OS settings: Wi-Fi, VPN, email profiles, certificates
Update management	Windows Update for Business, iOS, Android, macOS update rings
Endpoint Security	Antivirus, disk encryption, firewall, EDR policies
Autopilot	Zero-touch provisioning of new Windows devices
Endpoint Analytics	Performance and reliability scores

Supported Platforms

Platform	Versions Supported	Common Use
Windows	10/11 Pro, Enterprise, Education	Corporate desktops, laptops
macOS	13+	Designer, dev, exec laptops
iOS / iPadOS	15+	Corporate + BYOD phones, tablets
Android	10+ (Enterprise, Personally-Owned Work Profile)	Corporate + BYOD phones, kiosks
Linux	Ubuntu 20.04+, RHEL 8+	Developer machines (limited features)
Chrome OS	Via Cloud PKI / Chrome integration	Education

Architecture / Workflow



License Requirements

License	Intune Capability
Microsoft Intune (standalone)	Full Intune features
Microsoft 365 E3 / E5	Intune included
Microsoft 365 Business Premium	Intune included (SMB)
Enterprise Mobility + Security (EMS) E3 / E5	Intune + Entra ID P1/P2
Microsoft Intune Suite	Adds Remote Help, Endpoint Privilege Mgmt, Advanced Analytics
Microsoft Intune for Education	School-specific

Microsoft Portal Navigation

> 📍 Microsoft Intune Admin Center → `intune.microsoft.com`

Key Sections of the Console

- **Home** — Quick links + key metrics
- **Dashboard** — Tiles for compliance, enrollment, app status
- **Devices** — All enrolled devices, by platform
- **Apps** — App catalog, assignments, app protection policies
- **Endpoint security** — Antivirus, disk encryption, firewall, EDR
- **Reports** — Compliance, app install, update reports

- **Users** — Same as Entra users, with Intune context
- **Groups** — Same as Entra; used for policy/app targeting
- **Tenant administration** — Roles, terms of use, connectors

Intune RBAC Roles

Built-in Role	Purpose
Intune Administrator	Full control
Endpoint Security Manager	Security-focused subset
Policy and Profile Manager	Create policies but not apps
Application Manager	App lifecycle
Help Desk Operator	Limited remote actions: reboot, sync, locate, wipe
School Administrator	Education tenants
Read Only Operator	View-only

Combine with Intune Scope Tags (groups + role) to limit admins to specific devices/users.

Real-World Scenarios

Scenario: Modern workplace rollout

A 1,200-user company replaces aging laptops. Instead of imaging each manually (90 minutes per device, 1,800 hours total), they enroll devices via Windows Autopilot: vendor ships pre-configured to user homes; user opens box, signs in with corporate credentials; Intune provisions everything in 25 minutes. IT effort: nearly zero.

Scenario: BYOD policy

Sales team uses personal phones for email. Company wants email security but can't fully manage personal devices. Solution: deploy Outlook + MS Authenticator on devices; require Intune App Protection Policy (MAM). Corporate email encrypted, copy/paste blocked, no impact on personal apps. Lost phone? Selectively wipe just the corporate data.

Best Practices

- Standardize on Entra-joined Windows for new devices.
- Use Autopilot for new device provisioning.
- MAM for BYOD; MDM for corporate-owned.
- Enforce compliance via Conditional Access.

- Apply scope tags to delegate admin per region/department.
- Use Endpoint Analytics to identify performance issues.

Common Errors and Troubleshooting

Issue	Resolution
"User not licensed for Intune"	Verify Intune service plan in user's license
Enrollment fails	Check MDM authority, enrollment restrictions, Entra device limits
Policies don't apply	Sync device from Company Portal; check assignments
"Couldn't sign in to Intune"	Verify Intune license; check MDM authority is set

Interview Questions

Q: What's the difference between MDM and MAM?

A: MDM = device-level management. The whole device is enrolled, fully controlled. MAM = app-level management. Only specific apps (Outlook, Teams, Word) enforce policies; the device itself isn't enrolled. MDM for corporate-owned; MAM for BYOD.

Q: What is Microsoft Intune?

A: Cloud-based MDM/MAM service. Manages Windows, macOS, iOS, Android, Linux endpoints from a single console. Pushes configuration, apps, security policies, and compliance rules. Integrates with Conditional Access for "compliant device" enforcement.

Exam-Focused Notes

- Intune = MDM + MAM in one cloud service.
- Console URL: intune.microsoft.com.
- Microsoft Intune Suite adds Remote Help, EPM, Advanced Analytics.
- RBAC + scope tags for delegated admin.
- Replaces or complements on-prem SCCM (Configuration Manager).

Summary

Section 3.1 Summary

- Intune = cloud MDM/MAM platform.
- Manages Windows, macOS, iOS, Android, Linux.
- Included in M365 E3/E5, EMS, Business Premium.

- Console: intune.microsoft.com.
- Granular RBAC + scope tags.

3.2 Device Enrollment

Introduction

Enrollment is how a device becomes "Intune-managed." It establishes trust between the device and Intune, allowing policies to flow. Each platform has its own enrollment methods, ranging from fully automated to user-driven.

Enrollment Types by Platform

Platform	Method	Use Case
Windows	Autopilot	New corporate-owned devices
Windows	Entra Join + auto-MDM enrollment	BYOD or self-deployed
Windows	Bulk enrollment with provisioning packages	Imaging without Autopilot
Windows	GPO auto-enrollment	Hybrid AD-joined devices
Windows	Co-management with SCCM	Migrating from SCCM
iOS / iPadOS	Apple Business Manager + ADE	Corporate iPads/iPhones
iOS / iPadOS	User-driven via Company Portal	BYOD
iOS / iPadOS	Apple Configurator	Mass enrollment via cable
Android	Android Enterprise (Work Profile)	BYOD
Android	Android Enterprise (Fully Managed)	Corporate-owned
Android	Android Enterprise (Dedicated / Kiosk)	Single-purpose devices
macOS	Apple Business Manager + ADE	Corporate Macs
macOS	Manual via Company Portal	Existing Macs

Microsoft Portal Navigation

> 📍 Intune Admin Center → `Devices` → `Enrollment`

Prerequisites Before Enrolling

1. **Set MDM Authority:** Tenant administration → Connectors and tokens → MDM Authority must be "Microsoft Intune".
2. **Configure Entra automatic MDM enrollment:**
    - Entra Admin Center → Identity → Mobility (MDM and MAM) → Microsoft Intune.
    - MDM user scope: All (or specific group).
    - Verify MDM terms of use URL, MDM discovery URL.
3. **Assign Intune licenses** to users who will enroll.
4. **Configure enrollment restrictions:** Devices → Enrollment → Device platform restrictions.
5. **Configure device limit per user:** default 5; can raise to 15 or unlimited.

Windows Enrollment Methods (Detail)

1. Entra-Join + Auto-Enrollment (Most Common)

1. User signs into Windows 10/11 with corporate Entra account.
2. Settings → Accounts → Access work or school → Connect → Join this device to Entra ID.
3. Automatic MDM enrollment kicks in (if configured at tenant level).
4. Device appears in Intune within minutes.

2. Hybrid Entra Join

Device joins on-prem AD AND Entra ID. Best for organizations transitioning from on-prem to cloud:

- Requires Entra Connect with Device Write-back.
- Computer object syncs from AD to Entra.
- GPO can trigger MDM auto-enrollment.

3. Bulk Enrollment via Provisioning Package

1. Install Windows Configuration Designer.
2. Create Provisioning package (.ppkg) targeting Entra Join.
3. Apply via USB during Windows OOBE.
4. Device enrolls automatically.

iOS / iPadOS Enrollment

1. Apple Automated Device Enrollment (ADE) (Previously DEP)

1. Sign up for Apple Business Manager (business.apple.com).
2. Link Apple Business Manager to Intune via token.
3. Order devices from authorized reseller — they auto-appear in ABM.
4. Assign devices to Intune in ABM.
5. Create Intune ADE Enrollment Profile.
6. User unboxes, powers on, signs in with corporate creds; Intune deploys settings during setup.

2. BYOD via Company Portal

1. User installs Company Portal app from App Store.
2. Signs in with corporate email.
3. Follows enrollment prompts (downloads MDM profile, trusts profile).
4. Device appears as "personally owned" in Intune.

Android Enrollment (Android Enterprise)

1. Personally-Owned with Work Profile (Recommended for BYOD)

- Creates a separate "work" partition on device.
- Corporate apps and data isolated from personal.
- IT can wipe only the work profile, not personal data.

2. Fully Managed (Corporate-Owned)

- Entire device managed.
- Factory reset required before enrollment.
- Best for dedicated corporate phones.

3. Dedicated / Kiosk Mode

- Single-app or multi-app kiosk.
- Factory floor, retail, transit.

Step-by-Step: Configure Auto-MDM Enrollment for Windows

1. Entra Admin Center → Identity → Mobility (MDM and MAM) → Microsoft Intune.
2. MDM user scope: All (or a group).
3. MDM terms of use URL: leave default.

4. MDM discovery URL: leave default.
5. MDM compliance URL: leave default.
6. Save.
7. Now any user who joins a Windows 10/11 device to Entra automatically gets Intune enrollment.

Enrollment Restrictions

Limit who can enroll, with what platforms, and how many devices:

Restriction Type	Configures
Device platform restrictions	Block certain platforms (e.g., block jailbroken, block personal Android)
Device limit restrictions	Max devices per user (1-15)

Step-by-Step: Block Personal Devices

1. Intune Admin Center → Devices → Enrollment → Device platform restrictions.
2. Default → Properties → Edit.
3. For each platform (iOS, Android, Windows): toggle "Personally-owned": Block.
4. Save. Only corporate-owned devices can enroll.

PowerShell / Graph

```
# Get enrolled devices
Connect-MgGraph -Scopes "DeviceManagementManagedDevices.Read.All"
Get-MgDeviceManagementManagedDevice |
    Select-Object DeviceName, OperatingSystem, ComplianceState, EnrolledDateTime |
    Format-Table

# Get device count by platform
Get-MgDeviceManagementManagedDevice -All |
    Group-Object OperatingSystem |
    Select-Object Name, Count

# Get non-compliant devices
Get-MgDeviceManagementManagedDevice -Filter "complianceState eq 'noncompliant'" -All
|
    Select-Object DeviceName, UserDisplayName, LastSyncDateTime
```

Real-World Scenarios

Scenario: Windows Autopilot pilot

Procurement orders 100 new laptops from Dell. Dell registers them in Microsoft's Autopilot service via hardware hash upload. Each laptop ships directly to the employee. Employee opens box, connects to Wi-Fi, signs in with corporate credentials. Autopilot detects the device, applies the assigned profile, joins Entra ID, enrolls in Intune, installs apps, configures settings. 25 minutes later: user is productive. IT touch time per device: 5 minutes (profile setup, then zero).

Common Errors

Error	Resolution
"This device cannot be enrolled"	Check MDM scope; verify Intune license; check enrollment restrictions
"Account doesn't have permission"	User needs Intune license + MDM scope coverage
"Couldn't connect to server"	Firewall blocking Intune endpoints; verify network connectivity
"Maximum devices reached"	Raise device limit or remove old devices
iOS enrollment hangs at "Awaiting Final Configuration"	VPP/ADE token expired; renew Apple tokens

Summary

Section 3.2 Summary

- Enrollment = device + Intune trust establishment.
- Windows: Autopilot (preferred), Entra-Join, GPO auto-enroll, co-management.
- iOS: ADE (preferred for corp), Company Portal (BYOD).
- Android: Work Profile (BYOD), Fully Managed (corp), Dedicated (kiosk).
- Configure MDM scope and enrollment restrictions before mass enrollment.

3.3 Windows Autopilot

Introduction

Windows Autopilot is Microsoft's zero-touch provisioning service for Windows 10/11. Devices ship directly from OEM to end user; the user signs in once, and Autopilot handles everything else — domain join, Intune enrollment, app installation, settings, security configuration.

Why It Matters

Traditional Windows imaging: IT receives device, applies image (60-90 min), domain-joins, installs apps, configures, ships to user. With Autopilot: device ships from factory directly to user; user signs in, Autopilot does the rest. Saves hours per device and entire imaging infrastructure.

Autopilot Deployment Modes

Mode	Description	Use Case
User-driven	User signs in; device joins Entra; user is local admin (or not)	Standard corporate laptops
Self-deploying	No user interaction; for kiosks, shared devices	Conference rooms, factory floor
Pre-provisioning (formerly White Glove)	IT does most setup before shipping; user just signs in	Faster end-user experience
Existing Devices	Re-purpose existing Windows 10/11 install	Migration from existing image
Reset	Wipe and reprovision via Autopilot	Device handoff, theft recovery

Autopilot Workflow

```
1. OEM uploads hardware hash to Autopilot service
     |
     v
2. Admin assigns Autopilot profile (deployment mode, settings)
     |
     v
3. User unboxes device, connects to internet
     |
     v
4. Windows OOBE detects device is registered for Autopilot
     |
     v
5. Customized OOBE: skip pages, apply branding, prompt for sign-in
     |
     v
6. User signs in with corporate credentials
     |
     v
7. Device joins Entra ID, enrolls in Intune
     |
     v
8. Intune pushes apps, settings, security policies (ESP - Enrollment Status Page)
     |
     v
9. Device ready - user lands on desktop with apps installed
```

Step-by-Step: Configure Autopilot

1. Get Hardware Hashes

Three ways:

- OEM uploads directly (preferred — Dell, HP, Lenovo, Microsoft Surface all support)
- PowerShell on existing device: `Get-WindowsAutoPilotInfo`
- OOBE: Shift+F10, PowerShell, run script, upload to Intune

```
# Get hardware hash from an existing device
md c:\HWID
Set-Location c:\HWID
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted
Install-Script -Name Get-WindowsAutoPilotInfo
Get-WindowsAutoPilotInfo -OutputFile AutoPilotHWID.csv
```

2. Import Hashes to Intune

1. Intune Admin Center → Devices → Enrollment → Windows → Devices.
2. + Import → upload CSV.
3. Devices appear within 15 minutes.

3. Create Autopilot Deployment Profile

1. Devices → Enrollment → Windows → Deployment profiles → + Create profile → Windows PC.
2. Name: "Standard User Provisioning".
3. Convert all targeted devices to Autopilot: Yes.
4. Out-of-box experience:
    - Deployment mode: User-driven
    - Join to Entra ID as: Entra-joined
    - Skip EULA, privacy settings: Yes
    - User account type: Standard (or Administrator)
    - Apply device name template: `CONT-%RAND:5%`
5. Assignments: Autopilot device group (dynamic).
6. Create.

4. Configure Enrollment Status Page (ESP)

ESP shows progress to the user during provisioning:

1. Devices → Enrollment → Windows → Enrollment Status Page → + Create.
2. Show progress: Yes.
3. Block device use until apps/profiles install: Yes.
4. Specify required apps that must be installed: select up to 50.
5. Allow users to retry on failure: Yes.
6. Assign to All Users.
7. Create.

5. Dynamic Device Group for Autopilot

1. Entra → Groups → + New group → Dynamic Device.
2. Rule: `(device.devicePhysicalIds -any (_ -startsWith "[ZTDId]"))` — selects all Autopilot devices.
3. Save.
4. Assign Autopilot profile, apps, configurations to this group.

Hybrid Entra Join via Autopilot

For organizations needing on-prem AD join along with Entra:

- Requires Entra Connect with Domain Join Connector / Intune Connector for AD.
- Devices initially join on-prem AD, then Entra Joined.
- Slower than pure Entra-Join; usually not recommended unless required for legacy GPO/printing.

Best Practice
Use pure Entra-Joined (cloud-only) for new deployments. Hybrid Entra Join adds complexity and depends on connectivity to on-prem AD during enrollment. Microsoft's modern recommendation: cloud-native.

Pre-Provisioning (White Glove)

IT performs most of the heavy lifting before shipping device to user:

1. IT receives factory device.
2. Boots, presses Windows + 5 times at OOBE → Autopilot pre-provisioning.
3. Authenticates, downloads apps, profiles, security — all without user.
4. Reseals (back to OOBE).
5. Ships to user.
6. User opens box, signs in, lands on desktop in 2-5 minutes (vs. 25+ minutes).

Real-World Scenarios

Scenario: 500-device refresh

Acme Corp refreshes 500 laptops over 90 days. Traditional approach: 500 × 90 min = 750 hours of IT imaging. Autopilot: ship factory-fresh to users; IT spends 2 hours configuring Autopilot once; users spend 25 min each completing first-run. Total IT effort: ~10 hours.

Scenario: Theft / replacement

Sales user's laptop stolen. IT remotely wipes via Intune. Orders replacement; OEM ships directly to user. User signs in; identical apps and settings reappear. No re-imaging, no shipping device to IT.

Best Practices

- Register devices via OEM upload — fastest, no manual hash collection.
- Use dynamic groups based on ZTDId.
- Configure ESP with required apps to block desktop until ready.
- Use Autopilot profile to enforce naming convention.
- Test with one device before deploying broadly.
- Communicate to users: expect first sign-in to take 20-30 minutes.

- For self-deploying mode: enable TPM attestation.

Common Errors

Error	Resolution
"Something went wrong" during sign-in	Verify Autopilot profile assigned; check user has Intune license; verify network
ESP times out	Increase ESP timeout; reduce required apps; check app installation logs
Device not appearing in Intune after enrollment	Wait 15 min; force sync; verify hardware hash imported correctly
"Device is registered to another organization"	Hash was uploaded to wrong tenant; delete from other tenant first
Pre-provisioning fails	TPM not attested; check Autopilot self-deploying requirements (TPM 2.0)

Interview Questions

Q: What is Windows Autopilot?

A: Microsoft cloud service for zero-touch Windows provisioning. OEM uploads device hardware hashes; admin assigns deployment profile; user opens factory-fresh box, signs in once, and the device is fully configured — Entra-joined, Intune-enrolled, apps installed, secured.

Q: Compare user-driven vs self-deploying modes.

A: User-driven requires user sign-in during OOBE — for standard corporate laptops. Self-deploying requires no interaction — for kiosks, shared devices, conference rooms. Self-deploying needs TPM 2.0 attestation.

Exam-Focused Notes

- Autopilot uses hardware hash to identify devices.
- Five deployment modes: user-driven, self-deploying, pre-provisioning, existing device, reset.
- Requires Entra ID P1+ (for auto-MDM enrollment).
- ESP blocks user until apps/policies finish — critical for security.
- Hybrid Entra Join adds complexity; cloud-native preferred.

Summary

Section 3.3 Summary

- Autopilot = zero-touch Windows provisioning from cloud.
- OEM uploads hash → admin assigns profile → user signs in → done.
- Five modes; user-driven most common.
- ESP blocks user until ready.
- Saves 60+ minutes per device vs. traditional imaging.

3.4 Compliance Policies

Introduction

Compliance Policies define what makes a device "healthy" in your organization. A compliance policy might say: device must have encryption on, OS version above 22H2, not jailbroken, antivirus running, screen lock enabled. Devices that meet all rules are "compliant"; those that don't are "non-compliant" and can be blocked from accessing M365 via Conditional Access.

Why It Matters

Without compliance enforcement, an unpatched laptop running malware can access corporate email and files. Compliance + Conditional Access = "only healthy devices touch our data."

Compliance Settings by Platform

Setting	Windows	iOS	Android	macOS
Minimum OS version	✅	✅	✅	✅
BitLocker / FileVault	✅ BitLocker	Built-in	✅ encryption	✅ FileVault
Secure Boot	✅	—	—	—
TPM required	✅	—	—	—
Antivirus signature freshness	✅	—	—	—
Defender for Endpoint risk score	✅	✅	✅	✅
Password / PIN required	✅	✅	✅	✅
Jailbreak / Root detection	—	✅	✅	—
Microsoft Defender threat level	✅	✅	✅	✅
Custom compliance scripts	✅ (Windows only)	—	—	—

Microsoft Portal Navigation

> 📍 Intune Admin Center → `Endpoint security` → `Device compliance` → `+ Create policy`

Or: Devices → Compliance policies → Policies

Step-by-Step: Create a Windows Compliance Policy

1. Intune Admin Center → Devices → Compliance policies → + Create policy.
2. Platform: Windows 10 and later.
3. Profile type: Windows 10/11 compliance policy → Create.
4. Name: "Win10/11 - Baseline Compliance".
5. Compliance settings:
    - Device Health → Require BitLocker: Required
    - Device Health → Require Secure Boot: Required
    - Device Health → Require code integrity: Required
    - Device Properties → Minimum OS version: 10.0.22000 (Win 11) or 10.0.19045 (Win 10 22H2)
    - System Security → Password required: Yes

- System Security → Minimum password length: 8
- System Security → Require encryption of data storage on device: Required
- Microsoft Defender Antimalware → Active
- Defender for Endpoint → Require device to be at or under machine risk score: Medium

6. Actions for noncompliance:
   - Mark device noncompliant: Immediately
   - Send email to end user: 1 day after noncompliance
   - Add device to retire list: 30 days after noncompliance
7. Assignments: All Users (or test group first).
8. Create.

Connect to Conditional Access

1. Entra Admin Center → Protection → Conditional Access → + New policy.
2. Name: "CA-010 - Require Compliant Device".
3. Users: All users (excl break-glass).
4. Target resources: All cloud apps.
5. Grant: Require device to be marked as compliant.
6. Save with Report-only first, then On.

Now: non-compliant devices cannot access M365.

Compliance Notifications

Customize what users see when their device becomes non-compliant:

1. Endpoint security → Device compliance → Notifications.
2. + Create notification → name + email subject + message body.
3. Include: company logo, footer, support contact.
4. Use in Actions for noncompliance.

PowerShell / Graph

```
# List all compliance policies
Connect-MgGraph -Scopes "DeviceManagementConfiguration.Read.All"
Get-MgDeviceManagementDeviceCompliancePolicy |
    Select-Object DisplayName, '@odata.type', LastModifiedDateTime

# Get compliance state per device
Connect-MgGraph -Scopes "DeviceManagementManagedDevices.Read.All"
Get-MgDeviceManagementManagedDevice -All |
    Group-Object ComplianceState |
    Select-Object Name, Count

# Find non-compliant devices
Get-MgDeviceManagementManagedDevice -Filter "complianceState eq 'noncompliant'" -All
|
    Select-Object DeviceName, UserPrincipalName, OperatingSystem, LastSyncDateTime
```

Real-World Scenarios

Scenario: BitLocker enforcement

Compliance requires BitLocker. A user's laptop suspends BitLocker for repair. Device flips to non-compliant. CA blocks them from email and SharePoint after 24 hours. Helpdesk gets call; instructs user to re-enable BitLocker. Within 5 minutes of re-enabling and Intune sync, compliant again, access restored.

Scenario: Patched OS requirement

Critical Windows vulnerability disclosed (CVE). IT updates compliance policy: minimum Windows build to latest. Devices that haven't applied the patch become non-compliant within 24 hours, forcing user to install patch to regain access. Forces patching across fleet in 72 hours.

Best Practices

- Define a baseline policy per OS platform.
- Use "Mark device noncompliant: Immediately" for security-critical settings.
- Use longer grace periods for non-critical (e.g., OS version 7 days).
- Pair every compliance policy with a CA "Require compliant" policy.
- Test with pilot group before broad assignment.
- Customize end-user notifications with clear remediation steps.
- Build compliance dashboard with Endpoint Analytics.

Common Errors

Issue	Resolution
Device shows "Not evaluated"	Force sync from Company Portal; wait 1-2 hours
BitLocker compliance fails despite enabled	Verify BitLocker recovery key escrow to Entra; verify reporting setting in encryption policy
OS version compliance fails after update	Force device sync; sometimes takes 24h for new build to register
Compliance + CA = users locked out	Carefully scope CA; have an exception group; use report-only first

Interview Questions

Q: How does compliance + Conditional Access enforce Zero Trust?

A: Compliance defines "healthy device." CA enforces "only healthy devices access data." Together, they ensure a sign-in is allowed only if both the user identity is verified AND the device meets security baseline (encryption, patch level, AV running, not jailbroken). This is core Zero Trust: never trust, always verify.

Q: What's the difference between configuration profile and compliance policy?

A: Configuration profile = "make the device this way" (push settings, certificates, Wi-Fi profiles). Compliance policy = "evaluate the device for these health rules" (read-only check, marks compliant/non-compliant). Configuration is push; compliance is evaluation.

Exam-Focused Notes

- Compliance policies are per-platform.
- Actions for noncompliance include: mark, email user, retire, add to retirement list.
- Pair with CA "Require compliant device" for enforcement.
- Custom compliance via PowerShell scripts (Windows only).
- Defender for Endpoint risk score is a compliance signal.

Summary

Section 3.4 Summary

- Compliance = device health rules.
- Pair with CA "Require Compliant Device" for enforcement.
- Define baseline per platform.
- Test with pilot before broad rollout.

- Customize notifications with remediation steps.

3.5 Configuration Profiles

Introduction

Configuration Profiles push settings to managed devices: Wi-Fi networks, VPN connections, email accounts, certificates, hardware restrictions, browser homepage, Bluetooth, screen timeout, and thousands more. Once assigned, devices conform to those settings automatically.

Profile Types by Platform

Platform	Common Profile Types
Windows	Settings Catalog, Device restrictions, Endpoint Protection, Email, Wi-Fi, VPN, Certificates, Custom (CSP), Admin templates (GPO-equivalent), Delivery Optimization
iOS / iPadOS	Device features, Device restrictions, Email, Wi-Fi, VPN, Certificates, Custom (XML)
Android Enterprise	Device restrictions, Custom OEMConfig, Wi-Fi, VPN, Certificates
macOS	Device restrictions, Settings Catalog, Custom (.mobileconfig), FileVault, Wi-Fi, VPN, Certificates
Linux	Limited — Settings Catalog

Settings Catalog

Settings Catalog is the modern way to configure devices. Microsoft has consolidated thousands of CSP-based settings into a searchable catalog. Use it instead of older "Endpoint Protection" or "Device Restrictions" templates where possible.

Microsoft Portal Navigation

> 📍 Intune Admin Center → `Devices` → `Configuration` → `+ Create`

Step-by-Step: Push a Wi-Fi Profile to Windows

1. Devices → Configuration → + Create → New Policy.
2. Platform: Windows 10 and later; Profile type: Templates → Wi-Fi.
3. Name: "Corp-WiFi-Windows".

4. Wi-Fi type: Enterprise.
5. SSID: ContosoCorp; Network name: ContosoCorp.
6. Automatically connect when in range: Yes.
7. EAP type: EAP-TLS (with cert) or PEAP-MSCHAPv2.
8. Authentication method: Certificate (with deployed cert profile).
9. Assignments: All corporate Windows devices group.
10. Create.

Step-by-Step: Disable USB on Windows

1. Devices → Configuration → + Create → New Policy.
2. Platform: Windows 10 and later; Profile type: Settings Catalog.
3. Name: "Win - Disable USB Mass Storage".
4. + Add settings → search "USB" → Administrative Templates → System → Removable Storage Access.
5. Set "All Removable Storage classes: Deny all access" → Enabled.
6. Assignments: target group.
7. Create.

Step-by-Step: iOS Device Restrictions

1. Devices → Configuration → + Create.
2. Platform: iOS/iPadOS; Profile type: Templates → Device restrictions.
3. Name: "iOS - Corporate Restrictions".
4. Configure:
    - App Store, Doc Viewing, Gaming → block Game Center, restrict app rating
    - Built-in apps → disable Camera (or restrict to work apps), AirDrop, iCloud backup
    - Cloud and storage → require iCloud backup off
    - Connected devices → restrict Bluetooth pairing
    - Password → require passcode, 6-digit min, 5-minute timeout
    - Show in App Switcher: managed apps only
5. Assign and create.

Common Configurations (At a Glance)

Goal	Profile Type
Push corporate Wi-Fi	Wi-Fi profile
Push VPN config	VPN profile (per-app or device-wide)
Auto-configure Outlook	Email profile
Deploy SCEP/PKCS certificate	Certificate profile
Enforce screen lock	Settings Catalog / Device Restrictions
Disable USB storage	Settings Catalog (Removable Storage Access)
Push Edge favorites/homepage	Settings Catalog (Edge)
Disable Bluetooth	Settings Catalog
Block specific apps	App protection / restrictions
Apply security baseline	Endpoint security → Security baselines

Security Baselines

Pre-built sets of recommended security settings. Like a curated configuration profile:

Baseline	Source
Windows security baseline	Windows team
Microsoft Defender for Endpoint baseline	Defender team
Microsoft Edge baseline	Edge team
Windows 365 baseline	Win365 team

Apply a Baseline

1. Endpoint security → Security baselines → choose baseline.
2. + Create profile.
3. Review default values (already secure).
4. Customize if needed; assign; create.

Custom CSP Profiles (Windows)

If a setting isn't in Settings Catalog, use Custom OMA-URI:

1. + Create → Windows 10 and later → Templates → Custom.
2. Add row: Name + OMA-URI + Data type + Value.
3. Example: `./Device/Vendor/MSFT/Policy/Config/Browser/HomePages`
4. Assign.

Best Practices

- Prefer Settings Catalog over templates (more current settings).
- One profile per concern (Wi-Fi profile separate from password profile).
- Use dynamic groups based on device attributes.
- Don't conflict: never put same setting in two profiles assigned to same device.
- Use Security Baselines as a starting point, customize from there.
- Document each profile's purpose in description.
- Pilot, then rollout.

Common Errors

Issue	Resolution
"Conflict" status on profile	Two profiles set same setting differently; resolve by removing conflict
Profile not applying	Force sync; verify assignment; check device compliance state
Wi-Fi profile doesn't connect	Verify SSID, EAP type, certificate chain
Setting Catalog setting not enforced	OS may not support; check minimum OS version for that setting

Summary

Section 3.5 Summary

- Configuration profiles push settings to devices.
- Settings Catalog = preferred modern approach.
- Templates for specific scenarios (Wi-Fi, VPN, email, certs).
- Custom OMA-URI for advanced/legacy settings.
- Security Baselines for pre-built secure starting points.

3.6 Application Deployment

Introduction

Intune deploys apps to managed devices: line-of-business (LOB) apps, Win32 apps, Microsoft Store apps, Microsoft 365 Apps, web apps, iOS Store apps, Android Play apps. Apps can be required (auto-installed) or available (user opts in via Company Portal).

App Types Supported

Platform	App Types
Windows	Microsoft 365 Apps, Win32 (.exe/.msi via .intunewin), MSIX/AppX, Microsoft Store, LOB (.msi), Web link
iOS	iOS Store (free + VPP-purchased), LOB (.ipa), Web link
Android	Google Play (managed + public), LOB (.apk), Web link
macOS	Mac LOB (.pkg, .dmg), Microsoft 365 Apps for macOS, Microsoft Defender for macOS, Web link, Custom

Assignment Types

Type	Behavior
Required	Force-installs on assigned devices/users
Available for enrolled devices	Appears in Company Portal; user opts in to install
Uninstall	Force-removes app
Available with or without enrollment	For MAM-only users (no MDM)

Step-by-Step: Deploy Microsoft 365 Apps for Windows

1. Apps → Windows → + Add → Microsoft 365 Apps → Windows 10/11.
2. Suite name: "Microsoft 365 Apps Standard".
3. Configure app suite:
    - Configuration designer (GUI) or XML data
    - Apps: select Word, Excel, PowerPoint, Outlook, OneNote, Teams
    - Architecture: 64-bit
    - Update channel: Monthly Enterprise

- Languages: en-US (and others as needed)

4. Properties: Shared Computer Activation: No (unless VDI).
5. Assignment: Required → All corporate Windows users group.
6. Review + Create.

Step-by-Step: Deploy a Win32 App

1. Prepare the App Package

Download Microsoft Win32 Content Prep Tool from GitHub. Use it to convert your installer to .intunewin:

```
IntuneWinAppUtil.exe -c C:\source -s setup.exe -o C:\output
```

2. Upload to Intune

1. Apps → Windows → + Add → App type: Windows app (Win32).
2. Select .intunewin file.
3. App information: name, publisher, description, logo.
4. Program:
   - Install command: `setup.exe /silent /quiet`
   - Uninstall command: `"C:\Program Files\App\unins000.exe" /silent`
   - Install behavior: System (for system-wide) or User
5. Requirements: 64-bit OS, Windows 11.
6. Detection rules: registry key, file path, MSI product code, or custom script — to verify app is installed.
7. Dependencies / Supersedence (newer apps replacing older).
8. Assignment.
9. Create.

Detection Rules Examples

Detection Type	Example
MSI	MSI product code present in registry (preferred for MSI installers)
File	File exists: `C:\Program Files\AppName\app.exe`
Registry	Key/value exists: `HKLM\SOFTWARE\AppName\Version`
Custom script	PowerShell returning exit 0 + stdout if installed

iOS / Android App Deployment

iOS Store Apps (Free)

1. Apps → iOS/iPadOS → + Add → iOS store app.
2. Search App Store → select.
3. Properties auto-populate.
4. Assignment → Required for all iOS devices.

iOS VPP (Volume Purchase Program)

1. Apple Business Manager → buy app licenses.
2. Sync VPP token to Intune.
3. Apps appear under "Licensed apps".
4. Assign — Intune allocates licenses.

Android Managed Google Play

1. Apps → Android → + Add → Managed Google Play app.
2. Approve apps from Play Store interface (embedded in Intune).
3. Sync.
4. Assign.

App Configuration Policies

Push configuration to managed apps. Example: pre-configure Outlook with company server settings:

1. Apps → App configuration policies → + Add → Managed devices.
2. Platform: iOS or Android.
3. Targeted apps: Microsoft Outlook.
4. Configuration settings:
    - com.microsoft.outlook.EmailProfile.EmailAccountName: {{username}}
    - com.microsoft.outlook.EmailProfile.ServerAuthentication: Modern
    - com.microsoft.outlook.EmailProfile.EmailAddress: {{userprincipalname}}
5. Assign.

Real-World Scenarios

Scenario: Deploy a custom LOB app

Finance team needs SAP GUI installed on 200 laptops. IT wraps SAPGUI install via Content Prep Tool, uploads to Intune as Win32 app, configures detection rule by registry, assigns "Required" to Finance dynamic group. Within 24 hours all 200 finance laptops have SAP GUI installed.

Scenario: App removal

Company stops using a Slack alternative. IT changes assignment from "Required" to "Uninstall" for all users. Within 8 hours, Intune uninstalls the app from every device. Inventory cleaned up.

Best Practices

- Use Required for mandatory apps; Available for optional.
- Use dynamic device groups for targeting.
- Test detection rules carefully — bad detection = repeated install loops.
- Use Supersedence to replace old app versions cleanly.
- Monitor app install reports daily during deployment.
- For Microsoft 365 Apps, prefer Microsoft Apps deployment over standalone Office installs.
- Pre-stage app icons and branded names for Company Portal.

Common Errors

Error	Resolution
"Win32 app installation failed"	Check IntuneManagementExtension.log on device; verify install command syntax
App keeps reinstalling	Detection rule wrong; not detecting installed state
App not appearing in Company Portal	Check assignment; ensure "Available" not "Excluded"
iOS app stuck "Pending"	VPP token expired; renew Apple tokens
Microsoft 365 install slow	Normal for first install (~3-5 GB); ensure good network

Interview Questions

Q: What's the .intunewin format?

A: A wrapped package format for Win32 app deployment in Intune. The Microsoft Win32 Content Prep Tool compresses your installer and metadata into a single .intunewin file Intune can deploy. Required for non-Store Win32 apps.

Q: What's app Supersedence?

A: Newer app declares "supersedes" an older app. When deployed, Intune optionally uninstalls the older version, then installs the new. Cleaner than two separate apps. Required for many app upgrade scenarios.

Exam-Focused Notes

- Win32 apps require .intunewin packaging.
- Detection rules verify installation; getting them wrong = endless install loops.
- VPP for iOS app licensing.
- Managed Google Play for Android Enterprise.
- Assignment types: Required, Available, Uninstall, Available without enrollment.

Summary

Section 3.6 Summary

- Intune deploys apps to all major platforms.
- Win32 = .intunewin packaging.
- App Configuration Policies pre-configure managed apps.
- Detection rules are critical for Win32.
- Required vs Available vs Uninstall.

3.7 MDM vs MAM

Comparison Table

Aspect	MDM (Mobile Device Management)	MAM (Mobile App Management)
Scope	Entire device	Specific apps only
Device enrolled in Intune?	Yes	No (for MAM-only)
Use case	Corporate-owned devices	BYOD personal devices
Encryption control	Full disk encryption	App-level encryption only
Remote wipe	Full device wipe possible	Selective: only app data wiped
App restrictions	Block / allow specific apps	Restrict within managed apps
Settings control	OS-level (Wi-Fi, VPN, restrictions)	App-level (copy/paste, save-as)
User privacy	Lower (admin sees device info)	Higher (only managed apps visible)
License needed	Intune	Intune
Best for	Phones/laptops owned by company	Email on personal phones

App Protection Policies (APP)

APP is the cornerstone of MAM. It applies to specific managed apps regardless of device enrollment state.

Common APP Settings

Setting	What It Does
Backup data to iCloud / Google Drive	Block to prevent leak via consumer cloud
Send data to other apps	Block; allow only to other managed apps
Receive data from other apps	Block; allow only from managed apps
Save copies of org data	Block to corp OneDrive only
Cut, copy, paste	Restrict between managed apps
Encrypt app data	Required
Require PIN to access	4-6 digit PIN per app launch
Disable contact sync	Stop work contacts syncing to phone contacts
Disable printing	Block print of org data
Disable screen capture	Block screenshots in app (Android)

Step-by-Step: Create iOS App Protection Policy

1. Apps → App protection policies → + Create policy → iOS/iPadOS.
2. Name: "iOS - BYOD App Protection".
3. Public apps: Microsoft Outlook, Word, Excel, OneDrive, Teams, Edge, etc.
4. Data protection:
    - Backup org data: Block
    - Send org data to other apps: Policy managed apps
    - Receive data from other apps: Policy managed apps
    - Save copies of org data: To OneDrive for Business + SharePoint
    - Restrict cut/copy/paste: Policy managed apps with paste in
5. Access requirements:
    - PIN to access: Required, 6 digits, 30 min timeout
    - Touch ID / Face ID allowed: Yes
    - Block work apps if device is jailbroken: Yes
6. Conditional launch:
    - Max PIN attempts: 5 → Reset PIN
    - Offline grace period: 720 minutes → Block access

    - Jailbroken device: Block access
    - Min OS version: 16.0 → Warn
7. Target users: Include all users.
8. Create.

Conditional Access for MAM

Require App Protection Policy:

1. CA → New policy → "Require APP".
2. Users: All BYOD users.
3. Cloud apps: Office 365.
4. Conditions → Client apps: Mobile apps and desktop clients.
5. Grant: Require app protection policy.
6. Assignment.

Users now must use Outlook/Word/etc. that report being managed by APP. Native iOS Mail = blocked.

Selective Wipe (MAM)

If employee leaves or device lost:

1. Apps → App protection policies → Selective wipe.
2. + Create wipe request → user + device.
3. Wipe only removes managed app data; personal photos, contacts, apps preserved.

Real-World Scenarios

Scenario: BYOD email access

Sales reps want email on personal iPhones. Solution: don't enroll devices (MDM); deploy APP. They install Outlook from App Store, sign in with corporate credentials. APP detects sign-in, applies policy: PIN required, no copy/paste to personal apps, no iCloud backup. If lost: selective wipe Outlook only; personal photos untouched. User happy, company secure.

Best Practices

- MAM for personal devices; MDM for corporate.
- Combine with CA to require APP for mobile access.
- Customize PIN policy: 6 digits, biometric allowed, 30-min timeout.
- Block jailbroken/rooted devices.
- Educate users: APP doesn't manage their personal apps.

Summary

Section 3.7 Summary

- MDM = whole device; MAM = specific apps.
- MAM is BYOD-friendly: no enrollment needed.
- App Protection Policies enforce within apps.
- Pair with CA for enforcement.
- Selective wipe = remove only corporate app data.

3.8 Endpoint Security, BitLocker, Defender, Remote Wipe

Endpoint Security Overview

Intune's Endpoint Security blade consolidates security-focused policies and reports:

Section	Purpose
Antivirus	Microsoft Defender Antivirus settings
Disk encryption	BitLocker, FileVault, Android encryption
Firewall	Windows Defender Firewall rules
Endpoint detection and response (EDR)	Defender for Endpoint onboarding + settings
Attack surface reduction (ASR)	ASR rules
Account protection	Windows Hello, LAPS
Device compliance	Same as Devices → Compliance
Conditional Access	Link to Entra CA blade
Security baselines	Pre-built secure configuration sets

BitLocker Management

Create BitLocker Policy

1. Endpoint security → Disk encryption → + Create Policy.
2. Platform: Windows 10/11; Profile: BitLocker.

3. Settings:
    - BitLocker base settings: Enable full disk encryption for OS and fixed data drives
    - Configure encryption methods: XTS-AES 256-bit
    - OS drive settings: Require TPM 2.0; PIN startup; recovery key backup to Entra ID
    - Fixed data drive settings: Encrypt secondary drives
    - Removable drive settings: Optional - require encryption for write
4. Assignments: All Windows devices.
5. Create.

Recover BitLocker Key

1. Device → Properties → Recovery keys.
2. OR Entra Admin Center → Devices → Device → BitLocker keys.
3. OR end user via myaccount.microsoft.com → Devices → View BitLocker keys.

Microsoft Defender Antivirus

Create Antivirus Policy

1. Endpoint security → Antivirus → + Create Policy.
2. Platform: Windows 10/11; Profile: Microsoft Defender Antivirus.
3. Configuration:
    - Cloud protection: Enabled, High blocking level
    - Real-time protection: Enabled
    - Behavior monitoring: Enabled
    - Submit samples: Send safe samples automatically
    - Scan removable drives: Enabled
    - Quick scan daily at 2 AM
4. Assign and create.

Defender for Endpoint Integration

1. Endpoint security → Microsoft Defender for Endpoint.
2. "Connect Microsoft Defender for Endpoint to Microsoft Intune": On.
3. Configure compliance evaluation: ON.
4. Configure Defender for Endpoint risk score in compliance policies.

Now Defender for Endpoint risk signals can drive compliance and CA.

Attack Surface Reduction (ASR) Rules

ASR Rule	Blocks
Block executable content from email/webmail	Stops phishing payloads
Block Office macros from making child processes	Macro malware
Block credential stealing from LSASS	Mimikatz
Block process creations from PSExec/WMI commands	Lateral movement
Block untrusted/unsigned processes running from USB	USB malware
Block Adobe Reader from creating child processes	PDF exploits

Remote Wipe / Retire / Delete

Action	What Happens
Sync	Force device to check in with Intune
Restart	Force reboot (Windows, macOS)
Locate device	Map location (iOS supervised, Android Enterprise)
Lost mode	Lock + custom message (iOS supervised)
Reset passcode	Force passcode reset (iOS, Android)
Remote lock	Lock device with new code
Wipe	Full factory reset; all data destroyed
Retire	Remove company data + Intune mgmt; personal data preserved
Delete	Remove from Intune console (does not wipe device)
Fresh Start (Windows)	Reset to clean Windows, keep user data optionally
Autopilot reset (Windows)	Reset and re-enroll via Autopilot

Step-by-Step: Remote Wipe

1. Devices → All devices → select device.
2. ... → Wipe.

3. Confirm: "Wipe device".
4. Optional: Wipe device, but keep enrollment state and associated user account.
5. Optional: Continue to wipe even if device is offline (queues until reconnects).
6. Confirm.

Real-World Scenarios

Scenario: Lost laptop

Sales user reports lost laptop. IT response: 1) Block sign-in via Entra. 2) Issue Intune wipe to laptop. 3) When laptop next online (could be hours), it factory resets. 4) BitLocker key revoked. 5) Order replacement. 6) Autopilot delivers new device to user. Total recovery time: 24-48 hours; data loss: zero.

Best Practices

- Enforce BitLocker on every Windows endpoint.
- Apply Security Baselines as starting point.
- Enable ASR rules in Audit mode first; review impact; switch to Block.
- Integrate Defender for Endpoint for risk scoring.
- Document procedure for stolen device incidents.
- Test wipe scenarios in lab before production.

Summary

Section 3.8 Summary

- Endpoint Security = consolidated security policies.
- BitLocker via Intune; keys escrow to Entra.
- Defender for Endpoint integration drives risk-based CA.
- ASR rules prevent common attack patterns.
- Remote wipe options: Wipe (full), Retire (selective).

Section 3 — Wrap-Up

Section 3 Synthesis

- **Intune** = cloud MDM/MAM platform.
- **Enrollment**: Autopilot (Windows), ADE (iOS), Android Enterprise.
- **Compliance** + Conditional Access = "only healthy devices access data."
- **Configuration profiles**: push Wi-Fi, VPN, certs, settings; prefer Settings Catalog.
- **Apps**: Win32 (.intunewin), iOS Store/VPP, Managed Google Play, M365 Apps.

- **MDM vs MAM**: corporate vs BYOD.
- **Endpoint Security**: BitLocker, Defender AV, EDR, ASR rules.
- **Remote actions**: wipe, retire, lock, reset, locate.

Section 3 Mini-Quiz

Q1. Which Autopilot mode requires no user interaction?

A: Self-deploying mode (for kiosks, shared devices)

Q2. What's the difference between Wipe and Retire?

A: Wipe = factory reset (all data lost); Retire = remove only corporate data (personal preserved)

Q3. What file format does Intune use for Win32 app deployment?

A: .intunewin (created with Microsoft Win32 Content Prep Tool)

Q4. What's required for iOS automated device enrollment?

A: Apple Business Manager (ABM) account linked to Intune via token

Q5. What does App Protection Policy (APP) require for the device?

A: Nothing — APP works without device enrollment (MAM-only)

Q6. How is BitLocker recovery key recovered?

A: From Intune device properties, Entra device blade, or user self-service at myaccount.microsoft.com

Q7. What does the Enrollment Status Page do?

A: Shows provisioning progress and optionally blocks user access until required apps/policies install

Q8. Which Android Enterprise mode is best for BYOD?

A: Personally-Owned Work Profile (separates work from personal)

Q9. How does Intune integrate with Defender for Endpoint?

A: Defender for Endpoint risk score becomes a compliance signal; non-compliant blocks via CA

Q10. What's a Security Baseline?

A: Pre-built configuration profile with Microsoft-recommended secure settings (Windows, Edge, MDE, Win365)

Section 4
04
Exchange Online Administration
Email is still the backbone of business communication. Master mailboxes, mail flow, anti-spam, anti-malware, and the protective layers (SPF, DKIM, DMARC, EOP) that keep your tenant safe from the daily flood of phishing and malware.
Exam Weight: ~15%

4.1 Exchange Online Overview

Introduction

Exchange Online (EXO) is Microsoft's cloud-hosted email, calendar, and contact service. It's the email engine of Microsoft 365 — every user with a license gets a mailbox in EXO. Hundreds of millions of mailboxes live in Microsoft's global Exchange infrastructure.

Why This Topic Is Important

Email is the #1 entry vector for ransomware, phishing, and business email compromise. EXO admin skills are foundational: mailbox lifecycle, mail flow, anti-spam, anti-phishing, retention, and compliance all flow through Exchange Online.

Key Concepts

Mailbox Types

Type	Purpose	License Required
User mailbox	Individual employee	Yes
Shared mailbox	Department-wide (sales@, support@)	No, if < 50 GB
Room mailbox	Conference rooms — bookable resource	No
Equipment mailbox	Projectors, vehicles — bookable resource	No
Discovery mailbox	Holds eDiscovery search results	Built-in
Group mailbox	M365 Group shared mailbox	No
Public folder mailbox	Hosts public folder hierarchy	—

Storage Limits

License	Mailbox	Archive
F1/F3 (Frontline)	2 GB	—
Business Standard	50 GB	50 GB
E3	100 GB	1.5 TB (auto-expanding)
E5	100 GB	1.5 TB (auto-expanding)
Shared mailbox (no license)	50 GB	50 GB (with license)

Microsoft Portal Navigation

> 📍 Exchange Admin Center → `admin.exchange.microsoft.com`

Sections include: Recipients, Mail flow, Roles, Migration, Protection, Public folders, Reports.

Exchange Hierarchy

```
Microsoft 365 Tenant
     |
     +-- Exchange Online Organization
            |
            +-- Recipients (mailboxes, groups, contacts)
            +-- Mail flow (transport rules, connectors)
            +-- Protection (anti-spam, anti-malware in EAC; advanced in Defender)
            +-- Compliance (legal hold, retention)
            +-- Migration (batch tools)
```

License Plans & EXO

License	EXO Plan
Exchange Online Plan 1	Basic mailbox 50 GB
Exchange Online Plan 2	100 GB + auto-expanding archive + DLP
Microsoft 365 E3	EXO Plan 2 + Defender for Office 365 P1 included
Microsoft 365 E5	EXO Plan 2 + Defender P2 + Purview
Exchange Online Kiosk	F1/F3 frontline; 2 GB

Real-World Scenarios

Scenario: New tenant email setup

Acme just bought M365 E3 for 500 users. Email setup tasks: (1) Verify custom domain (acme.com). (2) Add domain in EAC → Accepted domains. (3) Update MX record to `acme-com.mail.protection.outlook.com`. (4) Update Autodiscover CNAME. (5) Configure SPF, DKIM, DMARC. (6) Migrate mail from existing provider via Migration in EAC. (7) Configure anti-spam, anti-phishing baselines.

Best Practices

- Always verify SPF, DKIM, DMARC after domain addition.
- Use shared mailboxes instead of licensing every functional address.
- Apply mailbox litigation hold or retention policies for legal.
- Audit mailbox permissions quarterly.
- Limit Exchange Admin role to 2-3 specialists.

Common Errors

Issue	Resolution
"Mailbox not found"	License not provisioned yet; wait 5-15 min after license assignment
EAC won't load	Need Exchange Admin role or higher; check role assignment
"Cannot connect to Exchange Online"	Modern auth issue; install latest Exchange Online Management module

Interview Questions

Q: What's the difference between Exchange Online and Exchange Server?

A: Exchange Online = Microsoft-hosted SaaS, no servers to manage. Exchange Server = on-premises product running on Windows Server. Hybrid Exchange connects both. New deployments almost universally choose EXO.

Q: When would you use Exchange Online Plan 1 vs Plan 2?

A: Plan 1: 50 GB mailbox, basic features — good for frontline workers, kiosks. Plan 2: 100 GB + auto-expanding archive + DLP + retention — for knowledge workers needing larger mailboxes and compliance.

Summary

Section 4.1 Summary

- EXO = cloud email/calendar/contacts.
- Mailbox types: user, shared, room, equipment, group.
- Storage 50 GB to 100 GB + auto-expanding archive on Plan 2.
- EAC: admin.exchange.microsoft.com.

4.2 Exchange Admin Center

Introduction

The Exchange Admin Center (EAC) is the web console for all Exchange Online administration. It's separate from the M365 Admin Center to provide deeper EXO-specific tools.

EAC Sections

Section	What's There
Dashboard	Quick metrics, recent recipients, alerts
Recipients → Mailboxes	All user mailboxes; manage features, permissions, properties
Recipients → Groups	DLs, Mail-enabled security, M365 Groups (Exchange view)
Recipients → Resources	Room and equipment mailboxes
Recipients → Contacts	External contacts
Recipients → Migration	Mailbox migration batches (cutover, staged, hybrid, IMAP, G Suite)
Mail flow → Rules	Transport rules (a.k.a. mail flow rules)
Mail flow → Message trace	Track delivery of any message in last 90 days
Mail flow → Remote domains	Behaviour for specific external domains
Mail flow → Accepted domains	Domains that EXO routes mail for
Mail flow → Connectors	Inbound/outbound to other email systems
Mail flow → Alerts	Notify on delivery issues
Mail flow → Queues	Stuck messages (rare in EXO)
Roles → Admin roles	Exchange RBAC (role groups)
Roles → User roles	What users can do in OWA
Public folders	Public folder hierarchy
Reports → Mail flow	Volume, delivery, top senders/receivers
Reports → Auto-forwarded messages	Detect data exfiltration via forwarding
Reports → Mail tips	Custom popups
Insights	Mail flow visualization, recommendations

Real-World Scenarios

Scenario: Message trace troubleshooting

"Did our partner receive my email at 9 AM?" — Admin opens EAC → Mail flow → Message trace. Filters: sender, date range, recipient. Sees the message was delivered to partner's MX successfully at 9:01 AM. The investigation closes in 2 minutes — proof of delivery, problem on partner's side.

Summary

Section 4.2 Summary

- EAC at admin.exchange.microsoft.com.
- Five main areas: Recipients, Mail flow, Roles, Public folders, Reports.
- Insights blade provides AI-driven recommendations.

4.3 Mailbox Management

Introduction

Mailbox management covers creating, modifying, monitoring, and migrating user mailboxes — features, permissions, quotas, calendar processing, mail forwarding, and dozens of other settings per mailbox.

Common Mailbox Operations

Operation	Where
Create mailbox	Auto on license assignment
Set mailbox quota	EAC → Mailbox → Manage email apps → Mailbox usage
Grant delegate access	EAC → Mailbox → Delegation → Send on behalf / Full access
Mail forwarding	EAC → Mailbox → Manage email forwarding
Email aliases	EAC → Mailbox → Manage email address types
Litigation hold	EAC → Mailbox → Other → Recover deleted items / Litigation hold
Convert to shared	EAC → Mailbox → Other → Convert
Archive mailbox	EAC → Mailbox → Others → Manage mailbox archive

Step-by-Step: Common Tasks

Grant Full Access to Another User

1. EAC → Recipients → Mailboxes → select user.
2. Delegation tab → "Read and manage (Full access)" → + Add.
3. Select user → Save.
4. Delegate sees the mailbox in Outlook after Outlook restart (auto-mapping).

Set Up Email Forwarding

1. EAC → Mailbox → Manage email forwarding.
2. Forward to: enter target.
3. Optional: Deliver to both forwarding address and mailbox.
4. Save.

Security Warning
External email forwarding is a common data exfiltration vector. Microsoft blocks it by default via the Outbound Spam Policy. Allow only when business-justified; monitor "Auto-forwarded messages" report.

Configure Auto-Reply (Out of Office)

1. EAC → Mailbox → Others → Manage automatic replies.
2. Toggle on; set internal + external messages.
3. Optional date range.
4. Save.

PowerShell — Exchange Online Module

```
# Install module (once)
Install-Module ExchangeOnlineManagement -Force

# Connect
Connect-ExchangeOnline -UserPrincipalName admin@contoso.com

# Get all mailboxes
Get-Mailbox -ResultSize Unlimited | Select-Object DisplayName, PrimarySmtpAddress,
RecipientTypeDetails

# Get mailbox details
Get-Mailbox -Identity "alice@contoso.com" | Format-List

# Get mailbox size
Get-MailboxStatistics -Identity "alice@contoso.com" |
    Select-Object DisplayName, TotalItemSize, ItemCount

# Grant Full Access
Add-MailboxPermission -Identity "shared-mailbox@contoso.com" `
    -User "alice@contoso.com" -AccessRights FullAccess -InheritanceType All

# Grant Send As
Add-RecipientPermission -Identity "shared-mailbox@contoso.com" `
    -Trustee "alice@contoso.com" -AccessRights SendAs

# Convert to shared mailbox
Set-Mailbox -Identity "former-employee@contoso.com" -Type Shared

# Enable archive
Enable-Mailbox -Identity "alice@contoso.com" -Archive

# Enable auto-expanding archive
Enable-Mailbox -Identity "alice@contoso.com" -AutoExpandingArchive

# Set litigation hold
Set-Mailbox -Identity "alice@contoso.com" -LitigationHoldEnabled $true `
    -LitigationHoldDuration 2555 # 7 years in days

# Set mailbox forwarding
Set-Mailbox -Identity "alice@contoso.com" `
    -ForwardingSmtpAddress "external@partner.com" `
    -DeliverToMailboxAndForward $true

# Find auto-forwarders (security audit)
Get-Mailbox -ResultSize Unlimited |
    Where-Object { $_.ForwardingSmtpAddress -ne $null } |
    Select-Object DisplayName, ForwardingSmtpAddress

# Disable IMAP/POP/SMTP basic auth on a mailbox (modernization)
Set-CASMailbox -Identity "alice@contoso.com" `
    -ImapEnabled $false -PopEnabled $false -SmtpClientAuthenticationDisabled $true
```

Mailbox Size and Quota Management

Quota Type	Default (E3/E5)	Behavior
IssueWarningQuota	~99 GB	Warning email to user
ProhibitSendQuota	~99.5 GB	User can't send new mail
ProhibitSendReceiveQuota	100 GB	User can't send OR receive

You can lower these per mailbox, but typically use defaults and rely on archive for large users.

Real-World Scenarios

Scenario: Employee on leave

Mary is on 6-month maternity leave. IT setup: (1) Auto-reply: "I'm on leave until October. Contact bob@ for urgent matters." (2) Delegate Full Access to her manager. (3) Manager can read mail without password sharing. (4) On return, remove delegate, disable auto-reply.

Scenario: Employee termination

John resigns. Sequence: (1) Block sign-in (Entra). (2) Revoke sessions. (3) Convert mailbox to Shared (preserves emails, no license consumed). (4) Grant manager Full Access. (5) Apply litigation hold if pending legal matter. (6) Remove user license. (7) Delete user after retention period.

Best Practices

- Convert ex-employee mailboxes to Shared (free up license).
- Disable external forwarding by default.
- Apply litigation hold for legal/HR cases.
- Audit Full Access permissions quarterly.
- Use auto-expanding archive for power users.

Common Errors

Issue	Resolution
Mailbox quota exceeded	Enable archive; encourage user to clean up; raise quota if justified
Delegate can't see mailbox	Wait 1 hour for auto-mapping; restart Outlook
"Cannot connect to mailbox"	Modern auth issue; clear cached creds; reinstall Outlook
Shared mailbox needs license at >50 GB	Apply E1 license

Summary

Section 4.3 Summary

- Mailboxes created on license assignment.
- Delegation: Full Access, Send As, Send on Behalf.
- Convert ex-employees to shared mailbox.
- Litigation hold for legal scenarios.
- External forwarding disabled by default — open only when justified.

4.4 Shared Mailboxes

Introduction

Shared mailboxes are mailboxes multiple users can access without each user having their own password for it. Common uses: support@, sales@, info@, hr@. Best part: no license required (up to 50 GB).

Step-by-Step: Create a Shared Mailbox

1. EAC → Recipients → Mailboxes → + Add a shared mailbox.
2. Display name: "Sales Team".
3. Email address: sales@contoso.com.
4. Add members (users granted access).
5. Members get Full Access + Send As (auto-mapped in Outlook).
6. Save.

Permissions

Permission	Allows
Full Access	Read, reply, delete
Send As	Send appearing as the mailbox
Send on Behalf	"User on behalf of Mailbox" in From

License or Not?

- < 50 GB + no archive + no litigation hold → no license needed
- > 50 GB → E1 license required
- Archive enabled → E3 license required
- Litigation hold → E3 license required

PowerShell

```
# Create shared mailbox
New-Mailbox -Shared -Name "Support" -DisplayName "Customer Support" `
    -Alias "support" -PrimarySmtpAddress "support@contoso.com"

# Grant access
Add-MailboxPermission -Identity "support@contoso.com" `
    -User "alice@contoso.com" -AccessRights FullAccess
Add-RecipientPermission -Identity "support@contoso.com" `
    -Trustee "alice@contoso.com" -AccessRights SendAs
```

Real-World Scenarios

Scenario: Customer support team

5-person support team needs to share an inbox. Solution: shared mailbox "support@contoso.com." All 5 get Full Access + Send As. When customer emails, all 5 see it; whoever responds first replies "from" support@ — customer sees consistent branding. No additional license cost.

Best Practices

- Configure auto-reply on shared mailboxes for off-hours.
- Use distribution group as members (easier rotation than individual permissions).
- Disable sign-in to the shared account (account is enabled but never used for direct login).

- Enable MFA on the underlying account anyway (defense in depth).
- Apply retention policy.

Summary

Section 4.4 Summary

- Shared mailboxes = multi-user inbox; no license up to 50 GB.
- Permissions: Full Access, Send As, Send on Behalf.
- Common uses: support@, sales@, info@, hr@.

4.5 Resource Mailboxes (Room & Equipment)

Introduction

Resource mailboxes represent bookable resources: conference rooms, projectors, cars, equipment. Users book them via calendar invites; the resource auto-accepts/declines based on availability.

Two Types

Type	Use Case
Room mailbox	Meeting rooms — has location, capacity
Equipment mailbox	Movable equipment — projector, conference phone, vehicle

Step-by-Step: Create Room Mailbox

1. EAC → Recipients → Resources → + Add a resource → Room.
2. Name: "Conf Room 12-A".
3. Email: confroom12a@contoso.com.
4. Capacity: 8.
5. Location: 12th Floor.
6. Save.

Booking Policies

1. EAC → Recipients → Resources → select room → Booking Options.

2. Configure:
    - Allow conflicts: No (don't double-book)
    - Allow recurring meetings: Yes
    - Booking window (days): 180
    - Maximum duration (minutes): 480 (8 hours)
    - Allow scheduling only during working hours: Yes
    - Auto-accept meeting requests: Yes
    - Delegates: optional approvers (for VIP rooms)
3. Save.

PowerShell

```
# Create room mailbox
New-Mailbox -Name "Boardroom" -DisplayName "Boardroom" `
    -Alias "boardroom" -Room

# Configure capacity and location
Set-Mailbox "Boardroom" -ResourceCapacity 20

Set-Place "Boardroom" -Floor 30 -FloorLabel "30F" -Building "HQ" `
    -City "Karachi" -Capacity 20 -AudioDeviceName "Crestron" `
    -VideoDeviceName "Logitech Rally" -DisplayDeviceName "Samsung 75in"

# Configure calendar booking
Set-CalendarProcessing -Identity "Boardroom" `
    -AutomateProcessing AutoAccept `
    -AllowConflicts $false `
    -BookingWindowInDays 365 `
    -MaximumDurationInMinutes 480 `
    -ScheduleOnlyDuringWorkHours $true
```

Room Lists

Group rooms for easier discovery in Outlook:

1. Create a distribution group with type "RoomList".
2. Add room mailboxes as members.
3. In Outlook, users can "Browse rooms" filtered by list.

```
New-DistributionGroup -Name "HQ-Karachi-Rooms" -RoomList
Add-DistributionGroupMember -Identity "HQ-Karachi-Rooms" -Member
"boardroom@contoso.com"
```

Summary

Section 4.5 Summary

- Resource mailboxes = bookable rooms and equipment.
- Auto-accept or require approval.
- Configure capacity, location, working hours.
- Group via Room Lists for easy discovery.

4.6 Distribution Groups

Introduction

Distribution Groups (DLs) are email-only groups for sending email to multiple recipients. They originated in Exchange and remain useful for pure email distribution scenarios.

DL vs M365 Group vs Mail-Enabled Security Group

Feature	DL	M365 Group	Mail-Enabled Security
Email distribution	Yes	Yes (shared inbox)	Yes
Access control (apps, resources)	No	Yes	Yes
Shared inbox / SharePoint / Teams	No	Yes	No
Membership management	Owner / Admin	Owner / Admin	Owner / Admin
Dynamic membership	Yes (Dynamic DL)	Yes	Yes

Step-by-Step: Create a DL

1. EAC → Recipients → Groups → + Add a group → Distribution.
2. Display name + email + alias.
3. Owners + members.
4. Save.

PowerShell

```
New-DistributionGroup -Name "AllEmployees" -DisplayName "All Employees" `
    -PrimarySmtpAddress "all@contoso.com"

Add-DistributionGroupMember -Identity "AllEmployees" -Member "alice@contoso.com"

# Restrict who can send to it (often required for big distribution lists)
Set-DistributionGroup -Identity "AllEmployees" `
    -AcceptMessagesOnlyFromSendersOrMembers "executives@contoso.com" `
    -RequireSenderAuthenticationEnabled $true

# Upgrade DL to M365 Group
# EAC GUI: select DL → "Upgrade distribution list"
```

Real-World Scenarios

Scenario: All-staff announcements

HR sends weekly newsletter to all 2,500 employees. Solution: dynamic DL "AllEmployees" with rule "user.accountEnabled = true." Restricted to senders in "Executives" group. HR member sends one email; all current staff receive it. New hires automatically included next day; offboarded users automatically excluded.

Summary

Section 4.6 Summary

- DLs for email distribution only.
- Restrict senders for large DLs to prevent spam.
- Consider upgrading to M365 Group for collaboration features.

4.7 Dynamic Distribution Groups

Introduction

Dynamic DLs compute membership at send-time from a filter — no manual management. Membership reflects directory state at the moment the email is sent.

Key Difference from Dynamic M365 Groups

- Dynamic DL: membership evaluated at send-time, never stored.
- Dynamic M365 Group: membership stored, evaluated periodically.

Step-by-Step

1. EAC → Recipients → Groups → + Add a group → Dynamic distribution list.
2. Name + email.
3. Recipient container: select OU or whole organization.
4. Recipient types: Users with mailbox.
5. Rules: Department equals "Sales".
6. Save.

PowerShell

```
# Create Dynamic DL
New-DynamicDistributionGroup -Name "AllSales" `
    -DisplayName "All Sales Team" `
    -PrimarySmtpAddress "allsales@contoso.com" `
    -IncludedRecipients "MailboxUsers" `
    -ConditionalDepartment "Sales"

# Preview members
$d = Get-DynamicDistributionGroup "AllSales"
Get-Recipient -RecipientPreviewFilter $d.RecipientFilter
```

Best Practices

- Always preview filter members before deployment.
- Document filter logic in description.
- Use HR-driven attributes (department, country, company).
- Restrict senders to prevent spam.

Summary

Section 4.7 Summary

- Dynamic DLs = filter-based membership at send-time.
- Self-maintaining — perfect for HR-driven groups.
- Always preview before deployment.

4.8 Mail Flow Rules (Transport Rules)

Introduction

Mail flow rules (also called transport rules) inspect messages as they flow through Exchange Online and take action: block, redirect, append disclaimer, flag, encrypt, route to specific connector, etc.

Why It Matters

Mail flow rules are the swiss army knife of EXO security and compliance. Every M365 admin uses them: legal disclaimer, executive impersonation protection, internal-only domain enforcement, attachment blocking, encryption triggering.

Anatomy of a Rule

Component	Purpose
Conditions (Apply if)	When does this rule fire?
Exceptions (Except if)	Skip the rule under these conditions
Actions (Do)	What happens when fired
Properties	Priority, mode (Enforce, Test with policy tips, Test with no tips), date range

Common Rule Use Cases

Use Case	Action
Append disclaimer to external mail	Apply HTML disclaimer at bottom
External email warning banner	Prepend HTML warning to body
Block specific attachments	Reject with custom message
Route mail to compliance team	Bcc compliance@contoso.com
Encrypt mail with sensitive keyword	Apply Microsoft Purview Encryption
Stop CEO impersonation	Block if From "CEO Name" but not from CEO's actual address
Force TLS to specific partner	Route via connector requiring TLS
Block .exe attachments	Reject by attachment type

Step-by-Step: External Email Warning Banner

1. EAC → Mail flow → Rules → + Add a rule → Create a new rule.
2. Name: "External Email Warning".
3. Apply this rule if:
    - The sender is located outside the organization
4. Do the following:
    - Prepend the disclaimer: HTML banner
5. Sample HTML:

```
<div style="background:#FFF3CD;border:1px solid #FFC107;padding:10px;margin-bottom:
10px;">
  <strong>⚠️ External Sender</strong>: This email is from outside Contoso.
  Be cautious with links and attachments.
</div>
```

1. Exceptions:
    - The message header includes: "X-Contoso-Warning-Applied" → ensures it only runs once if forwarded
2. Properties → Mode: Enforce → Save.

Step-by-Step: Block .exe Attachments

1. + Add a rule.
2. Name: "Block executable attachments".
3. Apply if: Any attachment file extension matches → .exe, .scr, .pif, .bat, .vbs, .js.
4. Do: Reject the message with explanation: "Executable attachments are not permitted for security reasons."
5. Mode: Enforce. Save.

Step-by-Step: CEO Impersonation Protection

1. + Add a rule.
2. Name: "CEO Impersonation Block".
3. Apply if:
    - The sender is located outside the organization
    - AND any of these conditions: The sender's address contains "ceo@" OR the sender's display name contains "CEO Full Name"
4. Do: Redirect message to ceo-impersonation-quarantine@contoso.com (or notify and quarantine).
5. Save.

PowerShell

```
# List all rules
Get-TransportRule | Select-Object Name, State, Mode, Priority

# Get details of one
Get-TransportRule "External Email Warning" | Format-List

# Create a rule via PowerShell
New-TransportRule -Name "Block .exe attachments" `
    -AttachmentExtensionMatchesWords @("exe","scr","pif","bat","vbs") `
    -RejectMessageReasonText "Executable attachments are not permitted." `
    -RejectMessageEnhancedStatusCode "5.7.1"

# Toggle rule on/off
Disable-TransportRule -Identity "External Email Warning"
Enable-TransportRule -Identity "External Email Warning"

# Export rules for backup
$rules = Get-TransportRule
$rules | Export-Csv -Path "transport_rules_backup.csv" -NoTypeInformation
```

Best Practices

- Test new rules with Mode = "Test with Policy Tips" first.
- Document each rule's purpose in Comments field.
- Use priorities deliberately — rules fire in priority order, can stop processing.
- Use exceptions to avoid double-processing on internal mail.
- Limit complex rules; performance can degrade with 100+ active rules.
- Backup rules quarterly via PowerShell export.

Common Errors

Issue	Resolution
Rule not firing	Check Mode (must be Enforce); check priority; review conditions
Disclaimer duplicates	Add exception checking X-header you also set in action
Rule blocks legitimate mail	Switch to Test mode, review reports, refine conditions
Performance issues	Consolidate rules; use simpler conditions

Summary

Section 4.8 Summary

- Mail flow rules = conditions + actions on every email.
- Common: external warning banner, attachment blocking, CEO impersonation, encryption triggering.
- Test mode before Enforce.
- Backup via PowerShell export.

4.9 Connectors

Introduction

Connectors define how mail flows between EXO and external systems: partner organizations, on-prem Exchange servers, hosted third-party security gateways (Proofpoint, Mimecast), SMTP appliances (printers, line-of-business apps).

Connector Types

Direction	Type	Use Case
Inbound	From your organization's email server	Hybrid Exchange routing on-prem → EXO
Inbound	From partner organization	Force TLS with a specific partner
Outbound	To your organization's email server	Hybrid: EXO → on-prem
Outbound	To partner organization	Encrypted relay to partner

Common Scenarios

1. Allow SMTP from a Multifunction Printer

Office printer needs to send scanned PDFs as email. Three methods:

Method	How	Pros / Cons
SMTP AUTH (basic)	Printer authenticates as a mailbox	Deprecated; insecure
SMTP relay via connector	Allow specific IP to relay via connector	Best for sending to internal AND external
Direct send (no auth)	Printer sends to MX of recipient domain	Internal only; no external delivery

2. Force TLS to a Specific Partner

1. EAC → Mail flow → Connectors → + Add a connector.
2. Connection from: Office 365.
3. Connection to: Partner organization.
4. Sender domains: partner.com.
5. Require TLS: Yes; require certificate name: `*.partner.com`.
6. Save.

3. Send Mail Through a Third-Party Gateway (Outbound Routing)

1. + Add a connector → from O365 → Partner.
2. Always use this connector for emails sent to "All recipients" or specific domains.
3. Route via SMTP server FQDN; require TLS.
4. Validate connector with test recipient.

PowerShell

```
# List connectors
Get-InboundConnector | Format-Table Name, ConnectorType, Enabled
Get-OutboundConnector | Format-Table Name, ConnectorType, Enabled

# Get details
Get-OutboundConnector "ToPartner" | Format-List
```

Real-World Scenarios

Scenario: Migrate to EXO with security gateway

Company uses Proofpoint as inbound mail gateway. After migrating to EXO, mail flow: MX → Proofpoint → EXO. Outbound: EXO → connector → Proofpoint → internet. This preserves Proofpoint investment. Configure inbound connector restricting EXO to accept only from Proofpoint IPs.

Best Practices

- Always require TLS on partner connectors.
- Restrict by IP for inbound connectors (lock down to known senders).
- Validate connector after creation using the built-in test.
- Avoid SMTP AUTH; use connectors with IP restriction for printers/scanners.
- Disable basic auth org-wide; force modern auth.

Summary

Section 4.9 Summary

- Connectors route mail between EXO and external systems.
- Inbound: from partner / on-prem / security gateway.
- Outbound: to partner / on-prem / security gateway.
- Force TLS, restrict by IP for security.

4.10 SPF, DKIM, DMARC

Introduction

SPF, DKIM, and DMARC are the three pillars of email authentication. Together they prevent attackers from spoofing your domain ("CEO Fraud," BEC). Without these, anyone can send email claiming to be from your domain.

SPF (Sender Policy Framework)

SPF = DNS record listing IPs/servers authorized to send mail "From: yourdomain.com."

SPF Record Example

```
v=spf1 include:spf.protection.outlook.com -all
```

Component	Meaning
v=spf1	SPF version 1
include:spf.protection.outlook.com	Trust Microsoft 365 sending servers
-all	Hard fail anything not matching (use ~all for softfail during testing)

Common SPF Patterns

Use Case	SPF Record
M365 only	`v=spf1 include:spf.protection.outlook.com -all`
M365 + SendGrid	`v=spf1 include:spf.protection.outlook.com include:sendgrid.net -all`
M365 + on-prem mail server	`v=spf1 include:spf.protection.outlook.com ip4:203.0.113.5 -all`
M365 + Mailchimp	`v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net -all`

Limit
SPF has a 10-DNS-lookup limit. Too many includes → "permerror." Use SPF flattening tools if you have many third-party senders.

DKIM (DomainKeys Identified Mail)

DKIM adds a cryptographic signature to outbound mail. The recipient verifies the signature using a public key in your DNS.

DKIM Records in DNS

Microsoft provides 2 selectors (so you can rotate keys):

```
selector1._domainkey.contoso.com  CNAME  selector1-contoso-
com._domainkey.contoso.onmicrosoft.com
selector2._domainkey.contoso.com  CNAME  selector2-contoso-
com._domainkey.contoso.onmicrosoft.com
```

Step-by-Step: Enable DKIM

1. Add the two CNAME records above to your DNS.
2. Microsoft Defender → Email & collaboration → Policies & rules → Threat policies → Email authentication settings → DKIM.
3. Select domain (contoso.com).
4. Click "Enable" for signing.
5. If CNAME records aren't found: Microsoft will report which records to add.
6. Wait for verification (DNS propagation).
7. Outbound mail now signed.

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

DMARC ties SPF + DKIM together and tells receivers what to do with failures.

DMARC Record

```
_dmarc.contoso.com  TXT  "v=DMARC1; p=reject; rua=mailto:dmarc-reports@contoso.com;
ruf=mailto:dmarc-forensics@contoso.com; fo=1; adkim=s; aspf=s"
```

Tag	Meaning
v=DMARC1	Version
p=	Policy: none (monitor), quarantine (junk folder), reject (block)
rua=	Aggregate reports daily summary go here
ruf=	Forensic reports per-failed-message (privacy-sensitive)
fo=	Forensic options (0,1,d,s)
adkim=	DKIM alignment strict (s) or relaxed (r)
aspf=	SPF alignment strict or relaxed
pct=	Percentage of mail policy applies to (use during ramp-up)

DMARC Rollout

Phase	Policy	Goal
1. Monitor	p=none	Collect reports to understand legitimate senders
2. Quarantine	p=quarantine; pct=5/25/50/100	Gradually quarantine spoofed mail
3. Reject	p=reject	Fully block spoofed mail

How They Work Together

```
Email arrives at receiving server
      |
      v
Check SPF: is sender IP allowed?
      |
      +-- Pass / Fail
      |
      v
Check DKIM: is signature valid?
      |
      +-- Pass / Fail
      |
      v
Check DMARC alignment:
      - Does SPF domain align with From header?
      - Does DKIM domain align with From header?
      |
      +-- If neither aligned: apply DMARC policy
      |       (none / quarantine / reject)
      |
      v
Delivery decision made
```

Real-World Scenarios

Scenario: BEC fraud

Attacker spoofs CEO email: "From: ceo@contoso.com" to send a fake wire-transfer request. Without DMARC reject, the message lands in CFO's inbox. With DMARC p=reject, receiving servers reject the spoofed mail. CFO never sees it. Wire fraud prevented.

Scenario: SaaS marketing tool not aligned

Company sends newsletters via Mailchimp from "marketing@contoso.com." After enabling DMARC p=reject, recipients reject newsletters. Why: Mailchimp signs DKIM as servers.mcsv.net, which doesn't align with contoso.com. Fix: add Mailchimp DKIM to contoso.com domain ("Authenticate domain" feature in Mailchimp).

Best Practices

- Enable SPF, DKIM, DMARC in that order.
- Start DMARC at p=none for 30 days; review reports.
- Identify all legitimate senders (M365, marketing tools, ticketing, HR systems).
- Ensure each sender is SPF + DKIM aligned.
- Move to p=quarantine with pct=10; ramp to 100%.
- Then move to p=reject.
- Use a DMARC report aggregation tool (dmarcian, Valimail, MXToolbox).

PowerShell

```
# Check DKIM status
Connect-ExchangeOnline
Get-DkimSigningConfig | Format-Table Domain, Enabled, Status

# Enable DKIM (after CNAMEs in DNS)
New-DkimSigningConfig -DomainName "contoso.com" -Enabled $true
Set-DkimSigningConfig -Identity "contoso.com" -Enabled $true

# Rotate DKIM keys
Rotate-DkimSigningConfig -KeySize 2048 -Identity "contoso.com"
```

Common Errors

Error	Resolution
"SPF too many lookups"	Over 10 DNS lookups; flatten or remove unused includes
DKIM "Disabled" with CNAMEs in place	Wait for DNS propagation; force enable from EAC
Mail rejected after DMARC reject	Identify failing sender; align their DKIM/SPF
"No DKIM signature found"	DKIM not enabled for sending domain

Interview Questions

Q: Explain SPF, DKIM, DMARC and how they work together.

A: SPF: DNS record listing servers authorized to send for your domain. DKIM: cryptographic signature on each message verified by public key in DNS. DMARC: ties them together, requires alignment with From header, tells receivers to none/quarantine/reject failures. SPF alone allows spoofing if sender controls a domain with SPF; DMARC closes that gap.

Q: Why start DMARC at p=none?

A: To collect reports without breaking legitimate mail. Reports reveal all senders using your domain. Once all legitimate senders are properly authenticated (SPF + DKIM aligned), gradually escalate to quarantine then reject.

Exam-Focused Notes

- SPF max 10 DNS lookups.
- DKIM: 2 selectors (rotation).
- DMARC policies: none → quarantine → reject.
- Alignment: SPF or DKIM must match From header domain.
- EAC and Defender portal both expose DKIM config.

Summary

Section 4.10 Summary

- SPF: authorized senders.
- DKIM: cryptographic signature.
- DMARC: enforcement + reporting.
- Rollout: SPF → DKIM → DMARC p=none → quarantine → reject.
- Prevents domain spoofing and BEC fraud.

4.11 Exchange Online Protection (EOP), Anti-Spam, Anti-Malware

Introduction

Exchange Online Protection (EOP) is the security layer included free with every EXO mailbox. It filters spam, malware, and phishing before mail reaches mailboxes. Defender for Office 365 P1/P2 adds advanced features on top.

EOP Architecture

```
Internet email
      |
      v
[EOP] Connection filtering (IP allow/block lists)
      |
      v
[EOP] Anti-malware scan
      |
      v
[EOP] Anti-spam (heuristics, reputation, content)
      |
      v
[EOP] Anti-phishing (impersonation, spoofing)
      |
      v
[EOP] Transport rules (mail flow rules)
      |
      v
[Defender O365 P1+] Safe Attachments, Safe Links
      |
      v
User mailbox
```

Anti-Malware Policy

What EOP Blocks

- Known malware via multiple signature engines
- Common malicious file types: .exe, .vbs, .js, .scr, .bat, etc.
- Password-protected archives (configurable)
- Multi-AV scanning + heuristic detection

Default Policy

- Always-on; cannot be fully disabled.
- Malicious attachments quarantined.
- Sender notified by default.

Customize

1. Microsoft Defender portal (security.microsoft.com) → Email & collaboration → Policies & rules → Threat policies → Anti-malware.

2. Default policy → Edit (or create custom for groups/domains).
3. Adjust common attachment filter (add file types).
4. Enable zero-hour auto purge (ZAP) for malware.
5. Configure quarantine vs reject actions.
6. Save.

Anti-Spam Policy

Inbound Anti-Spam

1. Defender → Anti-spam policies.
2. Edit default or create custom.
3. Settings:
    - Bulk email threshold: 7 (0=block all bulk, 9=allow most). 7 is balanced.
    - Spam confidence level (SCL) actions per category
    - Mark mail with SCL 5/6: Junk Email folder
    - Mark mail with SCL 7/8/9: Quarantine
    - Allowed/blocked senders
    - Allowed/blocked domains
    - End-user spam notifications (daily digest)
4. Save.

Outbound Anti-Spam

Prevents your users from being mass spammers (often via compromised accounts):

- Default external recipient limit per user per hour: 500
- Total recipients per day: 10,000
- Automatic external forwarding: Off by default
- Send warning to: alerts@contoso.com

Anti-Phishing Policy

1. Defender → Anti-phishing policies.
2. Edit default or create custom (preset: Standard or Strict).
3. Settings:
    - Impersonation protection: add up to 350 users (executives, finance) and up to 50 trusted domains
    - Mailbox intelligence: enabled (detects unusual patterns)
    - Spoof intelligence: enabled

- Phishing email threshold: 1-4 (higher = stricter)
- Action for impersonated user: Quarantine + safety tip

4. Save.

Preset Security Policies

Microsoft provides Standard and Strict preset policies that wrap anti-spam, anti-malware, anti-phishing, Safe Links, and Safe Attachments at recommended settings:

1. Defender → Threat policies → Preset security policies.
2. Apply Standard to most users.
3. Apply Strict to high-risk users (executives, IT admins, finance).

Quarantine

1. Defender → Review → Quarantine.
2. View quarantined messages (spam, phishing, malware, transport rule blocks).
3. Actions: release, release and report false positive, delete, view headers.
4. End users get daily digest emails and can release their own messages from low-confidence quarantine (configurable).

Message Trace

Track any message:

1. EAC → Mail flow → Message trace.
2. Sender / recipient / date range / status filter.
3. Last 10 days: real-time. 11-90 days: historical search (slower).
4. Click message → full delivery details, headers, applied policies.

PowerShell

```
# Get anti-spam policy
Get-HostedContentFilterPolicy | Format-List

# Adjust bulk threshold
Set-HostedContentFilterPolicy -Identity "Default" -BulkThreshold 6

# Get message trace (last 10 days)
Get-MessageTrace -StartDate (Get-Date).AddDays(-5) `
    -EndDate (Get-Date) `
    -SenderAddress "alice@contoso.com" |
    Select-Object Received, Subject, Status, RecipientAddress

# Historical message trace (more than 10 days back)
Start-HistoricalSearch -ReportTitle "JanInvestigation" `
    -StartDate "2026-01-01" -EndDate "2026-01-15" `
    -ReportType MessageTrace -SenderAddress "alice@contoso.com" `
    -NotifyAddress "admin@contoso.com"

# Release from quarantine
Get-QuarantineMessage | Where-Object { $_.Subject -match "Important" } |
    Release-QuarantineMessage -ReleaseToAll
```

Real-World Scenarios

Scenario: Phishing campaign

Mass phishing campaign targeting Contoso. Defender quarantines most; a few sneak through to mailboxes. Admin reports to Microsoft via "Report Message" — Defender's Threat Explorer identifies pattern, applies zero-hour auto purge (ZAP) which removes the phishing mail from EVERY mailbox in tenant. Within minutes, all instances gone.

Best Practices

- Apply Preset Strict policy for executives and finance.
- Apply Preset Standard for everyone else.
- Configure 1-day user spam digest for self-service.
- Enable ZAP for malware and phishing.
- Block external auto-forwarding except where business-justified.
- Use Submissions to report misses/false positives (Microsoft tunes for tenant).
- Review quarantine reports weekly.

Common Errors

Issue	Resolution
Important mail in spam	Allow sender/domain; check transport rules; report submission to Microsoft
Outbound spam alert	Investigate compromised account; reset password; check sign-in logs
Phishing impersonation false positive	Add legitimate exec lookalike domain to trusted senders
"Message could not be delivered"	Run message trace to see exact reason; check recipient validity

Summary

Section 4.11 Summary

- EOP = free baseline anti-spam, anti-malware, anti-phishing.
- Defender for Office 365 P1+ adds Safe Links, Safe Attachments, Threat Explorer.
- Apply Preset Standard (most) and Strict (VIPs).
- ZAP retroactively removes malicious mail.
- Message trace = your debugging tool.

4.12 Mail Migration to Exchange Online

Migration Types

Type	Description	Use When
Cutover	One-time migration of all mailboxes	< 150 mailboxes from on-prem Exchange or Exchange Online tenant-to-tenant; quick switch
Staged	Migrate in batches	Larger Exchange 2003/2007 environments
Hybrid (Express or Full)	Maintain coexistence between on-prem and EXO	Large enterprises planning long coexistence
IMAP	Pull from any IMAP source	Gmail, Zimbra, other IMAP-accessible systems
G Suite / Google Workspace	Special connector for Google	Migrating from Google
PST import	Bulk import PST files to mailboxes	From legacy archives or fileshares
Cross-tenant migration	Mailbox move between two M365 tenants	Mergers, acquisitions

Migration Workflow (Generic)

1. Plan: inventory mailboxes, sizes, special features (litigation hold, archive).
2. Prepare destination: license users, verify domains, configure SPF/DKIM/DMARC for migrated domain.
3. Migration endpoint: EAC → Migration → Endpoints → + Add. Configure source connection.
4. Migration batch: + Add → choose users to migrate, schedule, notifications.
5. Initial sync: copies mail (slow phase; depends on size and bandwidth).
6. Incremental sync: catches up daily.
7. Cutover: switch MX record → new mail routes to EXO; complete final sync.
8. Decommission source (after weeks of verified operation).

Step-by-Step: IMAP Migration

1. EAC → Migration → + Add migration batch.
2. Migration type: Migration to Exchange Online → IMAP migration.
3. Upload CSV with: EmailAddress (target M365), UserName (source login), Password (source password).

4. Configure IMAP migration endpoint: server: imap.example.com, port 993, SSL.
5. Schedule: start immediately or later.
6. Notification: admin email.
7. Create. Monitor in Migration dashboard.

PowerShell Migration

```
# Create IMAP migration endpoint
$securePwd = ConvertTo-SecureString "AdminPass" -AsPlainText -Force
$cred = New-Object PSCredential ("admin@source.com", $securePwd)

$endpoint = New-MigrationEndpoint -IMAP -Name "ImapEndpoint" `
    -RemoteServer "imap.source.com" -Port 993 -Security SSL `
    -Credentials $cred

# Create batch
New-MigrationBatch -Name "Wave1-Sales" `
    -SourceEndpoint $endpoint.Identity `
    -CSVData ([System.IO.File]::ReadAllBytes("C:\users.csv")) `
    -AutoStart -NotificationEmails "admin@contoso.com"

# Monitor
Get-MigrationBatch Wave1-Sales | Format-List

# Get migration user status
Get-MigrationUser -BatchId "Wave1-Sales" | Select-Object Identity, Status, Items
```

Hybrid Exchange Overview

Hybrid = on-prem Exchange + EXO coexist. Use cases:

- Long-term coexistence during migration
- Geographic / regulatory requirement to keep some mailboxes on-prem
- Phased migration of large environments (10k+ mailboxes)

Hybrid Features

- Shared address space (a single domain spans on-prem + cloud)
- Free/busy calendar sharing across
- Mail flow via Edge Transport or Send Connector
- Cross-premises mailbox moves
- OAuth modern auth across

Hybrid Configuration Wizard (HCW)

- Run from on-prem Exchange server
- Configures connectors, federation trust, OAuth, mail flow
- Microsoft updates HCW regularly — always run latest

Cross-Tenant Migration

Microsoft now supports native mailbox moves between two M365 tenants (e.g., merger). Key steps:

1. Establish trust between tenants (cross-tenant access settings).
2. Prepare source: users to migrate, verify mailbox sizes.
3. Prepare destination: matching users, licenses, MailUser objects.
4. Run migration batch using "RemoteAcrossTenant" endpoint.
5. Cutover and finalize.

Real-World Scenarios

Scenario: Migrating from Google Workspace to M365

Mid-sized company migrating 800 users from Gmail. Plan: (1) Set up M365 tenant; verify domain. (2) Provision all 800 users with E3 licenses. (3) Create migration endpoint to Gmail using Google Migration. (4) Migrate in batches of 100 over 3 weeks. (5) Communicate cutover date. (6) Switch MX. (7) Update SPF/DKIM/DMARC for new sending IPs. (8) Decommission Google after 30 days.

Best Practices

- Run network assessment before large migrations.
- Migrate in waves of 100-500 mailboxes.
- Schedule MX cutover for weekend or off-hours.
- Keep source available for 30-60 days post-cutover.
- Train users on Outlook + OWA before migration.
- Test with IT pilot before broad migration.
- Verify DKIM/DMARC don't break after MX cutover.

Common Errors

Issue	Resolution
"Migration endpoint not validated"	Test connectivity from EXO to source; firewall rule needed
"Throttled by source"	Stagger migrations; reduce concurrent count
Mailbox migration stuck "synced"	Run "Complete-MigrationBatch" or use EAC button
Mail flow breaks post-cutover	Verify MX, autodiscover, SPF/DKIM/DMARC for new sending

Summary

Section 4.12 Summary

- Migration types: Cutover, Staged, Hybrid, IMAP, Google, PST, Cross-tenant.
- Use EAC → Migration → Endpoints + Batches.
- Hybrid for long-term coexistence; HCW configures it.
- Test with pilot; stagger waves; communicate dates clearly.

Section 4 — Wrap-Up

Section 4 Synthesis

- **EXO** = cloud email; EAC at admin.exchange.microsoft.com.
- **Mailboxes**: user, shared, room/equipment, group.
- **Shared mailboxes**: free up to 50 GB.
- **DLs vs M365 Groups**: DLs for email-only; M365 for collaboration.
- **Mail flow rules**: Swiss army knife — disclaimers, blocks, encryption triggers.
- **Connectors**: TLS-secured routing to partners and gateways.
- **SPF, DKIM, DMARC**: three pillars of email authentication.
- **EOP**: free baseline; Defender O365 adds advanced.
- **Preset Security Policies**: Standard for most, Strict for VIPs.
- **Migration**: cutover/staged/hybrid/IMAP/Google/cross-tenant.

Section 4 Mini-Quiz

Q1. What's the SPF record syntax for M365-only sending?

A: v=spf1 include:spf.protection.outlook.com -all

Q2. How many SPF DNS lookups are allowed maximum?

A: 10

Q3. What does DMARC p=quarantine mean?

A: Failed messages should be delivered to junk/spam folder

Q4. What's the default mailbox size on E3?

A: 100 GB (with auto-expanding archive up to 1.5 TB)

Q5. Do shared mailboxes require a license?

A: Not up to 50 GB; license required beyond that or for archive/litigation hold

Q6. What does ZAP do?

A: Zero-hour Auto Purge — retroactively removes malicious mail from mailboxes after delivery

Q7. Which migration type is best for under 150 mailboxes from on-prem Exchange?

A: Cutover migration

Q8. What's the purpose of mail flow rule mode "Test with Policy Tips"?

A: Evaluate the rule without enforcement; show what would happen (with sender hints)

Q9. What are the two DKIM selectors Microsoft uses?

A: selector1 and selector2 (for key rotation)

Q10. Where do you find quarantined messages?

A: Defender portal → Review → Quarantine

Section 5
05
Microsoft Teams Administration
Teams is now the hub for collaboration: chat, meetings, calls, files, and apps. Master architecture, policies, governance, external/guest access, calling, and the troubleshooting moves you'll need every week.
Exam Weight: ~15%

5.1 Microsoft Teams Architecture

Introduction

Microsoft Teams is the unified collaboration hub of Microsoft 365 — chat, video meetings, voice calling, file sharing, app integration. Architecturally, Teams isn't a single product but a presentation layer sitting on top of Microsoft 365 Groups, SharePoint, OneDrive, Exchange, Azure Communication Services, and Stream.

Why This Topic Is Important

Teams replaced Skype for Business as Microsoft's collaboration platform. With 300+ million monthly active users globally, every M365 admin must understand how Teams fits together — because issues span multiple

workloads. A "Teams problem" might really be a SharePoint sync issue, an Exchange calendar bug, or a network firewall block.

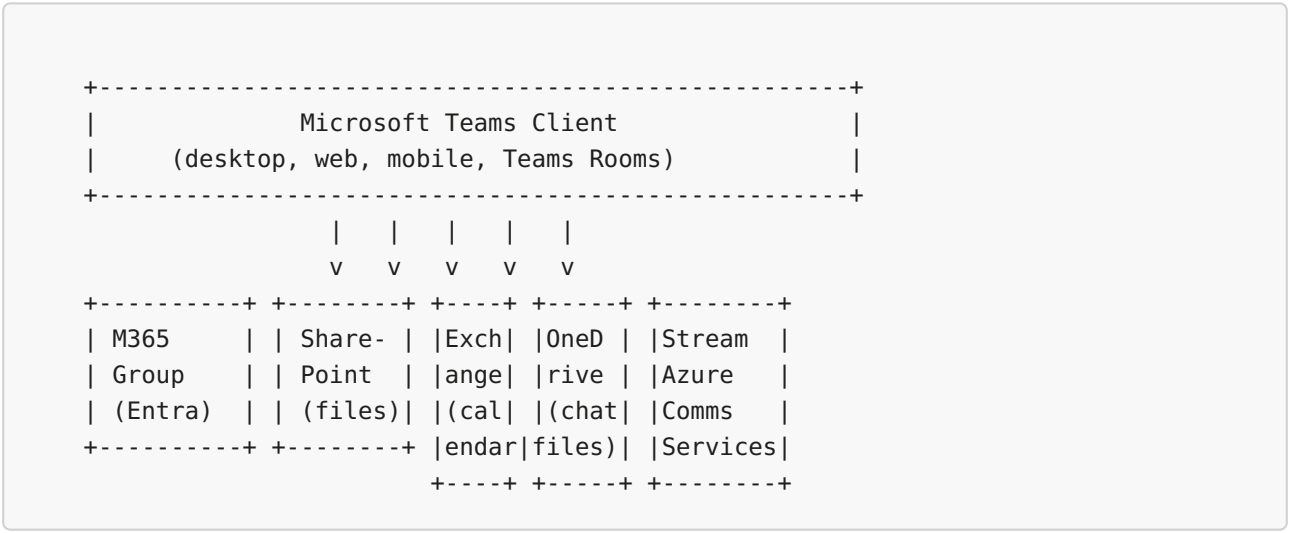
Key Architectural Components

Component	What Lives There	Underlying Tech
Team	The container	M365 Group + SharePoint site
Channels (Standard)	Conversations + files	SharePoint document library (folder)
Channels (Private)	Subset-only conversations	Separate SharePoint site
Channels (Shared)	Cross-tenant channels	Separate SharePoint site + cross-tenant
Chat (1:1 and group)	Persistent chats	Azure (compliance copies in Exchange)
Meetings	Audio/video, recording, transcripts	Azure Communication Services + Stream
Calls (PSTN)	External phone calls	Teams Phone + Calling Plan / Direct Routing
Files	Documents in channels and chats	SharePoint (channels) / OneDrive (chats)
Calendar	Meeting invites, scheduled meetings	Exchange Online
Apps	Tabs, bots, message extensions	Microsoft + ISV apps

Data Storage Locations

Data Type	Stored Where
Team membership	M365 Group in Entra ID
Channel posts	Azure (Cosmos DB) with compliance copy in group mailbox
1:1 / group chat	Azure with compliance copy in users' mailboxes
Team files (Standard channels)	SharePoint Online site behind the Team
Team files (Private channels)	Separate SharePoint site (one per private channel)
Chat files	Sender's OneDrive (Microsoft Teams Chat Files folder)
Meeting recordings	OneDrive (1:1) or SharePoint (channel meetings)
Wiki / Notes / Loop	SharePoint / Loop service

Architecture Diagram



Microsoft Portal Navigation

> 📍 Microsoft Teams Admin Center → `admin.teams.microsoft.com`

Teams Admin Roles

Role	Capability
Teams Administrator	Full Teams admin
Teams Communications Administrator	Manage call/meeting features
Teams Communications Support Engineer	Limited troubleshooting (full call info)
Teams Communications Support Specialist	Limited troubleshooting (partial call info, redacted user info)
Teams Devices Administrator	Manage Teams-certified devices

License Requirements

License	Teams Capability
Microsoft 365 Business Basic / Standard / Premium	Full Teams collab
Microsoft 365 E3 / E5	Full Teams collab; E5 includes Teams Phone
Office 365 E1 / E3 / E5	Teams included
Microsoft Teams Essentials	Standalone for small business
Frontline F1 / F3	Teams included with frontline features
Teams Phone (standalone)	Adds PSTN calling on top of any Teams license
Teams Rooms Pro	For Teams Rooms devices

Network Requirements

Teams is real-time collaboration — network matters more than for email. Microsoft's published guidance:

- Latency: <50 ms one-way to nearest Microsoft network edge.
- Jitter: <30 ms.
- Packet loss: <1%.
- Open required ports: UDP 3478-3481, 50000-50059, TCP 443.
- Allow domains: *.teams.microsoft.com, *.skype.com, *.lync.com, *.microsoft.com.
- Avoid double NAT, deep packet inspection of Teams traffic.

Real-World Scenarios

Scenario: Files not appearing in channel

User reports: "I uploaded a file to the Sales channel but I can't see it." Diagnosis: open the channel → Files tab → Open in SharePoint. The SharePoint site has the file. Issue: their Teams client cached an old view. Fix: Teams → ⋯ → Settings → Cache → Clear. Reopen Teams. File appears.

Best Practices

- Understand Teams ≠ a single workload; troubleshoot at the right layer.
- Run Network Planner before deploying Teams calling.
- Use Teams Admin Center for tenant-wide settings; Per-team owners can adjust team settings.
- Apply Communications Support Specialist for helpdesk (least privilege).

Summary

Section 5.1 Summary

- Teams = collaboration hub built on M365 Groups, SPO, Exchange.
- Channels = SharePoint folders; private channels = separate SharePoint sites.
- Chat data in Azure with compliance copies in Exchange.
- Admin Center: admin.teams.microsoft.com.
- Critical: low-latency network for real-time media.

5.2 Teams Admin Center

Introduction

The Teams Admin Center (TAC) is the dedicated portal for managing all Teams settings, policies, devices, calls, and reports.

Major Sections

Section	Purpose
Dashboard	Overview tiles: users, teams, devices, alerts
Teams → Manage teams	List of all Teams; manage membership, channels, sensitivity
Teams → Teams policies	Restrict who can create private channels, discover public teams
Teams → Templates / Update policies	Reusable team structures; client update behaviour
Users → Manage users	User profile + assigned policies
Users → External access	Federation with other Teams tenants and Skype
Users → Guest access	Global toggle: are guests allowed?
Teams devices	IP phones, Teams Rooms devices, Surface Hubs
Teams apps	Manage apps available to users; app permissions; setup policies
Meetings → Meeting policies	Recording, transcription, who can present, lobby behavior
Meetings → Meeting settings	Anonymous join, customization
Meetings → Live events policies	Who can host large broadcasts
Messaging policies	Edit / delete sent messages, GIFs, stickers, URL preview
Voice	Phone numbers, call queues, auto attendants, dial plans, calling policies
Locations	Emergency dispatch addresses (E911)
Enhanced encryption policies	End-to-end encryption for 1:1 calls
Policy packages	Pre-built sets of policies for roles (Education, Healthcare, Frontline)
Planning	Network Planner, TAC dashboards
Analytics & reports	Usage reports, call quality dashboard (CQD)
Notifications & alerts	Rule-based alerts

Policy Concept

Teams uses policies to configure features per user or per group. There are policy types for: meetings, messaging, calling, app permissions, app setup, live events, voice routing, dial plans, etc. Default "Global" policy applies to all users unless overridden by a custom policy assigned to them.

Real-World Scenarios

Scenario: Helpdesk diagnosing call quality

User reports terrible video call quality. Helpdesk opens TAC → Users → user → Meetings & calls tab. Sees recent call with packet loss 15% and jitter 80ms. Drills into call → identifies it was on guest Wi-Fi (low signal). Recommends user use Ethernet or higher-quality Wi-Fi. CQD confirms broader pattern: all calls from that office show degradation — escalate to network team.

Summary

Section 5.2 Summary

- TAC at admin.teams.microsoft.com.
- Major sections: Teams, Users, Meetings, Voice, Apps, Analytics.
- Policies override Global default per user/group.
- CQD (Call Quality Dashboard) for call quality investigations.

5.3 Teams Policies

Introduction

Teams Policies (specifically "Teams policies" in TAC, distinct from meeting/messaging/etc.) control what users can DO with the Teams feature — private channels, discoverable teams, etc.

Policy Types Overview

Policy Type	What It Controls
Teams policies	Create private channels, discover public teams
Meeting policies	Audio/video, recording, screen-share, lobby
Live events policies	Schedule live events; transcription, recording
Messaging policies	Edit/delete messages, GIFs, stickers, voice messages
Calling policies	Make private calls, busy on busy, voicemail
Call park policies	Pickup ranges
App permission policies	Which apps users can install (Microsoft, ISV, custom)
App setup policies	Pre-pin apps to user's left rail; allow user pinning
Voice routing policies	Direct Routing dial-out paths
Dial plans	Normalize phone numbers
Caller ID policies	Show/hide caller ID
Emergency calling policies	E911 behaviour

Step-by-Step: Restrict Private Channel Creation to Owners

1. TAC → Teams → Teams policies → Global (Org-wide default) → Edit.
2. Create private channels: Off.
3. Save.

To allow specific groups to still create them: create a new Teams policy with "Create private channels: On", assign to that group only.

Step-by-Step: Apply Policy via Group

1. TAC → Meetings → Meeting policies → + Add policy "Restricted-Meeting" (for kiosks, frontline).
2. Disable video, disable screen share, disable chat for that group.
3. Save.
4. TAC → Users → Group policy assignment → + Add → select "Restricted-Meeting" → assign to security group "Kiosk-Users".
5. Members of Kiosk-Users now have restricted meetings; others use Global.

PowerShell — Teams Module

```
# Install module (once)
Install-Module MicrosoftTeams -Force

# Connect
Connect-MicrosoftTeams

# List all teams in tenant
Get-Team | Select-Object DisplayName, Visibility, MailNickName, GroupId

# Get team members
Get-TeamUser -GroupId "abc-123-...."

# Add member to a team
Add-TeamUser -GroupId "abc-123-..." -User "user@contoso.com"

# List policies
Get-CsTeamsMeetingPolicy
Get-CsTeamsMessagingPolicy
Get-CsTeamsAppPermissionPolicy

# Assign policy to user
Grant-CsTeamsMeetingPolicy -Identity "alice@contoso.com" -PolicyName "Restricted-
Meeting"

# Assign policy to group
New-CsGroupPolicyAssignment -GroupId "group-guid" `
    -PolicyType "TeamsMeetingPolicy" `
    -PolicyName "Restricted-Meeting" `
    -Rank 1
```

Real-World Scenarios

Scenario: Sales-focused settings

Sales team needs full messaging features (GIFs, stickers OK for client rapport). Frontline workers need restricted (focus, less distraction). Solution: create "Sales-Messaging" policy with all features; "Frontline-Messaging" policy with disabled GIFs/stickers/voice messages. Assign via group policy assignment.

Summary

Section 5.3 Summary

- Many policy types in TAC: Teams, Meeting, Messaging, Calling, App, Voice.
- Global = default; custom policies override per user/group.
- Group policy assignment scales policy management.

- PowerShell: MicrosoftTeams module.

5.4 Messaging Policies

Introduction

Messaging policies control chat features: edit/delete messages, who can use GIFs/stickers/memes, link previews, read receipts, voice/video messages, immersive reader.

Common Settings

Setting	Use
Owners can delete sent messages	For compliance; lets team owners moderate
Users can edit their own messages	Allow typos to be fixed; default ON
Users can delete their own messages	Default ON; off for regulated industries
Read receipts	On, Off, User controlled
Chat with Skype consumer	Federation with Skype
Use Giphy	On/off; content rating
Use stickers, memes	On/off
Use URL previews	On/off
Voice messages	On, Off, On for chats only
Translation	On/off; auto-translation
Suggested replies	On/off (AI-generated)

Step-by-Step: Restrict Messaging for Frontline Workers

1. TAC → Messaging policies → + Add.
2. Name: "Frontline-Restricted".
3. Disable: Giphy, stickers, memes, voice messages, suggested replies.
4. Disable: edit messages, delete messages (compliance).
5. Save.
6. Assign to Frontline group.

Compliance Hold for Messages

Even if users delete messages, compliance copies are retained:

- Channel messages: in the M365 Group's hidden Exchange folder.
- 1:1/group chat: in each user's mailbox (hidden folder).
- Retention policies apply.
- eDiscovery can search all Teams content.

Summary

Section 5.4 Summary

- Messaging policies = chat feature control.
- Disable edit/delete for compliance scenarios.
- Compliance copies retained regardless of user delete.

5.5 Meeting Policies

Introduction

Meeting policies control everything about Teams meetings: who can join, who can present, video/audio defaults, recording, transcription, breakout rooms, whiteboard, lobby behaviour, anonymous join.

Common Meeting Policy Settings

Setting	Common Value	Why
Allow Meet Now in channels	On	Spontaneous channel meetings
Allow meeting scheduling	On	Standard for most users
Allow channel meeting scheduling	On	Schedule in channel
Allow private meeting scheduling	On	Calendar invites
Live captions	Disabled but user can enable	Default
Allow recording	On for most	Disable for sensitive groups
Store recordings outside region	Off for compliance	Data sovereignty
Allow transcription	On	Standard
IP video	On	Allow video
Screen sharing mode	Entire screen / Single app / Disabled	Tighten for kiosks
Allow PowerPoint sharing	On	Standard
Allow whiteboard	On	Standard
Allow shared notes	On	Loop integration
Lobby: Anonymous users	Bypass lobby: false	Anonymous wait in lobby
Designate roles	Everyone presenter, or only Org or Specific	Lock down for webinars
Allow chat in meetings	On	Standard
Live events policies	Separate policy	Large broadcasts

Step-by-Step: Webinar/External Meeting Policy

1. TAC → Meetings → Meeting policies → + Add.
2. Name: "External-Webinar".
3. Meeting join & lobby:
    - Anonymous users can join a meeting: On
    - Who can bypass lobby: Only organizers and co-organizers
    - People dialing in can bypass lobby: No

4. Engagement:
    - Allow whiteboard, shared notes, reactions: On
    - Chat in meetings: On for in-tenant, Off for anonymous
5. Audio & video:
    - Mode for IP audio: Outgoing and incoming audio enabled
    - Mode for IP video: Outgoing and incoming video enabled
6. Content sharing:
    - Screen sharing mode: Single application (prevents accidental over-sharing)
    - Allow a participant to give or request control: Off (prevents external takeover)
7. Recording & transcription:
    - Recording: On
    - Transcription: On
8. Save; assign to "Marketing-Webinar-Hosts" group.

Meeting Templates & Sensitivity Labels

Modern Teams supports Meeting Templates (pre-configured experiences) and integration with sensitivity labels:

- Public Webinar template — anonymous join allowed, lobby on, chat moderated.
- Confidential meeting template — Recording disabled, no copy/forward, watermark.
- Sensitivity label "Highly Confidential" can enforce these.

PowerShell

```
# Get meeting policies
Get-CsTeamsMeetingPolicy | Format-Table Identity, AllowMeetNow, AllowCloudRecording

# Create new meeting policy
New-CsTeamsMeetingPolicy -Identity "External-Webinar" `
    -AllowCloudRecording $true `
    -AllowTranscription $true `
    -AllowAnonymousUsersToJoinMeeting $true `
    -ScreenSharingMode "SingleApplication" `
    -AllowParticipantGiveRequestControl $false

# Assign to user
Grant-CsTeamsMeetingPolicy -Identity "alice@contoso.com" -PolicyName "External-
Webinar"
```

Real-World Scenarios

Scenario: Sensitive board meeting

Board meeting includes financials before earnings release. Risk: leak via recording. Solution: assign board members a "BoardMeeting" policy that disables Recording, Transcription, and anonymous join. Use Sensitivity Label "Highly Confidential" to enforce no copy/forward of chat. End-to-end encryption enabled. After meeting, no artifacts remain.

Best Practices

- Apply Strict meeting policy to executives and finance.
- Disable anonymous join for internal-only meetings.
- Set "Only organizers" as default presenter role for webinars.
- Enable transcription for compliance and accessibility.
- Train users on Lobby and Roles features.

Summary

Section 5.5 Summary

- Meeting policies = audio/video, recording, sharing, lobby, roles.
- Distinct from Messaging and Live Events policies.
- Restrict for sensitive groups; standard for most.
- Combine with sensitivity labels for enforcement.

5.6 Voice and Calling Overview

Introduction

Teams Phone turns Teams into a full PBX replacement. Users get phone numbers, can make/receive PSTN calls, voicemail, auto attendants, call queues. Replaces traditional desk phones and on-prem PBX infrastructure.

Calling Plans Options

Option	How It Works	Use
Microsoft Calling Plan	Microsoft provides PSTN service + numbers	Available in select countries; simplest
Direct Routing	You bring your own SBC + carrier	Existing telecom contracts; complex
Operator Connect	Microsoft partners provide PSTN via cloud	Middle ground; in-country carrier
Teams Phone Mobile	Single number across SIM + Teams	Mobile-first workforce

Teams Phone Components

Feature	Description
Phone number assignment	Number tied to a user enabled for calling
Caller ID policies	What number to show on outbound calls
Calling policies	Allow private calls, busy-on-busy, voicemail behaviour
Dial plans	Normalize dialed numbers (e.g., 4-digit extension → +92 21 1234 5678)
Auto Attendants	IVR menus (press 1 for sales)
Call queues	Distribute incoming calls to agents
Emergency calling (E911)	Map location to dispatchable address
Audio conferencing	Dial-in numbers for meetings
Voicemail	Stored in user's Exchange mailbox; transcription available

Step-by-Step: Assign a Phone Number

1. TAC → Voice → Phone numbers → + Add (or get from carrier).
2. Acquire or port numbers (depending on plan type).
3. Once numbers in inventory: TAC → Users → user → Account → Assigned phone number → + Edit.
4. Select number → save.
5. Verify in user's Teams client: phone icon now active; can call any number.

Auto Attendant Example

1. TAC → Voice → Auto attendants → + Add.
2. Name: "Main Reception".
3. Language: English.
4. Operator: optional human operator.
5. Business hours: 9 AM - 6 PM Mon-Fri.
6. Holidays: configure.
7. Call flow:
    - Greeting: "Welcome to Contoso. Press 1 for Sales, 2 for Support, 0 for operator."
    - Menu options: 1 → call queue Sales, 2 → call queue Support, 0 → operator
8. After-hours call flow: different greeting and voicemail.
9. Assign phone number to auto attendant.
10. Test by calling the number.

Call Quality Dashboard (CQD)

CQD aggregates call quality metrics across the tenant:

- Per-region quality trends
- Per-building dashboards (if subnet → building map uploaded)
- Wi-Fi vs Wired quality
- Network drop reasons

Real-World Scenarios

Scenario: Replace traditional PBX

500-user company has aging on-prem Avaya PBX. Replacement plan: (1) Audit calling patterns. (2) Choose Direct Routing with existing carrier (preserve number portability and contracts). (3) Deploy SBC pair. (4) Configure dial plans (3-digit internal extensions). (5) Migrate 50 pilot users; test for 2 weeks. (6) Port numbers in batches. (7) Decommission Avaya. Cost savings: 60% on telecom.

Best Practices

- Plan E911 thoroughly — emergency dispatch addresses are legally required.
- Use Communications Credits for international dialing or excess minutes.
- Train users: Teams calling has different UX than desk phone.
- Monitor CQD weekly during rollout.
- Have a fallback: keep some PSTN lines for emergencies.

Summary

Section 5.6 Summary

- Teams Phone = full PBX replacement.
- 4 PSTN options: Calling Plan, Direct Routing, Operator Connect, Teams Phone Mobile.
- Auto Attendants and Call Queues replace IVRs.
- CQD for call quality monitoring.
- E911 (location-based emergency) is legally important.

5.7 External Access and Guest Access

Introduction

Two distinct features confuse admins constantly:

- **External Access** (federation) = your users chat/call users in OTHER Teams tenants (or Skype consumer).
- **Guest Access** = external users invited INTO your tenant as guests, with full team membership.

External Access vs Guest Access

Feature	External Access	Guest Access
External user identity	Stays in their tenant	Becomes a guest in your tenant
Access to your teams	No — they remain outside	Yes — added as guest member
1:1 chat across tenants	Yes	Yes
Group chat across tenants	Yes	Yes (within shared/guest scope)
Call across tenants	Yes	Yes
See user's presence	Yes (if allowed)	Yes
Underlying tech	Teams federation	Entra B2B
Configured at	TAC → External access	TAC → Guest access (toggle); per-team add as guest

Configure External Access

1. TAC → Users → External access.

2. Choose mode:
    - Allow all external domains (most open)
    - Allow only specific external domains (curated list)
    - Block specific external domains
    - Block all external domains (most closed)
3. Skype consumer toggle: enable if your users need to chat with personal Skype users.
4. Save.

Configure Guest Access

1. TAC → Users → Guest access.
2. Allow guest access in Teams: On.
3. Configure granular toggles:
    - Make private calls: On
    - Allow IP video: On
    - Screen sharing: Entire screen / Single app
    - Meet Now: On
    - Edit/delete sent messages: On
    - Chat: On
    - Delete chat: On
    - GIFs, stickers, memes: configurable
    - Immersive Reader: On
4. Save.

Cross-Tenant Access Settings (Newer Model)

Entra cross-tenant access settings provide granular B2B controls per partner organization (overrides External Collaboration Settings):

- Per-tenant inbound/outbound rules.
- Allow/block specific users, groups, applications.
- Trust MFA claims from partner.
- Trust compliant device claims from partner.

Shared Channels (Teams Connect)

Shared channels let users in DIFFERENT tenants collaborate in a single channel — without inviting each other as guests:

- Each user keeps identity in their home tenant.
- No tenant switching in Teams client.
- Better for long-term, frequent partner collaboration.
- Requires cross-tenant access settings configured between both tenants.

Step-by-Step: Add a Guest to a Team

1. Verify Guest Access is enabled (TAC).
2. Verify Entra external collaboration allows their domain.
3. Team owner: ⋯ next to team → Add member.
4. Type guest's email; Teams creates Entra B2B invite.
5. Guest receives email → accepts.
6. Guest now in team; can chat, attend meetings, view files.

PowerShell

```
# External access settings
Get-CsTenantFederationConfiguration

Set-CsTenantFederationConfiguration `
    -AllowFederatedUsers $true `
    -AllowPublicUsers $false `
    -AllowedDomains @{Add="partner1.com","partner2.com"}

# Guest access
Get-CsTeamsClientConfiguration | Select-Object AllowGuestUser
Set-CsTeamsClientConfiguration -Identity Global -AllowGuestUser $true
```

Real-World Scenarios

Scenario: Vendor collaboration

Contoso works with Fabrikam vendor on a 6-month project. Choice: federation (external access) for ad-hoc chat/calls; OR add Fabrikam staff as guests in a dedicated Team. Best fit: Guests in Team — gives Fabrikam staff access to project files, channels, and meetings. After project, remove guests; access revoked.

Best Practices

- Default to allow-list (specific domains) for federation, not allow-all.
- Use Guest Access for project-specific collaboration.
- Use Shared Channels for long-term partner work.
- Enforce MFA for guests via Conditional Access.
- Periodically review guest access via Entra Access Reviews.
- Educate users: guests see your team's files, chats, calendar.

Summary

Section 5.7 Summary

- External Access = chat/call between tenants; users stay in home tenant.
- Guest Access = external user added as member of your team.
- Shared Channels = newer, no tenant switching needed.
- Configure via TAC + Entra Cross-Tenant Access Settings.
- Use Access Reviews to clean up guests.

5.8 Teams Security & Governance

Introduction

Teams security and governance covers: who can create teams, naming conventions, expiration, sensitivity labels, retention, eDiscovery, DLP. Without governance, you get "team sprawl" — thousands of unused teams clogging the directory.

Common Governance Problems

Problem	Symptom
Sprawl	10,000+ teams, most unused
Orphan teams	Owner left; no one can manage
Naming chaos	"Sales Team", "Sales-Team", "Team-Sales-2024"
External sharing too open	Sensitive files shared anonymously
Stale teams	Last activity 2 years ago, still consuming resources

Governance Controls

1. Restrict Team Creation

Block users from creating M365 Groups (and thus Teams) — only specific group of IT/team owners can:

```
Connect-MgGraph -Scopes "Directory.ReadWrite.All"

# Create an "M365 Group Creators" security group first, then:
$template = Get-MgBetaDirectorySettingTemplate |
    Where-Object { $_.DisplayName -eq "Group.Unified" }

$creators = (Get-MgGroup -Filter "displayName eq 'M365-Group-Creators'").Id

$params = @{
    TemplateId = $template.Id
    Values = @(
        @{ Name = "EnableGroupCreation"; Value = "false" }
        @{ Name = "GroupCreationAllowedGroupId"; Value = $creators }
    )
}
New-MgBetaDirectorySetting -BodyParameter $params
```

2. Naming Policy

Enforce prefix/suffix and ban words (Entra ID P1):

```
$params = @{
    TemplateId = $template.Id
    Values = @(
        @{ Name = "PrefixSuffixNamingRequirement"; Value =
"GRP_[Department]_[GroupName]" }
        @{ Name = "CustomBlockedWordsList"; Value =
"CEO,Confidential,Payroll,Legal" }
    )
}
Update-MgDirectorySetting -BodyParameter $params
```

3. Group Expiration

Auto-expire stale teams (Entra ID P1):

1. Entra Admin Center → Groups → Expiration.
2. Group lifetime: 180 days (or 365).
3. Email contact for renewals: admin@contoso.com.
4. Enable for: all M365 groups (or selected).
5. Owners get email at 30, 15, 1 day before expiry → renew or let expire.

6. Save.

4. Sensitivity Labels for Teams

Labels can enforce privacy + external sharing:

1. Purview Portal → Information Protection → Labels.
2. Create label "Confidential - Internal Only":
    - Scope: includes Groups & sites
    - Group settings: Privacy = Private; External users = block; Guest access = block
    - SharePoint site settings: External sharing = none; managed device only
3. Publish to users.
4. Team creators apply label at creation.

5. Templates

Pre-built team templates standardize new teams:

1. TAC → Teams → Templates.
2. + Add → name + description.
3. Pre-define channels, tabs, apps.
4. Owners select template at team creation.

6. Retention Policies

Keep or delete Teams chat/channel messages on schedule:

1. Purview → Data lifecycle management → Retention policies → + New.
2. Locations: Teams chats, Teams channel messages.
3. Retain for X days, then delete (or just retain).
4. Apply.

eDiscovery for Teams

Search Teams content for legal/HR investigations:

1. Purview → eDiscovery → Standard or Premium.
2. Create case; add custodians (users).
3. Search: keyword + date range + locations (mailboxes, sites, Teams chat).
4. Review results, export.

DLP for Teams

Prevent sensitive data sharing in Teams:

1. Purview → Data Loss Prevention → + New policy.
2. Locations: Teams chat and channel messages.
3. Conditions: contains credit card numbers, SSN, etc.
4. Actions: block sender + show policy tip; notify admin.
5. Apply.

Real-World Scenarios

Scenario: Team sprawl cleanup

Year-old M365 tenant has 4,000 teams. Discovery: 60% are unused (no activity in 90 days). Plan: enable group expiration (180 days), notify owners; orphaned teams reviewed by IT. After 60 days, 2,500 teams archived/deleted, freeing storage and reducing directory complexity.

Best Practices

- Restrict team creation; have a request workflow.
- Enforce naming policy.
- Enable group expiration (180-365 days).
- Use sensitivity labels.
- Apply DLP to Teams chat.
- Quarterly governance review.

Summary

Section 5.8 Summary

- Restrict team creation to designated creators.
- Enforce naming policy and ban words.
- Group expiration auto-removes stale teams.
- Sensitivity labels control privacy and sharing.
- DLP, retention, eDiscovery apply across Teams.

5.9 Teams Apps Management

Introduction

Teams Apps extend functionality: tabs, bots, message extensions, connectors. Microsoft has 1,000+ apps in the store (Microsoft + ISV + custom). As admin, you control which apps users can install and which are pinned by default.

App Types

Source	Description
Microsoft apps	Built-in: Files, Calendar, Tasks, Planner, OneNote
Third-party (ISV)	Public store: Trello, Polly, GitHub, Jira, etc.
Custom (LOB)	Your in-house apps uploaded as .zip manifests

App Permission Policies

Control which apps users can install:

1. TAC → Teams apps → Permission policies.
2. Global default: allow all.
3. Create "Restricted-Apps" policy:
    - Microsoft apps: Allow specific (Files, Calendar, Tasks only)
    - Third-party apps: Block
    - Custom apps: Block
4. Assign to high-risk groups (regulated industries).

App Setup Policies

Pre-pin apps to user's left rail; allow/disallow user customization:

1. TAC → Teams apps → Setup policies.
2. + Add policy "Sales-Setup":
    - Pinned apps: Activity, Chat, Teams, Calendar, Calls, Files, Dynamics 365 Sales
    - Installed apps: pre-install Dynamics 365 for them
    - Allow user pinning: Yes (let users adjust)
3. Assign to Sales group.

Approve Custom Apps

1. Developer uploads .zip manifest via TAC → Teams apps → Manage apps → Upload.
2. App goes to Approval queue.
3. Admin reviews permissions, capabilities.
4. Approve and publish to org app catalog.
5. Users find under "Built for your org" in app store.

Common Apps Worth Knowing

App	Use
Planner / Tasks by Planner	Task and project management
Lists	Structured tracking (assets, issues, contacts)
Approvals	Workflow for approvals (purchases, time off)
Forms	Surveys and quick polls
Praise	Recognition badges
OneNote	Notes integration
Power BI	Embed dashboards in tabs
Bookings	Self-service appointment scheduling

Summary

Section 5.9 Summary

- Apps extend Teams functionality.
- App Permission Policies = which apps users can install.
- App Setup Policies = pre-pinned + installed apps per role.
- Custom apps require admin approval.

5.10 Teams Troubleshooting

Common Issue Categories

Issue	First Action
Can't sign in to Teams	Check Entra sign-in logs; clear Teams cache
Audio/video quality	Check CQD; network test; switch wireless to wired
Files not showing in channel	Check via SharePoint; clear cache
Calendar items missing	Verify Exchange license; OWA shows them?
Guest can't access	Verify guest invite redeemed; CA policies; tenant guest access on
Can't share screen	Meeting policy disabling sharing
Notifications missing	Client notification settings; Teams app permissions on OS
App not appearing	App permission policy blocking

Clear Teams Cache (Windows)

```
# Close Teams; then:
%appdata%\Microsoft\Teams\
# Delete contents (cache, blob_storage, databases, GPUcache, IndexedDB, Local
Storage, tmp)

# For new Teams (Teams 2.x):
%localappdata%\Packages\MSTeams_8wekyb3d8bbwe\
# Reset via Settings → Apps → Microsoft Teams → Advanced options → Reset
```

Client Connectivity Test

Visit `https://aka.ms/sara` for Microsoft Support and Recovery Assistant (SaRA) — automated Teams diagnostics.

Call Quality Investigation

1. TAC → Analytics & reports → Call Quality Dashboard.
2. Drill into per-user, per-region, or per-building views.
3. Identify common causes: wired vs wireless, Wi-Fi signal, ISP, server location.

4. For one-off bad call: TAC → Users → user → Meetings & calls tab → click call → see media stats.

Real-World Scenarios

Scenario: "Teams won't load"

User opens Teams → blank screen. Steps: (1) Sign out, sign in. (2) Clear cache (folder above). (3) Try Teams Web (teams.microsoft.com) — if works, problem is local client. (4) Reinstall Teams client. (5) If Web also fails: check Entra license + Conditional Access; possibly compliance issue.

Scenario: Choppy meeting audio

VP complains audio cuts out in meetings. CQD: packet loss spikes correlate with VPN reconnects. Fix: split-tunnel Teams traffic to bypass VPN (Microsoft documented). Or, use Teams optimization on the VPN appliance. Audio quality fixed.

Diagnostics Tools

Tool	Purpose
Call Quality Dashboard (CQD)	Tenant-wide call quality data
Real-time analytics (in-meeting)	Live troubleshooting during a meeting
Microsoft Network Connectivity Test	connectivity.office.com
SaRA (Support & Recovery Assistant)	Client-side automated diagnostics
Teams logs	%appdata%\Microsoft\Teams\logs.txt (legacy) or %userprofile%\AppData\Local\Packages\MSTeams_*\LocalCache\Microsoft\MSTeams\Logs\

Best Practices

- Always start: is it just this user, or many? CQD answers.
- Verify license + CA before deep debugging.
- Test the same action in Teams Web — narrows down client vs service.
- Keep Teams client and OS updated.
- Document common issues in helpdesk runbook.

Summary

Section 5.10 Summary

- Common issues: sign-in, audio quality, files, calendar, guest access.
- First-line fixes: cache clear, web client test, Entra log check.
- CQD for call quality patterns.
- SaRA for client diagnostics.

Section 5 — Wrap-Up

Section 5 Synthesis

- **Teams architecture** = M365 Group + SharePoint + Exchange + Azure media.
- **TAC** at admin.teams.microsoft.com manages everything.
- **Policy types**: Teams, Meeting, Messaging, Calling, App.
- **External Access** (federation) vs **Guest Access** (members in your team).
- **Teams Phone**: Calling Plan, Direct Routing, Operator Connect.
- **Governance**: restrict creation, naming, expiration, sensitivity labels, retention.
- **Apps**: Permission policies, Setup policies; custom apps require approval.
- **Troubleshooting**: cache clear, CQD, Web test.

Section 5 Mini-Quiz

Q1. What is the URL for the Teams Admin Center?

A: admin.teams.microsoft.com

Q2. Where are channel files actually stored?

A: SharePoint Online site behind the team (one library per channel for standard; separate site for private channels)

Q3. Where are 1:1 chat files stored?

A: Sender's OneDrive in "Microsoft Teams Chat Files" folder

Q4. Difference between External Access and Guest Access?

A: External Access = federation (users stay in home tenant, chat/call only). Guest Access = external user added as member of your team.

Q5. What are the four PSTN connectivity options for Teams Phone?

A: Microsoft Calling Plan, Direct Routing, Operator Connect, Teams Phone Mobile

Q6. Which tool aggregates call quality data tenant-wide?

A: Call Quality Dashboard (CQD)

Q7. What does an App Setup Policy control?

A: Pre-pinned apps in the user's left rail and which apps are auto-installed

Q8. How would you prevent end-user team creation?

A: Configure Group.Unified directory setting: EnableGroupCreation=false, allow only specific group of creators

Q9. What feature auto-removes stale Teams?

A: Microsoft 365 Group expiration policy (Entra ID P1)

Q10. Are Teams compliance copies kept even if users delete messages?

A: Yes — channel messages in M365 Group mailbox; 1:1/group chats in each user's mailbox

Section 6
06
SharePoint Online & OneDrive
The Microsoft 365 content fabric. SharePoint hosts team and communication sites; OneDrive gives every user 1+ TB of personal cloud storage. Master site collections, permissions, sharing, sync, and data governance.
Exam Weight: ~10%

6.1 SharePoint Online Overview

Introduction

SharePoint Online (SPO) is Microsoft's cloud-based content management platform. It hosts documents, pages, lists, and apps in "sites." Teams channels, M365 Groups, viva connections, and content management all sit on SharePoint underneath.

Why This Topic Is Important

Almost everything in Microsoft 365 stores data in SharePoint or OneDrive: Teams files, group documents, intranet pages, news, employee handbooks, business records. Good SharePoint admin = good information architecture. Bad = chaos and security holes.

Site Types

Site Type	Purpose	Created Via
Team site (group-connected)	Collaboration; tied to an M365 Group + Team	Teams, M365 Group, OneDrive admin
Team site (not group-connected)	Classic project site with permissions managed independently	SharePoint admin center (legacy)
Communication site	Broadcast intranet content (news, departments)	SharePoint admin center / + Create site
Hub site	Associates other sites for navigation + branding	Promote existing site to hub
OneDrive (per user)	Personal cloud storage	Auto-provisioned on first OneDrive access
App catalog	Tenant-wide deployed SPO apps	+ Create from admin center

Key Concepts

Concept	What It Is
Site Collection	Top-level container; one URL like /sites/SalesTeam
Site	A site collection — modern SPO uses flat site collections, not subsites
Library	Collection of documents (with versioning, metadata)
List	Structured data records — like a database table
Page	Modern intranet page (news, landing)
Item	One row in a list, or one document in a library
App	SharePoint Framework (SPFx) extension
Hub	A central site with associated sites sharing branding + nav

License-Based Storage

License	OneDrive	SharePoint Tenant Pool
F1 / F3	2 GB	10 GB + 10 MB/license
Business Basic	1 TB	1 TB + 10 GB/license
E3 / E5 / Business Standard	1 TB (can expand to 5 TB)	1 TB + 10 GB/license
SharePoint Plan 1 standalone	—	—

Microsoft Portal Navigation

> 📍 SharePoint Admin Center → `admin.microsoft.com/sharepoint`

Admin Center Sections

- Home — quick metrics
- Sites → Active sites — manage every site collection
- Sites → Deleted sites — restore within 93 days
- Policies → Sharing — tenant-wide sharing controls
- Policies → Access control — restrict by network, unmanaged devices, app session
- Settings — sync client, OneDrive, search, classic features
- Content services → Term store, Content type gallery
- Migration — Mover, SharePoint Migration Tool
- Reports — usage

Best Practices

- Use modern Team sites + Communication sites; avoid creating subsites.
- Use hubs to associate related sites.
- Manage sharing tenant-wide first, then per-site.
- Apply sensitivity labels to sites.
- Configure retention policies.

Summary

Section 6.1 Summary

- SPO hosts content for Teams, intranet, project sites.
- Modern: flat site collections; Team + Communication site types.
- Each license adds 10 GB to tenant pool + 1 TB OneDrive.
- Admin center: admin.microsoft.com/sharepoint.

6.2 Site Collections, Team Sites, Communication Sites

Team Sites (Group-Connected)

- Created when a Microsoft 365 Group or Team is created.
- URL: `/sites/[GroupAlias]` or `/teams/[TeamAlias]`.
- Permissions managed via the M365 Group (owners, members, guests).
- Includes one document library "Documents" by default.
- Channel files appear as folders here.

Communication Sites

- Broadcast-style sites: news, departments, projects with wider audience.
- Author/edit by a small group; view by many.
- Three templates: Topic, Showcase, Blank.
- NOT tied to an M365 Group — permissions managed directly on site.
- URL: `/sites/[Name]`.

Hub Sites

A hub site is a regular site (Team or Communication) "promoted" to act as a hub for associated sites:

- Associated sites inherit hub navigation and branding.
- Search scope spans all associated sites.
- News from associated sites surfaces on the hub.
- Up to 2,000 hubs per tenant; up to 1,000 sites per hub.

Step-by-Step: Create a Communication Site

1. Sign in to SharePoint home (contoso.sharepoint.com).

2. + Create site → Communication site.
3. Choose design (Topic, Showcase, Blank).
4. Site name + description.
5. Site address (URL) + language.
6. Finish.
7. Configure owners and members via Site permissions.

Step-by-Step: Create a Hub Site

1. SharePoint Admin Center → Active sites → select an existing site.
2. … → Hub → Register as hub site.
3. Hub name + permissions for associating sites.
4. Save.
5. Now any site can associate: Site → Settings → Hub site → choose hub.

PowerShell — SPO Management Shell

```
# Install module
Install-Module Microsoft.Online.SharePoint.PowerShell -Force

# Connect
Connect-SPOService -Url https://contoso-admin.sharepoint.com

# List all sites
Get-SPOSite -Limit All | Format-Table Url, Owner, StorageUsageCurrent

# Get a site
Get-SPOSite "https://contoso.sharepoint.com/sites/Sales" | Format-List

# Create a Communication site
New-SPOSite -Url "https://contoso.sharepoint.com/sites/news" `
    -Owner "admin@contoso.com" `
    -StorageQuota 5120 `
    -Template "SITEPAGEPUBLISHING#0" `
    -Title "Company News"

# Create Team site (NOT group-connected — modern way is via M365 Group)
New-SPOSite -Url "https://contoso.sharepoint.com/sites/ProjectX" `
    -Owner "admin@contoso.com" -StorageQuota 1024 `
    -Template "STS#3" -Title "Project X"

# Set storage quota
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/Sales" -StorageQuota
10240

# Lock a site (e.g., during compliance hold)
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/OldProject" `
    -LockState NoAccess
```

Real-World Scenarios

Scenario: Departmental intranet

Need: HR, Finance, IT each want their own intranet. Create a Hub "Intranet". Create Communication sites HR-Hub, Finance-Hub, IT-Hub. Associate to Intranet hub. Users see consistent branding + cross-hub search. Each department manages their own site content.

Summary

Section 6.2 Summary

- Team site (group-connected) = collaboration with M365 Group.
- Communication site = broadcast, broader audience.

- Hub site = associates related sites for navigation + search.
- Modern SPO: flat site collections, not subsites.

6.3 Permissions Management

Permission Models

Site Type	Permission Model
Group-connected Team site	M365 Group: Owners, Members, Guests. Site Visitors group also available
Communication site	Owners, Members, Visitors (SharePoint groups, not M365 Group)
Library / List / Item	Can break inheritance and grant unique permissions

SharePoint Permission Levels

Level	Allows
Full Control	Everything including site settings
Edit	Add/edit/delete items + lists
Contribute	Add/edit/delete items (not lists)
Read	View items, download
Limited Access	Auto-applied when item-level shared
View Only	View in browser, no download

Best Practice: Use Groups, Not Direct Permissions

Don't grant individual users access to libraries — assign to security groups instead. Groups scale; individual permissions don't.

Permission Inheritance

By default, libraries inherit from site, items inherit from libraries. Breaking inheritance grants unique permissions but adds complexity. Avoid breaking inheritance more than a couple levels.

Step-by-Step: Grant Site Access

1. Site → ⋯ → Site permissions.
2. + Share site.
3. Add user or group; choose role: Owner, Member, Visitor.
4. Send email invite: optional.
5. Save.

Step-by-Step: Break Inheritance on a Library

1. Library → ⚙ → Library settings.
2. Permissions for this list → Stop inheriting permissions.
3. Now manage explicitly: add specific users or groups.

External Sharing

Configure tenant-wide first:

1. SharePoint Admin Center → Policies → Sharing.
2. External sharing slider for SharePoint: Anyone (most open) → New and existing guests → Existing guests only → Only people in your organization (most closed).
3. Same for OneDrive.
4. "More external sharing settings":
    - Limit external sharing by domain (allow/block lists)
    - Guests must sign in using the account they were invited with
    - Allow guests to share items they don't own
5. File and folder links default to: People in your organization / Anyone / Specific people.
6. Anyone link expiration: 30 days (recommended).
7. Save.

Per-Site Sharing Override

Lower (more restrictive) sharing per site:

1. Admin Center → Active sites → select site → Sharing.
2. Choose narrower setting (can't exceed tenant level).
3. Save.

PowerShell

```
# Set tenant-wide sharing
Set-SPOTenant `
    -SharingCapability "ExternalUserSharingOnly" `
    -RequireAcceptingAccountMatchInvitedAccount $true `
    -RequireAnonymousLinksExpireInDays 30

# Set per-site sharing
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/HR" `
    -SharingCapability "Disabled"

# Add user to site
Add-SPOUser -Site "https://contoso.sharepoint.com/sites/Sales" `
    -LoginName "alice@contoso.com" -Group "Sales Members"
```

Real-World Scenarios

Scenario: External partner access

Auditor needs access to one folder for 30 days. Solution: 1) Verify tenant external sharing allows specific people. 2) Right-click folder → Share → specific people → enter auditor email. 3) Permission: View only (no edit). 4) Link expiration: 30 days. 5) After 30 days, access auto-expires.

Best Practices

- Use SharePoint groups (Owners/Members/Visitors), not item-level breaks.
- Tighten tenant sharing first, loosen per-site as needed.
- Default file links to "People in your organization" (not Anyone).
- Anyone link expiration: 30 days max.
- Use sensitivity labels to enforce sharing scope.
- Quarterly review of external users + access reviews.

Summary

Section 6.3 Summary

- Permissions via SharePoint groups: Owners, Members, Visitors.
- Break inheritance sparingly.
- External sharing: configure tenant-wide; per-site only restricts further.
- Anyone link expiration: 30 days.

6.4 External Sharing

Five Levels of External Sharing

Level	Description
Anyone	Anyone with the link, no sign-in; max permissive; for general public files
New and existing guests	Must authenticate; new guests are invited via email
Existing guests only	Must already be in your directory as guest
Only people in your organization	No external sharing at all

Anyone Links — Pros and Cons

- **Pro:** easy — recipient just clicks link.
- **Con:** link can be forwarded; no audit trail of who accessed.
- **Mitigation:** expiration, password protection, view-only.

Sharing Settings Best Practice

Setting	Recommended
Tenant external sharing	New and existing guests (default)
Default link type	People in your organization
Anyone link expiration	30 days
Allow domain	Specific partner domains
Block guest sharing of items they don't own	Yes
Restrict access by managed device	For sensitive sites

Access Control Tab in Admin Center

Setting	Purpose
Unmanaged devices	Block / Limit web-only access from devices not enrolled in Intune
Idle session sign-out	Auto sign-out after X minutes inactivity
Network location	Restrict access to specific IP ranges
Apps that don't use modern authentication	Block legacy auth

Real-World Scenarios

Scenario: Confidential file leaked

Audit reveals a file marked Confidential was shared with an Anyone link to a personal Gmail. Investigation: user shared it intentionally. Fix forward: (1) Apply sensitivity label "Confidential" that disables Anyone links. (2) Configure DLP policy that blocks Anyone link creation when content is sensitive. (3) Conduct user awareness training.

Summary

Section 6.4 Summary

- Four sharing levels: Anyone, New+Existing guests, Existing only, Internal only.
- Default link type: People in your organization.
- Anyone link expiration: 30 days.
- Access Control: restrict by managed device, network location.

6.5 OneDrive Administration

Introduction

OneDrive for Business is each user's personal cloud storage — typically 1 TB. It's where users store individual work files, sync between devices, and share with collaborators. As admin, you manage tenant-wide OneDrive policies, storage, retention, and offboarding.

Key Concepts

Concept	Details
OneDrive URL	`contoso-my.sharepoint.com/personal/alice_contoso_com`
Provisioning	Auto on first OneDrive access (or pre-provisioned via PowerShell)
Default quota	1 TB; expandable to 5 TB → 25 TB with support request
Recycle bin	93 days (first stage) + 30 days (second stage admin)
Sync client	OneDrive.exe (Windows), OneDrive.app (macOS), mobile apps
Files On-Demand	Show files in Explorer without downloading until opened
Known Folder Move (KFM)	Redirect Desktop / Documents / Pictures to OneDrive

Microsoft Portal Navigation

> 📍 SharePoint Admin Center → `Settings` → `OneDrive`

(OneDrive admin center has been consolidated into SharePoint admin center.)

Configure OneDrive Settings

Setting	Where
Default storage size	Settings → OneDrive → Storage
Retention after user deletion	30 → 3650 days (default 30)
Sync settings	Settings → Sync
Allow sync only on PCs joined to specific domains	Settings → Sync → Allow only specific Entra IDs
Block sync of specific file types	Excluded file extensions
External sharing for OneDrive	Policies → Sharing

Known Folder Move (KFM)

KFM redirects Windows user folders to OneDrive. Benefits: laptop loss doesn't lose data; new device gets old files. Configure via Intune:

1. Intune → Devices → Configuration → + Create → Settings Catalog.
2. Search "OneDrive" → "Silently move Windows known folders to OneDrive".
3. Enable. Specify tenant ID.
4. Show notification: Yes (let user know).
5. Assign to all Windows devices.

Offboarding — Handle Departed User's OneDrive

1. When user is deleted in Entra, OneDrive enters retention period (default 30 days).
2. Within retention window: re-assign OneDrive to manager.
3. Re-assign:
    - Admin Center → Users → Deleted user → OneDrive tab → "Access files".
    - OR PowerShell: `Set-SPOUser -Site "$oneDriveUrl" -LoginName "manager@contoso.com" -IsSiteCollectionAdmin $true`
4. Manager downloads / migrates files.
5. After retention: OneDrive permanently deleted.

PowerShell

```
# Get all OneDrive sites
Get-SPOSite -IncludePersonalSite $true -Limit All `
    -Filter "Url -like '*-my.sharepoint.com/personal*'" |
    Select-Object Url, Owner, StorageUsageCurrent, StorageQuota

# Set tenant-wide OneDrive default quota
Set-SPOTenant -OneDriveStorageQuota 5120000 # in MB; 5TB here

# Set retention after user deletion (days)
Set-SPOTenant -OrphanedPersonalSitesRetentionPeriod 365

# Pre-provision OneDrive for new users (no waiting for first login)
Request-SPOPersonalSite -UserEmails @("user1@contoso.com","user2@contoso.com")

# Grant admin access to a former user's OneDrive
Set-SPOUser -Site "https://contoso-my.sharepoint.com/personal/exuser_contoso_com" `
    -LoginName "manager@contoso.com" -IsSiteCollectionAdmin $true

# Sync excluded file types
Set-SPOTenantSyncClientRestriction -ExcludedFileExtensions "pst;mp4;mov;exe"
```

Sync Client Configuration

Policy	Use
Files On-Demand	Default On — saves disk space
Block downloading files marked sensitive	Defender for Cloud Apps integration
Block sync of personal accounts	Prevents data leak to personal OneDrive
Sync admin: list of allowed Entra IDs	Devices must be enrolled in specific tenant

Real-World Scenarios

Scenario: Offboarding

John leaves Contoso. (1) HR signals — IT blocks sign-in. (2) Mailbox converted to Shared. (3) John's OneDrive enters 30-day retention. (4) Manager granted Site Collection Admin to John's OneDrive. (5) Manager moves needed files to Sales team site. (6) After 30 days, John's OneDrive auto-deletes.

Scenario: Ransomware on a laptop

User reports files appearing as "*.locked." OneDrive Files Restore: User → OneDrive Web → ⚙ → Restore your OneDrive → Pick yesterday (before encryption). All files revert to pre-ransomware state. Saves the day.

Best Practices

- Pre-provision OneDrive for all users on day 1.
- Enable KFM via Intune to auto-redirect Desktop/Documents/Pictures.
- Set retention after user deletion to 90-180 days.
- Limit sync to corporate devices only.
- Block sync of personal accounts.
- Educate users on OneDrive Files Restore (ransomware self-recovery).

Common Errors

Issue	Resolution
"OneDrive setup couldn't sign in"	Modern auth issue; clear creds; verify license
Sync stuck "Processing changes"	Reset OneDrive (Win+R → `%localappdata%\Microsoft\OneDrive\onedrive.exe /reset`)
"File path too long"	Windows path limit; rename folders or enable long paths via Group Policy / registry
Files not syncing	Check file size (250 GB limit), file type restrictions, file name (invalid chars)
"OneDrive is full"	Check quota; clean files; request quota increase

Summary

Section 6.5 Summary

- Each user gets 1 TB OneDrive (5 TB expandable).
- Auto-provisioned on first OneDrive access; pre-provision via PowerShell.
- Configure retention after user deletion (30-3650 days).
- Use KFM to redirect Windows folders.
- Files Restore for ransomware recovery.

6.6 SharePoint vs OneDrive — Comparison

Aspect	SharePoint Online	OneDrive for Business
Purpose	Team / org-wide content	Individual user content
Default storage	1 TB tenant pool + 10 GB per license	1 TB per user
Permissions model	Site/library/item (groups)	Owner + people user shares with
Sharing	Configured per site + tenant	Configured tenant-wide
Underlying tech	SharePoint Online	SharePoint Online (personal site collection)
Best for	Team documents, intranet, business apps	Personal work files, drafts, replicates Documents folder
Recycle bin	93 days first + 30 second stage	Same
Version history	500 major versions default	500 major versions default
Sync to desktop	Yes (via OneDrive client)	Yes
External sharing	Yes (tenant + site level)	Yes (tenant + user level)
App ecosystem	Rich (SPFx, Power Platform, lists)	Personal files only

Decision Guide

Scenario	Use
Department of 20 sharing weekly reports	SharePoint (Team site)
One person drafting a document before sharing	OneDrive
Company-wide policy documents	SharePoint (Communication site)
Personal scratch / drafts	OneDrive
Project with cross-functional team	SharePoint (Team site or Teams)
Replace Windows Documents folder	OneDrive (with KFM)

Summary

Section 6.6 Summary

- SharePoint = team/org content; OneDrive = individual content.
- Both underlying SPO infrastructure.
- Use SharePoint for collaboration; OneDrive for personal work.

6.7 Sync Client & Files On-Demand

OneDrive Sync Client

The OneDrive client (oneDrive.exe on Windows, OneDrive.app on macOS) syncs files between cloud and device. Same client handles personal OneDrive, OneDrive for Business, AND SharePoint document libraries.

Sync Library to Local PC

1. Browse to SharePoint library → Sync button (top of library).
2. OneDrive client launches; downloads files locally.
3. Library appears under "Contoso" in File Explorer with cloud icons.
4. Sync is bi-directional: edits offline → sync when online.

Files On-Demand

Shows all OneDrive/SharePoint files in Explorer but downloads only when opened:

- Cloud icon = online-only (no local space used)
- Green check = fully downloaded
- Green check filled = always available offline

Configure Always Available Offline

1. Right-click file/folder → Always keep on this device.
2. File downloads; available even without internet.

Group Policy / Intune Sync Controls

Setting	Effect
Use OneDrive Files On-Demand	Enable; saves disk
Silently sign in users with their Windows credentials	SSO; no manual sign-in
Silently move Windows known folders	KFM
Prevent users from syncing personal OneDrive	Block consumer OneDrive on corporate devices
Block syncing of specific file extensions	e.g., .pst, .exe
Coauthor and share in Office desktop apps	On

Common Sync Issues

Issue	Resolution
"Couldn't sign in"	Restart client; check Entra licensing; clear creds
Files won't sync	Check file name (no <>:"|?* characters); file size (250 GB max); path length
Sync stuck "Processing changes"	Reset: `%localappdata%\Microsoft\OneDrive\onedrive.exe /reset`
"Error syncing X items"	Click red error icon → see specific items; usually invalid filename
Computer slow	Pause sync during heavy work; or use Files On-Demand

Summary

Section 6.7 Summary

- Single OneDrive client syncs personal + business + SPO libraries.
- Files On-Demand saves disk space.
- KFM redirects Desktop/Documents/Pictures.
- Reset OneDrive: `onedrive.exe /reset`.

6.8 Storage Management & Data Governance

Storage Management

View Storage Usage

1. SPO Admin Center → Active sites → sort by storage.
2. Identify top consumers.
3. OneDrive: Active sites filter "OneDrive site".

Set Storage Quotas

1. Per site: Admin Center → Active sites → site → Storage limit.
2. Tenant-wide OneDrive default: Settings → OneDrive → Storage.
3. Receive notifications when X% reached: configurable.

Version History

Each document has version history (default 500 versions):

- Recover previous versions of overwritten files.
- Per-library setting; cannot disable entirely.
- Old versions count toward storage.

Configure Version Limit

1. Library → ⚙ → Library settings → Versioning settings.
2. Major versions limit: 50-500.
3. Or use PowerShell: `Set-SPOSite -EnableAutoExpirationVersionTrim $true` (automatic version cleanup feature).

Site Lifecycle & Cleanup

Lifecycle Step	Configurable Via
Auto-expire idle sites	M365 Group expiration policy (Entra)
Manual archive	Microsoft Archive (paid feature)
Delete unused sites	PowerShell + reporting
Read-only / lock	Site Lock state

Microsoft 365 Archive (Premium)

Microsoft 365 Archive lets you "cold storage" inactive SPO sites at lower cost. Re-activation is fee-based but quick:

- Cold storage: ~$0.05 / GB / month (vs $0.20 / GB / month standard).
- Re-activation: minutes to hours.
- Configure via SPO Admin Center → Active sites → site → ⋯ → Archive.

Data Governance via Sensitivity Labels

Sensitivity labels can be applied to SPO sites:

- "Confidential": Block external sharing, require managed device, watermark.
- "Public": Permit Anyone link.
- Applied at site creation; can be changed by admin.
- Underlies Microsoft Information Protection.

Retention Policies

1. Purview Portal → Data lifecycle management → Retention policies.
2. + New policy → name.
3. Locations: SharePoint sites, OneDrive accounts.
4. Retain for X years, then delete (or keep forever).
5. Apply broadly or to specific sites.

eDiscovery for SPO/OneDrive

Search across all SPO sites and OneDrive accounts for legal matters; export content; hold custodian content.

Real-World Scenarios

Scenario: Quota management at scale

5,000 users; tenant storage 60% full. Plan: (1) Identify top 50 sites consuming > 200 GB each. (2) Apply version trimming (cuts ~30% from old sites). (3) Move 200 sites with no activity in 2 years to Microsoft 365 Archive. (4) Establish governance: site owners renew or risk archive. Result: storage usage drops to 38%; cost predictable.

Summary

Section 6.8 Summary

- Tenant storage = 1 TB pooled + 10 GB per license.
- Set per-site quotas to prevent runaway growth.
- Use version trimming and M365 Archive to reduce cost.
- Apply retention and sensitivity labels for governance.

Section 6 — Wrap-Up

Section 6 Synthesis

- **SharePoint Online**: team + communication sites; hub for navigation.
- **OneDrive**: per-user 1 TB; KFM redirects Windows folders.
- **Permissions**: SharePoint groups (Owners/Members/Visitors).
- **External sharing**: configure tenant, restrict per-site.
- **Sync**: single OneDrive client; Files On-Demand saves disk.
- **Storage**: monitor, quota, version trim, Microsoft 365 Archive.
- **Governance**: sensitivity labels, retention policies, eDiscovery, DLP.

Section 6 Mini-Quiz

Q1. What's the default OneDrive storage per user on E3?

A: 1 TB (expandable to 5 TB)

Q2. How long do deleted users' OneDrive sites retain by default?

A: 30 days (configurable up to 3650)

Q3. What's the difference between Team site and Communication site?

A: Team site = collaboration (group-connected); Communication site = broadcast/intranet (not group-connected)

Q4. What does Files On-Demand do?

A: Shows all files in Explorer but downloads only when opened; saves disk space

Q5. What's KFM?

A: Known Folder Move — redirects Windows Desktop, Documents, Pictures to OneDrive

Q6. What command resets the OneDrive sync client?

A: %localappdata%\Microsoft\OneDrive\onedrive.exe /reset

Q7. What's the most restrictive external sharing setting that still allows sharing?

A: Existing guests only (must already be in directory)

Q8. Default Anyone link expiration recommendation?

A: 30 days

Q9. How do you grant a manager access to a deleted user's OneDrive?

A: Within retention period, Admin Center → Deleted users → user → Access files; or via PowerShell Set-SPOUser with IsSiteCollectionAdmin

Q10. What feature lets users self-recover from ransomware on OneDrive?

A: OneDrive Files Restore — revert OneDrive to any point in last 30 days

Section 7
07
Security & Threat Protection
Microsoft Defender for Office 365, Defender XDR, attack simulation, Secure Score, Zero Trust. The defense-in-depth stack that protects users, mail, endpoints, and cloud apps from real-world attacks.
Exam Weight: ~15%

7.1 Microsoft Defender Family Overview

Introduction

"Microsoft Defender" is no longer a single product — it's a family of integrated security tools collectively branded Microsoft Defender XDR (Extended Detection and Response). Each Defender protects a different surface; together they share signals and provide unified investigation.

The Defender Family

Product	Protects	Key Features
Microsoft Defender for Office 365 (MDO)	Email, Teams, SharePoint, OneDrive	Safe Links, Safe Attachments, anti-phishing, attack simulation
Microsoft Defender for Endpoint (MDE)	Windows, macOS, Linux, iOS, Android endpoints	EDR, AV, vulnerability management, threat hunting
Microsoft Defender for Identity (MDI)	On-prem AD identity	Detect identity attacks on AD, lateral movement, golden ticket
Microsoft Defender for Cloud Apps (MDA)	SaaS apps (CASB)	Discover shadow IT, control SaaS use, DLP for cloud apps
Microsoft Defender for Cloud	Azure / AWS / GCP infrastructure	CSPM and CWPP for multi-cloud workloads
Microsoft Defender XDR (portal)	Unified hub	Aggregated alerts, incidents, hunting across all Defenders
Microsoft Sentinel	SIEM/SOAR (separate Azure service)	Cross-source correlation, automation

Unified Portal

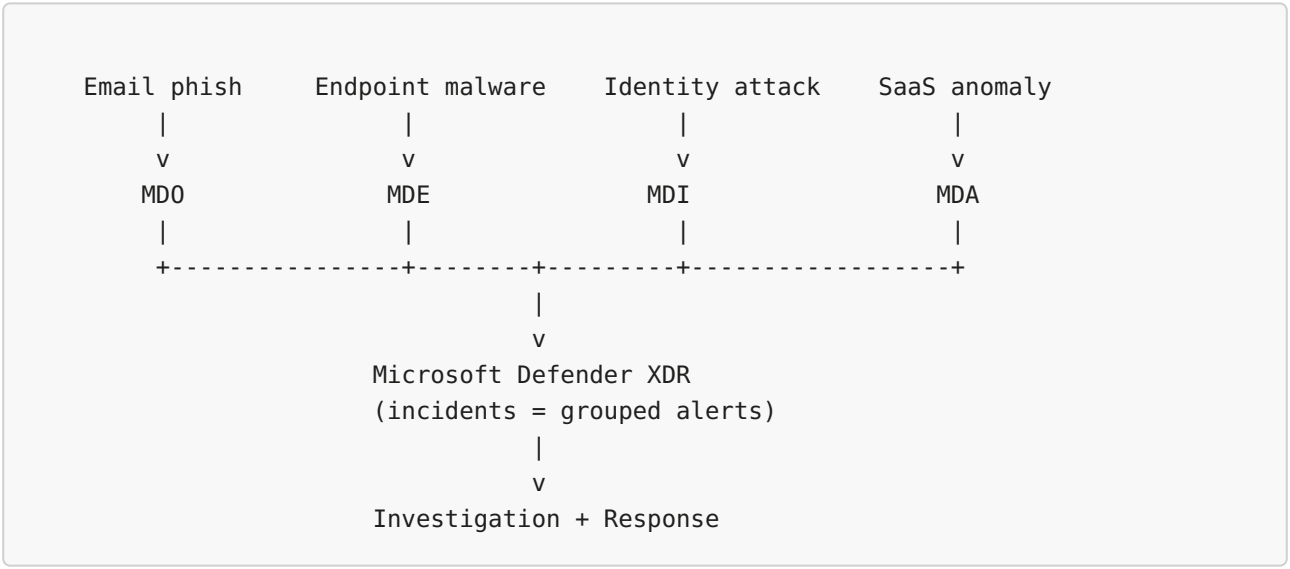
> 📍 Microsoft Defender Portal → `security.microsoft.com`

Consolidates alerts, incidents, hunting, attack simulation, Threat Explorer, Secure Score, and many sub-products.

License Mapping

License	Defender Tier
Microsoft 365 E3	Defender for Office 365 Plan 1 + Defender for Endpoint Plan 1
Microsoft 365 E5	Defender for Office 365 Plan 2 + Defender for Endpoint Plan 2 + Defender for Identity + Defender for Cloud Apps
Microsoft 365 E5 Security (add-on)	E5 security stack on top of E3
Microsoft 365 Business Premium	Defender for Office 365 P1 + Defender for Business (SMB)

How They Share Signal



Real-World Scenarios

Scenario: Cross-product attack chain

Attacker sends phishing email (MDO detects), user clicks link, malware drops on endpoint (MDE detects), attacker harvests creds and moves laterally to a domain controller (MDI detects), attempts to exfiltrate via SharePoint download burst (MDA detects). Without XDR: four separate alerts in four products. With XDR: one incident showing the full kill chain. Analyst handles in minutes instead of hours.

Summary

Section 7.1 Summary

- Defender = family of products: MDO, MDE, MDI, MDA, Defender for Cloud.
- XDR = unified portal correlating signals.
- Portal: security.microsoft.com.
- E5 includes the full stack; E3 includes Plan 1 of MDO + MDE.

7.2 Safe Links

Introduction

Safe Links wraps URLs in incoming email (and increasingly Teams, Word, Excel, PowerPoint) with Microsoft's time-of-click protection. When a user clicks a link, Microsoft checks the destination against threat intelligence in real time — even if the link was clean at delivery but later weaponized.

Why It Matters

Attackers commonly use "delayed weaponization": email sent with a benign URL that passes filters, then content of the URL changes to malicious AFTER delivery. Safe Links re-checks at click time, catching these.

License

- Defender for Office 365 Plan 1 or Plan 2 required.
- M365 E3, Business Premium → Plan 1.
- M365 E5 → Plan 2 with additional reporting.

How Safe Links Work

```
Email arrives with URL: https://example.com/page
      |
      v
Safe Links rewrites: https://safelinks.protection.outlook.com/?url=https%3A%2F%2Fexample.com%2F
      |
      v
User clicks link
      |
      v
Microsoft Safe Links service evaluates URL at time of click:
  - Check against URL reputation database
  - Detonate URL in sandbox if needed (P2)
  - Apply organizational allow/block lists
      |
      v
Decision: Allow, Block, Warn
      |
      v
User sees real destination OR warning page OR block
```

Microsoft Portal Navigation

📍 Defender Portal → `Email & collaboration` → `Policies & rules` → `Threat policies` → `Safe Links`

Step-by-Step: Configure Safe Links

1. Defender → Threat policies → Safe Links → + Create.

2. Name: "Safe Links — All Users".
3. Users and domains: include all users / specific groups / specific domains.
4. URL & click protection settings:
    - On: Safe Links checks list of known malicious links when users click links in email — Yes
    - Apply Safe Links to email messages sent within the organization — Yes
    - Apply real-time URL scanning for suspicious links — Yes
    - Wait for URL scanning to complete before delivering the message — Yes (recommended)
    - Do not rewrite URLs, do checks via Safe Links API only — No
5. Click protection for users:
    - Track user clicks — Yes (for reporting)
    - Let users click through to the original URL — Recommended: Off (block at warning)
    - Display the organization branding on notification and warning pages
6. Notification: customize warning text (your IT contact, what to do).
7. Assignments → All users.
8. Submit.

Safe Links for Teams

Safe Links also protects URLs in Teams chats. Same policy, additional toggle:

- "On: Safe Links checks list of known malicious links when users click links in Microsoft Teams" — Yes.

Safe Links for Office Apps

Word, Excel, PowerPoint, OneNote, and Outlook clients (Win, Mac, mobile) check URLs at click time:

- "On: Safe Links checks list of known malicious links when users click links in Office apps" — Yes.

Allow / Block Lists

Override Safe Links for specific URLs:

1. Defender → Policies → Tenant Allow/Block Lists → URLs.
2. Add URL with action Allow or Block.
3. Expiration date (or "Never expires").

PowerShell

```
# Get Safe Links policies
Get-SafeLinksPolicy | Format-Table Name, Enabled, EnableSafeLinksForEmail,
EnableSafeLinksForTeams

# Create policy
New-SafeLinksPolicy -Name "AllUsers-SafeLinks" `
    -EnableSafeLinksForEmail $true `
    -EnableSafeLinksForTeams $true `
    -EnableSafeLinksForOffice $true `
    -ScanUrls $true `
    -DeliverMessageAfterScan $true `
    -EnableForInternalSenders $true `
    -TrackClicks $true `
    -AllowClickThrough $false

# Bind to rule (this assigns to users)
New-SafeLinksRule -Name "AllUsers-SafeLinks-Rule" `
    -SafeLinksPolicy "AllUsers-SafeLinks" `
    -SentToMemberOf "all-employees@contoso.com" `
    -Priority 0

# Tenant Allow/Block list
New-TenantAllowBlockListItems -ListType Url -Block `
    -Entries "phishingsite.com" -NoExpiration
```

Reporting

Click-through reports show who clicked malicious URLs (so they can be retrained):

- Defender → Reports → Email & collaboration → URL protection report.
- Threat Explorer → URL clicks tab.

Real-World Scenarios

Scenario: Delayed weaponization caught

Attacker sends invoice phishing email with link to a "newly registered" benign-looking domain. Email passes filtering. Two hours later, attacker switches the page to a credential harvester. User clicks. Safe Links re-checks: now flagged as phishing. User sees warning page, doesn't enter credentials. MDO opens incident; admin investigates and blocks domain across tenant.

Best Practices

- Enable Safe Links for Email, Teams, AND Office apps.

- Apply to internal senders too (defense against insider compromise).
- Don't allow click-through unless absolutely necessary.
- Wait for scan to complete before delivering (slight delivery delay, much safer).
- Use Strict preset for executives.
- Train users to recognize Safe Links rewriting (they'll see "safelinks.protection.outlook.com" in links — normal).

Common Errors

Issue	Resolution
User reports "site blocked" for legitimate site	Submit false-positive to Microsoft; add to tenant allow list if justified
Warning pages without org branding	Customize in Safe Links policy
Safe Links not applied to a tenant	Verify license; verify policy targets user; preset policy might override custom

Summary

Section 7.2 Summary

- Safe Links = time-of-click URL protection.
- Covers email, Teams, Office apps.
- Requires Defender O365 P1+.
- Tenant Allow/Block lists override default behaviour.
- Don't allow click-through — block at warning.

7.3 Safe Attachments

Introduction

Safe Attachments detonates email attachments in a Microsoft cloud sandbox before delivery. If the attachment displays malicious behaviour during detonation, the message is held or stripped of the attachment.

Why It Matters

Signature-based AV catches known malware. Safe Attachments catches NEW malware via behavioural analysis: does the attachment try to download more files, encrypt the disk, contact known C2 servers, modify system files?

License

- Defender for Office 365 P1 or P2.
- P2 adds reporting and threat intelligence integration.

How Safe Attachments Work

```
Email arrives with attachment
      |
      v
EOP scans signature-based — clean? continue
      |
      v
Safe Attachments: detonate in cloud sandbox
      |
      v
Behavioural analysis (file operations, network, registry, persistence)
      |
      v
Malicious behaviour? → block / replace / monitor
Benign? → deliver
```

Safe Attachments Modes

Mode	Behaviour
Off	No detonation
Monitor	Detonate, log results, but always deliver
Block	Block message if malicious; quarantine
Replace	Strip attachment; deliver with notification (legacy)
Dynamic Delivery	Deliver body immediately + attachment after scan completes

Recommended
Use **Block** mode. Dynamic Delivery is fast but lets the email arrive even if the attachment is later found malicious (user might be confused). Block holds delivery until scan completes.

Step-by-Step: Configure Safe Attachments

1. Defender → Threat policies → Safe Attachments → + Create.

2. Name: "Safe Attachments — All Users".
3. Users and domains: All users.
4. Settings:
    - Safe Attachments unknown malware response: Block
    - Quarantine policy: AdminOnlyAccessPolicy
    - Redirect attachment on detection: Optional admin mailbox for forensics
    - Apply the above selection if malware scanning for attachments times out or error occurs: Enable
5. Submit.

Safe Attachments for SharePoint, OneDrive, Teams

Beyond email, Safe Attachments can scan files uploaded to SPO/OneDrive/Teams:

1. Defender → Threat policies → Safe Attachments → Global settings.
2. "Turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams": On.
3. "Turn on Safe Documents for Office clients": On (P2 only — protects files opened in Word/Excel).
4. Save.

If malware detected: the file is locked (still visible but can't be opened/downloaded) until admin reviews.

PowerShell

```
# Get Safe Attachments policies
Get-SafeAttachmentPolicy | Format-Table Name, Enable, Action

# Create policy
New-SafeAttachmentPolicy -Name "AllUsers-SafeAttach" `
    -Enable $true -Action Block `
    -QuarantineTag "AdminOnlyAccessPolicy"

# Bind to recipients
New-SafeAttachmentRule -Name "AllUsers-SafeAttach-Rule" `
    -SafeAttachmentPolicy "AllUsers-SafeAttach" `
    -SentTo "all-employees@contoso.com" `
    -Priority 0

# Enable Safe Attachments for SPO/OneDrive/Teams
Set-AtpPolicyForO365 -EnableATPForSPOTeamsODB $true `
    -EnableSafeDocs $true `
    -AllowSafeDocsOpen $false
```

Real-World Scenarios

Scenario: New ransomware

Attacker emails 100 employees with novel ransomware in an Excel file. Signature-based AV doesn't detect (new variant). Safe Attachments detonates: file tries to download a payload + modify boot sector + contact suspicious IP. Verdict: malicious. All 100 messages quarantined. ZAP retroactively removes any that bypassed. Attack neutralized.

Best Practices

- Use Block action.
- Enable Safe Attachments for SPO/OneDrive/Teams.
- Enable Safe Documents (P2) for protection in Office desktop apps.
- Apply Preset Strict for executives.
- Monitor quarantine + ZAP reports weekly.

Summary

Section 7.3 Summary

- Safe Attachments = sandbox detonation before delivery.
- Modes: Off, Monitor, Block, Replace, Dynamic Delivery.
- Recommended: Block.
- Extends to SPO/OneDrive/Teams uploads.
- Safe Documents protects Office desktop file opens (P2).

7.4 Anti-Phishing Policies

Introduction

Anti-phishing policies in Microsoft Defender detect phishing attempts via ML, sender reputation, impersonation detection, mailbox intelligence, and spoof intelligence. They complement EOP's anti-spam.

Key Features

Feature	What It Does
Impersonation protection — Users	Detect "John Smith" lookalike impersonating actual John Smith (CEO)
Impersonation protection — Domains	Detect contoso.com vs contos0.com (typosquat)
Mailbox intelligence	Build per-user normal sender pattern; flag anomalies
Spoof intelligence	Detect From-address spoofing
First contact safety tip	Shows "first time you received from this sender" banner
Phishing threshold	1 (least aggressive) → 4 (most aggressive)

Step-by-Step: Configure Anti-Phishing

1. Defender → Threat policies → Anti-phishing → + Create.
2. Name: "Anti-Phish — Executives".
3. Users to apply: include executives security group.
4. Phishing threshold: 3 (more aggressive than default).
5. Impersonation:
    - Add protected users: list of executives (CEO, CFO, etc., up to 350)
    - Add protected domains: contoso.com, contoso-eu.com
    - Add trusted senders: legitimate vendors you commonly receive from
    - Add trusted domains: vendor domains
    - Enable mailbox intelligence: Yes
    - Enable intelligence based impersonation: Yes
6. Spoof:
    - Enable spoof intelligence: Yes
    - Show first contact safety tip: Yes
    - Show user impersonation safety tip: Yes
    - Show domain impersonation safety tip: Yes
7. Actions:
    - If message is detected as a user impersonation: Quarantine the message
    - If message is detected as a domain impersonation: Quarantine the message
    - If message is detected as spoof: Move message to Junk Email folder (or quarantine)
8. Submit.

Tenant Allow/Block List for Spoofing

Sometimes legitimate senders fail SPF/DKIM/DMARC (e.g., a partner mass-mailer). Add to allow list:

1. Defender → Policies → Tenant Allow/Block Lists → Spoofed senders tab.
2. + Add allow → choose Sender (with spoof type Internal or External, infrastructure ID).
3. Or remove a false-positive block from this list.

PowerShell

```
# Get anti-phishing policies
Get-AntiPhishPolicy | Format-Table Name, Enabled, PhishThresholdLevel

# Configure impersonation users on the default policy
Set-AntiPhishPolicy -Identity "Office365 AntiPhish Default" `
    -EnableTargetedUserProtection $true `
    -TargetedUsersToProtect @{Add="CEO Name;ceo@contoso.com","CFO
Name;cfo@contoso.com"} `
    -EnableTargetedDomainsProtection $true `
    -TargetedDomainsToProtect @{Add="contoso.com","contoso-eu.com"} `
    -TargetedUserProtectionAction Quarantine `
    -TargetedDomainProtectionAction Quarantine `
    -EnableSpoofIntelligence $true `
    -EnableFirstContactSafetyTips $true `
    -PhishThresholdLevel 3
```

Real-World Scenarios

Scenario: CEO impersonation

Attacker creates "ceo.name@contos0.com" (typo, the o is a zero) and emails CFO requesting urgent wire transfer. Without anti-phishing: looks plausible at glance, CFO might be fooled. With impersonation protection: contoso.com is a protected domain; lookalike contos0.com triggers domain impersonation, message quarantined, CFO never sees it. Multi-million-dollar fraud prevented.

Best Practices

- Add up to 350 protected users (executives, finance, IT admins).
- Add all your domains as protected.
- Enable mailbox intelligence — it learns each user's normal correspondents.
- Phishing threshold 2 for general; 3-4 for high-risk groups.
- Action: Quarantine, not Junk Folder, for impersonation.
- Apply Preset Strict to VIPs.

- Submit false positives to Microsoft via Submissions to improve.

Common Errors

Issue	Resolution
Legitimate vendor's email blocked as phishing	Add to trusted senders; submit as false positive
Too many false positives	Lower threshold from 4 to 3 or 2
Impersonation not catching obvious lookalikes	Verify the user/domain is added to protected list

Summary

Section 7.4 Summary

- Anti-phishing complements anti-spam.
- Impersonation protection: protected users + domains.
- Mailbox intelligence learns normal sender patterns.
- Spoof intelligence flags failed SPF/DKIM/DMARC.
- Action: quarantine for high-confidence; junk for spoof.

7.5 Threat Explorer and Real-Time Detections

Introduction

Threat Explorer (P2) and Real-Time Detections (P1) are the investigation tools for email threats. They let analysts search across all email events: by sender, recipient, subject, URL, attachment, malware type, time.

License

- Real-Time Detections: P1 (limited features).
- Threat Explorer: P2 (full features).

Microsoft Portal Navigation

> 📍 Defender Portal → `Email & collaboration` → `Explorer`

Views

View	Shows
All email	Every message; filter by anything
Malware	Messages with malicious attachments
Phish	Phishing detections
Submissions	User and admin reports
Campaigns	Grouped phishing attempts targeting org
Top targeted users	Most-attacked users
URL clicks	Who clicked Safe Links URLs

Typical Investigation Flow

1. Alert fires: "Phishing email detected."
2. Open Threat Explorer → filter by alert ID.
3. See: sender, recipient, subject, attachment hashes, URLs, delivered/blocked.
4. Search broader: "any other emails from this sender in last 30 days?"
5. "Any user who clicked the URL?"
6. Actions:
    - Soft delete from inbox
    - Move to Junk
    - Submit to Microsoft
    - Block sender via tenant block list
7. Document findings; close incident.

Threat Explorer Actions

Action	Use
Move to inbox	Release false positive
Move to Junk	Reduce visibility
Move to Deleted Items	Remove from inbox
Soft delete	Permanent delete (recoverable from recoverable items)
Hard delete	Unrecoverable removal
Submit to Microsoft	Improve tenant detection

Campaigns View

Microsoft uses ML to cluster similar phishing emails into campaigns. View shows: scope (how many users targeted), origin (sender IPs/countries), payload (attachments, URLs), click-through rates.

Real-World Scenarios

Scenario: Threat hunting

Threat intel reports a new phishing kit using "support@microsoft365support.com" sender. SOC analyst opens Threat Explorer → search sender contains "microsoft365support". Finds 47 messages in last 7 days; 12 delivered to inboxes; 3 users clicked links. Actions: soft delete all 47; alert the 3 click-through users; force password reset; submit to Microsoft. Total time: 15 minutes.

Summary

Section 7.5 Summary

- Threat Explorer (P2) / Real-Time Detections (P1) = email investigation.
- Search by any property; take action across many messages.
- Campaigns view clusters related attacks.
- Critical SOC workflow.

7.6 Microsoft Secure Score

Introduction

Microsoft Secure Score is a quantitative measurement of your M365 security posture. Microsoft analyzes your tenant configuration, compares against recommended baseline, and gives a score out of a maximum (varies by license). Each recommended action carries points.

Why It Matters

Cyber insurance, audits, and board reports all need security posture metrics. Secure Score provides a measurable, comparable number across time and against industry peers.

Microsoft Portal Navigation

> 📍 Defender Portal → `Microsoft Secure Score`

Score Components

Category	Examples
Identity	MFA enabled, fewer than 5 Global Admins, legacy auth blocked, password protection on, password expiration disabled (with MFA)
Device	Defender for Endpoint deployed, compliance policies active, BitLocker on, ASR rules enabled
Apps	Defender for Cloud Apps configured, OAuth app review
Data	Sensitivity labels in use, DLP policies, retention

Each Recommendation Shows

- Description of the control
- Points achieved / possible
- User impact: low / medium / high
- Implementation cost
- Implementation guidance + direct link
- Status: To address / Planned / Risk accepted / Resolved

Status Workflow

Status	Meaning
To address	Default — not yet evaluated
Planned	You're working on it
Risk accepted	You've decided not to implement (with documented justification)
Resolved through third-party	Equivalent control via another product
Resolved through alternate mitigation	Compensating control

Step-by-Step: Improve Secure Score

1. Open Secure Score → Recommended actions tab.
2. Sort by Points achievable.
3. Pick top 3 unimplemented with low user impact.
4. Read implementation guidance; apply.
5. Wait 24-48 hours for re-evaluation.
6. Check score increase.
7. Repeat monthly.

Quick Wins (Common High-Impact Actions)

Action	Points	Effort
Require MFA for admins	10	Low
Block legacy auth	10	Medium
Enable Safe Links	5	Low
Enable Safe Attachments	5	Low
Reduce Global Admins to <5	10	Low
Enable SSPR	5	Medium
Apply Defender preset policies (Strict/Standard)	15	Low

Compare to Peers / Industry

Secure Score → History tab shows your score over time and industry-average comparison (by tenant size + sector).

Real-World Scenarios

Scenario: Quarterly board report

CISO presents security posture to board. Last quarter: 412 points. This quarter: 491 points (+79). Top improvements: MFA enforcement, legacy auth block, Safe Attachments. Compared to industry peers: at 75th percentile. Board approved budget for additional automation.

Best Practices

- Review monthly; aim for incremental gains.
- Don't blindly chase points — evaluate user impact.
- Mark "Risk accepted" with documented justification (audit trail).
- Use trend over time as KPI.
- Tie to security improvement program; assign owners per recommendation.

Summary

Section 7.6 Summary

- Secure Score = quantitative security posture measure.
- Recommendations across Identity, Device, Apps, Data.
- Mark status: Planned, Resolved, Risk Accepted.
- Compare to peers and track trend.

7.7 Security Defaults vs Conditional Access

Security Defaults

Security Defaults is a free tenant-wide preset that enforces:

- All users must register for MFA
- Admins must always use MFA
- Legacy authentication blocked
- Privileged actions like Azure portal require MFA

Pros and Cons

Pros	Cons
Free (no P1+ needed)	All-or-nothing — no granularity
One-toggle setup	Can't exclude break-glass accounts
Microsoft-managed (auto-updated)	Conflicts with CA — can only use one
Sensible defaults	Doesn't include risk-based or device-based controls

Conditional Access

CA provides granular if/then policies. Requires Entra ID P1+ (or M365 Business Premium, E3, E5, EMS).

Decision Matrix

Org Size / Complexity	Recommendation
Very small (1-50 users), no P1	Security Defaults
Small (< 100), with P1	Conditional Access (basic policies)
Medium (100-1000)	Conditional Access
Large enterprise	Conditional Access + Identity Protection (P2)

Summary

Section 7.7 Summary

- Security Defaults: free, simple, all-or-nothing.
- Conditional Access: P1+, granular, supports report-only.
- Can't run both at the same time.
- Modern orgs choose CA.

7.8 Attack Simulation Training

Introduction

Attack Simulation Training (in Defender for Office 365 P2) lets you safely send realistic phishing emails to your own users — and assign training to those who fall for them. It's user-awareness automation.

Why It Matters

Humans are the weakest link. Annual generic training doesn't work. Targeted, contextual training right after a user fails a simulation is far more effective.

Simulation Types

Type	What It Tests
Credential harvest	User clicks link → fake login page → enters creds
Malware attachment	User opens "attached invoice"
Link in attachment	User opens attached document, clicks link inside
Link to malware	User clicks link that "downloads" file
Drive-by URL	User clicks link to mock landing page
OAuth consent grant	User authorizes a malicious-looking app
How-to guide	Educational only

Microsoft Portal Navigation

> 📍 Defender Portal → `Email & collaboration` → `Attack simulation training`

Step-by-Step: Launch a Simulation

1. Defender → Attack simulation training → + Launch a simulation.
2. Select technique: Credential harvest.
3. Name + description: "Q1 2026 Phishing Test".
4. Payload: choose from Microsoft library (real-world templates) or custom.
5. Target users: all employees / specific groups (e.g., Finance, HR).

6. Assign training: automatically train users who fail (Microsoft training catalog).
7. Schedule: send over 2-3 days (mimics real attack distribution).
8. Submit.

Reporting

After simulation completes:

- Compromise rate: % who clicked link / entered creds
- Reported rate: % who reported the phish via Report Message
- Per-department, per-user results
- Repeated offenders → escalate

Training Automation

Configure Training campaigns to assign training:

- To users who clicked simulation links
- To users who clicked real phishing in last 90 days
- To everyone (general awareness)

Real-World Scenarios

Scenario: Quarterly campaign

Each quarter, security team runs different simulation: Q1 invoice phish, Q2 Microsoft password reset phish, Q3 HR document phish, Q4 OAuth consent. Year-over-year: compromise rate drops from 22% → 14% → 8%. Reported rate rises from 5% → 18% → 41%. Significant culture shift.

Best Practices

- Run simulations quarterly, varying techniques.
- Don't shame individuals — train them.
- Tie training completion to compliance.
- Identify repeated offenders for 1:1 coaching.
- Use industry-specific payloads.
- Communicate simulations broadly only after collecting data (otherwise users tell each other).
- Avoid simulations during high-stress periods (e.g., quarter-end close).

Summary

Section 7.8 Summary

- Attack Simulation Training = safe internal phishing tests + auto-assigned training.
- Requires Defender O365 P2.
- Multiple techniques: credential harvest, malware, link to malware, OAuth.
- Track compromise + report rates over time.
- Train automatically; don't shame.

7.9 Zero Trust Architecture

Introduction

Zero Trust is the modern security model: never trust, always verify. No network is implicitly trusted; every access request is evaluated based on identity, device, location, app, data sensitivity, and risk — even from inside the corporate network.

Three Principles

Principle	Meaning
Verify explicitly	Authenticate and authorize every request on all available signals
Use least-privilege access	Limit user access via Just-In-Time and Just-Enough-Access
Assume breach	Minimize blast radius; segment access; encrypt end-to-end; use analytics

Six Pillars

Pillar	Microsoft Solution
Identity	Entra ID + MFA + PIM + Identity Protection
Endpoint	Intune + Defender for Endpoint + compliance
Application	Defender for Cloud Apps + CA app session controls
Data	Sensitivity labels + DLP + encryption + Purview
Infrastructure	Azure Defender for Cloud + JIT VM access
Network	Microsoft segments / VNet + private endpoints

Zero Trust in Practice — M365

```
User signs in
     |
     v
[Identity] Entra MFA + Conditional Access evaluates risk
     |
     v
[Endpoint] Compliant device required? Intune attests.
     |
     v
[Network] From trusted location? Or VPN-bypass risk?
     |
     v
[App] Which application? Sensitive?
     |
     v
[Data] Sensitivity label of data being accessed?
     |
     v
Decision: Allow / Allow with MFA / Block / Limit access
```

Step-by-Step: Zero Trust Maturity Self-Assessment

1. Microsoft Zero Trust Assessment: zerotrustadviser.microsoft.com (publicly available).
2. Answer questions on each pillar.
3. Receive scorecard: Traditional / Advanced / Optimal per pillar.
4. Get tailored guidance to advance.

Quick Wins Mapped to Zero Trust

Quick Win	Pillar
Enable MFA	Identity
Block legacy auth	Identity
Enroll devices in Intune	Endpoint
Require compliant device via CA	Endpoint + Identity
Deploy sensitivity labels	Data
Deploy DLP	Data
Discover SaaS apps via MDA	Application

Real-World Scenarios

Scenario: Acquired company Zero Trust integration

Contoso acquires Acme (300 users). Acme's prior security: VPN-based perimeter; flat network; on-prem AD. 6-month Zero Trust integration: (1) Sync Acme AD to Entra; deploy MFA. (2) Enroll all Acme devices in Intune. (3) Deploy Conditional Access requiring compliant device. (4) Migrate from VPN to direct internet access via Microsoft Entra Private Access. (5) Apply M365 DLP and labels. Post: any Acme user can work from anywhere securely.

Summary

Section 7.9 Summary

- Zero Trust = verify explicitly, least privilege, assume breach.
- Six pillars: Identity, Endpoint, App, Data, Infrastructure, Network.
- Microsoft stack covers all pillars.
- Conditional Access is the policy engine.

Section 7 — Wrap-Up

Section 7 Synthesis

- **Defender family**: MDO, MDE, MDI, MDA, Defender for Cloud, XDR.
- **Safe Links**: time-of-click URL protection.
- **Safe Attachments**: sandbox detonation.

- **Anti-phishing**: impersonation + mailbox intelligence + spoof.
- **Threat Explorer**: investigation tool (P2).
- **Secure Score**: posture measurement.
- **Security Defaults** for small orgs; **Conditional Access** for the rest.
- **Attack Simulation**: train via realistic phishing tests.
- **Zero Trust**: verify explicitly, least privilege, assume breach.

Section 7 Mini-Quiz

Q1. What does Safe Links protect against that EOP alone misses?

A: Delayed weaponization — URL benign at delivery but later malicious; Safe Links re-checks at click time

Q2. Which Safe Attachments mode is recommended?

A: Block — hold delivery until scan complete

Q3. How many users can you protect with impersonation protection?

A: Up to 350

Q4. What is Microsoft Secure Score?

A: Quantitative measurement of your tenant's security posture across Identity, Device, Apps, Data

Q5. Difference between Security Defaults and Conditional Access?

A: Security Defaults = free, all-or-nothing. Conditional Access = P1+, granular per user/app/condition.

Q6. Which Defender plan includes Threat Explorer?

A: Defender for Office 365 Plan 2 (P1 has Real-Time Detections instead)

Q7. What's ZAP?

A: Zero-hour Auto Purge — retroactively removes malicious mail after delivery

Q8. What does Defender for Identity protect?

A: On-premises Active Directory — detects identity attacks, lateral movement, golden ticket

Q9. The three Zero Trust principles?

A: Verify explicitly, Use least-privilege access, Assume breach

Q10. What does Attack Simulation Training NOT replace?

A: Real security controls — it's user awareness, not a substitute for technical defenses

Section 8
08
Compliance & Data Governance
Microsoft Purview unifies data governance, risk, and compliance. Master sensitivity labels, DLP, retention, eDiscovery, audit, and insider risk — the regulatory backbone of every modern enterprise.
Exam Weight: ~15%

8.1 Microsoft Purview Overview

Introduction

Microsoft Purview is the unified compliance, risk, and data governance platform across Microsoft 365 (and now multi-cloud). It includes 25+ solutions: Sensitivity Labels, DLP, Retention, eDiscovery, Audit, Insider Risk, Compliance Manager, Communication Compliance, and more.

Why This Topic Is Important

Regulations like GDPR, HIPAA, PCI-DSS, SOX, CCPA require organizations to identify sensitive data, control access, retain records appropriately, respond to legal holds, and demonstrate compliance. Purview is Microsoft's answer to these obligations for M365 data.

Key Solutions

Solution	Purpose
Compliance Manager	Score + improvement actions against frameworks (GDPR, ISO 27001, etc.)
Information Protection (Sensitivity Labels)	Classify and protect content (Confidential, Public)
Data Loss Prevention (DLP)	Prevent data leaks via email, files, endpoints, chats
Data Lifecycle Management	Retain or delete content automatically
Records Management	Legally binding retention with disposition review
eDiscovery	Search and export content for legal cases
Audit	Comprehensive audit logs of all admin and user actions
Insider Risk Management	Detect risky behaviour (data exfiltration, IP theft)
Communication Compliance	Monitor communications for policy violations (harassment, financial)
Information Barriers	Prevent communication between specific groups (Chinese walls)
Privileged Access Management	Approval workflow for high-impact admin tasks
Customer Lockbox	Customer approval before Microsoft engineers access data

Microsoft Portal Navigation

> 📍 Microsoft Purview Portal → `purview.microsoft.com` (newer)

> 📍 Microsoft Purview Compliance Portal → `compliance.microsoft.com` (older but still active)

License Mapping

License	Purview Capability
Microsoft 365 E3	Sensitivity Labels (basic), Retention (basic), DLP (basic), eDiscovery Standard, Audit Standard
Microsoft 365 E5	Full Purview: Advanced eDiscovery, Insider Risk, Communication Compliance, Records Management, Information Barriers, Audit Premium
Microsoft 365 E5 Compliance	Add-on bringing E5 compliance to E3 tenants

Roles for Purview

Role	Purpose
Compliance Administrator	Full compliance management
Compliance Data Administrator	Sensitive types, DLP, retention, labels
eDiscovery Manager	Create and run cases
eDiscovery Administrator	Above + manage all cases
Records Management	Records management config
Insider Risk Management	IRM policy + alerts
Reviewer	Review case content

Real-World Scenarios

Scenario: GDPR readiness

European subsidiary needs GDPR compliance. Plan: (1) Compliance Manager → import GDPR assessment template. (2) Score baseline 38%. (3) Implement: DLP policies for EU PII; sensitivity labels for personal data;

retention policies for customer data; audit log for breach reporting; data subject request workflow for "right to be forgotten." (4) Score climbs to 78% over 6 months. (5) Internal audit confirms readiness.

Summary

Section 8.1 Summary

- Purview = unified compliance & governance platform.
- 25+ solutions: Labels, DLP, Retention, eDiscovery, Audit, Insider Risk.
- Portal: purview.microsoft.com.
- E3 basic; E5 full.

8.2 Compliance Manager

Introduction

Compliance Manager helps you assess and improve compliance posture against regulatory frameworks. It provides a Compliance Score, recommended Improvement Actions, and assessment templates for standards like GDPR, NIST, HIPAA, ISO 27001, SOC 2, PCI-DSS, etc.

How It Works

Concept	Description
Assessment	Predefined or custom evaluation against a framework
Improvement actions	Steps to satisfy specific controls (some auto-detected, some manual)
Compliance score	Weighted total of completed actions
Microsoft-managed controls	Microsoft's responsibility (already done; gives base points)
Your controls	Customer responsibility (you implement)
Shared controls	Both parties responsible

Step-by-Step: Add Assessment

1. Purview portal → Compliance Manager → Assessments → + Add assessment.
2. Choose template (e.g., "ISO 27001:2022", "GDPR", "NIST 800-53").
3. Name + description + group (helps organize).
4. Save.

5. Assessment populates with all controls and improvement actions.

Improvement Actions

Each action shows:

- Description + framework mapping
- Implementation: in-product link to configuration
- Test: how to verify (Microsoft Defender, Entra logs, etc.)
- Score impact: points contribution
- Status: Implemented / Implementation pending / Out of scope / Not implemented

Workflow Example

1. Pick action: "Enable MFA for all administrative users."
2. Read implementation guidance → link to Entra blade.
3. Enable MFA via CA.
4. Return to Compliance Manager → mark action Implemented.
5. Provide test evidence (screenshot, link to policy).
6. Compliance score increases.

Real-World Scenarios

Scenario: SOC 2 audit prep

Company needs SOC 2 Type II report. Adds SOC 2 assessment in Compliance Manager. Score: 47% Microsoft-managed + 23% customer-managed = 70%. Identifies 18 unimplemented customer controls. Assigns each to owner. Implements over 3 months. Final score 92%. Auditor uses report as evidence — saves weeks of evidence collection.

Best Practices

- Pick 2-3 priority frameworks; don't pile on all.
- Assign each improvement action to an owner.
- Document evidence in the test results field.
- Re-test annually.
- Export reports for auditor.

Summary

Section 8.2 Summary

- Compliance Manager scores you against frameworks (GDPR, HIPAA, ISO, NIST).
- Microsoft-managed + customer-managed + shared controls.
- Improvement actions guide implementation.
- Export for auditors.

8.3 Sensitivity Labels

Introduction

Sensitivity Labels classify content (emails, files, sites, meetings) with persistent labels like "Public," "Internal," "Confidential," "Highly Confidential." Labels travel with content — they apply protection (encryption, access restrictions, visual markings) wherever the file goes.

Why It Matters

A file marked "Confidential" stays protected even when downloaded to a personal device, attached to email, or shared externally. Without labels, sensitive data is undifferentiated — every Word doc looks the same to access controls.

What Labels Can Do

Capability	Description
Encryption	Apply rights management (cannot open without authentication)
Watermark / Header / Footer	Visual markings on docs and emails
Restrict access to specific users/groups	"Only employees + Legal can open"
Restrict rights	Read, edit, print, copy, forward — fine-grained
Apply to container (site, group, team)	Block external sharing, require managed device
Auto-apply	Automatically label if content matches sensitive info type
Endpoint DLP control	Labeled content triggers endpoint DLP rules
Coauthoring on encrypted docs	P2: real-time coauthoring of protected files

Microsoft Portal Navigation

> 📍 Purview Portal → `Information Protection` → `Labels`

Step-by-Step: Create a Sensitivity Label

1. Purview → Information Protection → Labels → + Create a label.
2. Name: "Confidential" + display name + tooltip.
3. Scope: Files & emails + Groups & sites + Schematized data assets.
4. Files & emails settings:
    - Encryption: Configure → assign permissions:
        - Internal: "All users in contoso.com" → Co-Author
        - Specific users: "Legal@contoso.com" → Co-Owner
    - Markings: header "CONFIDENTIAL," footer "Do not distribute," watermark "CONFIDENTIAL"
    - Auto-labeling: detect credit card numbers, SSN, financial data
5. Groups & sites settings:
    - Privacy: Private
    - External user access: Block
    - External sharing from SPO site: Existing guests only
    - Conditional Access requirement: Compliant device
6. Next; Submit.
7. Publish the label policy targeting users or groups.

Label Hierarchy

Best practice: 4-5 labels total. Too many = users confused.

Label	Description	Encryption
Public	Anyone can read; for marketing materials	No
General	Default for everyday business content	No
Confidential	Internal-only; can share with employees	Yes
Confidential / Restricted	Limited audience (e.g., finance only)	Yes + restricted distribution
Highly Confidential	Most sensitive; specific named users	Yes + tight controls

Auto-Labeling

Two types:

Type	Where	How
Client-side auto-label	Office desktop apps; user gets prompt or suggestion	Triggered on document open/save
Service-side auto-label	SharePoint, OneDrive, Exchange	Background scan + applies label

Step-by-Step: Auto-Labeling Policy

1. Purview → Information Protection → Auto-labeling → + Create.
2. Choose label to apply (e.g., "Confidential").
3. Conditions:
    - Sensitive info types: U.S. SSN with high confidence + at least 1 instance
    - Trainable classifiers: "Financial documents"
    - Content matches keywords (optional)
4. Locations: Exchange, SharePoint, OneDrive.
5. Run in simulation mode for 7 days.
6. Review simulation results; adjust.
7. Switch to On.

PowerShell

```
# Get labels
Connect-IPPSSession
Get-Label | Format-Table DisplayName, ParentId, Priority

# Create label
New-Label -Name "Confidential" -DisplayName "Confidential" `
    -Tooltip "Confidential internal content" `
    -EncryptionEnabled $true `
    -EncryptionProtectionType "Template" `
    -ApplyContentMarkingHeaderEnabled $true `
    -ApplyContentMarkingHeaderText "CONFIDENTIAL" `
    -ApplyContentMarkingFooterEnabled $true `
    -ApplyContentMarkingFooterText "Do not distribute"

# Publish label
New-LabelPolicy -Name "Default-LabelPolicy" `
    -Labels @("Public","General","Confidential","Highly Confidential") `
    -ExchangeLocation All `
    -SharePointLocation All `
    -OneDriveLocation All
```

Real-World Scenarios

Scenario: Acquisition NDA documents

M&A team handles documents about potential acquisitions. Labels: "Highly Confidential — M&A". When applied: only M&A team + senior execs can open. File can't be forwarded, copied, printed. Cannot upload to personal OneDrive (endpoint DLP). If file accidentally sent to wrong colleague: they get "You don't have permission to open this file." Investigation triggered, but no data leak.

Scenario: Auto-label PII

Auto-label policy: any file containing 10+ instances of credit card or SSN → label "Confidential". Sites containing 100+ such files → site labeled "Confidential" (blocks external sharing). Result: thousands of documents protected without user effort.

Best Practices

- Limit to 4-5 labels — clarity beats completeness.
- Provide tooltips and training so users pick right label.
- Use auto-labeling for known PII to reduce manual burden.
- Test in simulation mode for 7-14 days before enabling.
- Apply container labels to sites/groups, not just docs.
- Combine with DLP for end-to-end protection.

Common Errors

Issue	Resolution
User can't see label in Office app	Confirm label published to that user; latest Office build needed
"You don't have permission" on labeled file	User not in encryption permission scope; check label settings
Auto-label not firing	Check rule, sensitive type matches, location, policy mode
Performance slow on large libraries	Auto-label processing takes time; eventually catches up

Summary

Section 8.3 Summary

- Sensitivity Labels classify and protect content.
- Apply to files, emails, sites, groups, meetings.
- Encryption, watermarks, access restrictions follow the file.
- Auto-labeling reduces manual effort.
- Limit to 4-5 labels total.

8.4 Data Loss Prevention (DLP)

Introduction

DLP detects and prevents sensitive data leakage across email, files, chat, endpoints, and SaaS apps. Define what's sensitive (credit cards, SSN, custom keywords), where to apply (Exchange, SharePoint, OneDrive, Teams, Endpoint), and what to do when found (notify, block, encrypt).

Why It Matters

Regulators require demonstrable controls preventing PII leaks. Beyond compliance: data exfiltration is the #1 insider threat. DLP is the technical safeguard against accidental and malicious leaks.

License

- M365 E3: DLP for Exchange, SharePoint, OneDrive, Teams
- M365 E5: Endpoint DLP (Windows/macOS), DLP for on-prem repositories, Adaptive Protection

Sensitive Info Types

Microsoft maintains 300+ built-in types. Examples:

- U.S. Social Security Number
- Credit Card Number (Visa, MC, Amex, etc.)
- U.S./EU/UK Passport Number
- EU IBAN, Tax File Number
- Personal Health Information (PHI) — HIPAA
- Driver's license, ICD-9/10 codes
- Pakistan CNIC, India Aadhaar

Custom: regex-based or dictionary-based (your own product codes, customer IDs).

DLP Policy Components

Component	Description
Locations	Where to scan: Exchange, SPO, OneDrive, Teams, Endpoint, Defender for Cloud Apps
Rules	Conditions + exceptions + actions
Conditions	Sensitive info type, label match, content recipient, etc.
Actions	Block, restrict access, notify admin, notify user, generate alert, encrypt
User notifications	Policy tips shown in Office/Outlook
Overrides	Let user override with business justification

Step-by-Step: Create a DLP Policy for Credit Cards

1. Purview → Data loss prevention → Policies → + Create.
2. Use a template "U.S. Financial Data" OR custom.
3. Name: "DLP - Credit Card Data".
4. Locations: Exchange, SharePoint, OneDrive, Teams chat, Endpoint.
5. Rules:
    - Condition: Content contains "U.S. Financial Data" sensitive info type
    - Confidence: Medium
    - Instances: at least 1
    - Action: Restrict access (Anyone link); send notification; allow override with justification
    - Notification: educate user about why this matters

    - Severity: High
6. Test mode: Run policy in test mode and show policy tips → on.
7. Wait 1-2 weeks; review reports.
8. Move to Turn it on right away.

Endpoint DLP (E5)

Extends DLP to local file actions on Windows/macOS endpoints:

- Copy to USB drive
- Copy to network share
- Print
- Upload to non-corporate cloud (Dropbox, personal OneDrive)
- Paste into browser
- Screen capture
- Bluetooth transfer

Step-by-Step: Endpoint DLP

1. Onboard endpoints (typically already onboarded via Defender for Endpoint).
2. Purview → Endpoint DLP settings → review allowed/restricted apps, browsers, network shares.
3. Create DLP policy → enable "Devices" location.
4. Configure file activities:
    - Copy to clipboard: audit
    - Copy to USB removable device: block + override allowed
    - Print: audit
    - Copy to unallowed cloud: block
5. Combine with sensitive info type condition.
6. Save.

Adaptive Protection (E5)

Adaptive Protection ties Insider Risk to DLP. Users assessed as elevated/moderate/minor risk receive correspondingly stricter DLP actions. A user with rising risk gets blocked from exporting; one with low risk just gets policy tips.

PowerShell

```
# Get DLP policies
Connect-IPPSSession
Get-DlpCompliancePolicy | Format-Table Name, Mode, Enabled

# Get rules within a policy
Get-DlpComplianceRule -Policy "DLP - Credit Card Data"

# Create simple policy via PowerShell (full creation is complex; usually GUI)
New-DlpCompliancePolicy -Name "Block PII" -ExchangeLocation "All" `
    -SharePointLocation "All" -OneDriveLocation "All"

New-DlpComplianceRule -Name "Block PII Rule" `
    -Policy "Block PII" `
    -ContentContainsSensitiveInformation @{Name="U.S. Social Security Number (SSN)";
minCount="1"} `
    -BlockAccess $true `
    -GenerateIncidentReport SiteAdmin
```

Real-World Scenarios

Scenario: Accidental external share

HR employee shares a spreadsheet with employee SSNs externally by mistake. DLP detects, blocks the share, shows policy tip "This file contains 47 SSNs; sharing externally requires approval." User contacts HR director; properly redacted version shared instead. Audit log captures the attempt.

Scenario: USB exfiltration

Departing employee plugs in USB drive, drags 200 customer files. Endpoint DLP detects: each file contains customer PII. Blocks the copy + alerts security team. Investigation initiated; departure expedited; data not lost.

Best Practices

- Start in Test mode with policy tips visible.
- Use Microsoft templates for common scenarios (GDPR, HIPAA, PCI).
- Layer multiple policies: educate first, then restrict, then block.
- Always allow business-justified override (logged for audit).
- Combine with sensitivity labels for layered enforcement.
- Enable Adaptive Protection (E5) to tune by user risk.
- Review incident reports weekly.

Common Errors

Issue	Resolution
Policy tips not appearing	Office build, user has assignment, Test mode shows tips
False positives — too many	Increase instance count (require multiple matches); increase confidence; refine info types
Endpoint DLP not enforcing	Verify Defender for Endpoint onboarded; device in DLP scope; client up to date
"Justification" workflow not visible	Enable "Allow user to override" in rule action

Summary

Section 8.4 Summary

- DLP = detect & prevent data leak across Exchange, SPO, OneDrive, Teams, Endpoint.
- 300+ built-in sensitive info types + custom.
- Actions: notify, block, restrict, encrypt.
- Endpoint DLP (E5): USB, print, cloud upload control.
- Adaptive Protection (E5): risk-tuned enforcement.

8.5 Retention Policies and Labels

Introduction

Retention policies and labels manage how long content is kept and what happens when retention expires. Used for: legal compliance, tax records, employment records, business records, sensitive data minimization.

Retention Policy vs Retention Label

Aspect	Retention Policy	Retention Label
Scope	Whole location (Exchange, SPO, OneDrive, Teams)	Individual file or email
Applied by	Admin (automatic)	User or auto-classifier
Triggers	Item creation/received date	Same OR event-based
Use	Bulk: "all email 7 years"	Specific: "this contract 10 years from signing"

Retention Actions

Action	Result
Retain only	Keep at minimum X period; user can still delete (but recoverable for compliance)
Delete only	Permanently delete after X period (no retention)
Retain and then delete	Hold for X, then delete
Retain forever	Never auto-delete

Step-by-Step: Retention Policy

1. Purview → Data Lifecycle Management → Retention policies → + New.
2. Name: "Email - 7 Year Retention".
3. Locations: Exchange email (only).
4. Retention settings:
    - Retain items for: 7 years
    - From: When items were created
    - After retention period: Delete items automatically
5. Submit. Applied within 7 days.

Step-by-Step: Retention Label

1. Purview → Data Lifecycle → Retention labels → + Create.
2. Name: "Contract".
3. Retention settings: Retain 10 years from when labeled, then delete.
4. Mark items as records: Yes (locks editing/moving — Records Management).
5. Publish: target users.
6. Users can apply manually OR set up auto-apply via content match.

Auto-Apply Retention Labels

1. Retention labels → Auto-apply policy → + New.
2. Select label "Contract".
3. Conditions:
    - Content contains sensitive info type: "Signature on file" keyword
    - Or Trainable classifier: "Contracts"

4. Locations.
5. Save.

Records Management (E5)

Records Management adds advanced features to retention labels:

- Items marked as records cannot be edited, moved, or deleted.
- Disposition review: when retention expires, designated reviewer approves deletion.
- Event-based retention: trigger based on event ("employee left"). After event + retention period, dispose.
- File plan: registry of all retention categories.
- Proof of disposition.

Preservation Lock

For regulated industries, lock a policy so admins (even themselves) cannot delete or shorten it. Once locked, can only EXTEND retention — never relax. Use for SEC 17a-4, FINRA, regulatory immutability.

PowerShell

```
# Get retention policies
Get-RetentionCompliancePolicy | Format-Table Name, Mode, Enabled

# Create policy
New-RetentionCompliancePolicy -Name "Email 7yr" -ExchangeLocation All
New-RetentionComplianceRule -Name "Email 7yr Rule" `
    -Policy "Email 7yr" `
    -RetentionDuration 2555 `
    -RetentionComplianceAction Delete `
    -ExpirationDateOption CreationAgeInDays
```

Real-World Scenarios

Scenario: Legal hold during litigation

Lawsuit filed against company. Legal places eDiscovery hold on involved custodians. Their email, OneDrive, SharePoint content cannot be deleted regardless of retention policies. Once case closed, hold released; normal retention resumes.

Scenario: Employee termination records

HR auto-applies retention label "Employee Record - 7 years post-termination" to employee files. Event-based: triggered when employee's termination date is set. 7 years later, disposition review notifies HR; if approved, deleted.

Best Practices

- Document retention requirements from Legal / Compliance first.
- Use policies for broad rules, labels for specific records.
- Don't combine conflicting retention — most restrictive wins.
- Use Records Management (E5) for regulated records.
- Test with small scope before broad rollout.
- Use Preservation Lock for regulatory binding.

Common Errors

Issue	Resolution
Items not retained	Verify policy targets location; check workload-specific behaviour
Items deleted earlier than expected	Multiple retention rules in conflict — Microsoft picks most restrictive but be sure
"Cannot modify item" — record locked	Records Management label applied; expected behaviour
Preservation Lock can't be undone	By design — only Microsoft Support can remove via legal process

Summary

Section 8.5 Summary

- Retention policy = broad location-based rule.
- Retention label = per-item, can auto-apply.
- Actions: retain, delete, retain+delete.
- Records Management (E5) for immutable records.
- Preservation Lock for regulatory immutability.

8.6 eDiscovery

Introduction

eDiscovery finds, holds, and exports content for legal cases, investigations, and regulatory requests. It spans Exchange, SharePoint, OneDrive, Teams, and Yammer.

Two Tiers

Tier	License	Capabilities
eDiscovery (Standard)	E3+	Hold, search, export
eDiscovery (Premium)	E5	Above + custodian management, legal hold notifications, advanced indexing, machine learning analysis, review sets, redaction

Workflow

```
Legal team gets case
     |
     v
Create eDiscovery case
     |
     v
Add custodians (users involved)
     |
     v
Place holds (preserve content)
     |
     v
Custodian notifications (Premium only)
     |
     v
Run searches (keywords, dates, conditions)
     |
     v
Review results (review set, redact, tag)
     |
     v
Export results
```

Microsoft Portal Navigation

> 📍 Purview Portal → `eDiscovery` → `Standard` or `Premium`

Step-by-Step: Standard eDiscovery

1. Create Case

1. Purview → eDiscovery → Standard → + Create a case.
2. Name + description.

2. Add Custodians and Holds

1. Case → Holds → + Create.
2. Select locations (specific user mailboxes, sites, OneDrives).
3. Optional: keyword filter (only hold matching content).
4. Create. Content preserved.

3. Search Content

1. Case → Searches → + New search.
2. Conditions: keywords, sender, date range, locations.
3. Sample: "wire transfer OR routing number" + sent between 2026-01-01 and 2026-03-01.
4. Run search; review estimated results.

4. Export

1. Search → Actions → Export.
2. Options: include unrestored versions, encrypted content, etc.
3. Format: PST + native files + Excel index.
4. Download via eDiscovery Export Tool.

Premium eDiscovery Features

Feature	Use
Custodian management	Track who's a data custodian; their data sources
Legal hold notification	Email custodians asking acknowledgement of hold
Review sets	Working copy of search results; tag, annotate
Predictive coding	ML-assisted relevance ranking
Near-duplicate / threading	Group related items
Redaction	Black out specific text before export
Conversation reconstruction	Rebuild Teams chat conversations
Communication compliance integration	Move flagged items into eDiscovery

Content Search (Tool)

Content Search is a lighter-weight tool — search M365 content without creating a case:

- Purview → eDiscovery → Content search.
- Used by admins for general content discovery, security investigations.

PowerShell

```
# Create eDiscovery case
Connect-IPPSSession
New-ComplianceCase -Name "Smith vs Contoso" -Description "Litigation case 2026-Q1"

# Place hold
New-CaseHoldPolicy -Name "Smith Hold" -Case "Smith vs Contoso" `
    -ExchangeLocation @("smith@contoso.com","exec@contoso.com") `
    -SharePointLocation @("https://contoso.sharepoint.com/sites/Sales")

New-CaseHoldRule -Name "Smith Hold Rule" `
    -Policy "Smith Hold" `
    -ContentMatchQuery "wire transfer OR routing"

# Create search
New-ComplianceSearch -Name "Smith Q1 Search" -Case "Smith vs Contoso" `
    -ContentMatchQuery "wire transfer" `
    -ExchangeLocation "smith@contoso.com"

Start-ComplianceSearch -Identity "Smith Q1 Search"
Get-ComplianceSearch -Identity "Smith Q1 Search" | Select-Object Status, Items
```

Real-World Scenarios

Scenario: Lawsuit production

Plaintiff lawyer issues discovery request: "all emails between Alice and Bob related to Project X between 2024-2026." Legal team: (1) Create case. (2) Hold both mailboxes + their OneDrives. (3) Notify them they're under hold (don't delete anything). (4) Run search: from:alice TO/FROM:bob AND "Project X" 2024-2026. (5) Review 1,247 results in review set; tag relevant. (6) Redact PII before export. (7) Export to outside counsel. Time: 1 week vs months with traditional discovery.

Best Practices

- Place holds BEFORE communicating to custodian (avoids deletion).
- Use Premium for any litigation matter.
- Train Legal team on the tools.
- Document case progression with timestamps.
- Audit eDiscovery access — admin power tool.
- Don't grant eDiscovery roles permanently; use PIM.

Common Errors

Issue	Resolution
"Cannot place hold"	Verify eDiscovery role; license; location is supported
Search results incomplete	Index may not be current; some content unindexed; broader date range
Export fails	Size limit (default 750 GB); split into multiple exports
Custodian can still delete	Hold takes 15-60 min to propagate; preservation is invisible (item stays in mailbox)

Summary

Section 8.6 Summary

- eDiscovery = find, hold, export for legal/investigation.
- Standard (E3+) vs Premium (E5).
- Premium adds custodian mgmt, review sets, ML coding, redaction.
- Hold preserves content even if user deletes.
- Audit eDiscovery usage carefully.

8.7 Audit Logs

Introduction

Microsoft Purview Audit (unified audit log) records actions performed by users, admins, and the service across M365. Critical for security investigations, compliance audits, insider threat detection, and incident response.

Two Tiers

Tier	License	Retention
Audit (Standard)	E3	180 days (was 90, raised in 2023)
Audit (Premium)	E5 or E5 Compliance / Add-on	1 year default; up to 10 years with add-on; high-value events; longer-term searchable

What's Logged

Workload	Examples
Exchange	Mailbox access, mailbox permission changes, message read by delegate, email send by another user
SharePoint	File accessed, downloaded, shared, deleted
OneDrive	Same as SharePoint
Entra (Azure AD)	Sign-in, role assignments, password reset, app consent
Teams	Member added, channel created, settings changed
Power Platform	App created, flow modified
Defender	Alert acknowledged, threat policy changed
Purview	Policy created, label applied

Microsoft Portal Navigation

> 📍 Purview Portal → `Audit` → `New search`

Step-by-Step: Search Audit Log

1. Purview → Audit → New search.
2. Date and time range.
3. Activities: select specific or all.
4. Users: empty (all) or specific.
5. File, folder, site: optional path filter.
6. Workload: Exchange, SharePoint, Entra, etc.
7. Search → wait for results.
8. Export to CSV for further analysis.

Common Audit Investigations

Investigation	Activities to Search
Who accessed a sensitive file?	FileAccessed, FileDownloaded, FilePreviewed (SharePoint/OneDrive)
Who shared a file externally?	SharingSet, AnonymousLinkCreated, CompanyLinkCreated
Who changed admin role?	"Member added to Role" or "Add member to role" (Entra)
Compromised mailbox investigation	UserLoggedIn, MailItemsAccessed, Send (Exchange)
Auto-forwarding setup	Set-Mailbox (Forwarding)
Insider data exfiltration	FileDownloaded + sharing + suspicious volume

Mailbox Access Audit (MailItemsAccessed)

This Premium event (also available with E5 license tier) records EVERY message access in a mailbox — critical for breach investigation. Without it, you only know an account was compromised; with it, you know exactly which messages the attacker read.

PowerShell

```
# Check audit log enabled (default On in newer tenants)
Get-AdminAuditLogConfig | Select-Object UnifiedAuditLogIngestionEnabled

# Enable if disabled (legacy tenants)
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true

# Search audit log
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) `
    -EndDate (Get-Date) `
    -Operations FileDownloaded `
    -UserIds "suspicious-user@contoso.com" `
    -ResultSize 5000 |
    Export-Csv "filedown_audit.csv" -NoTypeInformation

# Search for external sharing events
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) `
    -EndDate (Get-Date) `
    -Operations AnonymousLinkCreated,CompanyLinkCreated,AnonymousLinkUsed |
    Select-Object CreationDate, UserIds, Operations, ObjectId
```

Real-World Scenarios

Scenario: Compromised account investigation

Sign-in log shows alice@contoso.com signed in from Romania at 3 AM. Investigation: Purview → Audit → user alice, last 7 days. Reveals: external sign-in created mail flow rule auto-forwarding all messages to attacker@yopmail.com; downloaded 47 files from OneDrive; accessed 230 messages. Response: kill session, reset password, revoke forwarding rule, restore from versions. Audit log = breach reconstruction tool.

Best Practices

- Verify Audit is enabled in tenant (default On in new tenants).
- Train SOC team on the search interface and query syntax.
- Use Audit Premium for E5 customers — longer retention, high-value events.
- Forward audit data to Sentinel/Splunk for correlation.
- Test investigation runbooks with tabletop exercises.
- Limit eDiscovery + audit access via PIM.

Common Errors

Issue	Resolution
"Audit log not enabled"	Legacy tenant; enable via Set-AdminAuditLogConfig
No results returned	Check date range; activity name spelling; user UPN exact
Search times out	Narrow scope; export query results to CSV; use Sentinel for big queries
MailItemsAccessed not appearing	Requires E5 license + mailbox auditing enabled

Summary

Section 8.7 Summary

- Audit = unified log of all M365 activity.
- Standard E3: 180 days. Premium E5: 1+ years; high-value events.
- Critical for SOC investigations.
- Use PowerShell for large queries.
- Forward to SIEM for correlation.

8.8 Insider Risk Management

Introduction

Insider Risk Management (IRM) detects internal threats: data theft by departing employees, accidental leaks, IP exfiltration, policy violations. Uses ML + indicators across M365 to surface concerning patterns.

Why It Matters

External attacks get attention but insiders cause 60%+ of data breaches. A departing engineer copies customer lists to personal drive. A disgruntled employee leaks proprietary code. IRM catches these patterns.

License

- M365 E5 or E5 Compliance Add-on.

Built-in Policy Templates

Template	Detects
Data theft by departing users	Downloads, prints, USB exfil shortly before departure
Data leaks	Unusual sharing or large data movement
Data leaks by priority users	Above, scoped to high-risk users
Data leaks by disgruntled users	Combined with sentiment / HR signals
General data leaks	Broad pattern of unusual data movement
Risky browser usage	Pasting sensitive data to non-corporate sites
Security policy violations	Disabling security features, defying restrictions
Patient data misuse (healthcare)	Unusual EHR access
Forensic evidence	Visual capture of risky activity (high-priv)

Step-by-Step: Create IRM Policy

1. Purview → Insider Risk Management → Policies → + Create policy.
2. Select template: "Data theft by departing users".

3. Configure:
    - Users in scope: All users / specific group
    - HR connector required (uploads termination dates)
    - Sensitive content sources: SharePoint sites, sensitivity labels, sensitive info types
    - Indicator selection: file downloaded, file copied to USB, email sent externally, etc.
    - Threshold customization: default values or custom
4. Save; activate.

HR Connector

For data theft template, IRM needs to know when an employee is departing:

1. Purview → Data connectors → + HR connector.
2. Configure: CSV upload (Resignation date, Last working day, Department).
3. Schedule daily upload.
4. IRM elevates risk score 30 days before departure.

Triage Alerts

1. IRM → Alerts.
2. Click alert: shows user activities over time, risk indicators, scoring.
3. Investigate: view activity, sensitive content involved, timing.
4. Confirm or dismiss.
5. If confirmed: escalate to case; notify HR / Legal / Security.

Investigation Cases

- Centralized case file per investigation.
- Tag users, evidence.
- Initiate eDiscovery from within case.
- Add notes; track decisions.

Adaptive Protection Integration

When IRM identifies a user as risky, Adaptive Protection automatically tightens DLP enforcement for them. A user at Major risk might be blocked from external sharing; a user at Minor risk just sees policy tips.

Real-World Scenarios

Scenario: Departing developer IP theft

Developer Alex resigns. HR uploads termination date to IRM. IRM monitors closely. Day before departure: Alex downloads 200 source code files, copies to USB drive, sends large attachments to personal Gmail. IRM alert fires; investigator reviews. HR + Legal contacted. Alex's last day moved up; legal letter sent. IP recovered.

Best Practices

- Activate HR connector for departure detection.
- Start with template, customize over time.
- Privacy: anonymize until escalation (recommend with HR + Legal).
- Pair with Adaptive Protection (E5) for automatic enforcement tuning.
- Document escalation procedure; brief HR + Legal.
- Audit IRM access carefully — sensitive role.

Summary

Section 8.8 Summary

- IRM (E5) detects insider threats: data theft, IP exfil, risky behaviour.
- Templates: departing users, data leaks, policy violations.
- HR connector triggers elevated monitoring before departure.
- Adaptive Protection ties IRM risk to DLP enforcement.
- Privacy-respecting: anonymize until escalation.

8.9 Communication Compliance and Information Barriers

Communication Compliance

Communication Compliance monitors Teams chats, channel messages, email, and Yammer for policy violations: harassment, sensitive content sharing, regulated communications.

Use Cases

- Harassment / discriminatory language
- Threats and weapons references
- Financial regulations (insider trading communications)

- Corporate code-of-conduct violations
- Adult / inappropriate content

Setup

1. Purview → Communication Compliance → Policies → + Create from template.
2. Template: "Inappropriate text" / "Inappropriate images" / "Regulatory compliance".
3. Configure:
    - Users to monitor: scope or all
    - Reviewers: list of designated reviewers (only they see matches)
    - Conditions: keywords, classifiers, attachments
4. Save.

Review Workflow

1. Reviewers see flagged items in Comm Compliance portal.
2. Per item: Acknowledge / Tag (compliant, non-compliant, questionable) / Escalate / Resolve / Remove from Teams.
3. Auditable trail.

Information Barriers

Information Barriers prevent communication between specific groups — preventing conflicts of interest. Used in finance (research vs trading), legal (Chinese walls), competitive M&A teams.

How It Works

1. Define segments: groups based on user attributes (e.g., Department = "M&A Buyer Side", "M&A Sell Side").
2. Define policies: "Block communication between M&A Buyer and M&A Sell segments."
3. Once applied:
    - Cannot Teams-chat across segments
    - Cannot add to same Team
    - Cannot search for each other in directory
    - Email may still flow (config dependent)

Setup

```
Connect-IPPSSession

# Create segments
New-OrganizationSegment -Name "MA-Buyer" `
    -UserGroupFilter "Department -eq 'M&A-Buyer'"
New-OrganizationSegment -Name "MA-Sell" `
    -UserGroupFilter "Department -eq 'M&A-Sell'"

# Create policy
New-InformationBarrierPolicy -Name "Block-Buyer-Sell" `
    -AssignedSegment "MA-Buyer" `
    -SegmentsBlocked "MA-Sell" `
    -State Active

# Apply
Start-InformationBarrierPoliciesApplication
```

Summary

Section 8.9 Summary

- Communication Compliance monitors Teams/email for violations.
- Templates: harassment, threats, regulatory.
- Information Barriers prevent communication between conflicting groups.
- Both require E5.

Section 8 — Wrap-Up

Section 8 Synthesis

- **Purview** = unified compliance & governance.
- **Compliance Manager**: framework scoring.
- **Sensitivity Labels**: classify + protect content.
- **DLP**: prevent leaks across Exchange, SPO, OneDrive, Teams, Endpoint.
- **Retention**: policies (broad) + labels (specific).
- **eDiscovery**: legal hold + search + export.
- **Audit**: all M365 actions; 180d (E3) / 1+yr (E5).
- **Insider Risk Management**: detect departing-user data theft, leaks.
- **Communication Compliance**: monitor for harassment, regulated content.
- **Information Barriers**: block communication between conflicting groups.

Section 8 Mini-Quiz

Q1. What's the difference between a retention policy and a retention label?

A: Policy = broad, location-based, automatic. Label = per-item, can be applied by user or auto-classifier.

Q2. What does Sensitivity Label encryption travel with?

A: The file itself — protection persists even when file is downloaded, attached, or moved

Q3. How many built-in sensitive info types does Microsoft maintain?

A: 300+

Q4. What does Endpoint DLP control that other DLP doesn't?

A: Local actions: USB copy, print, paste to browser, screen capture, Bluetooth transfer

Q5. Standard vs Premium eDiscovery — key differences?

A: Premium adds custodian management, legal hold notifications, review sets, ML coding, redaction, advanced indexing

Q6. How long does Audit Standard retain events?

A: 180 days (raised from 90 in 2023)

Q7. What does Preservation Lock do?

A: Locks a retention policy so no admin can shorten or remove it — only extend; for regulatory immutability

Q8. What's the HR Connector for in IRM?

A: Uploads HR data (termination dates) so IRM can elevate monitoring for departing users

Q9. Use case for Information Barriers?

A: Prevent communication between conflicting groups (M&A buyer/sell, research/trading, ethical walls)

Q10. What ties Insider Risk to DLP enforcement automatically?

A: Adaptive Protection (E5) — DLP enforcement automatically tunes based on user's IRM risk level

Section 9
09
Monitoring & Reporting
Service health, usage analytics, sign-in logs, alert policies, custom workbooks. Know what's happening across your tenant — proactively, not reactively.
Exam Weight: ~10%

9.1 Service Health and Message Center

Introduction

Service Health shows the current operational status of all Microsoft 365 services. Message Center delivers proactive announcements about upcoming changes, new features, and required actions. Together they're your tenant's news feed.

Why It Matters

Users complain "Teams is down" — is it really? Or is it just them? Service Health answers in seconds. Message Center warns you 30+ days before changes affect your tenant. Subscribe to relevant ones; ignore irrelevant.

Microsoft Portal Navigation

> 📍 M365 Admin Center → `Health` → `Service health`

> 📍 M365 Admin Center → `Health` → `Message center`

Service Health Views

View	Shows
All services	Status per workload (Exchange, Teams, SPO, Entra, Intune, Defender, etc.)
Issues	Active incidents and advisories
History	Last 30 days
Reported issues	Issues you've submitted to Microsoft

Status Indicators

Status	Meaning
Healthy	Operating normally
Service degradation	Some users experiencing issues
Service interruption	Major impact; users likely affected
Restoring service	Microsoft applying fix
Extended recovery	Fix applied; clearing backlog
Investigating	Microsoft engaged; cause unknown
Service restored	All clear
False positive	Initial report turned out to be no actual issue

Step-by-Step: Investigate a Service Issue

1. Admin Center → Health → Service health.
2. See banner indicating active incident.
3. Click incident → details.
4. Read:
    - Service: Teams
    - Status: Service interruption
    - Impact: Some users may be unable to access chat
    - Current status: Microsoft is rolling out fix
    - Next update: in 60 minutes
5. Save Incident ID (e.g., MO123456) for communication.
6. Optionally: notify users via internal channels.

Message Center

Type	What It Tells You
Plan for change	30+ days advance notice; new features, retirements
Prevent or fix issues	Recommended remediation steps
Stay informed	General announcements

Subscribe to Notifications

1. Admin Center → Health → Message center → Preferences.
2. Customize email notifications: services, frequency.
3. Forward to: distribution list (typically m365-changes@contoso.com).
4. Save.

Service Health App for Teams

Install the "Service Health" app in Teams for in-app notifications when incidents occur. Reduces "is it down?" interruptions.

PowerShell

```
# Service health via Graph
Connect-MgGraph -Scopes "ServiceHealth.Read.All","ServiceMessage.Read.All"

# Get service health overviews
Get-MgServiceAnnouncementHealthOverview |
    Select-Object Service, Status

# Get active issues
Get-MgServiceAnnouncementIssue -Filter "status ne 'serviceRestored'" |
    Select-Object Id, Title, Service, Status, ClassificationDisplayName

# Get message center posts
Get-MgServiceAnnouncementMessage -Top 50 |
    Where-Object { $_.Category -eq "planForChange" } |
    Select-Object Id, Title, EndDateTime |
    Sort-Object EndDateTime
```

Real-World Scenarios

Scenario: Teams chat outage

Helpdesk receives 50 tickets in 10 minutes — "Teams chat broken." Admin checks Service Health: confirms global Teams chat incident (MO987654), expected 2-hour recovery. Posts banner to intranet: "Microsoft has confirmed Teams chat issue, MO987654. Expected resolution: 2 PM." Helpdesk closes new tickets with link. Saves hundreds of duplicate tickets.

Scenario: Policy change preparation

Message Center post: "Basic Authentication retirement complete in 60 days." Admin reviews; identifies 3 line-of-business apps still using basic auth. Project to modernize each. Migration completes before deadline. Zero impact at retirement.

Best Practices

- Check Service Health before deep troubleshooting — it might not be you.
- Subscribe Message Center email digest weekly.
- Forward Message Center to broader IT distribution list.
- Add Service Health app to Teams admin channel.
- Save incident IDs in support tickets and user communications.

Summary

Section 9.1 Summary

- Service Health = real-time tenant operational status.
- Message Center = proactive change announcements.
- Subscribe to Message Center email.
- Service Health Teams app for in-app alerts.

9.2 Usage Reports and Analytics

Introduction

Usage reports show adoption: how many users actively use each workload, what they do, which features. Critical for understanding ROI, identifying low-adoption areas, and planning training.

Microsoft Portal Navigation

> 📍 M365 Admin Center → `Reports` → `Usage`

Available Reports

Workload	Reports
Microsoft 365	Active users, app usage, product summary
Email	Activity, app usage (Outlook web/mobile/desktop), mailbox usage
OneDrive	Active users, files synced, storage
SharePoint	Site usage, activity, files
Teams	User activity, device usage (desktop/web/mobile), meetings
Yammer / Viva Engage	Activity, device usage
Forms	Activity
Project	Activity
Office activations	How many apps installed per user

Privacy Considerations

By default, user names are visible in usage reports. Some orgs require anonymization:

1. Admin Center → Settings → Org settings → Reports.
2. "Display concealed user, group, and site names in all reports": Toggle on.
3. Save.
4. Names now show as MD5 hashes (consistent so you can correlate across reports without identifying).

Adoption Score

Microsoft Adoption Score shows your org's digital transformation across "People experiences" + "Technology experiences":

- Communication (Outlook, Teams)
- Meetings
- Content collaboration (SharePoint, OneDrive)
- Teamwork
- Mobility

Compared against organizations of similar size. Drill into specific KPIs to find improvement areas.

Productivity Score (Renamed Microsoft Adoption Score)

Same product, different branding over time. Provides organizational and peer-benchmark insights.

Viva Insights (Replaces MyAnalytics)

Per-user productivity insights and team insights (with privacy protections).

PowerShell — Graph Reports API

```
# Active users last 30 days
Connect-MgGraph -Scopes "Reports.Read.All"

$report = Get-MgReportOffice365ActiveUserDetail -Period D30 -OutFile activeusers.csv
# CSV downloaded

# Teams user activity
Get-MgReportTeamUserActivityUserDetail -Period D30 -OutFile teams_users.csv

# SharePoint activity
Get-MgReportSharePointSiteUsageDetail -Period D30 -OutFile sites.csv

# Mailbox usage
Get-MgReportMailboxUsageDetail -Period D30 -OutFile mailboxes.csv
```

Real-World Scenarios

Scenario: License optimization

Reports show 200 users licensed for M365 E5 but only using Outlook (no Teams, no SharePoint). Decision: downgrade them to Business Basic ($6 vs $57 per user/month). Saves $122,400/year. Compliance team verifies (some need E5 for legal hold) — net savings remain $90k+.

Scenario: Low Teams adoption in department

Sales has 50% Teams usage; Operations has 8%. Investigation: Operations still using Skype-replacement workflows. Action: targeted training, change-management campaign, executive sponsorship. 6 months later: Operations at 67%.

Best Practices

- Review usage reports monthly.
- Identify low adoption → engage owners + provide training.
- Use Adoption Score for executive reporting.
- Export reports for trend analysis.
- Consider anonymizing names if needed for privacy/works council.

Summary

Section 9.2 Summary

- Usage reports cover every M365 workload.
- Adoption Score benchmarks against peers.

- Anonymization toggle for privacy.
- Drive license optimization and training programs.

9.3 Sign-In Logs and Entra Logs

Introduction

Sign-In Logs (Entra) record every authentication: who, when, from where, with what device, against what app. Essential for security investigations and access analysis.

Microsoft Portal Navigation

> 📍 Entra Admin Center → `Identity` → `Monitoring & health` → `Sign-in logs`

Four Tabs

Tab	Shows
Interactive user sign-ins	User typed password / used MFA
Non-interactive user sign-ins	Cached token used (background sync, mobile app refresh)
Service principal sign-ins	App-to-app authentication
Managed identity sign-ins	Azure resource auto-identity

Key Fields

Field	What It Shows
Date and time	When sign-in attempted
User	UPN attempting sign-in
Application	App being accessed (Office 365 Exchange Online, Microsoft Teams, etc.)
Status	Success / Failure / Interrupted
IP address	Source IP
Location	Geo-derived city + country
Client app	Browser, modern auth, IMAP, legacy
Device	Device ID + OS + browser
Conditional Access	Policies evaluated + result
Risk level	Identity Protection score
Authentication details	MFA factor used, method
Sign-in error code	AADSTS error (look up at login.microsoftonline.com error code reference)

Common Error Codes

Code	Meaning
AADSTS50053	Account locked (Smart Lockout)
AADSTS50055	Password expired
AADSTS50057	User disabled
AADSTS50058	Sign-in required (session token expired)
AADSTS50074	Strong auth required (MFA missing)
AADSTS50076	MFA required by Conditional Access
AADSTS50105	User not assigned to app role
AADSTS50126	Invalid credentials
AADSTS50132	Sign-in requires CA-controlled device
AADSTS50158	External challenge — re-auth required
AADSTS53003	Access blocked by CA policy
AADSTS530002	Device must be compliant
AADSTS700016	App not configured (consent)
AADSTS900561	Endpoint only accepts POST, GET, OPTIONS

Step-by-Step: Investigate Failed Sign-in

1. Entra Admin Center → Sign-in logs.
2. Filter: Status = Failure + User = alice@contoso.com + last 24 hours.
3. Click an entry.
4. See:
    - IP: 203.0.113.5
    - Location: Karachi, Pakistan
    - App: Microsoft Teams
    - Error: AADSTS50126 — Invalid credentials
    - CA: No policies evaluated (auth never reached that point)
5. Conclusion: bad password entry (expected with new device).

6. For sustained failures: investigate Smart Lockout / password spray.

Audit Logs (Entra Audit)

Separate from sign-in logs:

> 📍 Entra Admin Center → `Monitoring & health` → `Audit logs`

Records admin actions: who added a user, who changed a CA policy, who assigned a role. Critical for change tracking.

Export Logs to Long-Term Storage

Default sign-in/audit retention is 30 days (P1) or 7 days (Free). For longer:

1. Entra → Monitoring → Diagnostic settings → + Add.
2. Send to: Log Analytics workspace + Storage account + Event Hub (Sentinel).
3. Logs: AuditLogs, SignInLogs, NonInteractiveUserSignInLogs, ServicePrincipalSignInLogs, ManagedIdentitySignInLogs.
4. Save.

PowerShell / Graph

```
# Get sign-in logs
Connect-MgGraph -Scopes "AuditLog.Read.All"

Get-MgAuditLogSignIn -Top 50 -Filter "userPrincipalName eq 'alice@contoso.com'" |
    Select-Object CreatedDateTime, AppDisplayName, IpAddress, Status,
ConditionalAccessStatus

# Get audit logs (admin actions)
Get-MgAuditLogDirectoryAudit -Top 100 -Filter "activityDateTime ge 2026-01-01" |
    Select-Object ActivityDateTime, InitiatedBy, ActivityDisplayName, Result
```

Real-World Scenarios

Scenario: Password spray detection

Sign-in logs show 500 failed attempts across 200 user accounts in 1 hour, all from IPs in same /24 subnet, all hitting "OWA" app, all failing with AADSTS50126 (invalid credentials). Pattern: password spray attack. Response: identify source IPs; block at network layer; raise CA risk threshold; enforce strict MFA. Users not compromised due to Smart Lockout + complex passwords.

Best Practices

- Forward sign-in + audit logs to Sentinel/Splunk for correlation.
- Set up alerts for: sign-in from new country, high-risk sign-ins, repeated failures.
- Use Sign-in workbook for visualizations.
- Document common error codes in helpdesk runbook.
- Practice tabletop: walk through an account compromise investigation quarterly.

Summary

Section 9.3 Summary

- Sign-in logs record every authentication attempt.
- Four types: interactive, non-interactive, service principal, managed identity.
- Audit logs record admin actions.
- Default retention 30 days (P1); export to Log Analytics for longer.
- AADSTS error codes guide root cause.

9.4 Security Reports and Threat Reports

Defender for Office 365 Reports

Report	Shows
Mail flow status	Volume, blocked, delivered, spam, phish
Threat protection status	Trends: malware blocked, phish caught, ZAP actions
Top malware	Most common malware families targeting users
Top targets	Most-attacked users
Top senders / recipients	By volume, useful for high-volume mailbox review
URL protection report	Safe Links clicks; clicked-through warnings
Spoof detections	Inbound spoof attempts blocked
Submissions	User and admin reports
Compromised user report	Users with suspicious activity

Defender for Endpoint Reports

Report	Shows
Device health	AV status, OS version, sensor status
Vulnerable devices	Devices with critical CVEs unpatched
Attack surface	ASR rule activations
Threat analytics	Known threat actor / campaign overlaps
Web protection	Blocked websites
Firewall	Connection block summaries

Entra ID Protection Reports

- Risky users — users with active or remediated risk
- Risky sign-ins — events flagged by ML
- Risk detections — individual signal hits

Defender XDR Hunting

Advanced Hunting (KQL queries across all Defender signals):

```
// Find users with multiple failed sign-ins followed by success (possible spray
success)
SigninLogs
| where TimeGenerated > ago(7d)
| summarize FailureCount = countif(ResultType != 0),
           SuccessCount = countif(ResultType == 0)
           by UserPrincipalName
| where FailureCount > 50 and SuccessCount > 0
| order by FailureCount desc
```

Real-World Scenarios

Scenario: Monthly security review

Security team's monthly cadence: (1) Defender → Threat protection status — see trend down on phish (good). (2) Top targeted users — VPs at top, ensure strict policies applied. (3) Compromised users — 0 confirmed (good). (4) Vulnerable devices — 8 out-of-band patches needed, assigned to IT ops. (5) Adoption + Secure Score — review delta. Total time: 30 minutes. Outcome: prioritized actions for the month.

Summary

Section 9.4 Summary

- Defender reports cover threat protection, top targets, URL clicks.
- Defender for Endpoint: vulnerable devices, ASR, threat analytics.
- Advanced Hunting (KQL) for custom queries.
- Monthly review cadence highly effective.

9.5 Compliance Reports

Available Compliance Reports

Report	Source
Compliance score history	Purview Compliance Manager
DLP policy matches	Purview DLP
DLP false positive submissions	Purview DLP
Sensitivity label usage	Purview Information Protection
Retention policy applied items	Purview Data Lifecycle
eDiscovery case status	Purview eDiscovery
Insider risk alerts	Purview IRM
Communication compliance violations	Purview Comm Compliance
Audit search results	Purview Audit

DLP Reports Detail

Purview → DLP → Reports:

- DLP policy matches over time
- Top rules triggered
- Top sensitive types matched
- Top users triggering DLP
- Policy tip displayed / overridden / blocked

Sensitivity Label Usage

Purview → Information Protection → Reports:

- Files by label
- Sites and emails by label
- Label adoption trend
- Auto-label simulation results

Real-World Scenarios

Scenario: Audit prep

External auditor requests evidence of DLP enforcement. Steps: (1) Purview → DLP → Reports → past 12 months. (2) Export CSV: rule matches, blocked sharing events, user overrides with justification. (3) Cross-reference with audit log entries. (4) Provide to auditor with cover letter. Audit completes successfully.

Summary

Section 9.5 Summary

- Compliance reports across Purview solutions.
- DLP, labels, retention, eDiscovery, IRM all produce reports.
- Use for audits, trends, tuning.

9.6 Alert Policies

Introduction

Alert policies generate notifications when specific activities or thresholds are detected. They span M365: suspicious sign-in, malware detection, DLP rule match, external sharing, mailbox forwarding, large download volume.

Microsoft Portal Navigation

> 📍 Defender Portal → `Email & collaboration` → `Policies & rules` → `Alert policy`

(Or Purview portal for compliance-related alerts.)

Built-in Alerts

Alert	Triggers On
Creation of forwarding/redirect rule	User sets up auto-forward
Email reported by user as malware/phish	Microsoft Submission
Suspicious email forwarding activity	Pattern of forwarding
User restricted from sending email	Outbound spam protection triggered
Tenant restricted from sending email	Tenant-level spam
Elevation of Exchange admin privilege	Role assignment
Phishing/malware email detected after delivery	ZAP triggered
Unusual external user file activity	Volume spike
Unusual volume of file deletion	Possible ransomware or insider

Step-by-Step: Create Custom Alert

1. Defender → Policies → Alert policy → + New alert policy.
2. Name: "Mass file deletion".
3. Severity: High.
4. Activity: "Deleted files and folders" (SharePoint).
5. Conditions: "Activities is greater than 100 occurrences within 5 minutes by single user."
6. Recipients: security-alerts@contoso.com.
7. Threshold settings: limit alerts to 1/hour to avoid noise.
8. Status: On.
9. Save.

Alert Investigation

1. Defender → Incidents & alerts → Alerts.
2. Filter by date, severity, category.
3. Click alert → details:
    - What triggered
    - Who/what affected
    - Recommended investigation steps

4. Take action: investigate, resolve, suppress, assign to analyst.

PowerShell

```
# List alert policies
Connect-IPPSSession
Get-ProtectionAlert | Format-Table Name, Severity, Category, Disabled

# Get triggered alerts
Get-ActivityAlert | Format-Table Name, Severity
```

Real-World Scenarios

Scenario: Ransomware early warning

Custom alert: "Unusual volume of file deletion (more than 100 files in 5 minutes by single user)." Fires at 11:47 PM Sunday. SOC notified instantly. Investigation: user laptop infected; ransomware encrypting OneDrive files. Response: isolate device, restore OneDrive Files Restore to 11:30 PM, wipe and reimage laptop. 12 files affected (vs. 50,000 without alert). Saved by early detection.

Best Practices

- Tune alert thresholds — too sensitive = alert fatigue.
- Send to security distribution list, not single mailbox.
- Document response procedure per alert type.
- Suppress known false-positive patterns.
- Forward to SIEM for correlated investigation.

Summary

Section 9.6 Summary

- Alert policies notify on suspicious or critical events.
- Many built-in; custom alerts for specific scenarios.
- Tune to avoid noise.
- Integrate with SIEM for full SOC workflow.

9.7 Monitoring Best Practices

A Practical Monitoring Stack

Layer	Tool	Purpose
Tenant operational	Service Health + Message Center	Microsoft-side issues
Authentication	Sign-In Logs + Audit Logs	Identity events
Threat detection	Defender XDR	Email + Endpoint + Identity threats
Compliance	Purview Audit + Alert Policies	Policy violations, data movement
User adoption	Usage Reports + Adoption Score	Engagement, ROI
SIEM/SOAR	Microsoft Sentinel (or 3rd party)	Correlation, automation, retention

SOC Workflow Example

```
Tier 1 SOC: Defender XDR queue
     |
     v (alert triage)
Investigate: sign-in logs, audit, file activity, threat intel
     |
     v (confirmed incident)
Tier 2: response actions (block account, isolate device, etc.)
     |
     v (advanced cases)
Tier 3: forensics + advanced hunting (KQL queries)
     |
     v
Resolution + after-action review
     |
     v
Update detection rules / playbooks
```

Recommended Monthly Review Items

- Secure Score change
- Total active incidents (opened, resolved, mean time to resolve)
- Top targeted users (any new VIPs to add to Strict policies?)

- Privileged role activations (PIM)
- External sharing activity
- DLP rule matches
- Conditional Access policy changes
- Defender for Endpoint exposed devices
- Patch compliance
- License utilization

Microsoft Sentinel Integration

Sentinel (Azure-hosted SIEM) consumes M365 logs:

- Sign-in + audit logs (Entra)
- Defender for Office 365 alerts
- Defender for Endpoint alerts
- Defender for Cloud Apps
- Defender for Identity
- Office 365 activity logs

Workbooks visualize; analytics rules detect; playbooks automate response.

Summary

Section 9.7 Summary

- Build a layered monitoring stack: operational, identity, threat, compliance, adoption.
- Defender XDR + Sentinel = unified SOC platform.
- Monthly review cadence keeps everyone aligned.
- Automate response with playbooks.

Section 9 — Wrap-Up

Section 9 Synthesis

- **Service Health** + **Message Center**: Microsoft-side news.
- **Usage Reports**: adoption analytics; Adoption Score for benchmarking.
- **Sign-In Logs**: every authentication; 4 types.
- **Audit Logs**: admin actions.
- **AADSTS error codes**: structured failure reasons.
- **Defender reports**: threat trends, top targets, compromised users.
- **Compliance reports**: DLP, labels, retention, eDiscovery.

- **Alert policies**: notify on suspicious or critical events.
- **Sentinel**: SIEM for correlation, automation.

Section 9 Mini-Quiz

Q1. Where do you check current tenant service status?

A: M365 Admin Center → Health → Service health

Q2. How long does Entra retain sign-in logs by default (P1)?

A: 30 days

Q3. Which error code indicates Conditional Access blocked the sign-in?

A: AADSTS53003

Q4. What does Adoption Score compare you to?

A: Organizations of similar size and industry

Q5. Where do you find Service Principal sign-in logs?

A: Entra Admin Center → Monitoring → Sign-in logs → Service principal sign-ins tab

Q6. What's KQL?

A: Kusto Query Language — used in Defender Advanced Hunting and Sentinel for log queries

Q7. To retain Entra logs longer than 30 days, where do you send them?

A: Diagnostic settings → Log Analytics workspace + Storage account + Event Hub (Sentinel)

Q8. What's the recommended response when ransomware is suspected on a managed device?

A: Isolate device via Defender for Endpoint; restore from OneDrive Files Restore; reimage

Q9. How do you forward Message Center posts to a wider audience?

A: Admin Center → Message center → Preferences → email digest to distribution list

Q10. What does Microsoft Sentinel add to M365 monitoring?

A: SIEM/SOAR: cross-source correlation, long-term retention, workbooks, analytics rules, playbooks for automation

Section 10
10
PowerShell for Microsoft 365
The admin's universal automation language. From single user creation to massive multi-thousand-user operations, PowerShell makes you 100× faster than the GUI. Master the modules that touch every M365 workload.
Exam Weight: ~10%

10.1 PowerShell Modules for M365

Introduction

Microsoft 365 administration via PowerShell uses multiple modules, each connecting to a specific service. Modern administration centers on Microsoft Graph PowerShell SDK (the future) while legacy modules (MSOnline, AzureAD, AzureADPreview) are deprecated but still in use.

Module Overview

Module	Service	Status
Microsoft.Graph	Entra ID, Intune, Teams, M365 broadly	Current/preferred
ExchangeOnlineManagement	Exchange Online + Security & Compliance Center	Current
MicrosoftTeams	Teams policies, voice, devices	Current
Microsoft.Online.SharePoint.PowerShell	SharePoint Online	Current
PnP.PowerShell	SharePoint Online (community module, broader functionality)	Current (community)
MSOnline	Legacy Azure AD (cmdlets like Get-MsolUser)	Deprecated; retiring
AzureAD	Legacy Azure AD v2 (Get-AzureADUser)	Deprecated; retiring
AzureADPreview	Preview features	Deprecated
Az	Azure resources (not M365 specifically)	Current

Microsoft Direction
Microsoft has been retiring MSOnline + AzureAD modules in favour of Microsoft Graph PowerShell. New scripts should use Microsoft.Graph; existing scripts should be migrated. Some MSOnline functionality remains for things like federated domain conversion until parity is reached.

PowerShell Version

Version	Status
Windows PowerShell 5.1	Built into Windows; sufficient for most modules
PowerShell 7+	Cross-platform (Windows/macOS/Linux); recommended; faster

Install Modules

```
# Install for current user (no admin rights needed)
Install-Module Microsoft.Graph -Scope CurrentUser
Install-Module ExchangeOnlineManagement -Scope CurrentUser
Install-Module MicrosoftTeams -Scope CurrentUser
Install-Module Microsoft.Online.SharePoint.PowerShell -Scope CurrentUser
Install-Module PnP.PowerShell -Scope CurrentUser

# Verify
Get-Module -ListAvailable Microsoft.Graph*, ExchangeOnlineManagement, MicrosoftTeams
|
    Select-Object Name, Version

# Update (run periodically)
Update-Module Microsoft.Graph
Update-Module ExchangeOnlineManagement
```

Connection Patterns

```
# Microsoft Graph
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"

# Exchange Online
Connect-ExchangeOnline -UserPrincipalName admin@contoso.com

# Security & Compliance Center (Purview)
Connect-IPPSSession -UserPrincipalName admin@contoso.com

# SharePoint Online
Connect-SPOService -Url https://contoso-admin.sharepoint.com

# Microsoft Teams
Connect-MicrosoftTeams

# Disconnect
Disconnect-MgGraph
Disconnect-ExchangeOnline -Confirm:$false
```

Authentication Methods

Method	Use
Interactive (browser)	Manual admin tasks; MFA supported
Device code	Headless / VDI scenarios
Certificate	Automation (scheduled scripts, Azure Automation)
Managed Identity	From Azure resources (Functions, VMs)
Client secret (deprecated)	Avoid; use certificate

Microsoft Graph Permission Scopes

Scope	Allows
User.Read.All	Read all user info
User.ReadWrite.All	Read + modify users
Group.Read.All	Read groups
Group.ReadWrite.All	Read + modify groups
Directory.Read.All	Read directory
Directory.ReadWrite.All	Full directory write
DeviceManagementManagedDevices.Read.All	Read Intune devices
DeviceManagementConfiguration.ReadWrite.All	Modify Intune configs
Policy.Read.All	Read CA policies, etc.
Policy.ReadWrite.ConditionalAccess	Modify CA policies
AuditLog.Read.All	Audit logs
Reports.Read.All	Usage reports

Best Practices

- Always run latest module versions.
- Use Microsoft.Graph for new scripts; migrate old MSOnline/AzureAD scripts.

- Use certificate auth for automation (no passwords in scripts).
- Request minimum scopes needed.
- Disconnect when done — frees session.
- Use try/catch for error handling.
- Add comments + version headers in scripts.

Summary

Section 10.1 Summary

- 5 main modules: Microsoft.Graph, ExchangeOnlineManagement, MicrosoftTeams, SPO, PnP.
- MSOnline + AzureAD = deprecated; migrate to Microsoft.Graph.
- Connect-* cmdlet per module.
- Certificate auth for automation.
- Request minimum Graph scopes.

10.2 User Management Scripts

Create a User (Microsoft Graph)

```
Connect-MgGraph -Scopes "User.ReadWrite.All"

$PasswordProfile = @{
    Password = "TempP@ssw0rd123!"
    ForceChangePasswordNextSignIn = $true
}

New-MgUser `
    -DisplayName "Sara Khan" `
    -GivenName "Sara" `
    -Surname "Khan" `
    -UserPrincipalName "sara.khan@contoso.com" `
    -MailNickname "sara.khan" `
    -AccountEnabled `
    -PasswordProfile $PasswordProfile `
    -UsageLocation "PK" `
    -JobTitle "Marketing Manager" `
    -Department "Marketing"
```

Bulk Create from CSV

```
# CSV: DisplayName,GivenName,Surname,UPN,Title,Department,UsageLocation
$users = Import-Csv "new_hires.csv"
$results = @()

foreach ($u in $users) {
    try {
        $pwd = @{
            Password = "TempPw" + (Get-Random -Min 1000 -Max 9999) + "!"
            ForceChangePasswordNextSignIn = $true
        }

        $newUser = New-MgUser `
            -DisplayName $u.DisplayName `
            -GivenName $u.GivenName `
            -Surname $u.Surname `
            -UserPrincipalName $u.UPN `
            -MailNickname ($u.UPN.Split('@')[0]) `
            -AccountEnabled `
            -PasswordProfile $pwd `
            -UsageLocation $u.UsageLocation `
            -JobTitle $u.Title `
            -Department $u.Department

        $results += [PSCustomObject]@{
            UPN = $newUser.UserPrincipalName
            Status = "Created"
            TempPassword = $pwd.Password
        }
    } catch {
        $results += [PSCustomObject]@{
            UPN = $u.UPN
            Status = "Failed: $($_.Exception.Message)"
            TempPassword = ""
        }
    }
}

$results | Export-Csv "creation_results.csv" -NoTypeInformation
$results | Format-Table
```

Update User Properties

```
# Update a single property
Update-MgUser -UserId "sara.khan@contoso.com" -JobTitle "Director of Marketing"

# Multiple at once
Update-MgUser -UserId "sara.khan@contoso.com" `
    -Department "Executive" `
    -JobTitle "VP Marketing" `
    -OfficeLocation "HQ-Karachi-Floor30"

# Set manager
$manager = Get-MgUser -UserId "ceo@contoso.com"
Set-MgUserManagerByRef -UserId "sara.khan@contoso.com" `
    -BodyParameter @{"@odata.id" = "https://graph.microsoft.com/v1.0/users/$
($manager.Id)"}
```

Find and Filter Users

```
# All enabled users
Get-MgUser -All -Filter "accountEnabled eq true"

# Users in a department
Get-MgUser -Filter "department eq 'Sales'"

# Users created in last 30 days
$cutoff = (Get-Date).AddDays(-30).ToString("yyyy-MM-ddTHH:mm:ssZ")
Get-MgUser -All -Filter "createdDateTime ge $cutoff" `
    -Property DisplayName, UserPrincipalName, CreatedDateTime

# Users without MFA registered
Get-MgReportAuthenticationMethodUserRegistrationDetail -All |
    Where-Object { -not $_.IsMfaRegistered } |
    Select-Object UserPrincipalName

# Users not signed in in 90 days (P1+ required for sign-in data)
$cutoff = (Get-Date).AddDays(-90)
Get-MgUser -All -Property SignInActivity, DisplayName, UserPrincipalName |
    Where-Object { $_.SignInActivity.LastSignInDateTime -lt $cutoff -or
$_.SignInActivity.LastSignInDateTime -eq $null } |
    Select-Object DisplayName, UserPrincipalName,
        @{Name="LastSignIn";Expression={$_.SignInActivity.LastSignInDateTime}}
```

Disable / Delete / Restore Users

```
# Disable
Update-MgUser -UserId "departing@contoso.com" -AccountEnabled:$false

# Revoke all sessions (force re-auth or block)
Revoke-MgUserSignInSession -UserId "departing@contoso.com"

# Delete (goes to recycle bin for 30 days)
Remove-MgUser -UserId "departing@contoso.com"

# List deleted users
Get-MgDirectoryDeletedItemAsUser

# Restore deleted user
$deletedUser = Get-MgDirectoryDeletedItemAsUser |
    Where-Object { $_.UserPrincipalName -eq "departing@contoso.com" }
Restore-MgDirectoryDeletedItem -DirectoryObjectId $deletedUser.Id

# Permanently delete (purge from recycle bin)
Remove-MgDirectoryDeletedItem -DirectoryObjectId $deletedUser.Id
```

License Assignment

```
# Get available SKUs
Get-MgSubscribedSku | Select-Object SkuPartNumber, SkuId,
    @{Name="Active";Expression={$_.PrepaidUnits.Enabled}},
    @{Name="Consumed";Expression={$_.ConsumedUnits}}

# Sample SkuPartNumber values:
# SPE_E3 = Microsoft 365 E3
# SPE_E5 = Microsoft 365 E5
# ENTERPRISEPACK = Office 365 E3
# ENTERPRISEPREMIUM = Office 365 E5

# Assign license to a user
$sku = Get-MgSubscribedSku | Where-Object { $_.SkuPartNumber -eq "SPE_E3" }
Set-MgUserLicense -UserId "sara.khan@contoso.com" `
    -AddLicenses @(@{SkuId = $sku.SkuId}) `
    -RemoveLicenses @()

# Remove license
Set-MgUserLicense -UserId "sara.khan@contoso.com" `
    -AddLicenses @() `
    -RemoveLicenses @($sku.SkuId)

# Bulk assign license to a group of users
$users = Get-MgUser -All -Filter "department eq 'Sales'"
foreach ($u in $users) {
    Set-MgUserLicense -UserId $u.Id `
        -AddLicenses @(@{SkuId = $sku.SkuId}) `
        -RemoveLicenses @()
}

# Group-based licensing (preferred)
$group = Get-MgGroup -Filter "displayName eq 'Lic-M365-E3'"
Set-MgGroupLicense -GroupId $group.Id `
    -AddLicenses @(@{SkuId = $sku.SkuId; DisabledPlans = @()}) `
    -RemoveLicenses @()
```

Summary

Section 10.2 Summary

- Microsoft.Graph cmdlets: New/Get/Update/Remove-MgUser.
- Bulk operations via CSV import + foreach.
- License assignment by SKU GUID.
- Group-based licensing for scale.

10.3 Group Management Scripts

Create Groups

```
# Security Group
New-MgGroup `
    -DisplayName "Lic-M365-E3" `
    -MailEnabled:$false `
    -MailNickname "lic-m365-e3" `
    -SecurityEnabled

# Microsoft 365 Group
New-MgGroup `
    -DisplayName "Sales-Team" `
    -MailEnabled:$true `
    -MailNickname "sales-team" `
    -SecurityEnabled:$false `
    -GroupTypes @("Unified") `
    -Description "Sales department collaboration"

# Dynamic Group (P1 required)
New-MgGroup `
    -DisplayName "All Sales Dynamic" `
    -MailEnabled:$false `
    -MailNickname "all-sales-dyn" `
    -SecurityEnabled `
    -GroupTypes @("DynamicMembership") `
    -MembershipRule '(user.department -eq "Sales")' `
    -MembershipRuleProcessingState "On"

# Dynamic Microsoft 365 Group
New-MgGroup `
    -DisplayName "Engineering" `
    -MailEnabled:$true `
    -MailNickname "engineering" `
    -SecurityEnabled:$false `
    -GroupTypes @("Unified","DynamicMembership") `
    -MembershipRule '(user.department -eq "Engineering")' `
    -MembershipRuleProcessingState "On"
```

Manage Membership

```
# Add member
$group = Get-MgGroup -Filter "displayName eq 'Sales-Team'"
$user = Get-MgUser -UserId "alice@contoso.com"
New-MgGroupMember -GroupId $group.Id -DirectoryObjectId $user.Id

# Add multiple from list
$members = @("alice@contoso.com", "bob@contoso.com", "carol@contoso.com")
foreach ($email in $members) {
    $u = Get-MgUser -UserId $email
    try {
        New-MgGroupMember -GroupId $group.Id -DirectoryObjectId $u.Id
        Write-Host "Added $email"
    } catch {
        Write-Host "Failed $email : $($_.Exception.Message)"
    }
}

# Get members
Get-MgGroupMember -GroupId $group.Id -All |
    ForEach-Object { Get-MgUser -UserId $_.Id } |
    Select-Object DisplayName, UserPrincipalName

# Add owner
New-MgGroupOwner -GroupId $group.Id -DirectoryObjectId $user.Id

# Remove member
Remove-MgGroupMemberByRef -GroupId $group.Id -DirectoryObjectId $user.Id
```

Find Empty / Orphan Groups

```
# Groups with no members
Get-MgGroup -All | ForEach-Object {
    $count = (Get-MgGroupMember -GroupId $_.Id -All).Count
    if ($count -eq 0) {
        [PSCustomObject]@{
            DisplayName = $_.DisplayName
            Id = $_.Id
            Created = $_.CreatedDateTime
        }
    }
} | Format-Table

# Groups with no owners (orphaned)
Get-MgGroup -All | ForEach-Object {
    $owners = (Get-MgGroupOwner -GroupId $_.Id -All).Count
    if ($owners -eq 0) {
        [PSCustomObject]@{
            DisplayName = $_.DisplayName
            Id = $_.Id
        }
    }
} | Format-Table
```

Summary

Section 10.3 Summary

- New/Get/Remove-MgGroup, MgGroupMember, MgGroupOwner.
- Dynamic groups via -GroupTypes "DynamicMembership" + rule.
- Audit empty/orphan groups periodically.

10.4 Exchange Online Scripts

Mailbox Operations

```
Connect-ExchangeOnline

# Get mailbox info
Get-Mailbox -Identity "alice@contoso.com" | Format-List

# Get mailbox size
Get-MailboxStatistics -Identity "alice@contoso.com" |
    Select-Object DisplayName, TotalItemSize, ItemCount, LastLogonTime

# All mailboxes > 50 GB
Get-Mailbox -ResultSize Unlimited |
    Get-MailboxStatistics |
    Where-Object { $_.TotalItemSize.Value.ToGB() -gt 50 } |
    Sort-Object @{Expression={$_.TotalItemSize.Value};Descending=$true} |
    Select-Object DisplayName, TotalItemSize, ItemCount

# Convert to shared mailbox (after employee leaves)
Set-Mailbox -Identity "departed@contoso.com" -Type Shared

# Enable archive
Enable-Mailbox -Identity "alice@contoso.com" -Archive

# Litigation hold (7 years)
Set-Mailbox -Identity "executive@contoso.com" `
    -LitigationHoldEnabled $true `
    -LitigationHoldDuration 2555

# Disable auto-forwarding to external addresses (security)
Set-RemoteDomain Default -AutoForwardEnabled $false

# Find users with external forwarding
Get-Mailbox -ResultSize Unlimited |
    Where-Object { $_.ForwardingSmtpAddress -ne $null } |
    Select-Object DisplayName, UserPrincipalName, ForwardingSmtpAddress,
DeliverToMailboxAndForward
```

Permissions Management

```
# Grant Full Access
Add-MailboxPermission -Identity "shared@contoso.com" `
    -User "alice@contoso.com" `
    -AccessRights FullAccess `
    -InheritanceType All `
    -AutoMapping $true

# Grant Send As
Add-RecipientPermission -Identity "shared@contoso.com" `
    -Trustee "alice@contoso.com" `
    -AccessRights SendAs

# Find who has access to a mailbox
Get-MailboxPermission -Identity "shared@contoso.com" |
    Where-Object { $_.User.ToString() -notlike "NT AUTHORITY*" -and
$_.User.ToString() -notlike "S-1-5-21*" } |
    Select-Object User, AccessRights

# Audit all FullAccess permissions in tenant (security review)
Get-Mailbox -ResultSize Unlimited | ForEach-Object {
    $mbx = $_
    Get-MailboxPermission -Identity $mbx.Identity |
        Where-Object {
            $_.User.ToString() -notlike "NT AUTHORITY*" -and
            $_.User.ToString() -notlike "S-1-5-21*" -and
            $_.AccessRights -contains "FullAccess" -and
            $_.IsInherited -eq $false
        } |
        Select-Object @{Name="Mailbox";Expression={$mbx.UserPrincipalName}},
                      @{Name="DelegatedTo";Expression={$_.User}},
                      AccessRights
} | Export-Csv "mailbox_permissions_audit.csv" -NoTypeInformation
```

Distribution Groups

```
# Create DL
New-DistributionGroup -Name "AllEmployees" -DisplayName "All Employees" `
    -PrimarySmtpAddress "all@contoso.com" `
    -Type Distribution

# Restrict to internal senders
Set-DistributionGroup -Identity "AllEmployees" `
    -RequireSenderAuthenticationEnabled $true `
    -AcceptMessagesOnlyFromSendersOrMembers "executives@contoso.com"

# Add members
Add-DistributionGroupMember -Identity "AllEmployees" -Member "alice@contoso.com"

# Bulk add via CSV
Import-Csv "members.csv" | ForEach-Object {
    Add-DistributionGroupMember -Identity "AllEmployees" -Member $_.UPN
}

# Dynamic DL
New-DynamicDistributionGroup -Name "DD-AllSales" `
    -DisplayName "All Sales" `
    -PrimarySmtpAddress "allsales@contoso.com" `
    -IncludedRecipients "MailboxUsers" `
    -ConditionalDepartment "Sales"
```

Mail Flow / Transport Rules

```
# List all transport rules
Get-TransportRule | Select-Object Name, State, Mode, Priority

# Create external email warning rule
$banner = '<div style="background:#FFF3CD;border:1px solid #FFC107;padding:10px;">⚠️
External Sender: Verify before clicking links.</div>'
New-TransportRule -Name "External Warning" `
    -FromScope NotInOrganization `
    -ApplyHtmlDisclaimerLocation Prepend `
    -ApplyHtmlDisclaimerText $banner `
    -ApplyHtmlDisclaimerFallbackAction Wrap `
    -SetHeaderName "X-ExternalWarning" -SetHeaderValue "Applied"

# Backup all transport rules to JSON
Get-TransportRule | ConvertTo-Json -Depth 10 |
    Out-File "transport_rules_backup_$(Get-Date -Format 'yyyy-MM-dd').json"
```

Anti-Phishing & Safe Links

```
# Configure default anti-phishing policy
Set-AntiPhishPolicy -Identity "Office365 AntiPhish Default" `
    -EnableTargetedUserProtection $true `
    -TargetedUsersToProtect @{Add="CEO Name;ceo@contoso.com","CFO
Name;cfo@contoso.com"} `
    -EnableTargetedDomainsProtection $true `
    -TargetedDomainsToProtect @{Add="contoso.com"} `
    -TargetedUserProtectionAction Quarantine `
    -PhishThresholdLevel 3 `
    -EnableMailboxIntelligence $true `
    -EnableFirstContactSafetyTips $true

# Safe Links policy
New-SafeLinksPolicy -Name "AllUsers-SafeLinks" `
    -EnableSafeLinksForEmail $true `
    -EnableSafeLinksForTeams $true `
    -EnableSafeLinksForOffice $true `
    -ScanUrls $true `
    -DeliverMessageAfterScan $true `
    -EnableForInternalSenders $true `
    -TrackClicks $true `
    -AllowClickThrough $false

New-SafeLinksRule -Name "AllUsers-SafeLinks-Rule" `
    -SafeLinksPolicy "AllUsers-SafeLinks" `
    -SentToMemberOf "all-employees@contoso.com" `
    -Priority 0
```

Summary

Section 10.4 Summary

- Connect-ExchangeOnline for EXO; Connect-IPPSSession for Purview.
- Get/Set-Mailbox + permission cmdlets.
- Audit external forwarding and FullAccess regularly.
- Transport rules via Get/New/Set-TransportRule.
- Defender policies via Set-AntiPhishPolicy, New-SafeLinksPolicy, etc.

10.5 Teams Administration Scripts

Common Teams Operations

```
Connect-MicrosoftTeams

# List all Teams
Get-Team | Select-Object DisplayName, MailNickName, Visibility, GroupId

# Get team members
Get-TeamUser -GroupId $teamId

# Add user to team
Add-TeamUser -GroupId $teamId -User "alice@contoso.com" -Role Member
Add-TeamUser -GroupId $teamId -User "bob@contoso.com" -Role Owner

# Remove user from team
Remove-TeamUser -GroupId $teamId -User "departed@contoso.com"

# Create a team
$team = New-Team -DisplayName "Project Alpha" `
    -Description "Cross-functional project team" `
    -Visibility Private `
    -Owner "pm@contoso.com"

# Add channels
New-TeamChannel -GroupId $team.GroupId -DisplayName "Engineering"
New-TeamChannel -GroupId $team.GroupId -DisplayName "Design"

# Private channel
New-TeamChannel -GroupId $team.GroupId -DisplayName "Leadership" `
    -MembershipType Private
```

Teams Policies

```
# List policies
Get-CsTeamsMeetingPolicy
Get-CsTeamsMessagingPolicy
Get-CsTeamsAppPermissionPolicy
Get-CsTeamsCallingPolicy

# Create meeting policy
New-CsTeamsMeetingPolicy -Identity "Restricted-Meeting" `
    -AllowCloudRecording $false `
    -AllowTranscription $false `
    -AllowAnonymousUsersToJoinMeeting $false `
    -ScreenSharingMode "SingleApplication" `
    -AllowParticipantGiveRequestControl $false

# Assign policy to user
Grant-CsTeamsMeetingPolicy -Identity "alice@contoso.com" -PolicyName "Restricted-
Meeting"

# Assign policy to group
New-CsGroupPolicyAssignment `
    -GroupId "group-guid-here" `
    -PolicyType "TeamsMeetingPolicy" `
    -PolicyName "Restricted-Meeting" `
    -Rank 1

# Remove policy from user (reverts to Global)
Grant-CsTeamsMeetingPolicy -Identity "alice@contoso.com" -PolicyName $null
```

External & Guest Access

```
# Federation settings
Get-CsTenantFederationConfiguration
Set-CsTenantFederationConfiguration `
    -AllowFederatedUsers $true `
    -AllowPublicUsers $false `
    -AllowedDomains @{Add="partner1.com","partner2.com"}

# Guest access (in TAC, also via PowerShell)
Set-CsTeamsClientConfiguration -Identity Global -AllowGuestUser $true
Set-CsTeamsGuestMeetingConfiguration -Identity Global `
    -AllowIPVideo $true `
    -ScreenSharingMode "EntireScreen"
```

Teams Voice (Phone)

```
# List phone numbers
Get-CsPhoneNumberAssignment

# Assign phone number to user
Set-CsPhoneNumberAssignment -Identity "alice@contoso.com" `
    -PhoneNumber "+12025551234" `
    -PhoneNumberType CallingPlan

# Configure user calling policy
Grant-CsTeamsCallingPolicy -Identity "alice@contoso.com" `
    -PolicyName "AllowCalling"

# Dial plan
Get-CsTenantDialPlan
```

Summary

Section 10.5 Summary

- MicrosoftTeams module: Get/New/Add-TeamUser, Get/New-TeamChannel.
- Policy cmdlets: Get/New/Grant-Cs*Policy.
- Federation + guest via Set-CsTenantFederationConfiguration.
- Phone number assignment via Set-CsPhoneNumberAssignment.

10.6 SharePoint Online Scripts

Site Management

```
Connect-SPOService -Url https://contoso-admin.sharepoint.com

# List all sites
Get-SPOSite -Limit All |
    Select-Object Url, Owner, Template, StorageUsageCurrent, StorageQuota

# Create Communication site
New-SPOSite -Url "https://contoso.sharepoint.com/sites/news" `
    -Owner "admin@contoso.com" `
    -StorageQuota 5120 `
    -Template "SITEPAGEPUBLISHING#0" `
    -Title "Company News"

# Set storage limit
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/news" `
    -StorageQuota 10240 -StorageQuotaWarningLevel 9216

# Delete site
Remove-SPOSite -Identity "https://contoso.sharepoint.com/sites/old" -NoWait

# Restore deleted
Restore-SPODeletedSite -Identity "https://contoso.sharepoint.com/sites/old"
```

OneDrive Management

```
# List OneDrive sites
Get-SPOSite -IncludePersonalSite $true -Limit All `
    -Filter "Url -like '*-my.sharepoint.com/personal*'" |
    Select-Object Url, Owner, StorageUsageCurrent, StorageQuota

# Pre-provision OneDrive
Request-SPOPersonalSite -UserEmails @("new1@contoso.com","new2@contoso.com")

# Grant access to departed user's OneDrive
Set-SPOUser -Site "https://contoso-my.sharepoint.com/personal/departed_contoso_com"
`
    -LoginName "manager@contoso.com" `
    -IsSiteCollectionAdmin $true

# Set OneDrive retention after user deletion
Set-SPOTenant -OrphanedPersonalSitesRetentionPeriod 180
```

Sharing Settings

```
# Tenant-wide sharing
Set-SPOTenant `
    -SharingCapability "ExternalUserSharingOnly" `
    -RequireAcceptingAccountMatchInvitedAccount $true `
    -RequireAnonymousLinksExpireInDays 30 `
    -DefaultSharingLinkType "Internal" `
    -PreventExternalUsersFromResharing $true

# Per-site sharing
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/HR" `
    -SharingCapability "Disabled"

# Restrict by domain
Set-SPOTenant `
    -SharingDomainRestrictionMode "AllowList" `
    -SharingAllowedDomainList "partner1.com partner2.com"
```

Summary

Section 10.6 Summary

- Connect-SPOService for SPO admin.
- Get/New/Set-SPOSite for site management.
- Set-SPOTenant for tenant-wide sharing.
- Request-SPOPersonalSite for pre-provisioning OneDrive.

10.7 Reporting and Automation Scripts

Comprehensive User Report

```
Connect-MgGraph -Scopes "User.Read.All","AuditLog.Read.All"

$users = Get-MgUser -All -Property DisplayName, UserPrincipalName, AccountEnabled,
    CreatedDateTime, Department, JobTitle, AssignedLicenses, SignInActivity

$report = $users | ForEach-Object {
    [PSCustomObject]@{
        DisplayName = $_.DisplayName
        UPN = $_.UserPrincipalName
        Enabled = $_.AccountEnabled
        Created = $_.CreatedDateTime
        Department = $_.Department
        JobTitle = $_.JobTitle
        LicenseCount = $_.AssignedLicenses.Count
        LastSignIn = $_.SignInActivity.LastSignInDateTime
        LastNonInteractive = $_.SignInActivity.LastNonInteractiveSignInDateTime
    }
}

$report | Export-Csv "user_full_report_$(Get-Date -Format 'yyyy-MM-dd').csv" -
NoTypeInformation
```

License Utilization Report

```
Get-MgSubscribedSku |
    Select-Object SkuPartNumber,
        @{Name="Total";Expression={$_.PrepaidUnits.Enabled}},
        @{Name="Consumed";Expression={$_.ConsumedUnits}},
        @{Name="Available";Expression={$_.PrepaidUnits.Enabled - $_.ConsumedUnits}},
        @{Name="UtilizationPct";Expression={
            [math]::Round(($_.ConsumedUnits / $_.PrepaidUnits.Enabled) * 100, 1)
        }} |
    Sort-Object Consumed -Descending |
    Format-Table
```

External Sharing Audit

```
Connect-IPPSSession

$startDate = (Get-Date).AddDays(-30)
$endDate = Get-Date

Search-UnifiedAuditLog -StartDate $startDate -EndDate $endDate `
    -Operations AnonymousLinkCreated,CompanyLinkCreated,SharingSet,AddedToSecureLink
`
    -ResultSize 5000 |
    Select-Object CreationDate, UserIds, Operations, ObjectId, AuditData |
    Export-Csv "external_sharing_audit.csv" -NoTypeInformation
```

MFA Status Report

```
Connect-MgGraph -Scopes "AuditLog.Read.All","UserAuthenticationMethod.Read.All"

Get-MgReportAuthenticationMethodUserRegistrationDetail -All |
    Select-Object UserPrincipalName, IsMfaRegistered, IsMfaCapable,
        IsSsprRegistered, DefaultMfaMethod |
    Export-Csv "mfa_status.csv" -NoTypeInformation

# Count by status
$all = Get-MgReportAuthenticationMethodUserRegistrationDetail -All

"Total users: $($all.Count)"
"MFA registered: $($all | Where-Object { $_.IsMfaRegistered } | Measure-Object |
Select-Object -ExpandProperty Count)"
"MFA NOT registered: $($all | Where-Object { -not $_.IsMfaRegistered } | Measure-
Object | Select-Object -ExpandProperty Count)"
```

Stale User Detection

```
# Users not signed in 90 days — candidates for license reclamation
$cutoff = (Get-Date).AddDays(-90)
$stale = Get-MgUser -All -Property DisplayName, UserPrincipalName, SignInActivity,
AssignedLicenses |
    Where-Object {
        $_.SignInActivity.LastSignInDateTime -lt $cutoff -and
        $_.AssignedLicenses.Count -gt 0
    }

$stale |
    Select-Object DisplayName, UserPrincipalName,
        @{Name="LastSignIn";Expression={$_.SignInActivity.LastSignInDateTime}},
        @{Name="LicenseCount";Expression={$_.AssignedLicenses.Count}} |
    Export-Csv "stale_users.csv" -NoTypeInformation

Write-Host "Found $($stale.Count) stale users with licenses."
```

Scheduled Automation via Azure Automation

For unattended scheduled scripts (e.g., daily license report, weekly stale user check):

1. Create Azure Automation account.
2. Create an App Registration in Entra; generate self-signed certificate.
3. Upload certificate to Azure Automation (Certificates).
4. Grant App Registration Graph API permissions.
5. Create runbook (PowerShell 7.2+).
6. Use Connect-MgGraph with certificate thumbprint + Tenant ID + Client ID.
7. Schedule daily/weekly.

```
# Cert-based auth from automation
Connect-MgGraph `
    -ClientId "your-app-id" `
    -TenantId "your-tenant-id" `
    -CertificateThumbprint "thumbprint"

# Run script...

Disconnect-MgGraph
```

Summary

Section 10.7 Summary

- Reporting scripts pull from Graph, Audit, Reports APIs.
- Combine multiple data sources for comprehensive views.
- Schedule via Azure Automation with certificate auth.
- Export CSV for consumption / further analysis.

10.8 PowerShell Best Practices

Script Structure

```
<#
.SYNOPSIS
    Brief description.

.DESCRIPTION
    Detailed description.

.PARAMETER ParamName
    Description of parameter.

.EXAMPLE
    .\script.ps1 -ParamName "value"

.NOTES
    Author: Haroon Ejaz
    Version: 1.0
    Date: 2026-01-15
#>

[CmdletBinding()]
param(
    [Parameter(Mandatory=$true)]
    [string]$InputFile,

    [Parameter(Mandatory=$false)]
    [switch]$WhatIf
)

# Requires version
#Requires -Version 7
#Requires -Modules Microsoft.Graph

# Connect
try {
    Connect-MgGraph -Scopes "User.ReadWrite.All" -NoWelcome -ErrorAction Stop
} catch {
    Write-Error "Failed to connect to Graph: $_"
    exit 1
}

# Main logic
try {
    $items = Import-Csv -Path $InputFile -ErrorAction Stop

    foreach ($item in $items) {
        if ($WhatIf) {
            Write-Host "Would process: $($item.UPN)"
        } else {
            # actual operation
            Write-Host "Processing: $($item.UPN)"
        }
    }
```

```
} catch {
    Write-Error "Error: $_"
} finally {
    Disconnect-MgGraph
}
```

Error Handling Patterns

```
# Try/Catch with details
try {
    Update-MgUser -UserId $upn -JobTitle "Manager" -ErrorAction Stop
    Write-Host "Updated: $upn"
} catch {
    Write-Host "Failed $upn : $($_.Exception.Message)" -ForegroundColor Red
    $errors += $upn
}

# Set ErrorAction globally
$ErrorActionPreference = "Stop"

# Common gotchas:
# - Get-* cmdlets sometimes return $null silently if not found; check before using
# - Always test in -WhatIf or pilot scope first
```

Performance Patterns

```
# Use -All instead of -ResultSize Unlimited (Graph)
Get-MgUser -All  # preferred

# Use -Filter where possible (server-side filter is faster than client-side)
Get-MgUser -Filter "department eq 'Sales'"  # server-side
Get-MgUser -All | Where-Object { $_.Department -eq "Sales" }  # client-side (slow)

# Use -Property to select only needed fields
Get-MgUser -All -Property Id, DisplayName, UserPrincipalName

# Avoid putting Get-MgUser inside a loop calling Get-MgUser; cache
$allUsers = Get-MgUser -All  # once
foreach ($u in $allUsers) { ... }  # operates on cached list
```

Security Best Practices

- NEVER hardcode passwords or secrets in scripts.
- Use SecureString or Azure Key Vault for sensitive data.
- Prefer certificate authentication over client secrets.

- Minimum Graph permissions per script.
- Audit script execution — log all changes.
- Disconnect at the end of scripts to release sessions.
- Sign scripts in production (Set-AuthenticodeSignature).

Common Mistakes

Mistake	Fix
Not handling pagination	Use -All flag
No error handling	Wrap in try/catch
Tested on prod first time	Run in pilot tenant or -WhatIf mode
No logging	Use Write-Host or Start-Transcript
Hardcoded values	Use parameters
Running with too many permissions	Request only needed scopes
Mixing modules (Graph + MSOnline) inconsistently	Stick with Graph; migrate legacy

Summary

Section 10.8 Summary

- Structure: comment-based help + param block + try/catch + cleanup.
- Use -Filter and -Property for performance.
- Cache results; avoid nested API calls.
- Never hardcode secrets — use cert auth or Key Vault.
- Test with -WhatIf or in pilot tenant.

Section 10 — Wrap-Up

Section 10 Synthesis

- **Modules**: Microsoft.Graph, ExchangeOnlineManagement, MicrosoftTeams, SharePoint, PnP.
- **Legacy**: MSOnline, AzureAD — deprecated, migrate to Graph.
- **Users**: Get/New/Update/Remove-MgUser; license via Set-MgUserLicense.
- **Groups**: Get/New-MgGroup; dynamic via -GroupTypes.
- **Exchange**: Get/Set-Mailbox, Add-MailboxPermission, transport rules.

- **Teams**: Get/New-Team, Cs* policy cmdlets.
- **SharePoint**: Get/New/Set-SPOSite, Set-SPOTenant.
- **Reporting**: combine Graph + Audit + Reports for comprehensive output.
- **Automation**: Azure Automation + certificate auth.
- **Best Practices**: try/catch, -Filter server-side, minimum permissions, no hardcoded secrets.

Section 10 Mini-Quiz

Q1. Which PowerShell module is Microsoft's recommended replacement for MSOnline?

A: Microsoft Graph PowerShell SDK (Microsoft.Graph module)

Q2. Cmdlet to connect to Exchange Online?

A: Connect-ExchangeOnline

Q3. Cmdlet to connect to Security & Compliance Center (Purview)?

A: Connect-IPPSSession

Q4. How do you create a dynamic security group via Graph?

A: New-MgGroup -GroupTypes @("DynamicMembership") -MembershipRule "..."

Q5. Cmdlet to assign a phone number for Teams calling?

A: Set-CsPhoneNumberAssignment

Q6. What's the difference between -Filter and Where-Object?

A: -Filter executes server-side (much faster); Where-Object filters client-side after downloading all results

Q7. How do you bulk-assign a policy in Teams to a group?

A: New-CsGroupPolicyAssignment -GroupId X -PolicyType Y -PolicyName Z

Q8. How would you find users without MFA registered via PowerShell?

A: Get-MgReportAuthenticationMethodUserRegistrationDetail -All | Where-Object { -not $_.IsMfaRegistered }

Q9. Best authentication method for unattended automation scripts?

A: Certificate-based authentication via App Registration (not client secret)

Q10. Recommended approach when running a script on production for the first time?

A: Test in pilot tenant or use -WhatIf if available; pilot to small scope; review logs; expand gradually

Final

★

Exam Prep & Reference Appendix

Everything you need for the final stretch: study plan, lab checklist, PowerShell & portal cheat sheets, common mistakes, mock interview questions, and the real-world admin checklist you'll use on day one.

Your Last 30 Days

MS-102 Exam Preparation Strategy

Exam Overview

Aspect	Detail
Exam code	MS-102
Title	Microsoft 365 Administrator
Format	40–60 questions (multiple choice, drag-drop, case studies)
Duration	~120 minutes
Passing score	700/1000
Cost	$165 USD (price varies by region)
Languages	English (primary); Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese
Delivery	Pearson VUE — at-home (proctored) or test center
Validity	1 year initially; renews via Learn online assessment

Skills Measured (Microsoft's Official Weightings)

Domain	Weight
Deploy and manage a Microsoft 365 tenant	25-30%
Manage users, groups, and identity synchronization with Microsoft Entra ID	20-25%
Implement and manage identity, security, and access	15-20%
Manage compliance and security in Microsoft 365	20-25%
Manage Microsoft 365 from the Microsoft 365 admin center (operations)	10-15%

Microsoft does update weights periodically — always verify on the official exam page at learn.microsoft.com/en-us/certifications/exams/ms-102.

What to Focus On

Identity (heavy weight)

- Entra ID concepts (tenants, users, groups, roles)
- Hybrid identity (PHS, PTA, Federation)
- MFA, SSPR
- Conditional Access policies + creating + report-only
- Identity Protection (P2)
- PIM (Privileged Identity Management)

Security (heavy weight)

- Defender for Office 365: Safe Links, Safe Attachments, anti-phishing
- Defender for Endpoint basics
- Secure Score
- Attack simulation training
- Quarantine + Threat Explorer

Compliance (heavy weight)

- Sensitivity labels (create, publish, apply)
- DLP policies
- Retention policies + labels
- eDiscovery (Standard + Premium)
- Audit logs
- Insider Risk Management

Tenant & Operations

- Tenant configuration, domains, DNS
- Service Health, Message Center
- Licenses
- Reports

Workload Specifics

- Exchange: mailbox types, mail flow, SPF/DKIM/DMARC, EOP, transport rules, connectors
- Intune: enrollment (Autopilot), compliance, configuration profiles, app deployment
- Teams: policies, governance, guest access
- SharePoint/OneDrive: sharing, permissions, retention

Question Format Tips

Format	Strategy
Multiple choice	Read every option; eliminate obviously wrong; pick "most correct"
Multiple select	Read every option independently — "this also true?" yes/no
Drag and drop	Read instructions carefully — sometimes one option matches multiple slots
Case study	Read scenario first; questions then make sense; refer back as needed
Yes/No series	Each question independent; don't second-guess earlier answers
Hot area (click on diagram)	Visual recognition; usually click admin center icons or menu items
Build list (order)	Read steps carefully; logical sequence; prerequisites first

Time Management

- 120 min / 50 questions = ~2.4 min/question average.
- Case studies eat 8-15 minutes each — budget accordingly.
- Flag and skip if stuck; come back at end.
- Last 10 minutes: review flagged questions.

Resources to Use

Resource	What It Provides
Microsoft Learn (free)	Official learning paths for MS-102; includes labs
Microsoft official practice tests	Sample questions in exam-like format
This guide	Structured deep-dive with labs and PowerShell
Hands-on tenant (developer free or sandbox)	Real practice with the admin centers
YouTube creators (John Savill, etc.)	Visual concept explanations
Microsoft Tech Community	Real-world Q&A; latest changes
r/Microsoft365 + r/AzureAD	Practitioner discussions

Common Pitfalls

- **Outdated info:** Microsoft changes products often. Check Learn for current.
- **Trick questions about license:** Know which features need P1 vs P2 vs E5.
- **Mixing up products:** Defender for Office 365 ≠ Defender for Endpoint ≠ Defender for Identity.
- **Underestimating PowerShell:** Expect 3-5 cmdlet questions.
- **Skipping hands-on:** You'll remember things you've actually clicked through.

30-Day Study Plan

Week 1: Foundations

Day	Focus	Lab
1	Section 1: Tenant Management — Architecture, licensing	Tour admin.microsoft.com
2	Section 1 cont. — Custom domain, DNS, branding	Add domain to your dev tenant; verify; configure MX
3	Section 1 cont. — Org settings, Service Health, billing	Configure org branding
4	Section 2: User Management — Create, edit, delete	Create 5 test users via portal + PowerShell
5	Section 2: Groups — Security, M365, dynamic	Create security group + dynamic group; add members
6	Section 2: Identity — MFA, SSPR	Enable MFA via Security Defaults; test SSPR
7	Week 1 review + quiz	Mock quiz on Sections 1-2

Week 2: Identity & Access

Day	Focus	Lab
8	Conditional Access — Architecture, policies	Create "block legacy auth" CA in Report-only
9	CA continued — Risk-based, named locations, app filters	Create "require MFA" CA
10	Identity Protection (P2)	Review Risky users; sign-in risk policies
11	Roles, RBAC, PIM, Administrative Units	Create AU; assign Helpdesk role scoped to AU
12	Hybrid Identity — PHS, PTA, Federation	Read Entra Connect docs; compare models
13	External Identities — Guests, B2B, Cross-tenant access	Invite a guest; configure External Identities
14	Week 2 review + quiz	Mock quiz on Identity

Week 3: Workloads

Day	Focus	Lab
15	Section 3: Intune basics, enrollment	Tour Intune admin center; configure MDM scope
16	Autopilot, compliance, configuration profiles	Create Win compliance policy + assign
17	App deployment, Endpoint Security, BitLocker	Deploy a test app; configure BitLocker policy
18	Section 4: Exchange — mailboxes, distribution, shared	Create shared mailbox; grant Full Access
19	Mail flow rules, connectors, SPF/DKIM/DMARC	Add disclaimer rule; enable DKIM
20	EOP, anti-spam, anti-malware, anti-phishing	Configure Strict preset for executives
21	Week 3 review + quiz	Mock quiz on Workloads

Week 4: Security, Compliance & Final Prep

Day	Focus	Lab
22	Section 5: Teams admin, policies, governance	Create restricted meeting policy
23	Section 6: SharePoint + OneDrive sharing, retention	Configure sharing; OneDrive offboarding
24	Section 7: Defender — Safe Links, Safe Attachments	Verify Defender preset Strict applied
25	Section 7: Secure Score, Attack Simulation, Zero Trust	Review Secure Score; pick 5 wins
26	Section 8: Purview — Labels, DLP	Create sensitivity label; create DLP policy
27	Section 8: Retention, eDiscovery, Audit, IRM	Create retention policy; eDiscovery case
28	Section 9: Reporting, Monitoring, Alerts	Review usage reports; configure alert policy
29	Section 10: PowerShell + Mock exam (timed)	Practice exam under conditions
30	Light review of weak areas + Take exam	Last-minute notes review

Daily Time Estimate

- Reading + Notes: 60 min
- Lab work: 60-90 min
- Quiz/Practice: 30 min
- Total: 2-3 hours/day average

Practical Lab Checklist

Tenant Setup (Foundational)

✓	Task
☐	Sign up for free M365 developer tenant (developer.microsoft.com)
☐	Verify a custom domain
☐	Configure organization branding
☐	Add an admin user with Global Reader (read-only safe)
☐	Subscribe to Message Center email digest
☐	Review Service Health
☐	Set up break-glass account

Identity

✓	**Task**
☐	Create 10 test users via portal
☐	Create 10 more via PowerShell (CSV bulk)
☐	Create security group + add members
☐	Create M365 Group; verify SharePoint site auto-provisioned
☐	Create dynamic group with department rule
☐	Configure group-based licensing
☐	Enable Security Defaults; observe MFA registration prompt
☐	Disable Security Defaults; configure CA "Block Legacy Auth" in Report-only
☐	Create CA "Require MFA"; flip to On after monitoring
☐	Set up SSPR; test password reset as user
☐	Configure password protection (banned passwords)
☐	Invite a guest user via Entra; verify B2B flow
☐	Create Administrative Unit; assign Helpdesk role scoped
☐	Activate PIM for a role assignment

Devices & Intune

✓	Task
☐	Tour Intune admin center; verify MDM authority
☐	Enroll a Windows VM via Entra Join
☐	Create Windows compliance policy; assign
☐	Create CA "Require Compliant Device"
☐	Deploy Microsoft 365 Apps to test device
☐	Configure BitLocker policy + verify encryption
☐	Create configuration profile (e.g., disable USB or restrict browser)
☐	Perform a test wipe/retire
☐	Create iOS / Android app protection policy

Exchange Online

✓	Task
☐	Tour Exchange admin center
☐	Create shared mailbox; grant Full Access + Send As
☐	Create room mailbox; configure booking policies
☐	Create distribution group; restrict senders
☐	Create dynamic distribution group
☐	Create transport rule: external email warning banner
☐	Verify SPF, configure DKIM (CNAMEs in DNS)
☐	Configure DMARC: start with p=none
☐	Apply Preset Strict security policy to executives
☐	Run a message trace
☐	Review and release quarantined message

Teams

✓	Task
☐	Create a team; add channels (standard + private)
☐	Add a guest to a team; verify access
☐	Configure External Access (federation)
☐	Create custom meeting policy; assign via group
☐	Configure messaging policy
☐	Create app permission policy
☐	Configure app setup policy (pin apps)
☐	Restrict team creation to a group
☐	Enable group expiration (180 days)

SharePoint & OneDrive

✓	Task
☐	Create Communication site
☐	Create Hub site; associate other sites
☐	Configure tenant external sharing
☐	Test per-site sharing override
☐	Pre-provision OneDrive for new users
☐	Configure OneDrive retention after deletion
☐	Grant manager access to a deleted user's OneDrive
☐	Install OneDrive client; sync a library
☐	Test OneDrive Files Restore

Defender / Security

✓	Task
☐	Configure Safe Links policy (all locations)
☐	Configure Safe Attachments policy (Block mode)
☐	Configure anti-phishing with protected users + domains
☐	Review Secure Score; mark 5 actions Planned
☐	Run an attack simulation (Credential Harvest)
☐	Review Threat Explorer / Real-Time Detections
☐	Configure tenant allow/block list

Compliance / Purview

✓	Task
☐	Create a sensitivity label (Confidential with encryption)
☐	Publish labels to users
☐	Configure auto-labeling policy
☐	Create DLP policy (block credit card sharing)
☐	Create retention policy (5 years email)
☐	Create retention label (legal hold)
☐	Open eDiscovery Standard case; place hold; run search
☐	Run audit log search
☐	Add Compliance Manager assessment (e.g., NIST 800-53)

Reporting / PowerShell

✓	Task
☐	Install all 5 main PowerShell modules
☐	Connect to Microsoft Graph; run Get-MgUser
☐	Connect to Exchange Online; run Get-Mailbox
☐	Connect to Teams; run Get-Team
☐	Connect to SharePoint; run Get-SPOSite
☐	Bulk-create users via CSV PowerShell script
☐	Export license utilization report
☐	Export stale users report
☐	Run a unified audit log search

PowerShell Cheat Sheet

Connection Cmdlets

```
Connect-MgGraph -Scopes "User.ReadWrite.All", "Group.ReadWrite.All"
Connect-ExchangeOnline -UserPrincipalName admin@contoso.com
Connect-IPPSSession -UserPrincipalName admin@contoso.com
Connect-MicrosoftTeams
Connect-SPOService -Url https://contoso-admin.sharepoint.com

# Disconnect (good hygiene)
Disconnect-MgGraph
Disconnect-ExchangeOnline -Confirm:$false
Disconnect-MicrosoftTeams
Disconnect-SPOService
```

Users

```
Get-MgUser -All
Get-MgUser -UserId "alice@contoso.com"
Get-MgUser -Filter "department eq 'Sales'"
New-MgUser -DisplayName "x" -UserPrincipalName "x@y.com" -AccountEnabled `
    -MailNickname "x" -PasswordProfile @{Password="Pa$
$w0rd";ForceChangePasswordNextSignIn=$true} `
    -UsageLocation "PK"
Update-MgUser -UserId "x@y.com" -JobTitle "Manager"
Remove-MgUser -UserId "x@y.com"
Restore-MgDirectoryDeletedItem -DirectoryObjectId $id
Revoke-MgUserSignInSession -UserId "x@y.com"
```

Licenses

```
Get-MgSubscribedSku
Set-MgUserLicense -UserId "x@y.com" -AddLicenses @(@{SkuId=$sku.SkuId}) -
RemoveLicenses @()
Set-MgGroupLicense -GroupId $id -AddLicenses @(@{SkuId=$sku.SkuId}) -RemoveLicenses
@()
```

Groups

```
Get-MgGroup -All
Get-MgGroupMember -GroupId $id
New-MgGroup -DisplayName "x" -MailEnabled:$false -MailNickname "x" -SecurityEnabled
New-MgGroupMember -GroupId $id -DirectoryObjectId $userId
Remove-MgGroupMemberByRef -GroupId $id -DirectoryObjectId $userId
```

Conditional Access

```
Get-MgIdentityConditionalAccessPolicy
$policies = Get-MgIdentityConditionalAccessPolicy
$policies | ConvertTo-Json -Depth 10 | Out-File backup.json
```

Exchange Online

```
Get-Mailbox -ResultSize Unlimited
Get-Mailbox -Identity "x@y.com" | Format-List
Get-MailboxStatistics -Identity "x@y.com"
Set-Mailbox -Identity "x@y.com" -Type Shared
Set-Mailbox -Identity "x@y.com" -LitigationHoldEnabled $true
Enable-Mailbox -Identity "x@y.com" -Archive
Add-MailboxPermission -Identity "shared@y.com" -User "user@y.com" -AccessRights
FullAccess
Add-RecipientPermission -Identity "shared@y.com" -Trustee "user@y.com" -AccessRights
SendAs

# Mail flow
Get-TransportRule
New-TransportRule -Name "x" -FromScope NotInOrganization -
ApplyHtmlDisclaimerLocation Prepend `
    -ApplyHtmlDisclaimerText "<b>External</b>"

# Anti-phish
Get-AntiPhishPolicy
Set-AntiPhishPolicy -Identity "Office365 AntiPhish Default" -PhishThresholdLevel 3

# DKIM
Get-DkimSigningConfig
New-DkimSigningConfig -DomainName "contoso.com" -Enabled $true

# Message trace
Get-MessageTrace -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) -
SenderAddress "x@y.com"
```

Teams

```
Get-Team
Get-TeamUser -GroupId $id
Add-TeamUser -GroupId $id -User "x@y.com" -Role Member
New-Team -DisplayName "Project X" -Owner "pm@y.com" -Visibility Private
New-TeamChannel -GroupId $id -DisplayName "General"

# Policies
Get-CsTeamsMeetingPolicy
New-CsTeamsMeetingPolicy -Identity "x" -AllowCloudRecording $false
Grant-CsTeamsMeetingPolicy -Identity "user@y.com" -PolicyName "x"
New-CsGroupPolicyAssignment -GroupId $gid -PolicyType "TeamsMeetingPolicy" -
PolicyName "x" -Rank 1

# Federation
Get-CsTenantFederationConfiguration
Set-CsTenantFederationConfiguration -AllowFederatedUsers $true
```

SharePoint Online

```
Get-SPOSite -Limit All
Get-SPOSite -Identity "https://x.sharepoint.com/sites/y"
New-SPOSite -Url "..." -Owner "x@y.com" -StorageQuota 1024 -Template "STS#3" -Title
"x"
Set-SPOSite -Identity "..." -StorageQuota 10240
Set-SPOTenant -SharingCapability "ExternalUserSharingOnly" `
    -RequireAnonymousLinksExpireInDays 30

# OneDrive
Get-SPOSite -IncludePersonalSite $true -Limit All -Filter "Url -like '*-
my.sharepoint.com/personal*'"
Request-SPOPersonalSite -UserEmails @("x@y.com")
Set-SPOUser -Site "..." -LoginName "manager@y.com" -IsSiteCollectionAdmin $true
```

Audit & Reports

```
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) `
    -Operations FileDownloaded -UserIds "x@y.com"

Get-MgReportAuthenticationMethodUserRegistrationDetail -All
Get-MgReportOffice365ActiveUserDetail -Period D30 -OutFile users.csv
```

Microsoft 365 Admin Portal Cheat Sheet

Admin Center URLs (Memorize These)

Portal	URL
Microsoft 365 Admin Center	admin.microsoft.com
Microsoft Entra Admin Center	entra.microsoft.com
Microsoft Intune Admin Center	intune.microsoft.com
Exchange Admin Center	admin.exchange.microsoft.com
Microsoft Teams Admin Center	admin.teams.microsoft.com
SharePoint Admin Center	admin.microsoft.com/sharepoint (or contoso-admin.sharepoint.com)
Microsoft Defender Portal	security.microsoft.com
Microsoft Purview Portal	purview.microsoft.com
Microsoft Purview Compliance (legacy)	compliance.microsoft.com
Azure Portal	portal.azure.com
Microsoft Graph Explorer	developer.microsoft.com/en-us/graph/graph-explorer
My Account (end users)	myaccount.microsoft.com
SSPR Setup	aka.ms/ssprsetup
MFA Setup	aka.ms/mfasetup
Security Info	mysignins.microsoft.com

Common Navigation Paths

Task	Path
Create user	Admin Center → Users → Active users → + Add a user
Assign license	Admin Center → Users → user → Licenses and apps
Create Conditional Access policy	Entra → Protection → Conditional Access → + New policy
Configure MFA	Entra → Identity → Overview → Manage Security Defaults (or via CA)
Configure SSPR	Entra → Protection → Password reset
Assign admin role	Entra → Identity → Roles & admins → role → + Add assignments
Create dynamic group	Entra → Groups → + New group → Dynamic User
Enroll Windows device	Intune → Devices → Enrollment → Windows
Compliance policy	Intune → Devices → Compliance policies
App deployment	Intune → Apps → All apps → + Add
Mailbox permission	EAC → Recipients → Mailboxes → user → Delegation
Mail flow rule	EAC → Mail flow → Rules → + Add
Configure DKIM	Defender → Email auth settings → DKIM
Teams policy	TAC → relevant policy type
SharePoint sharing	SPO Admin Center → Policies → Sharing
OneDrive settings	SPO Admin Center → Settings → OneDrive
Safe Links / Attachments	Defender → Policies → Threat policies → Safe Links / Attachments
Secure Score	Defender → Secure Score
Quarantine	Defender → Review → Quarantine
Threat Explorer	Defender → Email & collaboration → Explorer
Sensitivity labels	Purview → Information Protection → Labels
DLP	Purview → Data loss prevention → Policies
Retention policies	Purview → Data lifecycle → Retention policies
eDiscovery	Purview → eDiscovery → Standard / Premium

Audit log	Purview → Audit → New search
Service Health	Admin Center → Health → Service health
Message Center	Admin Center → Health → Message center
Usage reports	Admin Center → Reports → Usage
Sign-in logs	Entra → Identity → Monitoring → Sign-in logs
Audit logs (Entra)	Entra → Identity → Monitoring → Audit logs

Common MS-102 Exam Mistakes

Conceptual Mistakes

Mistake	**The Truth**
Confusing MDM and MAM	MDM = whole device; MAM = specific apps. MAM works without enrollment.
Confusing External Access and Guest Access (Teams)	External Access = federation (cross-tenant chat); Guest Access = invited member in your team.
Confusing Conditional Access and Security Defaults	Security Defaults: free, all-or-nothing. CA: P1+, granular.
Thinking Defender for Office 365 = Defender for Endpoint	Different products. MDO protects email/Teams; MDE protects endpoints.
Forgetting break-glass account exclusion	Always exclude 2+ break-glass accounts from CA policies.
Hybrid identity model confusion	PHS = cloud auth; PTA = on-prem real-time; Federation = AD FS.
Mailbox license rules	Shared mailbox <50 GB = no license. With archive/litigation hold = needs license.
Sensitivity label vs Retention label	Sensitivity = classification + protection; Retention = how long to keep.
DLP without sensitivity labels	You can do DLP without labels using sensitive info types directly. Both can combine.
SPF too many lookups	SPF max 10 DNS lookups; many third-party includes break this.

License Mistakes

Mistake	Correct Answer
Risk-based CA on E3	Wrong — requires P2 (or Identity Protection separately)
Endpoint DLP on E3	Wrong — requires E5
PIM on E3	Wrong — requires P2
Advanced eDiscovery on E3	Wrong — requires E5
Auto-expanding archive on F1	Wrong — requires Plan 2 / E3
Customer Lockbox on E3	Wrong — requires E5

Operational Mistakes

Mistake	Better Practice
Production-test new CA	Use Report-only mode first
Per-user license assignment	Use group-based licensing
Per-mailbox transport rule duplication	One rule with multiple recipients
Manual user creation for bulk	CSV import or PowerShell
Direct user access to libraries	SharePoint groups
Permanent role assignment	PIM eligible
Always-on Global Admin	2-5 max; PIM for activation

Last-Minute Revision Notes

Numbers to Memorize

Number	What
30 days	Deleted user recycle bin; default OneDrive retention after user deletion
93 days	SharePoint recycle bin stage 1
180 days	Audit log retention Standard E3 (raised from 90)
1 year	Audit log Premium default; CA policy retention default for Sign-in logs (Standard)
10 days	Message trace real-time search range (older = historical)
90 days	Message trace historical range
50 GB	Shared mailbox max without license
100 GB	Default mailbox quota E3/E5
1.5 TB	Auto-expanding archive max
1 TB	Default OneDrive quota
5 TB	Expanded OneDrive max
10 lookups	Max SPF DNS lookups
10 attempts / 60 sec	Smart Lockout default
2-5	Recommended max Global Admins
2 (min)	Break-glass accounts
250 GB	OneDrive file size limit
30 days	Anyone link expiration recommended
30 minutes	Default Entra Connect sync interval
2 minutes	Password hash sync interval
500	Major version history default per file
350	Max protected users for impersonation
50	Max protected domains for impersonation
1000	Custom banned password list max
250,000	Max users in single bulk CSV upload

Acronym Cheat Sheet

Acronym	Full
MDO	Microsoft Defender for Office 365
MDE	Microsoft Defender for Endpoint
MDI	Microsoft Defender for Identity
MDA	Microsoft Defender for Cloud Apps
XDR	Extended Detection and Response
EOP	Exchange Online Protection
EAC	Exchange Admin Center
TAC	Teams Admin Center
SPO	SharePoint Online
EXO	Exchange Online
OD4B	OneDrive for Business
MFA	Multi-Factor Authentication
SSPR	Self-Service Password Reset
CA	Conditional Access
PIM	Privileged Identity Management
AU	Administrative Unit
PHS	Password Hash Sync
PTA	Pass-Through Authentication
ADE	Apple Automated Device Enrollment
KFM	Known Folder Move
ZAP	Zero-hour Auto Purge
SCL	Spam Confidence Level
ASR	Attack Surface Reduction
DLP	Data Loss Prevention

IRM	Insider Risk Management
TAP	Temporary Access Pass
RBAC	Role-Based Access Control
SPF	Sender Policy Framework
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Auth, Reporting, Conformance
CSP	Configuration Service Provider (mobile config) — also Cloud Service Provider
SCP	Service Connection Point
UPN	User Principal Name
FQDN	Fully Qualified Domain Name
OAuth	Open Authorization
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SBC	Session Border Controller (Teams Direct Routing)
FIDO2	Fast IDentity Online — phishing-resistant key
WebAuthn	Web Authentication standard
EDR	Endpoint Detection and Response
CSPM	Cloud Security Posture Management
CWPP	Cloud Workload Protection Platform
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, Response

Mock Interview Questions

Identity

Q1. How would you onboard 500 new hires for a company merger?

A: Source HR feed for accurate data. Bulk create via PowerShell from CSV, setting standard UPN format, UsageLocation, department. Use group-based licensing (auto-assign E3 to "All Employees" group). Pre-provision OneDrive. Enforce MFA via Conditional Access. Send welcome email with temporary credentials and SSPR registration link. Monitor for sign-in errors first week.

Q2. A user reports being unable to sign in after travel. How do you investigate?

A: Check Entra Sign-in logs filtered by user, recent timeframe. Look for: error code (AADSTS50126 = bad password, AADSTS53003 = CA block, AADSTS50053 = Smart Lockout). Check if CA is blocking due to new location. Check if account is enabled. Check if MFA is required and user's phone is reachable. Resolve based on root cause: unlock, reset, or adjust CA temporarily.

Q3. Compare PHS, PTA, and Federation. Which would you recommend?

A: PHS = hash-of-hash synced to cloud; auth in cloud; resilient to on-prem outage; enables Identity Protection leaked credentials. PTA = passwords stay on-prem; cloud forwards auth to on-prem agent. Federation = AD FS handles auth; complex; legacy. Recommendation: PHS + Seamless SSO for most orgs — simplest, most resilient, enables advanced security.

Q4. Explain Conditional Access in detail.

A: CA is Entra's policy engine evaluating each sign-in: who (user), what (app/resource), where/how (location, device, risk), then (grant/block/require MFA/compliant device). All applicable policies evaluated together; most restrictive wins. Use Report-only mode for safe testing. Always exclude break-glass accounts. P1 required (P2 for risk-based).

Q5. What's the difference between MFA and Passwordless?

A: MFA = password + 2nd factor (something you know + have/are). Still has a phishable password. Passwordless = no password exists — credential is hardware-bound (FIDO2, Windows Hello) or biometric. Phishing-resistant. Microsoft recommends moving toward passwordless via Authenticator phone sign-in, FIDO2 keys, or Windows Hello.

Security & Compliance

Q6. Walk me through investigating a phishing email reported by a user.

A: User clicks Report Message in Outlook. Defender → Submissions → user-reported. Validate as phishing. Open Threat Explorer; search same sender / URL / hash. Identify scope: how many recipients, who clicked. Actions: ZAP delivers retroactive purge across mailboxes; soft-delete in inboxes; block sender via tenant block list; reset credentials of users who clicked; submit pattern to Microsoft.

Q7. How would you protect against CEO email impersonation?

A: Layered defense: (1) SPF, DKIM, DMARC at p=reject — blocks domain spoofing. (2) Anti-phishing policy with CEO as protected user + protected domain — catches lookalikes. (3) External email warning banner via mail flow rule. (4) User training. (5) Mailbox intelligence — learns CEO's normal patterns. (6) Quarantine impersonation matches for review.

Q8. Explain DLP and how you'd roll it out.

A: DLP detects sensitive data (PII, financial, custom) across Exchange, SPO, OneDrive, Teams, Endpoint, and acts on detection (notify, block, encrypt). Rollout: (1) Identify sensitive data via Content Explorer. (2) Create policies in Test mode with policy tips visible. (3) Educate users. (4) Monitor matches for 2-4 weeks; tune false positives. (5) Switch to Enforce. (6) Combine with sensitivity labels for layered enforcement.

Q9. What's eDiscovery and when do you use it?

A: eDiscovery searches, holds, and exports M365 content for legal/HR/compliance matters. Standard (E3): hold, search, export. Premium (E5): custodian management, legal hold notification, review sets, ML coding, redaction. Workflow: case → custodians → holds → search → review → export.

Q10. How would you improve your tenant's Secure Score?

A: Review Recommended Actions sorted by Points achievable. Quick wins: enforce MFA, block legacy auth, enable Safe Links, enable Safe Attachments, reduce Global Admins, apply Defender preset policies. Mark each as Planned, implement, mark Resolved. Track delta monthly. Compare to industry baseline.

Devices & Workloads

Q11. How does Windows Autopilot work?

A: OEM uploads device hardware hash to Microsoft. Admin assigns Autopilot profile (mode, settings) to the hash. User unboxes device; Windows OOBE detects Autopilot registration; customized OOBE prompts for corporate credentials; device joins Entra, enrolls in Intune; ESP applies apps/policies; user lands on desktop in 20-30 min. Zero IT touch.

Q12. Difference between MDM and MAM?

A: MDM = full device management; device enrolled in Intune. Use for corporate-owned. MAM = app-level only; device NOT enrolled. Use for BYOD — corporate apps protected (PIN, no copy/paste to personal apps), but personal apps untouched. Selective wipe removes only corporate data.

Q13. How would you handle a ransomware incident on a managed Windows device?

A: (1) Isolate via Defender for Endpoint — quarantines device from network. (2) Block compromised user account; revoke sessions. (3) Trigger Intune wipe. (4) Restore OneDrive Files Restore to point before encryption. (5) Reimage device via Autopilot. (6) Investigate vector (phishing? RDP? supply chain?). (7) Strengthen control causing the breach.

Q14. Explain SPF, DKIM, DMARC.

A: SPF lists IPs authorized to send for your domain. DKIM cryptographically signs each message; recipient verifies with public key in DNS. DMARC ties them: requires SPF or DKIM to align with From header; policy tells receivers to none/quarantine/reject failures. Together prevent domain spoofing and BEC.

Q15. Difference between Team site and Communication site?

A: Team site: collaboration; tied to M365 Group; members co-author. Comm site: broadcast; smaller author group, larger reader audience; news, intranet. Both modern SPO sites with different templates and default permission models.

Q16. What's Sensitivity Label vs Retention Label?

A: Sensitivity Label: classifies content (Public, Confidential) and applies protection (encryption, restrictions, watermarks). Travels with file. Retention Label: defines how long content is kept and what happens at expiration (delete or trigger disposition review). Used together: a "Customer Contract" label might be Confidential AND retained 10 years.

Q17. How would you secure Teams meetings for executives?

A: Create restrictive Meeting Policy: disable recording, anonymous join, presenter role only for organizer, screen share = Single App, no Give Control. Apply via group policy assignment. Use sensitivity label "Confidential" on meetings for additional enforcement. Enable end-to-end encryption for 1:1. Brief execs on Lobby + Roles features.

Q18. How would you approach a 500-mailbox migration from G Suite to M365?

A: Plan: (1) M365 tenant setup; verify domain. (2) License provisioning. (3) SPF/DKIM/DMARC for new sending. (4) Migration endpoint to G Suite. (5) Pilot 20 users; validate. (6) Batches of 50-100 over 4 weeks. (7) Communicate cutover date; train on Outlook/OWA. (8) Switch MX over weekend. (9) Final sync. (10) Keep G Suite available 30 days; decommission.

PowerShell & Operations

Q19. Write a PowerShell snippet to find all users without MFA.

A:

```
Connect-MgGraph -Scopes "AuditLog.Read.All"
Get-MgReportAuthenticationMethodUserRegistrationDetail -All |
    Where-Object { -not $_.IsMfaRegistered -and $_.UserType -eq "Member" } |
    Select-Object UserPrincipalName |
    Export-Csv "no_mfa.csv" -NoTypeInformation
```

Q20. How do you schedule a PowerShell script to run daily?

A: Azure Automation: (1) Create Automation Account. (2) Create App Registration with certificate for auth. (3) Grant Graph permissions. (4) Upload script as runbook. (5) Schedule daily/weekly. (6) Test in lab tenant first. Cert-based auth means no stored passwords. Alternatively: Task Scheduler on a hardened server, but less elegant.

Real-World Admin Checklist (Day 1 in Your New Role)

Week 1 — Get Oriented

✓	Item
☐	Get Global Admin (or appropriate role) access
☐	Set up break-glass accounts (document credentials in physical safe)
☐	Document tenant ID, primary domain, key admins
☐	Review existing Service Health subscriptions
☐	Review Message Center; identify pending changes affecting you
☐	Map current licenses to user count
☐	Identify any expiring subscriptions
☐	Inventory all custom domains and verify status
☐	Take a Secure Score baseline screenshot
☐	List all CA policies; export to JSON backup

Week 2 — Identity Audit

✓	Item
☐	Count Global Admins — reduce to 2-5 + break-glass
☐	Audit role assignments; remove unnecessary
☐	Verify MFA on all admins (Security Defaults or CA)
☐	Block legacy auth via CA (Report-only first)
☐	Audit guest users; remove stale
☐	Enable SSPR if not already
☐	Audit password protection settings
☐	Set up Entra audit log export to Sentinel/Splunk if needed
☐	Document hybrid identity setup (if any)

Week 3 — Security Audit

✓	Item
☐	Apply Defender preset policies: Standard (most) + Strict (VIPs)
☐	Verify Safe Links and Safe Attachments are enabled
☐	Configure anti-phishing with protected users + domains
☐	Verify SPF, DKIM (CNAMEs), DMARC for each domain
☐	Review quarantine; release/reject pending items
☐	Audit external sharing settings; tighten if too open
☐	Audit user mailbox forwarding (data exfil risk)
☐	Audit mailbox Full Access permissions
☐	Review Secure Score; mark planned actions; implement top 5
☐	Schedule first attack simulation campaign (if E5)

Week 4 — Compliance & Operations

✓	Item
☐	Review retention policies; map to legal requirements
☐	Document sensitivity label hierarchy (or deploy if missing)
☐	Audit DLP policies; tune false positives
☐	Test eDiscovery case workflow
☐	Verify Audit log is enabled
☐	Document escalation playbooks (account compromise, ransomware)
☐	Setup monthly reporting cadence (license, security, adoption)
☐	Document offboarding procedure
☐	Document onboarding procedure
☐	Plan governance: group expiration, naming policy, team templates

Ongoing

Cadence	Items
Daily	Check Service Health; review Defender incidents queue
Weekly	Quarantine review; Secure Score check; CA changes review
Monthly	Usage reports; license utilization; security report; DLP review
Quarterly	Access reviews; Secure Score deep dive; backup verification; tabletop exercise
Annually	Disaster recovery drill; full security audit; compliance audit; framework reassessment

Final Words

You Are Ready

If you've worked through this guide chapter by chapter, completed the labs, run the PowerShell commands in your dev tenant, and worked through the mini-quizzes, you have more than enough knowledge to pass MS-102. More importantly: you have the practical skills to do the job.

The certification is the start, not the end. Microsoft 365 changes monthly. The skills you build here — understanding identity, security, compliance, and the operational rhythm of a M365 admin — outlast any specific feature.

Go take the exam. You've got this.

End

✦

Best of Luck!

Take the exam confidently. Use what you've learned. Build something great with Microsoft 365.

— MS-102 Microsoft 365 Administrator Study Guide

📘 Complete