Ace the Exam Series®

2022

FIRST EDITION

MS-900

MICROSOFT 365 FUNDAMENTALS

EXAM CRAM NOTES

IPSpecialist

MS-900: Microsoft 365 Fundamentals

Exam Cram Notes

First Edition

COURSE INTRODUCTION

Microsoft 365 Fundamentals - Course Introduction

The fundamentals of cloud computing and the Software as a Service (SaaS) cloud model are covered in this course, focusing on Microsoft 365's cloud service offerings. You will start by learning about the principles of cloud computing, including an introduction to Microsoft cloud services. You will learn about Microsoft Azure and look at how Microsoft 365 and Office 365 differ from one another. After that, you will thoroughly examine Microsoft 365, which will include a comparison of Microsoft on-premises services and Microsoft 365 cloud services, a look at enterprise mobility in Microsoft 365, and a look at how Microsoft 365 services support collaboration.

The course then examines how Microsoft 365 handles security, compliance, privacy, and trust before reviewing subscriptions, licenses, invoicing, and support for Microsoft 365.

User Profile

This course is intended for business decision-makers and IT professionals who want to deploy cloud services within their company or who just want to learn the foundations of cloud computing. With a general focus on Microsoft 365 cloud service offerings, this includes the factors to take into account and the advantages of implementing cloud services in general and the SaaS cloud model in particular.

Prerequisites

Candidates must be familiar with the following to pass the MS-900: Microsoft 365 Fundamentals Certification exam.

- The choices that are open to you and the advantages that using

Microsoft's 365 Cloud Service products could bring you.

- The approaches that need to be suggested to handle the organization's frequent IT problems.
- What could set it apart from other market competitors, are Microsoft 365 Solutions.
- Grouping together different Microsoft services and goods, including Azure, Dynamics 365, and Microsoft 365.
- Provision of services and cost-effective licensing optimization.
- There are many organizational support possibilities.

CHAPTER 01: INTRODUCTION TO MICROSOFT 365

Introduction

What is Cloud Computing?

Cloud Computing is storing data and accessing computers over the internet. It is the delivery of different computing services like servers, software, analytics, databases, and storage via the internet. Computing resources are delivered on-demand through a cloud service platform with pay-as-you-go pricing. The companies that are providing services are termed as "Cloud Providers." There is a number of cloud providers, with the major ones being Amazon, Google, and Azure.

Benefits of Cloud Computing

We all know that cloud computing has brought a great change in the traditional business thinking for IT resources. There are many benefits of cloud computing. Some of which are:

1. **Cost**

   Cloud computing eliminates the capital cost of buying hardware and software and of building and running in-house datacenters – server racks, 24 hours' electricity for power and cooling, etc.

2. **Scale Globally**

   Cloud computing services have the capacity to scale with elasticity. In the cloud, IT resources are provided more or less computing power, storage, bandwidth – as per requirement and from the right place.

3. **Increase Speed and Agility**

   New IT resources are readily available so that resources can be scaled up infinitely according to demand. This leads to a dramatic increase in agility for organizations.

4. **Reliability**

Cloud computing allows data backup, disaster recovery, and business continuity as data can be replicated in the network of the cloud supplier on multiple redundant sites.

5. **Security**

The protection of their data is one of the main problems for any organization regardless of its size and industry. Infringements of data and other cyber-crimes can devastate a company's revenue, customer loyalty, and positioning. Cloud provides many advanced security features to strengthen the security of the overall company. It also helps in protecting your data, application, and infrastructure.

The Economy of Cloud Computing

Cloud reduces the Capital Expenditure (CapEx) cost and comes with many other benefits. In the traditional environment of organizations, as there is a need for large investments in CapEx, the cloud is the best way to switch to the pay-as-you-go model. With cloud computing, you can easily move toward Operational Expenditure (OpEx).

Technical Terms

To understand Cloud Computing, you need to understand some technical terms.

- **High Availability (HA)** - It is the core of cloud computing. As we know, in traditional server environments, companies own a number of hardware, and the workload is limited to this hardware capacity. In case of extra load, capacity cannot be increased whereas sometimes this hardware seems extra for the workload. In the cloud, you do not own any hardware, and adding servers is just a click away. With this method, you get high availability for your servers by replacing the failed server instantly with the new one. HA depends on the number of VMs that you set up to eventually cover in case one goes down
- **Fault Tolerance** - For resilience in the cloud, fault tolerance is also an important factor. Fault tolerance gives you zero downtime, meaning that if there is any fault from the Azure side, then it is immediately mitigated by Azure itself

- **Disaster Recovery (DR)** – This is used in case of any catastrophic disaster like a cyber-attack. There is a plan in DR to recover your business from these critical systems or in normal operation if such an event occurs. DR has designated time to recover and a recovery point
- **Scalability** - In cloud computing, scalability means adding or removing the resources in an easy and quick way as per demand. It is important in such a situation where you do not know the actual number of resources that are needed. Auto-scaling is an approach for scalability depending on your requirement by defining the threshold
- **Elasticity** - Elasticity is the capacity to dynamically extend or minimize network resources to respond to autonomous working load adjustments and optimize the use of resources. This can contribute to overall cost savings for services
- **Agility** - Agility is the capability to adapt quickly and efficiently to changes in the business environment. Agility also refers to the ability to quickly develop, test and deploy business-led software applications. Instead of providing and managing services, Cloud Agility lets them concentrate on other issues such as security, monitoring, and analysis

Types of Cloud Computing

Cloud computing services are divided into four broad categories: IaaS, PaaS, Serverless, and SaaS. These are also known as a stack in cloud computing because each of them is built on top of another. Let's discuss each of them.

1. **Infrastructure as a Service (IaaS)**

It gives you a basic IT infrastructure for Cloud IT like VMs, Data Storage, Networks, and OS on a pay-as-you-go model.

2. **Platform as a Service (PaaS)**

Cloud computing platforms that provide an on-demand environment to build, test, deliver and manage software applications are referred to as Platform as a Service. PaaS is designed to facilitate the fast development of web or mobile apps for developers without setting or maintaining the underlying server, storage, network, and database infrastructure needed for development.

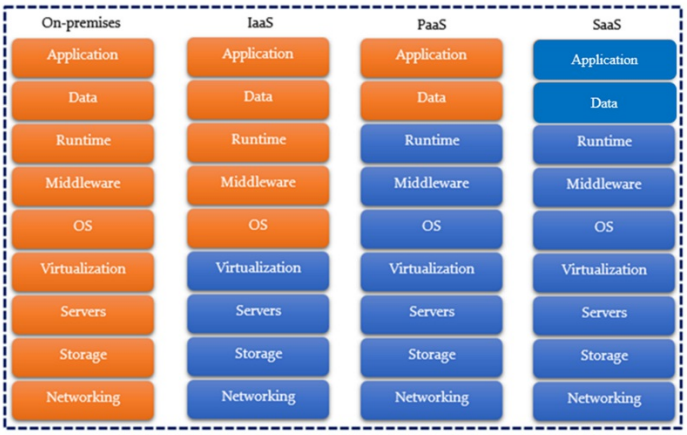
3. **Serverless**

Overlapping PaaS, serverless computing concentrates on creating application functionality without continually spending time

maintaining the required server and infrastructure. The cloud provider is responsible for configuration, capacity planning, and server governance. The highly scalable and event-based serverless architectures only use resources when a particular task or trigger takes place.

4. **Software as a Service (SaaS)**

Cloud providers take over both servers and code. Cloud providers host and maintain the applications and underlying infrastructure for SaaS and handle updates such as software upgrades and security patches. Users link the app over the Internet, usually through their phone, tablet, or PC through their web browser.



Cloud Computing Deployments Models

We know that all clouds are not the same, and not every business requirement for cloud computing is the same. So, in order to meet the requirements, different models, types, and services have been used. Firstly, you have to decide how the cloud service is being applied by finding out the cloud deployment type or Architecture. There are three different types of Cloud Computing: Public, Private and Hybrid.

Microsoft 365

A cloud-based subscription service called Microsoft 365 includes a portfolio of integrated goods like Office applications, Teams, Windows, top-notch security, and more. Any size organization, including yours, may benefit from Microsoft 365. It represents the workplace of the future. Whether at home, in the office, out in the field, or on the go, these Microsoft 365 features help enhance productivity, collaboration, and communication securely across numerous devices. Microsoft 365 ensures a trustworthy, secure, and contemporary experience for every employee at any time and everywhere while integrating everyone into the digital revolution.

Microsoft 365 Fundamentals

Your gateway and guide to everything Microsoft 365 is Microsoft 365 Fundamentals. Three understanding routes make up Microsoft 365 fundamentals, introducing you to the platform's many features through its range of products and services.

The three learning paths are outlined in the list below:

- Describe the basic features and principles of Microsoft 365. Learn how Microsoft 365's productivity, collaboration, and business management tools enable individuals and companies to do more
- Demonstrate a fundamental understanding of the security and compliance features of Microsoft 365. Discover how Microsoft's security, compliance, and identity solutions assist individuals and companies in securing their whole digital footprint, streamlining compliance, and lowering the risk
- Show that you are knowledgeable about Microsoft 365 licensing, service, and support. Find out how adoption guidance, ongoing support, and license options that suit your needs can help people and businesses make the most of their Microsoft 365 investments

Microsoft 365 productivity in the cloud

Organizations are heading toward digitization, profoundly changing when, where, and how we work. Employees seek more job flexibility while yet

feeling connected to their coworkers. Employees are expected to sync and operate across various devices, including personal devices, making management and security tough. Organizations strive to remain competitive in a constantly changing economic environment and prepare for economic turbulence. They want to help their staff reach their maximum potential without inducing burnout. Organizations seek to automate processes, but their employees use too many apps, resulting in a fragmented experience. They want to be safe against security risks, but they do not have the resources to keep up with the sophistication of attacks. Organizations seek top-line growth, cost-cutting, and improved customer service. Below are the benefits enlisted to remember of Microsoft 365.

Benefits of Microsoft 365

- Problem solving and provision of security
- Stimulation of productivity
- Security through modern technology
- Cost-effective solutions

Microsoft 365 Subscription Options

Microsoft offers various subscriptions to meet your organization's demands because every organization has different requirements. Let's look at some of the more well-known subscription options.

Microsoft 365 Home

To give your personal and family life the same fantastic productivity benefits, Microsoft 365 Home was created. Two plans are available for

family and individual use of Microsoft 365 Home.

Microsoft 365 Education

Educational institutions can use Microsoft 365 Education. Microsoft 365 Education gives teachers the tools to foster collaboration and unleash creativity with a single, cost-effective solution. Academic licenses can be customized to meet the requirements of every institution, including security and productivity solutions for faculty, staff, and students.

Microsoft 365 for business

Small and medium-sized businesses are the target audience for Microsoft 365 for business. By lowering costs, enhancing cybersecurity, and enabling workers to work remotely, Microsoft 365 for Business can benefit your company. It contains security and device management features in addition to the complete set of Office 365 productivity tools.

Microsoft 365 Enterprise

Large enterprises can use Microsoft 365 Enterprise. Every person, from the office to frontline staff, can be connected and empowered by Microsoft 365 Enterprise, increasing efficiency and spurring innovation. Organizations looking for a productivity solution with strong threat prevention, security, compliance, and analytics features can get enterprise-class services from this company.

Microsoft 365 Amin Center

You may administer your cloud-based company through the Microsoft 365 admin center. You can add and take away users, change licenses, and reset passwords. For more precise control, use specialized workspaces like Security or Device management.

Two perspectives are available in the Microsoft 365 admin center.

- Simplified view
- Dashboard view

Azure Active Directory Admin Center

Azure Active Directory (Azure AD) is a service for managing identities and access in the cloud. This solution facilitates access to thousands of additional SaaS applications, the Azure portal, and external resources like Microsoft 365 for your staff members.

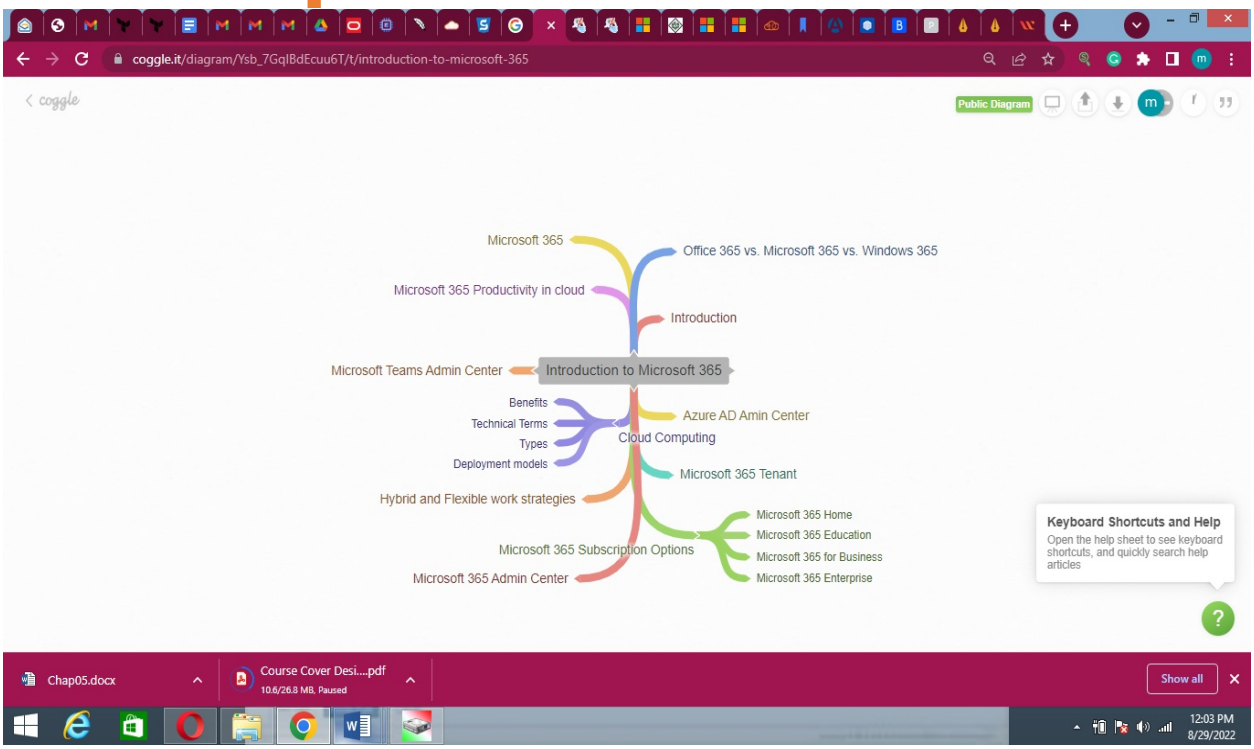
Microsoft Teams Admin Center

The controls you will find in the Microsoft Teams admin center are comparable to those accessible in the Microsoft 365 admin center, such as those for managing users, adding users, deleting users, enabling add-ons, assigning responsibilities, etc.

As an admin, you might need to inspect or update your company has established teams for collaboration, or you might need to take corrective action like giving ownerless teams an owner. Both the Microsoft Teams admin center and the Microsoft Teams PowerShell module let you manage the teams used by your company. The admin center can be accessed at https://admin.microsoft.com. You should make sure that you are allocated one of the following roles if you want to have full administrative powers with these two toolkits:

- Teams Administrator
- Global Administrator

Mind Map


coggle.it/diagram/Ysb_7GqlBdEcuu6T/t/introduction-to-microsoft-365
coggle
Public Diagram
Introduction to Microsoft 365
Microsoft 365
Office 365 vs. Microsoft 365 vs. Windows 365
Microsoft 365 Productivity in cloud
Introduction
Microsoft Teams Admin Center
Benefits
Technical Terms
Types
Deployment models
Cloud Computing
Azure AD Amin Center
Microsoft 365 Tenant
Hybrid and Flexible work strategies
Microsoft 365 Subscription Options
Microsoft 365 Home
Microsoft 365 Education
Microsoft 365 for Business
Microsoft 365 Enterprise
Microsoft 365 Admin Center
Keyboard Shortcuts and Help
Open the help sheet to see keyboard shortcuts, and quickly search help articles
Chap05.docx
Course Cover Desi....pdf
10.6/26.8 MB, Paused
Show all
12:03 PM
8/29/2022

CHAPTER 02: PRODUCTIVITY SOLUTIONS IN MICROSOFT 365

Introduction

Working wherever and whenever is the meaning of productivity in today's world. Industry-leading tools are conveyed and delivered by Microsoft 365, powered by Artificial Intelligence (AI) that unbridles the creativity and potential embedded inside. Microsoft 365 has been playing a significant role in providing solutions to the problems faced by each one of us. With the help of Microsoft 365, we can easily get our hands on the versatility of its apps like Word, Excel, PowerPoint, OneNote, and Outlook. Apps like Exchange offer us an intuitive email box with a calendar. Microsoft 365's work management tools help us spend more time on our work and less time on managing it. Such tools include Project, Planner, Bookings, and To-Do.

All of these solutions have been combined into a connected platform by Microsoft. Discover how Microsoft 365's productivity tools improve operations, engage users, and enable workers to carry out activities in real-time from almost anywhere.

Core Productivity Tools in Microsoft 365

Microsoft 365 helps us ace productivity through its variety of productivity tools. Below are given the tools that will assist in achieving productivity.

- All-time collaboration
- Creation of content in real-time
- Initiation of a cohesive file-sharing experience
- Engaging and informing an organization
- Staying connected
- Working smartly with business-class email and calendaring
- Organizing well-endowed content tasks
- Staying on the right track seamlessly
- Simplifying lineups to save time

Increments in Productivity through Microsoft 365 Apps

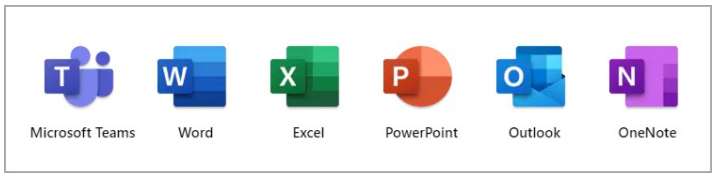
Microsoft 365 Tools is a collection of apps that help you stay connected and productive. Create beautiful content, collaborate in real-time, and transform data into insights with Microsoft 365 Apps. Microsoft 365 Apps are offered in two subscriptions: Microsoft 365 Apps for Business and Microsoft 365 Apps for Enterprise. These programs include the Office suite, which includes Word, Excel, PowerPoint, OneNote, Outlook, Teams, Publisher, and Access (Publisher and Access are only available on PC).

Microsoft 365 Apps offers the benefits of the cloud, allowing you to work from anywhere, at any time, on any device, and be more productive.

- Working across multiple devices
- Working with up-to-date apps
- Working inventively through connected experiences

Features of connected experiences:

- Use built-in intelligence capabilities like Microsoft Editor and Researcher to produce amazing documents and enhance your writing
- Excel may assist you in simplifying complex data and creating simple spreadsheets and visuals
- With sophisticated tools like Presenter Coach and PowerPoint Designer, PowerPoint can help you produce professional presentations that stand out effortlessly
- Outlook allows you to manage your email, calendar, tasks, and contacts all in one location
- OneNote may assist you with your note-taking requirements by arranging your notes into tabs and subsections, resulting in a single digital notebook



Work Management Tools in Microsoft 365

Your team is not productive if it is always managing tasks. In order to concentrate on producing high-quality work on schedule, you and your team need an effective procedure for managing that work. Through a suite of specifically designed tools that add structure to all the components that go into producing high-quality business results, such as tasks, status updates, schedules, and projects, Microsoft 365 streamlines job management. Your team will have more time to work together on the actual project if the work process is handled more effectively.

Work management solutions from Microsoft 365 enable your employees to work the way they want, providing companies with the outcomes they want. The Project, Planner, Bookings, and To-Do are among the job management tools provided. Each tool is built with unique characteristics to allow you to select the ideal tool to assist you in managing your specific sort of job.

Microsoft Project

Project is a strong project management application intended for more complicated work initiatives. Microsoft's current cloud-based work and project management option is Project for the Web. Project for the Web offers easy, robust work management tools that can be tailored to most needs and roles. Take on little undertakings as well as huge efforts. Regardless of team size, project managers and team members may utilize Project for the Web to plan and manage work involving dynamic scheduling,

subtasks, and/or dependent tasks.

Microsoft Planner

The Planner is an easy-to-use, collaborative task management application that allows users to plan, organize, and accomplish task-based activities. Planner allows teams to plan their work straightforwardly and visually. The Planner is a web-based application accessible from anywhere and has a mobile app for iOS and Android.

Microsoft Bookings

Bookings is an appointment scheduling and management system accessible over the internet. Bookings make it easier to schedule and manage appointments. It features a web-based booking calendar and interacts with Outlook to optimize your staff's schedule and allow your clients to book at a time that works best for them.

Microsoft To Do

To Do is a smart task management program that helps you plan and organize your day. To Do is a better, more personal, and intuitive method for individuals to remain organized and make the most of their days. It works with Outlook and Planner and is powered by Office 365 Exchange Online. To Do is accessible via iOS, Android, Windows, and the web. To Do encourages you to do the most critical tasks you need to get done every day, whether for work, school, or home.

Business-class email and calendaring with Microsoft Exchange

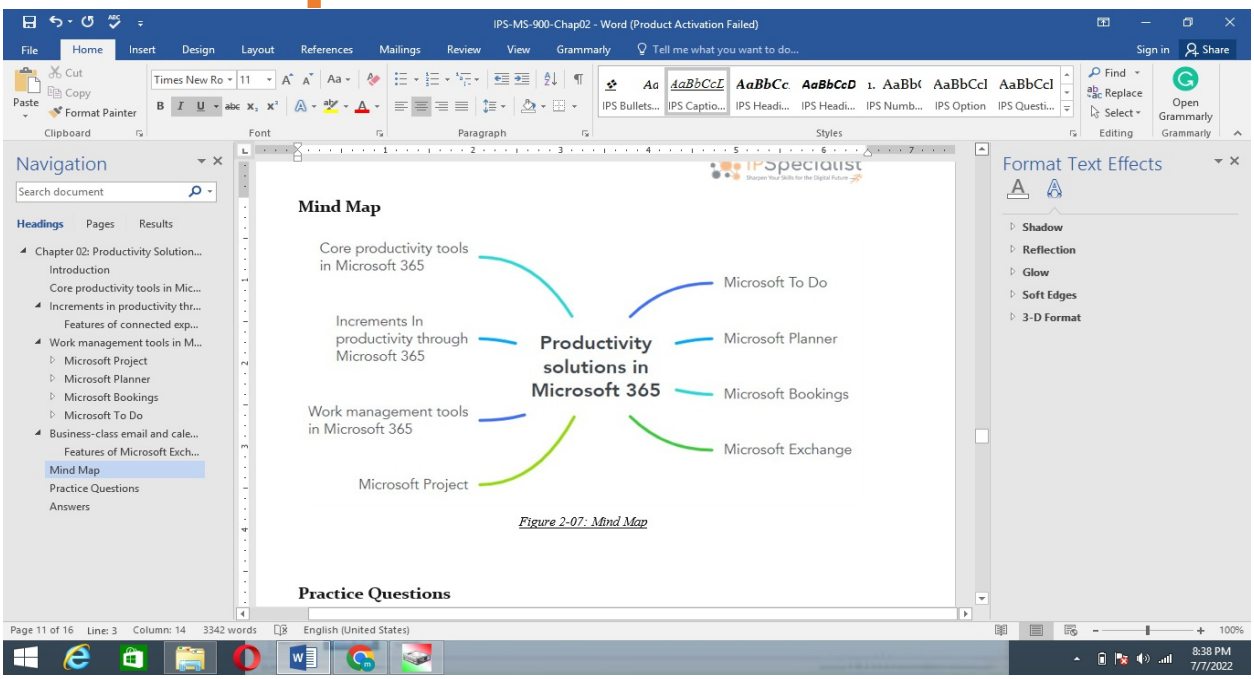
Microsoft Exchange Online is a cloud-based messaging system that provides

the functionality of the Microsoft Exchange Server. It allows users to access email, calendar, contacts, and tasks from PCs, the web, and mobile devices all in one location. It fully interfaces with all other Microsoft 365 workloads, making management simple.

Microsoft corporate email and calendaring assist you in staying on top of your work by providing a clear, uniform perspective of what is important.

-

Mind Map


IPS-MS-900-Chap02 - Word (Product Activation Failed)
Navigation
Mind Map
Core productivity tools in Microsoft 365
Increments In productivity through Microsoft 365
Work management tools in Microsoft 365
Microsoft Project
Productivity solutions in Microsoft 365
Microsoft To Do
Microsoft Planner
Microsoft Bookings
Microsoft Exchange
Figure 2-07: Mind Map
Practice Questions
Format Text Effects

CHAPTER 03: COLLABORATION SOLUTIONS IN MICROSOFT 365

Introduction

People work together more often, in different groups and across multiple locations. They create, share, and collaborate on content to move their teams and organizations forward. Organizations need modern content management and collaboration solutions that are intelligent, secure, and integrated into their daily tools. Microsoft 365 has the tools required for these individuals to connect, collaborate, and get work done swiftly.

Teams provide engaging and inclusive meetings and real-time messaging to connect with colleagues wherever they are. Viva is an employee experience platform that supports organizations create a thriving culture with engaged employees and inspiring leaders. SharePoint lets you collaborate, share content and coordinate your work within your organization. OneDrive gives you secure access and file storage from anywhere. Yammer is an enterprise social connection that lets people engage and connect across the organization. Learn how these Microsoft 365 tools unlock new forms of collaboration to help people stay connected and engaged, ensuring fluid communication across organizations.

Collaboration Workloads of Teams

Microsoft Teams is a hub for teamwork. It is an app for people and teams to come together, stay connected, and get things done across work, home, school, and on the go. Teams help you pull together a team and connect with colleagues through real-time messaging and engaging and inclusive meetings. You can use channels to share files and data, manage tasks, and collaborate on documents with people inside and outside your organization. All these features can be done while staying secure and compliant. Make Teams your own by adding notes and websites and integrating them with your team's other apps and processes.

Users can access Teams through their internet browser or by installing Teams on their computer or mobile device. Teams have many features and functionalities to help your users connect and work together to get things done.

Teams and Channels

Teams encourage your users to organize and collaborate across projects and workloads. Get started by creating a **team** and **channel**.

- **Teams** are a group of people, content, and tools surrounding different organizational projects and outcomes. It is designed to bring together a group of people who work closely to get things done. Teams can be formed to be private to only invited users, and teams can also be public and open to anyone within the company. A team has a limit of up to 10,000 simultaneous members
- **Channels** are assigned sections within a team to keep conversations organized by specific topics, projects, disciplines, or whatever works for your team. It is a place where users can discuss and get hands-on with work. Channels facilitate features like tabs and enable users to access and work on the same content. For instance, users in a team could have a channel with a tab for a specific report they are all contributing to. You share files in a channel (on the Files tab) stored in SharePoint
    - **Standard channels** can be open to all team members
    - **Private channels** are for selected team members
    - **Shared channels** can select people both inside and outside the team

Chat and Instant Messaging

Chat and instant messaging let you work together without cluttering up your email and keeping it clear for important messages. Instant messaging is ideal if you need to check something with a colleague or ask a quick question. You can also have a group discussion to encourage open

discussion and promote thoughtful debate.

Online Meetings

Meetings help teams share status updates, brainstorm ideas, and solve issues. Microsoft Teams is designed to help you have more productive meetings, collaborating through online meetings, webinars, live events, or audio and video conferencing. Microsoft Teams has many features that help your team quickly engage and improve how they work together through meetings.

Microsoft Teams Phone

Stay linked with voice and video calling using **Microsoft Teams Phone** on your computer, tablet, mobile device, or desk phone. Teams phone provides a secure, integrated calling program that unifies classic and modern calling features. You can start a call from chat, contact card, Outlook, or the Calls app, to save time and reduce costs. Teams phone has updated cloud calling features like voicemail transcription and group call pickup to elevate your experience beyond traditional calls. No matter where you decide to work, your calls, voicemail, and call history move with you. Transition calls from your home Wi-Fi to your cellular service while on the go, and then to your office Wi-Fi when you arrive, all from one number using Teams phone.

Extend Teams by Using Collaborative Apps

A **collaborative app** is a solution integrated or built into Teams that enables employees to work better, using the tools they already know. Microsoft Teams is an extensible platform that allows you to create custom applications.

Security and Compliance

Teams are built on Microsoft 365 groups, Microsoft Graph, and the same enterprise-level security, compliance, and manageability as the rest of Microsoft 365 and Office 365.

Core Employee Experience Capabilities in Microsoft Viva

Viva is an EXP that empowers people and teams to be their best from anywhere. Viva brings communications, insights, knowledge, learning, and resources within everyday work and collaboration flow. Viva includes four modules – Viva Connections, Viva Insights, Viva Topics, and Viva Learning.

Viva Connections

Viva Connections was formed to keep everyone in the workforce connected. Today, Microsoft 365 has many capabilities for employee communications and engagement. We have SharePoint, Yammer, Teams, and Stream. Viva Connections brings all of these capabilities into a company-branded app in Teams. It is a gateway to the employee experience, with personalized news, communications, tasks, people, and resources. It offers a single curated employee destination that can be configured for specific roles like frontline workers. Leaders can discuss and engage their employees, and employees can easily access the tools and resources they need from one place.

Viva Insights

Viva Insights provides privacy-protected insights and actionable recommendations that help everyone in the organization work smarter and achieve balance. Viva Insights is accessed in Microsoft Teams. It uses quantitative and qualitative data to empower individuals, managers, and leaders to improve organizational productivity and wellbeing.

Viva Topics

Viva Topics focuses on knowledge and expertise. It uses Artificial Intelligence (AI) to identify knowledge and experts and organizes them into shared topics. Viva Topics helps address many companies' critical business issues: providing users with information when needed. For example, new employee hires need to learn much new information quickly and encounter terms they know nothing about when reading company information. Viva Topics brings knowledge to your users in the Microsoft 365 apps they use daily.

Viva Learning

Viva Learning is a learning hub in Microsoft Teams that lets you seamlessly integrate learning and building skills into your day. In Viva Learning, your team can discover, share, advise, and learn from your organization's and your partners' content libraries.

There are three main views in the Viva Learning app:

- **Home** - Discover new content and trending content, and browse learning content libraries
- **My Learning** - Access your recommendations and assignments, bookmarked, recently viewed, and completed courses
- **Manage -** Track the progress of recommendations that you made

Features of SharePoint and OneDrive Promote Collaboration

When it comes to filing storage, you want your work to be accessible and secure. You want to be able to work with others, co-author, and share files, both inside and outside your organization. **SharePoint** and **OneDrive** enable you to access, share, and collaborate on your files from anywhere.

SharePoint

SharePoint, the intelligent intranet, can help you transform employee communications and digital experiences. It is a rich collaboration tool for creating websites, publishing content, and storing files.

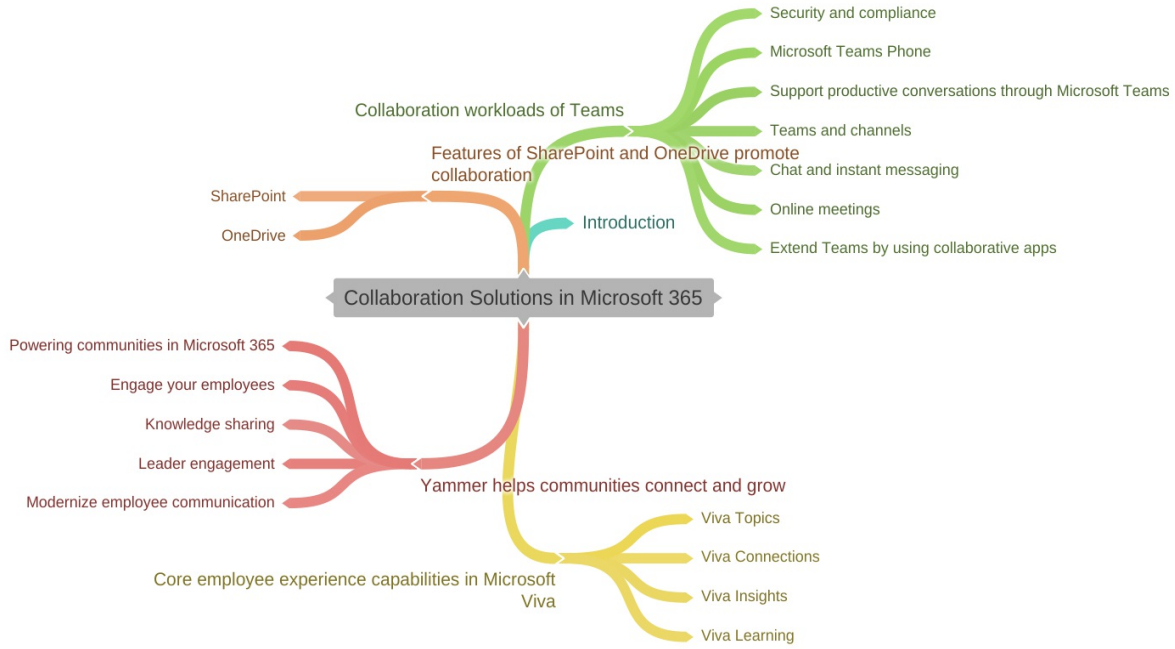
OneDrive

OneDrive is the underlying technology that powers the collaborative files experience across Microsoft 365. OneDrive is a cloud-based service that enables you to access, share, and collaborate on files from anywhere. OneDrive lets users view files within a browser, share and find content, and sync that content so they can access it offline. You can work with others inside or outside your organization and terminate sharing whenever you want. OneDrive also empowers your organization to control, secure, and retain that content when necessary.

Yammer Helps Communities Connect and Grow

Yammer is an enterprise social network internal to an organization. Yammer enables leaders and coworkers to connect and engage from anywhere to share ideas, co-create culture, align on strategy, and innovate. It was designed to help you connect with people you might not work with directly across your organization, and Yammer helps facilitate community collaboration and idea-sharing for your organization. Access Yammer through your browser, or you can install Yammer on your desktop or mobile device.

Mind Map


Collaboration Solutions in Microsoft 365
Introduction
Collaboration workloads of Teams
Security and compliance
Microsoft Teams Phone
Support productive conversations through Microsoft Teams
Teams and channels
Chat and instant messaging
Online meetings
Extend Teams by using collaborative apps
Features of SharePoint and OneDrive promote collaboration
SharePoint
OneDrive
Yammer helps communities connect and grow
Powering communities in Microsoft 365
Engage your employees
Knowledge sharing
Leader engagement
Modernize employee communication
Core employee experience capabilities in Microsoft Viva
Viva Topics
Viva Connections
Viva Insights
Viva Learning

CHAPTER 04: ENDPOINT MODERNIZATION, MANAGEMENT CONCEPTS, AND DEPLOYMENT OPTIONS IN MICROSOFT 365

Introduction

As organizations move more of their workload to the cloud, they can now have employees work from any location and device. Microsoft has built comprehensive cloud computer management solutions as a cloud provider and Operating System (OS) provider. These solutions provide IT departments with remote computer configurations and simplified management tools.

Microsoft Endpoint Manager helps you deploy and manage your organization's devices and Microsoft 365 Apps while delivering a better end-user experience. Windows-as-a-service is a way to simplify the lives of IT pros and maintain a consistent Windows experience for its users through more frequent updates. Windows 365, the new Cloud PC, securely streams your personalized Windows experience to any device, including all your apps, content, and settings. Azure Virtual Desktop, a Virtual Desktop Infrastructure (VDI) solution, allows you to quickly deploy virtual desktops and apps to enable secure remote work. These solutions enable you to meet security and productivity needs while providing a streamlined user experience in a changing workforce.

Endpoint Management Capabilities of Microsoft 365

In today's workplace, IT departments support different devices configured differently. Your organization might have Android and iOS mobile phones, Windows and macOS PCs, and custom devices your users bring to work. **Microsoft 365** provides the tools and services to enable you to simplify the management of all these devices through **Microsoft Endpoint Manager (MEM).**

MEM is a secure and intelligent management solution that improves productivity and collaboration with the familiar experiences users expect.

MEM allows IT to support diverse scenarios for Bringing Your Own Device (BYOD) and corporate-owned devices. MEM helps you solve the device management challenge in today's mobile and remote work environment.

Endpoint Manager mixes services you may know and already be using.

Microsoft Endpoint Manager includes the following service and capabilities:

- **Microsoft Intune**
- **Configuration Manager**
- **Co-management**
- **Desktop Analytics**
- **Windows Autopilot**
- **Azure AD**
- **Endpoint Manager admin center**

Compare Capabilities of Windows 365 and Azure Virtual Desktop.

Windows 365 and **Azure Virtual Desktop** services are virtual desktop solutions, also known as Desktop-as-a-Service. Now explore some of the different capabilities of each.

Windows 365

Windows 365 is a cloud-based service that automatically creates a new type of Windows virtual machine, known as **Cloud PCs,** for your end-users. Securely stream the full Windows experience, including apps, data, and settings, from the Microsoft cloud to any personal or corporate device. Windows 365 provides productivity, security, and collaboration benefits of Microsoft 365. Windows 365 is optimized for simplicity with predictable per-user pricing.

Azure Virtual Desktop

Azure Virtual Desktop (AVD) is a modern and secure desktop and app virtualization solution on Azure. AVD allows users to connect to a Windows desktop running in the cloud, and it is the only solution that delivers multi-session on Windows. AVD optimizes Microsoft 365 Apps for Enterprise, simplifies management with Citrix and VMware, and supports Remote Desktop Service environments. AVD is optimized for flexibility with flexible consumption-based pricing.

Microsoft Office 365 ProPlus

Office ProPlus is a part of Microsoft Office included with our Microsoft 365 license. Like other versions of Microsoft Office, it consists of Access, Excel, OneDrive, OneNote, Outlook, PowerPoint, Publisher, and Skype for Business, Teams, and Word. It is a complete version of the application suite, with the same features and functionality as other versions. Although Office ProPlus is related to other versions of Microsoft Office, there are also differences, which are contained below:

- **For Personal Use:** Unlike other versions of Office on campus, Office ProPlus is supposed to be installed on your systems only (e.g., your home PC or iPad)
- **Licensing:** The licensing model for Office ProPlus is like a subscription - if you remove your subscription, you lose functionality. Suppose you do not connect to the internet after 30 days. In that case, Office ProPlus will go into reduced functionality mode (once you link to the internet again and your status is verified, all features and functionality will be retrieved)
- **Installation & Deployment:** Thanks to Microsoft's "Click-to-Run" technology, you can install Office ProPlus in minutes. You can install this yourself - on your home computer - without the need for additional media or license keys

Deployment and Release Models for Windows-as-a-Service (WaaS)

Windows client is a comprehensive desktop operating system that allows you to work efficiently and securely. It is essential to keep the desktop operating system up to date because it helps devices run efficiently and stay

protected. The WaaS model is designed to simplify life for users and IT professionals, and WaaS maintains a consistent and current Windows client experience for users.

Release Types

With Windows client, there are two release types:

- **Feature updates** add new functionality and are released twice a year. Because these updates are more frequent, they are smaller.
- **Quality updates** provide security and reliability fixes. These updates are issued monthly as **non-security releases** or **combined security + non-security releases.** Non-security releases allow IT admins to do an early validation of content.

Servicing Channels

Servicing channels are the first way to direct users into deployment groups for a feature and quality updates. There are three servicing channels, and each chain channel provides different levels of flexibility when these updates are delivered to client computers.

- **Windows Insider Program** lets organizations test and provide feedback on features shipped in the next update. These features will be delivered during the development cycle. This process will allow organizations to see exactly what Microsoft is developing and start testing as soon as possible. Microsoft recommends that all organizations enroll at least a few devices in this program
- **General Availability Channel** offers new functionality with feature update releases annually. Organizations can choose when to deploy updates. This model is ideal for pilot deployments and testing of feature updates, and it is also ideal for users such as developers who have to work with the latest features
- **A long-term servicing channel** is designed for specialist devices that do not run Office apps, such as medical equipment or ATMs. This channel receives new features every two or three years

Deployment Rings

Deployment rings are a deployment method that separates devices into a deployment timeline, and Microsoft has found that a ring-based deployment works well. Each "ring" contains a group of users or devices that receive a particular update.

Deployment Methods for Windows

To successfully deploy Windows in your organization, it is important to understand how it can be deployed. There are three types of deployment categories or methods:

- **Modern deployment methods** embrace traditional on-premises and cloud services to deliver a streamlined, cost-effective deployment experience. These methods are recommended and are supported by existing tools such as Microsoft Deployment Toolkit (MDT) and Microsoft Endpoint Configuration Manager
- **Dynamic deployment methods** let you configure applications and settings for specific use cases without having to deploy a new custom organization image to the device
- **Traditional deployment methods** use existing tools to install operating system images

Modern Deployment Methods

- **Windows Autopilot** allows IT professionals to customize the Out-Of-Box Experience (OOBE) to deploy pre-configured apps and settings for your organization
- **The in-place upgrade** provides a simple, automated process that uses the Windows setup process to upgrade from an earlier version. This process automatically migrates existing data, settings, drivers, and applications. In-place upgrade requires the least IT effort because no complex deployment infrastructure is needed

Dynamic Deployment Methods

- **Subscription activation** uses a subscription to switch from one edition of Windows to another when a licensed user signs into a device. For example, you can switch from Windows 10 Pro to Windows 10 Enterprise
- **Azure Active Directory (Azure AD) joined with automatic Mobile Device Management (MDM) enrollment** automatically joins the device to Azure AD and is configured by MDM. The organization member must provide their work or school user ID and password
- **Provisioning package configuration** uses the Windows Imaging and Configuration Designer (ICD) tool. This tool creates provisioning packages containing all the configurations, settings, and apps that can be applied to devices

Traditional deployment methods

- **A new computer,** or bare metal, is when you deploy a new device or wipe an existing one with a fresh image
- **Computer refresh,** also called wipe-and-load, is when you redeploy a device by saving the user state, wiping the disk, then restoring the user state
- **Computer replace**ment is when you replace an existing device with a new one. You replace the device by saving the user state on the old device and restoring it to the new one

Manage Windows-as-a-Service

In **Configuration Manager**, you can see the state of WaaS in your environment. You can create service plans to form deployment rings and ensure that Windows systems are up to date when new versions are released.

Identify deployment and servicing methods for Microsoft 365 apps

Microsoft 365 Apps can be installed individually by users on their devices. But it is often beneficial to manage updates and deploy a customized

selection of apps to users' devices to ensure that all users have the apps they need. There are four methods to perform larger-scale deployments of Microsoft 365 Apps in the following list:

- Install from a local source with Configuration Manager
- Install from the cloud with the Office Deployment Tool (ODT)
- Install from a local source with the Office Deployment Tool (ODT)
- Self-install from the cloud

Types of Updates Channels for Microsoft 365 Apps

One of the advantages of Microsoft 365 Apps is that Microsoft offers new and updated features for Office apps regularly. For example, adding improved translation capabilities to Word or supporting 3D animations in PowerPoint. Microsoft provides you options called update channels that allow you to control how often your organization gets these new feature updates.

As needed, Microsoft also provides each update channel with two other types of updates that are updated on the 2nd Tuesday of every individual month:

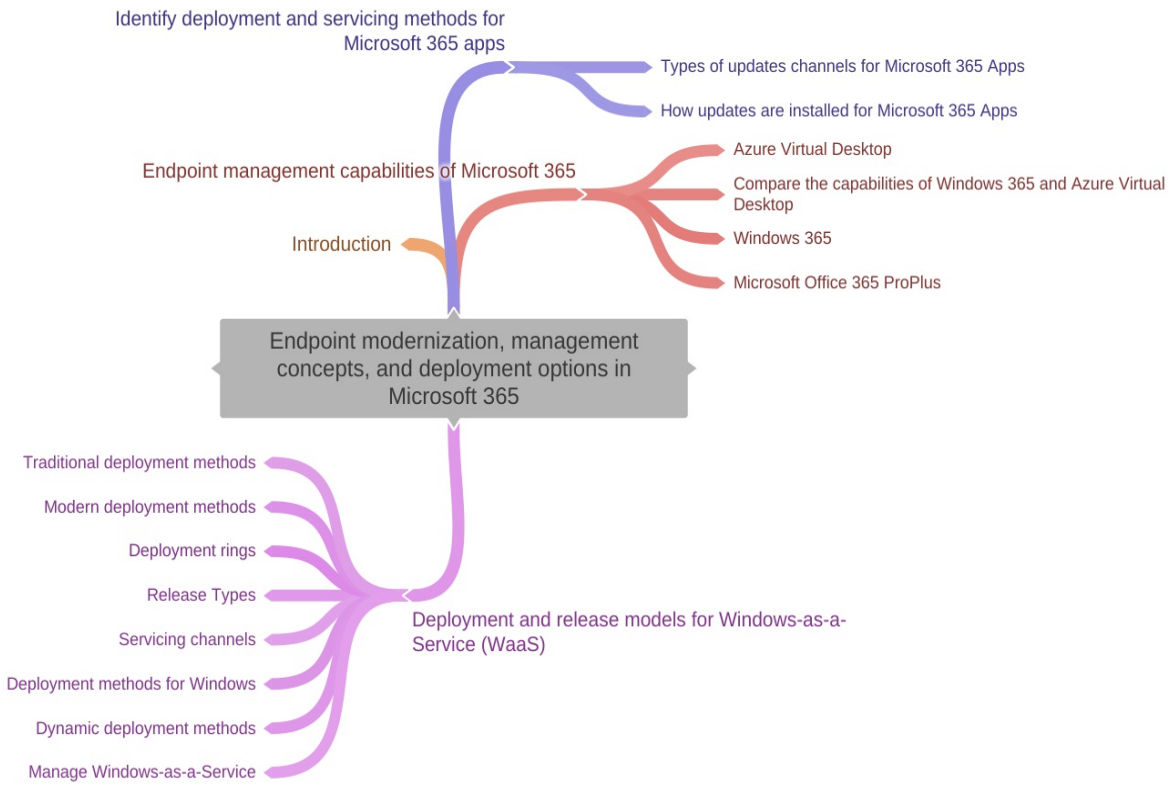
- **Security updates,** such as updates that help keep Office protected from potential malicious attacks
- **Non-security updates (quality updates),** such as updates that provide stability or performance improvements for Office

How Updates are installed for Microsoft 365 Apps

Microsoft 365 Apps regularly check for updates and are downloaded and installed automatically. There are no separate downloads for feature, security, or non-security updates. The updates are cumulative, so the most

current update includes all the updates that have been previously released for that update channel. While updates are being downloaded, your users can continue to use Office apps. After they are downloaded, all the updates for that update channel will install simultaneously

Mind Map


Identify deployment and servicing methods for Microsoft 365 apps
Types of updates channels for Microsoft 365 Apps
How updates are installed for Microsoft 365 Apps
Endpoint management capabilities of Microsoft 365
Azure Virtual Desktop
Compare the capabilities of Windows 365 and Azure Virtual Desktop
Windows 365
Microsoft Office 365 ProPlus
Introduction
Endpoint modernization, management concepts, and deployment options in Microsoft 365
Traditional deployment methods
Modern deployment methods
Deployment rings
Release Types
Servicing channels
Deployment methods for Windows
Dynamic deployment methods
Manage Windows-as-a-Service
Deployment and release models for Windows-as-a-Service (WaaS)

CHAPTER 05: ANALYTICS CAPABILITIES IN MICROSOFT 365

Introduction

Organizations adapting to hybrid work environments focus on encouraging their employees to build better work habits. They want their staff to achieve a balance between productivity and wellbeing. Microsoft Viva Insights gives leaders, managers, and employees privacy-protected insights that help everyone work smarter and thrive. Furthermore, the capabilities of the Microsoft 365 admin center, like the activity reports, can help organizations understand how people are adopting Microsoft 365 products and services. These analytic tools gather data and use Artificial Intelligence (AI) to provide actionable insights that help individuals and organizations do their best work.

Capabilities of Viva Insights

Viva Insights provides privacy-protected insights and actionable recommendations that help everyone in the organization work smarter and achieve balance. Individuals can receive personal insights visible only to them to help identify opportunities to change their habits to do their best work. Insights make it easy for managers to understand current team norms and act to help their groups strike a balance between productivity and wellbeing. Organizational insights for business leaders provide broad visibility across the organization, helping them understand where a change in organizational norms could improve employee experience and business outcomes.

Personal Insights

Individuals can gain valuable insights to improve work patterns through actionable recommendations from the personalized **Viva Insights app in Teams**. For example, prepare for the day with a briefing email, protect time

for focused work, and mindfully disconnect after-hours.

Manager Insights

Manager insights can provide insight to foster a healthy and prosperous team. Understand the work patterns that can lead to burnout and stress for your teams, such as regular after-hours work, meeting overload, or too little focus time. The **Viva Insights App in Teams** makes it easy for managers to understand current team norms and take action to create positive change.

Organizational Insights

Viva Insights provide organizational views to senior business leaders, CEOs, business unit leaders, and other department heads. These experiences in the **Viva Insights App in Teams** show leaders an aggregated view of work and collaboration patterns across their organizations. Leaders can see how people protect personal time, stay connected, manage focus time, and prioritize manager coaching.

Capabilities of the Microsoft 365 Admin Center and Microsoft 365 User Portal

Microsoft 365 admin center

The **Microsoft 365 admin center** is designed for IT professionals and administrators to manage the organization's Microsoft 365 subscription. The admin center allows you to carry out various tasks, like managing users, viewing reports, and much more. Admins can also customize their home page by adding tile cards that point to apps, SharePoint sites, external sites, and more. This customization feature makes it easy for admins to find the relevant sites, apps, and resources to do their job. The following list defines

some of the main tasks that are done in the admin center:

- Manage users by adding, deleting, or restoring users
- Manage licenses by adding and removing their license
- Manage a Microsoft 365 group by creating a group, deleting a group, and editing the name or description
- Manage the bill
- View or create service requests
- Manage global settings for apps
- View activity reports
- View service health

Microsoft 365 User Portal

The **Microsoft 365 user portal** allows users to access their email, calendar, and documents through Microsoft 365 apps like Office, Teams, Outlook, and more. Users can sign in with their email account and password through www.office.com. Only the apps the user has licenses for will appear. The portal allows for quick and easy viewing and editing of files saved online through OneDrive.

Reports Available in the Microsoft 365 Admin Center and Other Admin Centers

Reports in the Microsoft 365 Admin Center

Gather insights on security and see how employees use Microsoft 365 products and services through the available reports in the **Microsoft 365 Admin Center.** You need to have admin permissions to be able to view these types of reports. To access the admin center, go to admin.microsoft.com and sign in with your admin account. Alternatively, you can access the Microsoft 365 admin mobile app.

The following list describes the two types of reports available in the admin center:

- **Productivity score** - The score in this report measures the work done in your organization compared to other organizations like yours. It provides metrics, insights, and recommended actions you can take to help your organization use Microsoft 365 products and services efficiently
- **Usage** - View these reports by time period and Microsoft 365 product or service to understand how people in your organization are using the products and services. You can drill down into each product report to get more detailed insights into the activities within each product. For example, view the number of files stored within OneDrive and SharePoint or Exchange's email and mailbox activity.

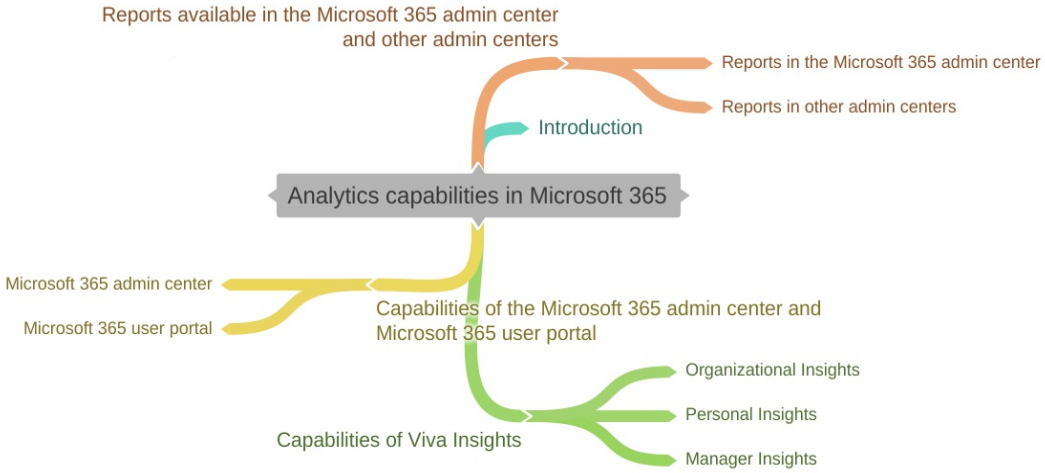
Reports in other admin centers

The **Microsoft 365 Admin Center** also gives you access to other admin centers for specific products and services, such as Exchange, Teams, and more. To access the other admin centers, go to admin.microsoft.com and sign in with your admin account. Once logged in, select **Show** in the navigation menu to find the other admin centers.

Each specialist admin center gives you more options for that area, including reports. The following list describes some of the other admin centers and the reports available:

- **Azure Active Directory**
- **Endpoint Manager**
- **Exchange**
- **Security & Compliance**
- **SharePoint**
- **Teams**
-

Mind Map

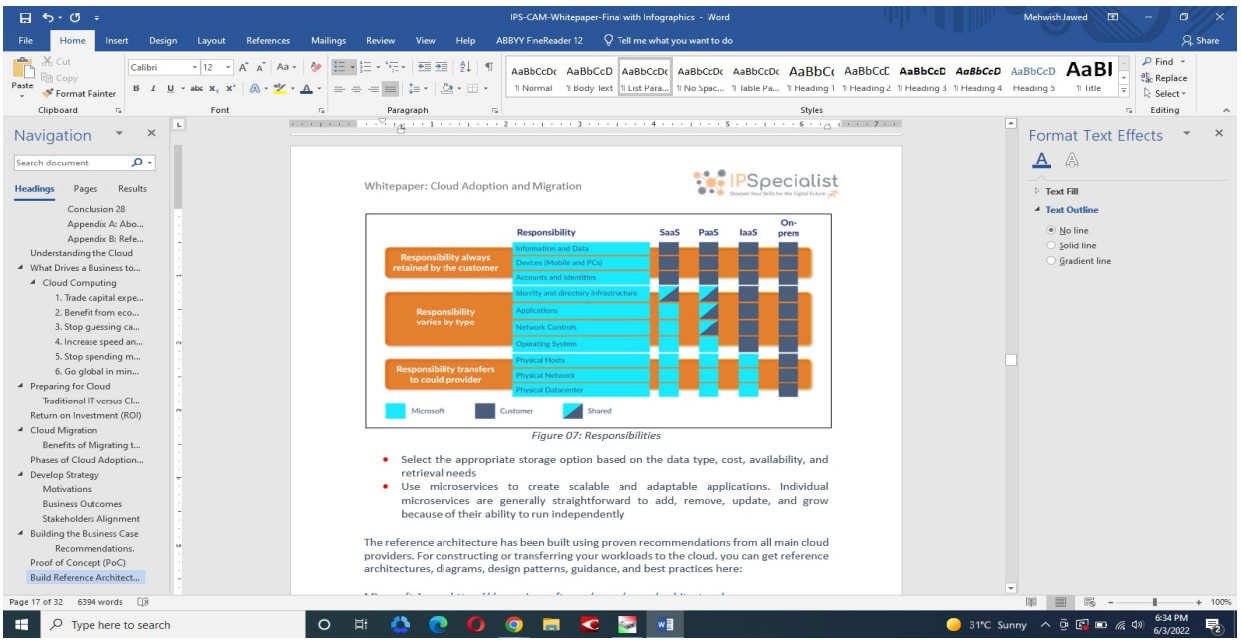

Reports available in the Microsoft 365 admin center and other admin centers
Reports in the Microsoft 365 admin center
Reports in other admin centers
Introduction
Analytics capabilities in Microsoft 365
Microsoft 365 admin center
Microsoft 365 user portal
Capabilities of the Microsoft 365 admin center and Microsoft 365 user portal
Organizational Insights
Personal Insights
Manager Insights
Capabilities of Viva Insights

CHAPTER 06: SECURITY AND COMPLIANCE CONCEPTS

Introduction

Security and compliance have become dominant concerns as more business data is accessed from locations outside the traditional corporate network. In addition, organizations need to ensure they are compliant with industry and regulatory requirements to ensure the protection and privacy of data.

This chapter introduces some critical security and compliance concepts. You will learn about shared responsibility, defense-in-depth, and Zero Trust models. You will be introduced to encryption and hashing as ways to protect data. Lastly, you will learn about concepts that relate to compliance.



Shared Responsibility Model

The *shared responsibility model* defines which security tasks are managed by the cloud provider and which security tasks are managed by you, the customer. The responsibilities differ depending on where the workload is hosted:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)

- Software as a Service (SaaS)
- On-premises datacenter

The following diagram defines areas of responsibility between customer and cloud provider, as per the location of data.

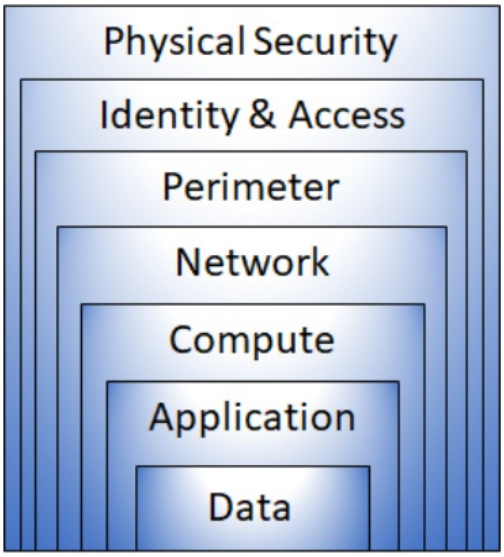
- **Infrastructure as a Service (IaaS)**. With IaaS, you are using the cloud provider's computing infrastructure. The cloud customer is not responsible for the physical components, such as computers, the network, or the data center's physical security
- **Platform as a Service (PaaS)**. PaaS offers an environment for building, testing, and deploying software applications. With PaaS, the cloud provider operates the hardware and operating systems, and the customer is accountable for applications and data
- **Software as a Service (SaaS)**. It is usually licensed through a monthly or annual subscription, and SaaS requires the minimum amount of management by the cloud customer

Defense in Depth

Each layer offers protection so that if one layer is breached, a subsequent layer will remove an attacker getting unauthorized access to data.

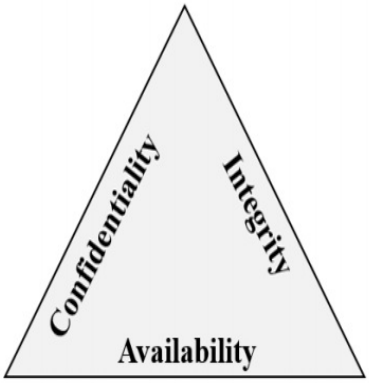
Example layers of security might include:

- **Physical** security limits the view of a data center to only allowed personnel
- **Perimeter** security of your corporate network consists of Distributed Denial of Service (DDoS) protection to filter large-scale attacks before they can form a denial of service for end-users
- **Network** security, such as network segmentation and access controls, limits the link between resources
- **Application** layer security ensures applications are secure and free of security vulnerabilities
- **Data** layer security contains controls to manage access to business and customer data and encryption to secure data



Confidentiality, Integrity, Availability (CIA)

All the different mechanisms (technologies, processes, and training) are key to a cybersecurity strategy, whose goals consist of ensuring confidentiality, integrity, and availability, often referred to as CIA.



- **Confidentiality** defines the need to keep confidential, sensitive data such as customer information, passwords, or financial data
- **Integrity** defines as keeping data or messages correct. Integrity is the confidence that data has not been tampered with or modified
- **Availability** is making data available to those who need it when needed

While the goals of a cybersecurity strategy are to preserve the confidentiality, integrity, and availability of systems, networks, applications,

and data, it is the goal of cybercriminals to disrupt these goals. Microsoft's portfolio includes the solutions and technologies to enable organizations to deliver on the goals of the CIA triad.

Zero Trust Model

Introduction

"Trust no one, verify everything" is a principle upon which Zero Trust Methodology operates. It believes that nothing is worth our trust, even the resources behind the firewalls of a corporate network. The way the attackers are getting their hands-on conventional access controls proves that traditional security strategies are no longer satisfactory and, hence, have been marked as inadequate to serve all types of security needs. Multifactor authentication should be used to provide appropriate scrutiny for the networks and data to validate the user. Another way to shield all networks is by limiting the access to data of corporate networks.

Principles of Zero Trust Model

The Zero Trust Model works on three principles that perfectly show how the security is actually carried through. These three principles are jotted down below:

Verify Explicitly

Verification and authentication of these data points are necessary: user identity, location, device, service or workload, data classification, and anomalies.

Least Privileged Access

To protect data effectively, you must limit user access through ingenious tactics, such as risk-based adaptive policies, data protection to protect data

and productivity, and Just-In-Time and Just-Enough Access (JIT/JEA).

Assume Breach

Division of access should be conducted amongst the user, devices, and the application. Analytics are used to promote security and detect threats, while encryption protects all the data.

Six Foundational Pillars of Zero Trust Model

To provide end-to-end security, six elements that act as the foundational pillars of a Zero Trust Model work together to secure grounds.

Identities

This includes the identities of users, services, or devices. Proper and strong authentication is required when any sort of identity tries to access anything.

Devices

Monitoring devices to be in the service of safeguarding and complying is the most crucial aspect of security. Devices create large attack grounds when the data flow from devices to workloads and the cloud; hence, their security should be the goal.

Applications

This pillar encapsulates how data is consumed; it includes discovering all applications being used, sometimes called Shadow IT because all the applications are sometimes not managed midway. Moreover, this pillar also includes managing permissions and access.

Data

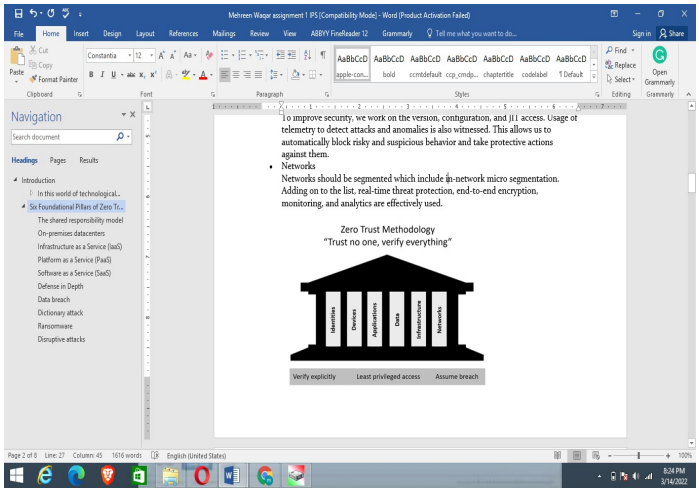
Data should be classified, labeled, and encrypted according to its attributes. Security efforts are solely about protecting data and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization has in control.

Infrastructure

We work on the version, configuration, and JIT access to improve security. Usage of telemetry to detect attacks and anomalies is also witnessed. This allows us to automatically block risky and suspicious behavior and take protective actions against them.

Networks

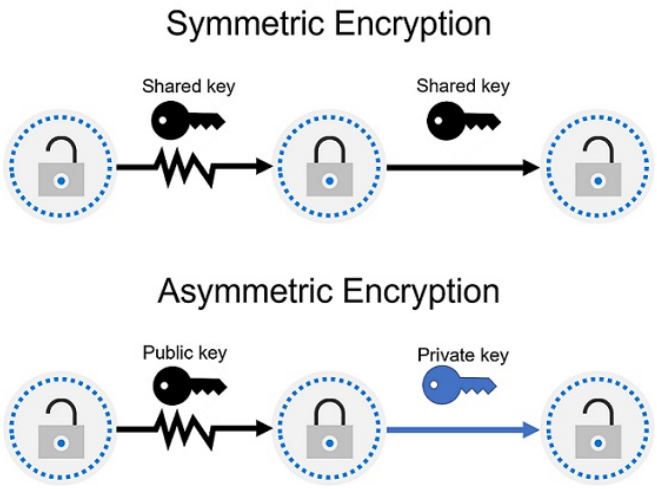
Networks should be segmented, which includes in-network micro-segmentation. Adding on to the list, real-time threat protection, end-to-end encryption, monitoring, and analytics are effectively used.



A security strategy that employs the three principles of the Zero Trust model across the six foundational pillars helps companies deliver and enforce security across their organization.

Encryption and Hashing

Either key can encode data, but a single key cannot be used to decrypt encrypted data. To decrypt, you need a paired key. Asymmetric encryption is used to access sites on the internet using the HTTPS protocol and electronic data signing solutions.



Encryption for Data at Rest

Data at rest is the data that is stored on a physical device, such as a server.

If an attacker receives a hard drive with encrypted data and does not have a view of the encryption keys, they will be unable to view the data.

Encryption for Data in Transit

Several different layers can handle the secure transfer, which could be done by encrypting the data at the application layer before sending it on a network.

Encrypting data in transit prevents it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

Encryption for Data in Use

An everyday use case for encryption of data in use involves securing data in non-persistent storage, such as RAM or CPU caches. This can be achieved through technologies that create an enclave (a secured lockbox) that protects and keeps data encrypted while the CPU processes the data.

Hashing

Hashing utilizes an algorithm to convert text to a *unique* fixed-length value

called a hash. The same hash value is produced each time the exact text is hashed using the same algorithm.

Compliance Concepts

Data has become more critical than ever. Organizations, institutions, and entire societies generate and rely on data to function daily. The sheer scale of data generated and the increasing reliance on it means that the privacy and protection of that data have become pivotal. As organizations and institutions move their data to service provider clouds, with data centers worldwide, additional considerations come into play.

Government agencies and industry groups have issued regulations to help protect and govern the use of data. Listed below are some essential concepts and terms that relate to data compliance.

- **Data residency** - When it comes to compliance, data residency regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally. These regulations can differ significantly depending on the jurisdiction
- **Data sovereignty** - Another important consideration is data sovereignty, the concept that data, particularly personal data, is subject to the rules of the country/region in which it is physically collected, held, or processed. This can add a layer of complexity regarding compliance because the same data can be collected in one location, stored in another, and processed in another, subjecting it to laws from different countries/regions
- **Data privacy** - Providing notice and transparency about collecting, processing, using, and sharing personal data are fundamental principles of privacy laws and regulations. Privacy

laws previously referenced "PII" or "personally identifiable information," but the laws have expanded the definition to any data directly linked or indirectly linkable to a person. Organizations are subject to and must operate consistently with many laws, regulations, codes of conduct, industry-specific standards, and compliance standards governing data privacy

In most cases, laws and regulations do not define or prescribe specific technologies organizations must use to protect data. They leave it to an organization to identify compliant technologies, operations, and other appropriate data protection measures.

Microsoft 365 Compliance Center

The Microsoft 365 compliance center combines the tools and data needed to help understand and manage an organization's compliance needs.

The compliance center is available to customers with a Microsoft 365 SKU with one of the following roles:

- Global Administrator
- Compliance Administrator
- Compliance Data Administrator

Compliance Manager

Microsoft Compliance Manager is a Microsoft 365 compliance center feature that helps admins manage an organization's compliance requirements with greater ease and convenience. It can help organizations throughout their compliance journey, from taking inventory of data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Mind Map


coggle.it/diagram/YsGL1-PT1iLZw_bY/t/-
coggle
Public Diagram
Share Responsibility Model
Compliance Concept
Compliance Center
Compliance Manager
Compliance Score
Availability
Confidentiality
Integrity
Defense in depth
Introduction
Security and Compliance Concept
Encryption for data in use
Encryption for data at rest
Encryption for data in transit
Encryption and Hashing
Introduction
Guiding Principles
Foundational Pillars
Least Privileged Access
Zero Trust Model
Keyboard Shortcuts and Help
Open the help sheet to see keyboard shortcuts, and quickly search help articles
MS-900 CHAP 10....docx
MS-900 CHAP 11....docx
MS-900 CHAP 12....docx
Show all
5:39 PM
7/3/2022

CHAPTER 07: IDENTITY CONCEPTS

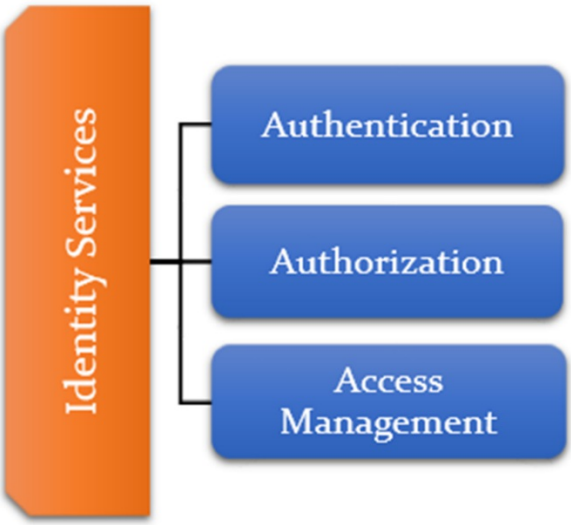
Introduction

Identity is how people and things are identified on your corporate network and in the cloud. Knowing who or what is accessing your organization's data and other resources is a fundamental part of securing your environment.

In this section, you will study critical concepts of authentication and authorization and why identity is essential in securing corporate resources. You will also learn about some identity-related services.

Identity Services

When users use an online service with no privacy criteria, the user requires at least a username (the User ID) and password. Identity services include authentication, authorization, and access management policies.



Authentication and Authorization

Authentication

Authentication is proving that a person is who they say they are. Anyone purchasing an item with a credit card may be required to show an extra form of identification, proving that they are the person whose name appears on the card. In this example, the user may show a driver's license that is a

form of authentication and proves their ID.

You will encounter similar authentication when you want to access a computer or device. You may get asked to enter a username and password. The username states who you are, but by itself is not enough to grant you access. When combined with the password, which only that user should know, it allows access to your systems. The username and password are a form of authentication, and authentication is sometimes shortened to AuthN.

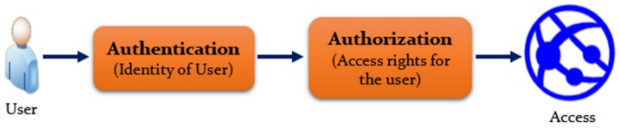
Authorization

Once you authenticate a user, you must decide where they can go and what they are allowed to see and touch. This process is called authorization.

Suppose you want to spend the night in a hotel. The first thing you will do is go to reception to start the "authentication process." After the receptionist has verified you, you are given a keycard and can go to your room. Think of the keycard as the authorization process. The keycard will only let you open the doors and elevators you are permitted to access, such as your hotel room.

In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to AuthZ.

The process of identity service is clearly shown in the scenario defined in Figure 7-02.



Access Management

Access management is a critical part of any cloud infrastructure as it ensures the restriction of access to services toward other users. It provides confidentiality, integrity, and availability. This means that access to any online application should be confidential for an unauthorized user and immediately available to authorized users. Access management policies should also be responsible for the following:

- **Authentication and Authorization:** The user must be authenticated first, then authorized for the particular application
- **Faraway from Unauthorized Users:** Access management policies must be designed in such a way that no unauthorized person can access the information.

Identity as the Primary Security Perimeter

Digital collaboration has changed. Your employees and partners now need to collaborate and access organizational resources from anywhere, on any device, and without affecting their productivity.

Enterprise security requires adapting to this new reality. The security perimeter can no longer be performed as the on-premises network, and it now extends to:

- SaaS applications for business-critical workloads that might be formed outside the network
- The personal devices that users are using to let corporate resources (BYOD or bring your device) while working from home
- The unmanaged devices used by users or customers when letting with corporate data or collaborating with employees
- Internet of things, referred to as IoT devices, are installed throughout your professional network and inside customer locations

Four Pillars of an Identity Infrastructure

There is a collection of processes, technologies, and policies for managing

digital identities and controlling how they are used to access resources. These can be organized into four fundamental pillars that organizations should consider when creating an identity infrastructure.

- **Administration** - The administration is about the formation and management/governance of identities for users, devices, and services
- **Authentication** - The authentication pillar describes the story of how much an IT system needs to know about identity to have sufficient proof that they are who they say they are
- **Authorization** - The authorization pillar lets the incoming identity data define the level of access
- **Auditing** - The auditing pillar tracks who does what, when, where, and how. Auditing contains in-depth reporting, alerts, and governance of identities

Role of the Identity Provider

With modern authentication, all services are supplied by a central identity provider. Information used to authenticate the user with the server is stored and managed centrally by the identity provider.

Organizations can establish authentication and authorization policies with a central identity provider, monitor user behavior, identify suspicious activities, and reduce malicious attacks.

The server checks the security token through its *trust relationship* with the identity provider. The user or application accesses the required resources on the server by using the security token and the information. In this case, the token and the information it contains is stored and managed by the identity provider, and the centralized identity provider supplies the authentication service.

Single sign-on

Another essential capability of an identity provider and "modern authentication" is the Single Sign-On (SSO) support. With SSO, the end-user logs in once, and that request is used to view multiple applications or resources. When you set up SSO between multiple identities providers, it is called federation.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) provides a layer-based authentication using more than one form of authentication. This means that if attackers compromise one, then they will still not be able to get in. MFA is recommended as a default. It is a part of AAD that enables other ways to authenticate users. MFA is needed in organizations that have a large number of users, devices, and resources. To avoid any collapse, extra security is required for protection and efficient throughput.

Concept of Directory Services and Active Directory

In the view of a computer network, a directory is a hierarchical structure that keeps data about users on the network.

Active Directory

Active Directory (AD) is a group of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks. Active Directory Domain Services (AD DS) is the best-known service of this kind. It stores information about domain members, containing devices and users, verifies their credentials, and describes their view rights.

AD DS is the main component in organizations with on-premises IT infrastructure. AD DS allows organizations to operate multiple on-premises

infrastructure components and systems using a single identity per user. AD DS does not, however, natively verifies mobile devices, SaaS applications, or line of business apps that require *modern authentication* methods.

The growth of cloud services, SaaS applications, and personal devices being used at work has resulted in the need for modern authentication and the evolution of Active Directory-based identity solutions.

Active Directory (AD) is a directory service created by Microsoft for storing information about users, resources, and other networked objects. Offices, educational institutions, and management departments all employ AD.

- **Limitation of Active Directory:** Active Directory provides information for authentication and authorization, but it has some limitations;
  - **Traditional Use Only:** Active Directory provides directory services for physical access only. It is most commonly used in the on-premises network
  - **Not Permitted for Web Applications:** Active Directory is not applicable to serve its services for web applications
  - **Authentication:** Active Directory provides such directory services for authentication that is not available on Azure

Concept of Federation

Federation lets the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain's identity providers. With federation, users are not required to maintain a different username and password when viewing resources in other domains.

Conditional Access

By establishing conditions that must be satisfied before allowing access to a piece of material, conditional access safeguards controlled content in a system. If-then clauses are the most basic form of conditional access restrictions. The completion of an activity is required for users to access a resource.

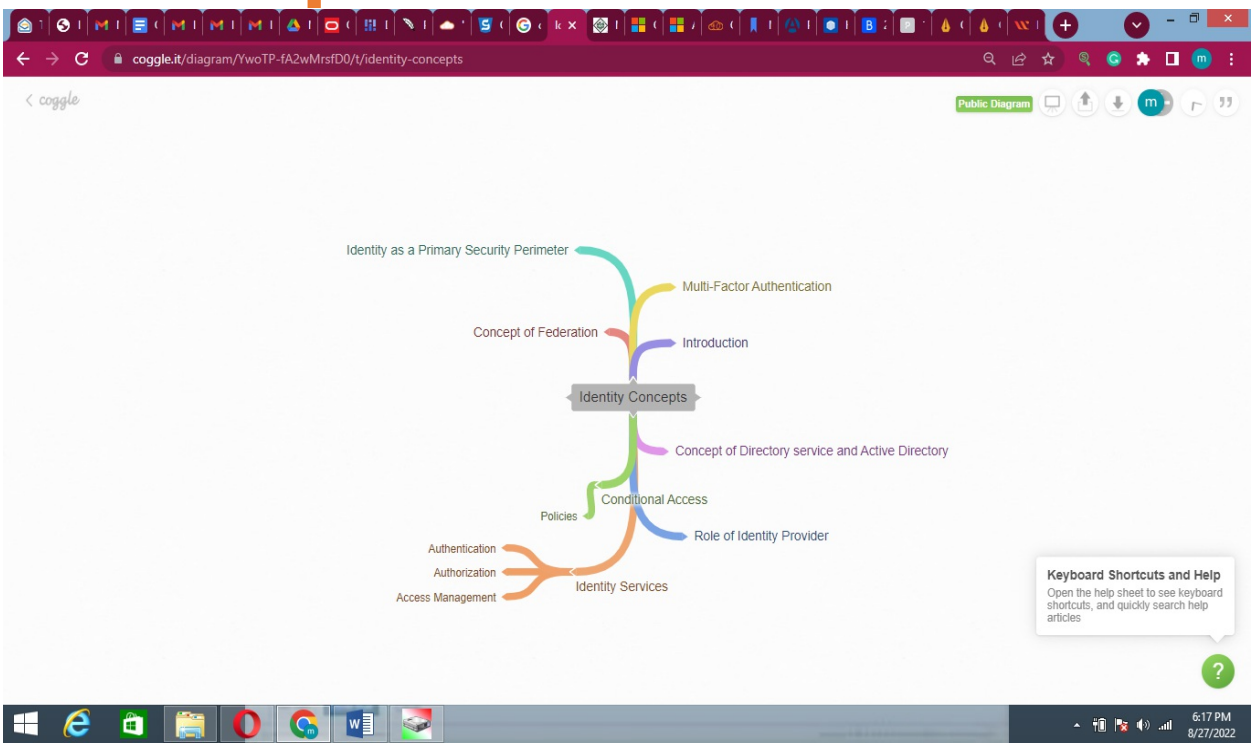
Conditional Access Policies

Conditional Access policies might provide you greater control if your company needs more precise sign-in security requirements. With conditional access, you can design rules that respond to sign-in events and demand further steps before allowing a user access to a service or application.

Customers who have purchased Azure AD Premium P1 or licenses that contain it, such as Microsoft 365 Business Premium and Microsoft 365 E3, are eligible for Conditional Access. Create a Conditional Access policy for additional details.

Through the Azure AD Premium P2 license or licenses that contain it, such Microsoft 365 E5, risk-based conditional access is allowed.

Mind Map



CHAPTER 08: THREAT PROTECTION WITH MICROSOFT 365 DEFENDER

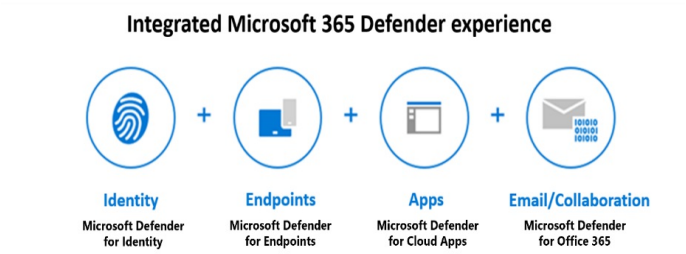
Introduction

This chapter will teach you how Microsoft 365 Defender can help protect your organization. You will explore each of the different Defender services to understand how they can protect: Identity, Office 365, Endpoint, and cloud apps. You will also explore the capabilities of the Microsoft 365 Defender portal, including Microsoft Secure Score, reports, and incident management.

Microsoft 365 Defender Services

Microsoft 365 Defender is a defense suite that prevents cyberattacks. With Microsoft 365 Defender, you can natively communicate the detection, prevention, investigation, and response to threats across endpoints, identities, emails, and applications.

Microsoft 365 Defender gives administrators the ability to evaluate danger signals from endpoints, applications, emails, and identities to ascertain the breadth and effect of an assault. It sheds more light on how the threat materialized and which systems were impacted. The assault can then be prevented or stopped automatically by Microsoft 365 Defender.



Microsoft 365 Defender suite prevents:

- **Indicate with Microsoft Defender for Identity and Azure AD Identity Protection** - It utilizes Active Directory signals to identify, define, and investigate advanced threats, compromised identities, and malicious insider actions formed at your company

- **Endpoints with Microsoft Defender for Endpoint** - It is a single endpoint for preventative protection, post-breach identification, automated investigation, and response
- **Applications with Microsoft Defender for Cloud Apps** - Microsoft Defender for Cloud Apps is a leading cross-SaaS solution that offers deep visibility, strong data controls, and identify threat protection
- **Email and collaboration with Microsoft Defender for Office 365** protect your organization against malicious threats from email messages, links (URLs), and collaboration tools

Microsoft Defender for Office 365

Microsoft Defender for Office 365 protects your organization against malicious threats from email messages, links (URLs), and collaboration tools containing Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.

Microsoft Defender for Office 365 contains these key areas:

- **Threat protection policies**: Describe threat protection policies to set the appropriate level of protection for your organization
- **Reports**: View real-time reports to monitor your organization's Microsoft Defender for Office 365 performance
- **Threat investigation and response capabilities**: Use leading-edge technologies to identify, understand, simulate, and modify threats

Microsoft Defender for Office 365 is accessible in two plans. The plan you choose influences the tools you will see and use. It is important to make sure you select the best plan to meet your organization's needs.

Microsoft Defender for Office 365 Plan 1

This plan offers configuration, protection, and identification tools for your Office 365 suite:

- **Safe Attachments**: Verifies email attachments for harmful content
- **Safe Links**: A safe link remains accessible but stops harmful links
- **Safe Attachments for SharePoint, OneDrive, and Microsoft Teams**: Prevents your organization when users collaborate and share files by defining and blocking malicious files in team sites and document libraries
- **Anti-phishing protection**: Recognize attempts to impersonate your users and internal or custom domains
- **Real-time detections**: A real-time report lets you detect and analyze recent threats

Microsoft Defender for Office 365 Plan 2

This plan contains all the core features of Plan 1 and provides automation, investigation, remediation, and simulation tools to help prevent your Office 365 suite:

- **Threat Trackers**: Offer the latest intelligence on prevailing cybersecurity issues, allowing an organization to take countermeasures before an actual threat
- **Threat Explorer**: A real-time report that lets you detect and analyze new threats
- **Automated Investigation and Response (AIR)**: This contains a set of security playbooks that can be formed automatically, such as when an alert is formed or manually
- **Attack Simulator**: This lets you run realistic attack cases in your organization to identify vulnerabilities.
- **Proactively hunt for threats with advanced hunting in Microsoft 365 Defender**: Advanced hunting is a query-based threat hunting tool that lets you explore up to 30 days of raw data
- **Investigate alerts and incidents in Microsoft 365 Defender**: Microsoft Defender for Office 365 P2 customers can view Microsoft 365 Defender integration to efficiently detect, review, and respond to incidents and alerts

Microsoft Defender for Office 365 Availability

If the subscription does not contain Defender for Office 365, you can buy it as an add-on. Use Microsoft 365 Defender for Office 365 to prevent your organization's collaboration tools and messages.

Microsoft Defender for Endpoint

This technology contains endpoint behavioral sensors that gather and prevent signals from the operating system, cloud security analytics that converts signals into insights, detections, and recommendations, and threat intelligence to detect attacker tools & techniques and generate alerts.

Microsoft Defender for Endpoint includes:

- **Attack Surface Reduction**
- **Next-Generation Protection**
- **Endpoint Detection and Response**
- **Microsoft Threat Experts**

Microsoft Defender for Cloud Apps

Moving to the cloud enhances flexibility for employees and IT teams. Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB). It is a comprehensive cross-SaaS solution that operates as an intermediary between a cloud user and the provider.

What is a Cloud Access Security Broker?

In order to facilitate real-time access between your enterprise users and the cloud resources they need, regardless of where they are located or the device they are using, a CASB serves as a gatekeeper. CASBs offer a broad range of capabilities across the following pillars to assist organizations in protecting their environment:

- **Visibility** - Detect cloud services and app use and provide visibility into Shadow IT

- **Threat protection** - Monitor user activities for abnormal behaviors, control access to resources through access controls, and mitigate malware
- **Data security** - Identify, classify and control sensitive information, protecting against malicious actors
- **Compliance** - Assess the compliance of cloud services

Office 365 Cloud App Security

Office 365 Cloud App Security is a part of Microsoft Defender for Cloud Apps that offer enhanced visibility and control for Office 365. Office 365 Cloud App Security consists of threat detection based on user activity logs.

It offers a subset of the core Microsoft Defender for Cloud Apps features. It also provides a reduced subset of the Microsoft Defender for Cloud Apps discovery capabilities.

Use Microsoft Defender for Cloud Apps to intelligently and proactively identify and respond to threats across your organization's Microsoft and non-Microsoft cloud services.

Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution. It utilizes your on-premises Active Directory data (called signals) to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions moved at your organization.

Microsoft Defender for Identity provides security professionals managing hybrid environments functionality to:

- Monitor and profile user behavior and activities
- Prevent user identities and reduce the attack surface
- Identify and investigate suspicious activities and advanced attacks

across the cyberattack kill chain

Monitor and Profile User Behavior and Activities

Defender for Identity manages and analyzes user activities and information across your network, containing permissions and group membership, forming a baseline for each user. Defender for Identity then describes anomalies with adaptive built-in intelligence.

Protect User Identities and Lower the Attack Surface

Defender for Identity provides insights on identity configurations and suggested security best practices. It offers extra insights into how to improve security posture and policies.

For hybrid environments in which Active Directory Federation Services (AD FS) is present, Defender for Identity protects the AD FS by detecting on-premises attacks and providing visibility into authentication events generated by the AD FS.

Detect Suspicious Activities and Advanced Attacks Across the Cyberattack Kill-Chain

These assets might comprise sensitive accounts, domain administrators, and highly sensitive data. Defender for Identity identifies these advanced threats at the source throughout the entire cyber-attack kill-chain:

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance

Microsoft Defender Protection

Microsoft's 365 Defender services defend against:

- Endpoints equipped with Defender for Endpoint – Defender for Endpoint is a unified endpoint platform for proactive security, post-breach detection, automated investigation, and response
- Defender's assets Microsoft Defender Vulnerability Management provides continuous asset visibility, intelligent risk-based assessments, and built-in remediation tools to assist your security and IT teams in prioritizing and addressing important vulnerabilities and misconfigurations throughout your organization
- Email and collaboration with Defender for Office 365 - Defender for Office 365 protects your business from harmful threats from collaboration tools, links (URLs), and email communications
- Defender for Identity uses your on-premises Active Directory Domain Services (AD DS) signals to identify, detect, and look into advanced threats, compromised identities, and malicious insider actions targeted at your company. Identity protection with Azure Active Directory (Azure AD) and Defender for Identity. Azure AD Identity Protection automates identifying and correcting identity-based hazards in your cloud-based Azure AD

Microsoft 365 Defender portal

Microsoft 365 Defender natively coordinates detection, prevention, investigation, and response across endpoints, identities, emails, and applications to provide integrated protection against sophisticated attacks. The Microsoft 365 Defender portal combines this functionality into a central place designed to meet security teams' needs and emphasizes quick access to information and more straightforward layouts. You can view your organization's security health through the Microsoft 365 Defender portal.

Incidents and Alerts

Individual alerts offer valuable clues about a completed or ongoing attack,

and Microsoft 365 Defender automatically aggregates these alerts. The grouping of these related alerts forms an incident, and the incident provides a comprehensive view and context of an attack.

The incidents queue is a central location that lists each incident by severity.

Hunting

Advanced hunting is a query-based threat-hunting option that lets security professionals explore up to 30 days of raw data. Advanced hunting queries enable security professionals to proactively search for threats, malware, and malicious activity across your endpoints, Office 365 mailboxes, and more. Threat-hunting queries can be used to build custom detection rules. These rules automatically check for and respond to suspected breach activity, misconfigured machines, and other findings.

Threat Analytics

Threat analytics is our in-product threat intelligence solution from expert Microsoft security researchers. It is designed to assist security teams in tracking and responding to emerging threats. The threat analytics dashboard highlights the most relevant reports to your organization. It includes the latest threats, high-impact threats (threats with the most active alerts affecting your organization), and high-exposure threats.

Secure Score

An indicator of a company's security posture is the Microsoft Secure Score, one of the features in the Microsoft 365 Defender site. Your protection will be better the higher the score. The security of an organization's Microsoft 365 identities, apps, and devices can be monitored and improved via a single dashboard through the Microsoft 365 Defender site.

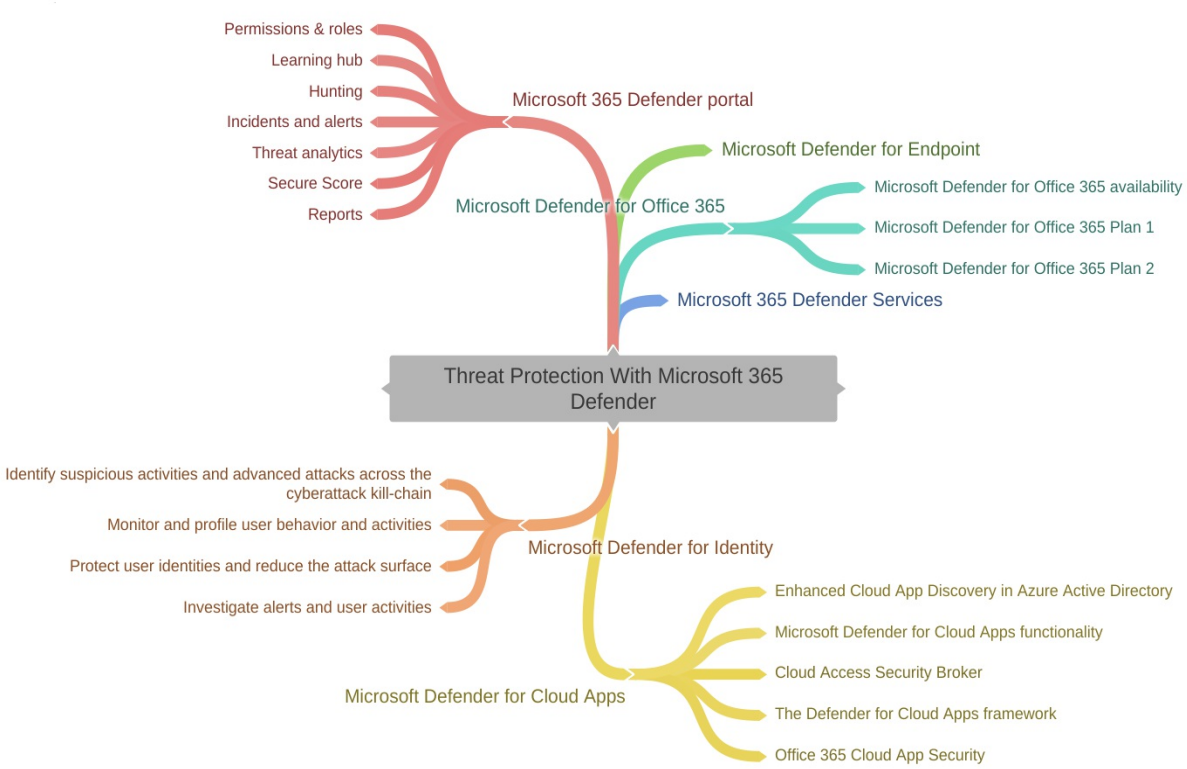
Using Secure Score, enterprises can:

- Provide an update on their security posture.
- By offering discoverability, visibility, direction, and control, their security posture will be strengthened.
- Identify benchmarks and important performance indicators (KPIs).

Incidents Capabilities

Incidents are a group of correlated alerts made when a suspicious event is found. Alerts are created from different devices, users, and mailbox entities. They can come from many different domains. Microsoft 365 Defender automatically aggregates these alerts.

Mind Map


Threat Protection With Microsoft 365 Defender
Microsoft 365 Defender portal
Permissions & roles
Learning hub
Hunting
Incidents and alerts
Threat analytics
Secure Score
Reports
Microsoft Defender for Office 365
Microsoft Defender for Endpoint
Microsoft Defender for Office 365 availability
Microsoft Defender for Office 365 Plan 1
Microsoft Defender for Office 365 Plan 2
Microsoft 365 Defender Services
Microsoft Defender for Identity
Identify suspicious activities and advanced attacks across the cyberattack kill-chain
Monitor and profile user behavior and activities
Protect user identities and reduce the attack surface
Investigate alerts and user activities
Microsoft Defender for Cloud Apps
Enhanced Cloud App Discovery in Azure Active Directory
Microsoft Defender for Cloud Apps functionality
Cloud Access Security Broker
The Defender for Cloud Apps framework
Office 365 Cloud App Security

CHAPTER 09: SERVICE TRUST PORTAL AND PRIVACY AT MICROSOFT

Introduction

Organizations all across the world are very concerned about data protection and compliance. Thanks to the Service Trust Portal launch, those striving to support or safeguard users' right to privacy in Microsoft's online environment may now rest comfortably.

Microsoft Cloud services are built on trust, security, and compliance. The Microsoft Service Trust Portal provides various content, tools, and other resources about Microsoft security, privacy, and compliance practices.

Microsoft also helps organizations meet their privacy requirements with Microsoft Priva. Priva helps organizations protect personal data and build a privacy-resilient workplace.

Trust Center

Trust Center is a shortcut to knowing everything that Microsoft does to ensure you do not lose trust in Microsoft. With this, you have a link to learn about security, privacy, GDPR, data location, compliance, and more. This link lets you know more about security implementations, privacy implementations, etc.

The Trust Center demonstrates how Microsoft implements and supports security, privacy, compliance, and transparency in all of its cloud products and services and the company's guiding principles for preserving data integrity in the cloud. The Microsoft Trusted Cloud Initiative's Trust Center is a key component that offers materials and assistance to the legal and compliance sector.

The Trust Center gives you:

- Comprehensive details on the capabilities, offerings, rules, and practices used by Microsoft cloud solutions in terms of security, privacy, and compliance

- Additional sources for every subject.
- Links to forthcoming events and the security, privacy, and compliance blogs
- For additional employees in your company who might be involved in compliance, security, and privacy, the Trust Center is a valuable resource. These individuals consist of business managers, privacy and risk officers, and legal compliance teams

Service Trust Portal (STP)

The Service Trust Portal, often known as STP, is a tool included in Microsoft Office 365 that offers existing and potential users of the software a variety of information on how the tech giant maintains privacy, compliance, and security.

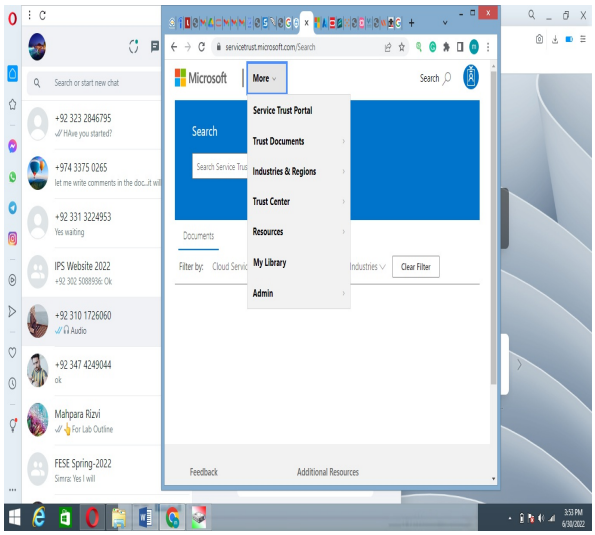
Microsoft publishes information on this platform that businesses need to do due diligence on and assess all of Microsoft's cloud services. Microsoft introduced this service to make its users' assessments more transparent, better understood, and simpler.

What is contained in the STP?

A lot of helpful data has been compiled from all of the Microsoft cloud services and is available in the Microsoft Service Trust Portal (STP). Additionally, it includes the information and tools that enterprises require for everything related to security, compliance, and privacy.

The Service Trust Portal offers information, tools, and other resources about Microsoft security, privacy, and compliance practices.

From the main menu, you access:



Microsoft's Privacy Principles

Introduction

The development and rising popularity of cloud computing bring up crucial policy issues, such as geographical location, shared data storage, transparency, access, and security. Cloud computing services and their uptake are still constrained by competing legal duties and competing claims of governmental jurisdiction over data usage. Different laws governing data retention, privacy, and other topics are ambiguous and present serious legal difficulties.

Since the introduction of the Microsoft Network in 1994, Microsoft has been addressing privacy concerns relating to cloud computing and online services. Microsoft is still dedicated to keeping its customers' information private. We are aware that trustworthy privacy measures are crucial to fostering cloud computing's growth and enabling it to realize its full potential. Because of this, we carefully considered data protection when developing Office 365, working with a specialized team of privacy experts.

Privacy Principles

Microsoft privacy principles and standards provide our staff with a clear framework to ensure that we manage data responsibly. These guidelines are used to gather and use customer and partner information at Microsoft. We have made significant investments to create an extensive privacy governance program to put our values and standards into practice. In addition to the hundreds of other employees who help ensure privacy policies, processes, and technologies are used across all of Microsoft's products and services, the company employs many full-time privacy professionals.

Microsoft Priva

Privacy is critical for organizations and consumers today, and concerns about managing private data are steadily increasing. Regulations and laws impact people worldwide, setting rules for how organizations keep personal data and giving people rights to operate personal data collected by an organization.

Organizations must take a "privacy by default" stance to meet regulatory requirements and build customer trust. Instead of manual processes and a patchwork of tools, organizations require a comprehensive solution to address common challenges such as:

- Helping users adopt sound data handling practices and training them to identify and solve issues
- Understanding the risks in the amount and type of personal data they store and share
- Fulfilling subject data requests, or subject rights requests, efficiently and on-time

Microsoft Priva helps you meet these challenges to achieve your privacy goals. Priva's capabilities are available through two solutions: **Priva Privacy**

Risk Management, which provides visibility into your organization's data and policy templates for reducing risks; and **Priva Subject Rights Requests**, which provides automation and workflow tools for fulfilling data requests.

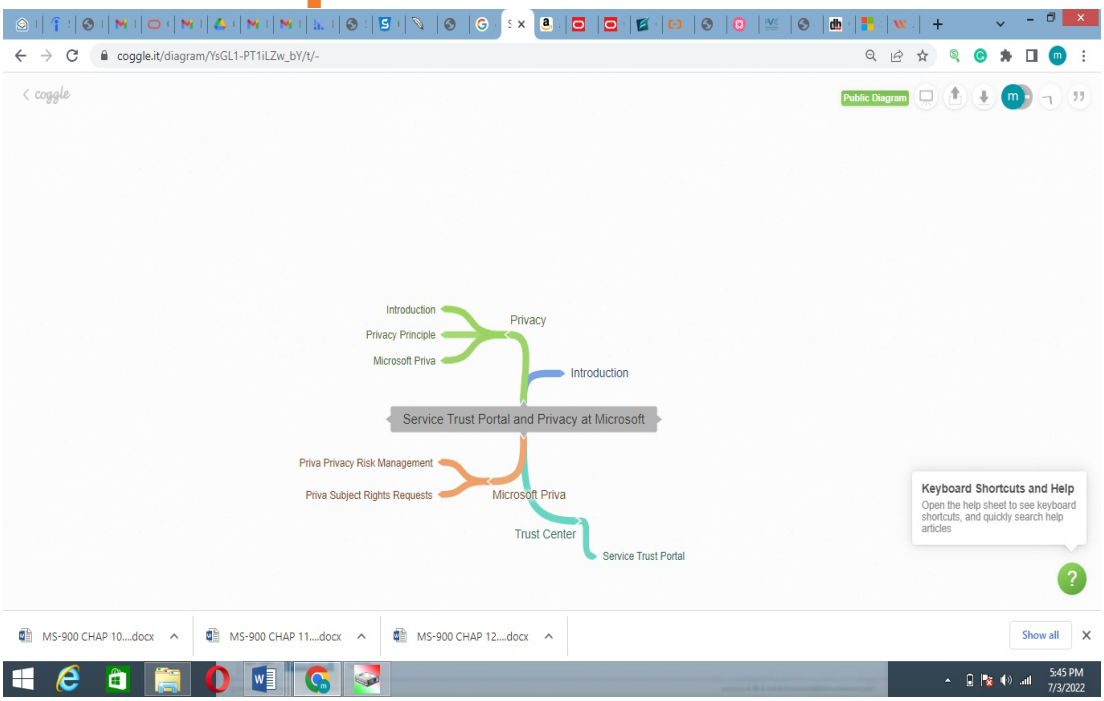
Priva Privacy Risk Management

Microsoft Priva helps you manage the data your organization keeps by automating the discovery of personal data assets and visualizing essential information. These visualizations can be seen on the overview and data profile pages, currently accessible through the Microsoft Purview compliance portal.

Priva evaluates your organization's data stored in the following Microsoft 365 services within your Microsoft 365 tenant:

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Microsoft Teams

Mind Map



CHAPTER 10: IDENTIFY LICENSING OPTIONS AVAILABLE IN MICROSOFT 365

Introduction

Microsoft 365 is available through various licensing models and home, business, enterprise, and subscription plans. These options let you choose the best model and plan for your management and operational needs. By choosing the optimum subscription and license, you can be sure that the functionality you need is in the most cost-effective package.

Explore the Pricing Model for Microsoft Cloud Services

Microsoft offers various licensing programs and channels where you can buy Microsoft 365 products and services. These programs include Microsoft Volume Licensing (VL), Cloud Solution Provider Program (CSP), or Web Direct Programs (MOSP). For example, in Volume Licensing, Microsoft 365 is available for customers through the **Enterprise Agreement (EA).** If you need a dedicated expert to provide hands-on support, Microsoft has many qualified partners in their **Cloud Solution Provider (CSP) program** who can help.

Cloud Solution Provider Model

The **Cloud Solution Provider (CSP) model** is a Microsoft partner program that provides the expertise and services you need through an expert CSP partner.

Your Microsoft 365 subscription is provided through a CSP partner who can manage your entire subscription and provide billing and technical support. The CSP partner will have admin privileges that will allow them to access your tenant, and they will be able to support, configure and manage licenses and settings directly. The CSP partner can provide extra consultancy and

advice to meet security and productivity targets. Furthermore, other Microsoft cloud-based products and services can be added to your subscription, such as Microsoft Azure services and Dynamics 365.

The Cloud Solution Provider (CSP) program provides a pay-as-you-go subscription model with per-user, per-month pricing that lets your business scale up or down from month to month as your needs change.

Enterprise Agreements

The **Microsoft Enterprise Agreement (EA)** is designed for organizations that want to license software and cloud services for a minimum three-year period. The Enterprise Agreement describes the best value to organizations with 500 or more users or devices. One of the benefits of the Enterprise Agreement is that it is manageable, giving you the flexibility to bring cloud services and software licenses inside a single organization-wide agreement. Another benefit is that your organization can get 24x7 technical support, planning services, end-user and technical training, and unique technologies with Software Assurance.

Explore the Billing and Bill Management Options

Microsoft Bill Account

When you register to sample or purchase Microsoft goods, a billing account is generated. You control your account settings, invoices, payment options, and purchases through your billing account. Access to several billing accounts is possible. For instance, you have access to your company's Enterprise Agreement, Microsoft Products & Services Agreement, or Microsoft Customer Agreement, or you directly signed up for Microsoft 365. You would have a different billing account for each of these situations.

The following billing account types are now supported by the Microsoft 365 admin center:

Microsoft Online Service Program: This billing account is created when you immediately sign up for a Microsoft 365 subscription through the Microsoft Online Services Program.

Microsoft Products % Services Agreement (MPSA) Program: When your company enters an MPSA Volume Licensing agreement to buy software and online services, a billing account called the Microsoft Products & Services Agreement (MPSA) Program is formed.

The Microsoft Customer Agreement: It states that when your company works with a Microsoft agent, an authorized partner, or makes an independent purchase, a billing account is formed.

Billing Account Options

A **billing account** is formed when you sign up to try or buy Microsoft products. You use your billing account to control your account settings, invoices, payment methods, and purchases. The **Microsoft 365 admin center** currently supports the below billing accounts:

- **Microsoft Online Services Program.** This billing account is created when you sign up for a Microsoft 365 subscription directly
- **Microsoft Products & Services Agreement (MPSA) Program:** This billing account is created when your organization signs an MPSA Volume Licensing agreement to purchase software and online services
- **Microsoft Customer Agreement:** This billing account is created when your organization works with a Microsoft representative, an authorized partner, or purchases independently

Bill Management

Microsoft 365 billing is managed from the **Microsoft 365 admin center.** The admin center allows you to manage subscriptions, view billing statements, update payment methods, change your billing frequency, and more.

Explore the Available Licensing and Management Options

Subscription Plans

The pricing associated with your account depends on the subscription and the number of licensed users. Microsoft 365 offers various subscription plans for home users and organizations and various licensing options to meet your needs. Each service has a specified price that is typically rated on a per-user, per-month basis. The following list describes the subscription plans offered:

- **Microsoft 365 for home** consists of **Microsoft 365 Personal** and **Microsoft 365 Family.** Personal is for a single person with multiple devices, and family is for up to six people
- **Microsoft 365 Education** is for the education department and has two subscription plans for faculty and students that include different features: A1, A3, and A5
- **Microsoft 365 Government** is for government institutions and has two subscription plans with different features: G1, G3, and G5
- **Microsoft 365 Business** is for small to medium-sized organizations with up to 300 employees. It has four subscription tiers that include different features: Apps for Business, Business Basic, Business Standard, and Business Premium
- **Microsoft 365 for frontline workers** is designed to empower and optimize frontline impact. It has three subscription tiers that include different features: F1, F3, and F5
- **Microsoft 365 Enterprise** is for enterprise-sized organizations and has four subscription tiers that include different features: Apps for Enterprise, E3, E5, and F3

Licenses

A **license** allows your users to use the features and services included in the subscription plan. Microsoft 365 products and services are available as **user subscription Licenses (USLs)** and are licensed per-user basis. The following list describes the options available:

- **Full USLs** are for new users without previously paid Microsoft products and services
- **Add-on USLs** are for on-premises software customers who want to add Microsoft 365 cloud products and services
- **From SA, USLs** are for on-premises Software Assurance customers that want to transition to the cloud
- **Step Up USLs** are for customers who want to upgrade their service level

Types of add-ons

Microsoft 365 business plans have **add-ons** you can purchase for your subscriptions, and Add-ons provide more capabilities to enhance your subscription. There are two kinds of add-ons:

- **Traditional add-ons** are connected to a specific subscription; the linked add-on is canceled if you cancel the subscription
- **Standalone add-ons** appear as a separate subscription on the products page within the Microsoft 365 admin center. They have their expiration date and are managed the same way you would any other subscription

Group-based Licensing

According to the membership of a group, group-based licensing automatically gives or removes licenses for a user account. Dynamic group membership allows for adding or deleting group members based on user account attributes like Department or Country.

Group-based licensing is now a feature of Azure AD to help with these

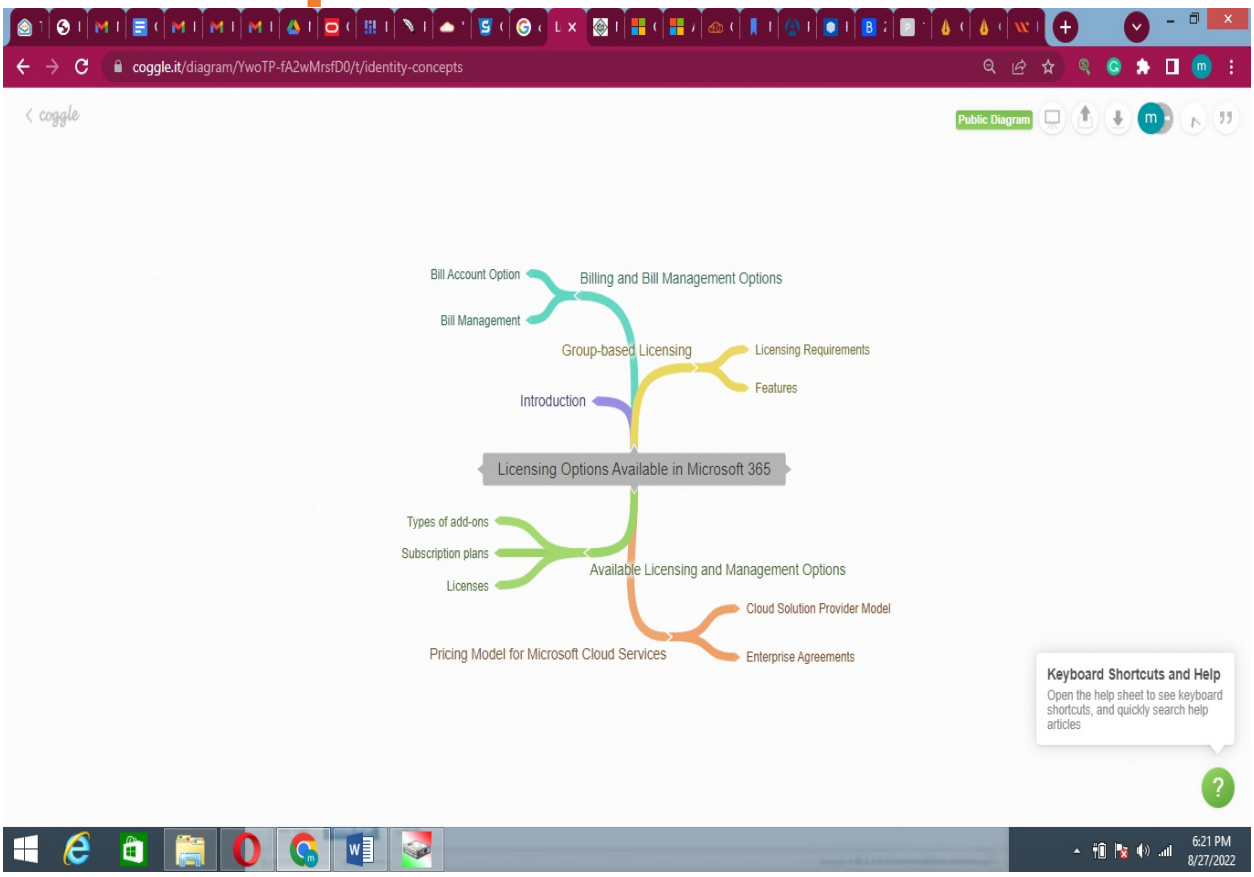
issues. A group may be given access to one or more product licenses. Azure AD makes sure that the licenses are distributed to each group member. Any new members are given the proper licenses as soon as they join the club. Those licenses are taken away when they leave the group. With the help of this licensing management, it is no longer necessary to automate license management using PowerShell to take account of changes in the organizational and departmental structure on an individual user basis.

Licensing Requirements

Each user who gains access to group-based licensing must own one of the following licenses:

- Azure AD Premium P1 and above subscription, whether it is paid or trial
- Microsoft 365 Business Premium, Office 365 Enterprise E3, Office 365 A3, Office 365 GCC G3, Office 365 E3 for GCCH, or Office 365 E3 for DOD and above, whether it is a paid-for or trial version.

Mind Map


coggle.it/diagram/YwoTP-fA2wMrsfD0/t/identity-concepts
coggle
Public Diagram
Licensing Options Available in Microsoft 365
Billing and Bill Management Options
Bill Account Option
Bill Management
Group-based Licensing
Licensing Requirements
Features
Introduction
Available Licensing and Management Options
Types of add-ons
Subscription plans
Licenses
Pricing Model for Microsoft Cloud Services
Cloud Solution Provider Model
Enterprise Agreements
Keyboard Shortcuts and Help
Open the help sheet to see keyboard shortcuts, and quickly search help articles
6:21 PM
8/27/2022

CHAPTER 11: DESCRIBE SUPPORT OFFERINGS FOR MICROSOFT 365 SERVICES

Introduction

Support plays an important role in the cloud environment. As we have learned, at least some portion of infrastructure management moves to the cloud provider when we move to the cloud. When something goes wrong, you must get the help you need to keep your applications available. It is also important to understand what level of support is being provided for specific services, in particular services that may be in previewing and not published officially.

Microsoft is committed to helping you get the best out of your Microsoft 365 services. You can rely on easy-to-access support options with Microsoft 365 to help your organizations remain productive and efficient. Microsoft 365 services guarantee your organization's service level through Service Level Agreements. When you need help using Microsoft 365, create or view an existing support request through the Microsoft 365 admin center. Your organization will also benefit from transparent service health status updates on your Microsoft 356 products or services. Lastly, your organization can use open feedback sharing to help improve products and services based on user experience.

Explore Support Options for Microsoft 365 Services

Administrators and users in your organization might find it challenging to resolve issues independently. Knowing they can receive assistance for Microsoft 365 services whenever they need it through various **support options is helpful.**

The support option chosen to deal with a particular issue depends on:

- The tool or service where the issue has arisen

- The type of subscription your organization uses
- The kind of support your organization needs

Explain Service Level Agreement (SLAs) Concepts

Organizations must know that the products and services are reliable and secure. Microsoft 365 services guarantee the level of service for your organization. The level of service is detailed in a legal agreement referred to as a **Service Level Agreement.** Microsoft details its commitment to provide and maintain agreed service levels for Microsoft 365 services through its **Microsoft Online Services Agreement.**

Monthly Uptime Percentage Service Credit

< 99.9%	25%
< 99%	50%
<95%	100%

Office 365 Support

Microsoft offers a range of plans to help you get the assisted business assistance you need, including pay-per-incident choices and premium care that is available day and night.

Your Microsoft Office 365 subscription includes basic technical help, which you can request via the Microsoft Office 365 online site. You can buy Microsoft Office 365 support plans directly from Microsoft or through volume licensing programs for extra services and quicker response times.

Microsoft 365 Technical Support

Technical support is included with Microsoft 365. However, when purchased alone or as part of a Microsoft 365 service plan, the following restrictions apply to Microsoft 365 subscription support for Microsoft 365 Apps for

enterprise or Microsoft 365 Apps for business.

Professional assistance covers most break-fix issues or technical issues you encounter while using Microsoft 365 Apps. A term used in the industry, "break-fix," describes the "effort involved in supporting a technology when it fails in the normal course of its function and needs the assistance of a support organization to be returned to working order."

Identify How to Track the Service Health Status

View Health Status of Microsoft 365 Services

An organization must know the health status of the Microsoft 365 services. Your organization's administrators can use the **Microsoft 365 admin center** to view the current **health status** of each of your Microsoft 365 services and tenant. They can also view the history of services that have been affected in the last 30 days and information about current outages or disruptions to services. It is helpful to view the health to find out whether you are dealing with a known issue with a progress solution, so you do not have to spend time troubleshooting or calling support.

Keep track of incidents

Your organization can set up notifications for any new incidents or updates to any active incidents that might affect your organization. Microsoft will provide two different types of notifications:

- **Unplanned downtime** - Where an incident has caused a service to become unresponsive or unavailable
- **Planned maintenance -** Where Microsoft regularly carries out service updates to the software and infrastructure that run services

Explore How Organizations Share Feedback on Microsoft 365 Services

There is always room for modification, and Microsoft is committed to improving its services. Your organization's administrators and users often have great insight into how specific elements of products and services can be improved based on their daily experiences. Microsoft encourages idea sharing to improve products and services for everybody.

Microsoft has various channels for you to submit feedback about Microsoft 365 products and services. For example, if you are using feedback from the community feedback web portal, you can submit new feedback directly within the web portal. Community feedback is publicly displayed within different forums. You can participate in existing feedback by voting or commenting on existing topics. Review your submitted feedback, impact, and status by viewing official responses from the Microsoft product teams.

The following list defines the ways you can communicate directly with Microsoft:

- Feedback
- In-product experiences
- Windows Feedback Hub
- Microsoft Tech Community
- Microsoft Store
- UserVoice forums

Mind Map


Service level agreement (SLAs) concepts
Monthly uptime percentage Service credit
Support options for Microsoft 365 services
Support request
Support offerings for Microsoft 365 services
View the health status of Microsoft 365 services
Track the service health status
Keep track of incidents

CHAPTER 12: DESCRIBE THE SERVICE LIFE CYCLE IN MICROSOFT 365

Introduction

Every product or service has a lifecycle, including those in Microsoft 365. Microsoft envisions, designs, develops and tests everything internally. Once these features, products, and services are mature enough, they are made available to evaluate and test by users in a preview release. After the tests succeed, the feature, product, or service is released and generally available. Over time, as more product releases occur, older products and services can no longer be supported, and they will reach the end of support. Your organization can stay current on the feature, product, and service updates and releases by using the Microsoft 365 Roadmap.

Service Life Cycle

Microsoft 365 is an evergreen product that is always being improved. Development, testing, and release of new features occur often. In comparison to conventional software, Microsoft 365 has a different life cycle.

Microsoft Lifecycle offers uniform and predictable principles for support throughout a product's life, assisting clients in managing their IT investments and environments while making long-term plans.

Describe Private, Public Preview, and General Availability Releases

A product or service lifecycle typically has three phases:

1. **Private Preview**
2. **Public Preview**
3. **General Availability (GA)**

When a product or a service retires, it reaches the phase **end of support.**

Private preview

In this phase, Microsoft might release a product or service to a limited number of users to test and evaluate new features or functionality. This phase does not include legal support. Typically, users can sign up to be members of a private preview, but the preview release is not made available to the public.

Public preview

In this phase, Microsoft typically releases public previews of products and services before their GA release to receive suggestions from a wide range of users. They are marked as previews and include beta or pre-release features and services. Doing this allows users to explore and test upcoming functionality. Users may also receive some limited support depending on the product or service.

General Availability (GA)

After the public preview is completed, Microsoft releases the product or service. The product or service becomes available to all customers with proper support, known as the **release version.** The products and services in this phase have been through complete development and test lifecycle to ensure stability and reliability. With Microsoft 365, new features are periodically added to the products and services. It is helpful for IT developers and administrators to be aware of preview features before they have their general availability released. Organizations can then educate users about these new features, ensure products are used optimally and be aware of the change in existing functionality.

End of support

Eventually, older products or retired services can no longer be supported, and they will reach the end of support. Once that happens, the product or service will no longer receive updates or assisted support. Customers are encouraged to shift to the latest version.

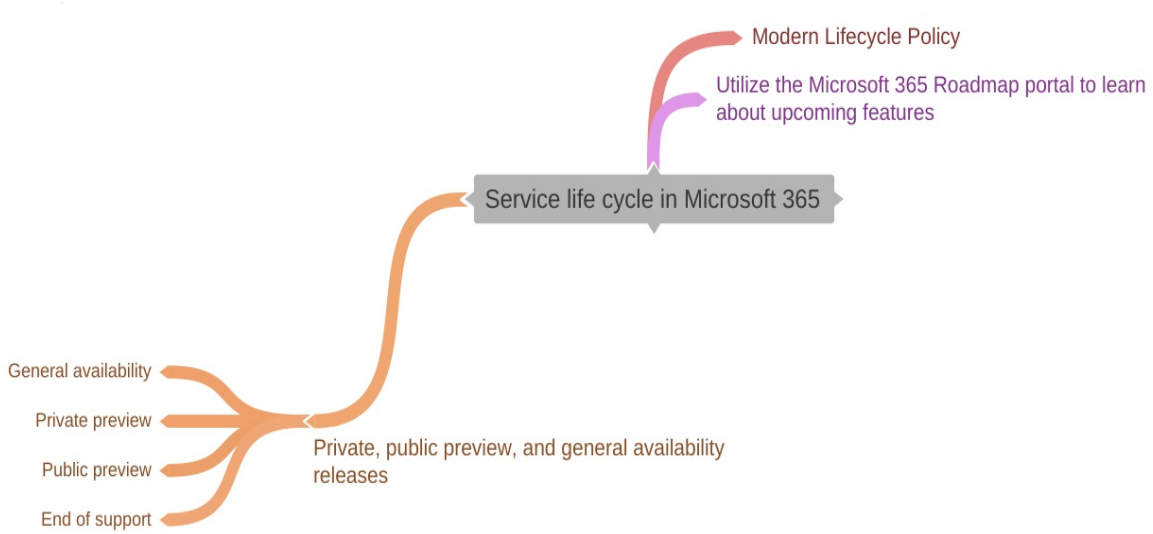
Describe the Modern Lifecycle Policy

Microsoft 365 is covered by the **Modern Lifecycle Policy.** The policy includes products and services that are serviced and supported continuously. Products and services managed by the Modern Lifecycle Policy are supported as long as the following criteria are met:

- Customers stay current as per the servicing and system requirements published for the product or service. Staying current means that customers accept and apply all servicing updates for their products and services
- Customers must be licensed to use the product or service
-

- Microsoft must currently offer support for the product or service

Mind Map


Modern Lifecycle Policy
Utilize the Microsoft 365 Roadmap portal to learn about upcoming features
Service life cycle in Microsoft 365
General availability
Private preview
Public preview
End of support
Private, public preview, and general availability releases

CHAPTER 13: MOBILE DEVICE MANAGEMENT

Introduction

This chapter focuses on implementing Mobile Device Management (MDM) in Microsoft 365. Before the introduction of MDM solutions, companies traditionally joined desktop devices to on-premises AD DS and managed them through Group Policies and Configuration Manager. But in today's world, users employ desktops and various devices. Most devices are mobile, and they are used from anywhere. They are often not connected to the company network, and some run non-Windows operating systems. In many cases, joining such devices to an on-premises AD DS is unsuitable or even possible.

In this chapter, you will learn that Mobile Device Management manages all popular mobile devices without joining them to an on-premises AD DS. To manage a device with MDM, enroll it in your MDM solution. At Microsoft, enrolling it in Intune or Basic Mobility and Security. After the device is enrolled in MDM, you can still manage it through group policies and profiles if you want. However, MDM provides more device management features not available in on-premises AD DS, such as device compliance and Conditional Access.

Device Management Overview

Protecting and securing the data and resources of an organization on devices within that organization is a crucial responsibility of any Administrator. Device management is the task at hand. Users use personal accounts to send and receive email, access websites when dining out and at home, and download apps and games. Students and employees are also among these users. They desire easy access to work and school resources on their devices, such as email and OneNote. In addition to keeping users'

access to these resources simple across all of their various devices, it is your responsibility as an administrator to keep them safe.

Organizations may use device management to safeguard their data and resources from various devices.

A business can ensure that only authorized individuals and devices have access to confidential information by using a device management provider. Similar to this, customers who know their smartphone satisfies their organization's security criteria can feel at peace accessing work data from their phone. You can question as a company, "What should we utilize to secure our resources?"

Intune by Microsoft is the solution. Mobile device management (MDM) and mobile application management are services provided by Intune (MAM). Some essential duties of any MDM or MAM solution include:

- Support a variety of mobile environments and safely manage Windows, macOS, Android, iOS, and iPadOS devices.
- Check that devices and apps adhere to the security standards set by your company.
- Make policies to protect your company's data on both company-owned and personal devices.
- Use a single, integrated mobile solution to manage users, groups, devices, apps, and enforcement of these policies.
- Control how your staff accesses and shares data to protect the information that belongs to your business.

Microsoft Azure, Microsoft 365, and Azure Active Directory all come with Intune (Azure AD). Controlling who has access and what they can access is made easier by Azure AD.

Microsoft Intune

Microsoft is just one of many companies that utilize Intune to protect

confidential information that users access from both company-owned and personal devices. Software update guidelines, installation statuses, and device and app configuration standards are all part of Intune (charts, tables, and reports). These tools support you in securing and managing data access.

Explore Mobile Device Management

Mobile Device Management manages all popular mobile devices without joining them to an on-premises AD DS. To manage a device with MDM, you just need to enroll it in your MDM solution. At Microsoft, enrolling it in Intune or Basic Mobility and Security. After the device is enrolled in MDM, you can still manage it through group policies and profiles if you want. However, MDM provides more device management features not available in on-premises AD DS, such as device compliance and Conditional Access.

An organization should first plan its MDM solution before deploying MDM, enrolling devices in it, and managing device compliance. This section examines the features of effective MDM planning, including the built-in capabilities of mobile device management for Microsoft 365, a comparison of Microsoft's two MDM solutions, policy settings for mobile devices, and controlling email and document access.

Explore Mobile Device Management in Microsoft 365

Mobile device management (MDM) is an industry-standard for managing mobile devices, such as smartphones, tablets, laptops, and desktop computers. Before using Microsoft 365 services with your device, you first need to enroll it in MDM.

MDM is implemented by using an MDM authority and MDM clients. Microsoft offers two MDM authority solutions:

- Basic Mobility and Security
- Microsoft Intune

MDM client functionality is comprised as part of the Windows 10 operating system. MDM authority can manage several devices that contain MDM client functionality, such as Android, iOS, and Windows 10. Some device settings can be controlled on all MDM enrolled devices, while other settings are device-specific and can only be configured using device-specific MDM policies.

MDM functionality includes the distribution of applications, data, and configuration settings to devices enrolled in MDM. Windows 10 devices can be enrolled in MDM using any of the following methods:

- Manually
- By using the Settings app
- By submitting a package
- By using Group Policy
- By enrolling into Azure AD, if integration between Azure AD and MDM is configured

Explore the Mobile Device Management Services in Microsoft 365

Microsoft 365 includes two Mobile Device Management (MDM) services: Basic Mobility and Security and Microsoft Intune. This section provides a detailed examination of each offer.

Introduction to Basic Mobility and Security

The Basic Mobility and Security service provide a built-in MDM solution within Microsoft 365. This service provides the core device management features available in Microsoft 365. It is hosted by the Intune service and

includes a subset of Intune services. Even though it includes some Intune features, it is not an "Intune-lite" solution. The Basic Mobility and Security service provide core MDM functionality within Microsoft 365 for managing devices in your organization.

After Basic Mobility and Security is set up and your users have enrolled, you can manage the devices, block access, or even wipe a device if needed.

Introduction to Microsoft Intune

Microsoft Intune provides the core features within Basic Mobility and Security, plus more advanced device management features. Intune is Microsoft's gold-level standard for MDM solutions. It is not only a cloud-based service; its focus extends beyond Mobile Device Management (MDM) and includes Mobile Application Management (MAM).

- **Device Management -** Intune enables an organization to control how its devices are used, including mobile phones, tablets, and laptops. It also enables people in your organization to use their devices for school or work. Intune helps ensure that organization data stays protected on personal devices and can isolate organizational data from personal data
- **Application Management**

  Many organizations, such as Microsoft, use Intune to secure proprietary data users access from their company-owned and personal mobile devices. Intune helps organizations secure and monitor data access by including:

  - Device and app configuration policies
  - Software update policies
  - Installation statuses (charts, tables, and reports)

MDM within Microsoft 365 Plans

Basic Mobility & Security is part of the Microsoft 365 plans, while Microsoft Intune is a standalone product with specific Microsoft 365 plans.

Examine MDM Policy Settings in Microsoft 365

MDM policies and profiles are groups of settings that control features on mobile devices. Whether related to encryption, passwords, security, email management, or another fundamental issue, policies are the cornerstone of MDM in an organization.

When organizations create policies or profiles, they can only deploy them by assigning them to groups of users, and they cannot assign them directly to individual devices or users. When policies are assigned to groups, the users in those groups get an enrollment message on their devices. When they have completed device enrollment, their devices are restricted by the policies you have set up. You can then monitor policy deployment in the MDM management tool.

Microsoft offers two solutions for managing devices with MDM: Basic Mobility and Security and Microsoft Intune. Both solutions can manage enrolled devices, but they offer different capabilities. Both solutions use Microsoft 365 Endpoint Manager for administering their MDM solutions.

MDM Policy Settings in Basic Mobility and Security

The Basic Mobility and Security service enable organizations to create device policies that help protect their company information on Microsoft 365 from unauthorized access. An organization can apply policies to any mobile device in the company where the user has an applicable Microsoft 365 license and enrolled the device in Basic Mobility and Security.

MDM Policy Settings in Microsoft Intune

Organizations can manage the same settings in Microsoft Intune as in Basic Mobility and Security, along with many other settings. These different device settings that Intune can manage include:

- Device enrollment and restrictions

- Device compliance policies
- Device configuration policies
- Conditional Access
- Software updates include Windows 10 update rings and update policies for iOS
- Apps deployment, app configuration policies, and app protection policies

Policy and Security Configuration

Microsoft 365 includes default MDM policies based on Microsoft's digital security requirements. These policies help ensure that corporate security is maintained while also providing a good user experience. Their data on their work devices is more secure when policies manage other users and devices in the same environment. The following list provides examples of how these policies affect the entire Microsoft 365 experience:

- **Security.** The default policies enforce Microsoft corporate compliance settings on mobile devices, such as password policy and encryption settings
- **Messaging.** The default policies for Exchange align policy settings between Exchange ActiveSync (EAS) and MDM
- **Compliance.** Microsoft took advantage of the default compliance rules for mobile devices built into Configuration Manager. Microsoft then created a configuration baseline for those CIs and targeted the configuration baseline to the collection of mobile devices

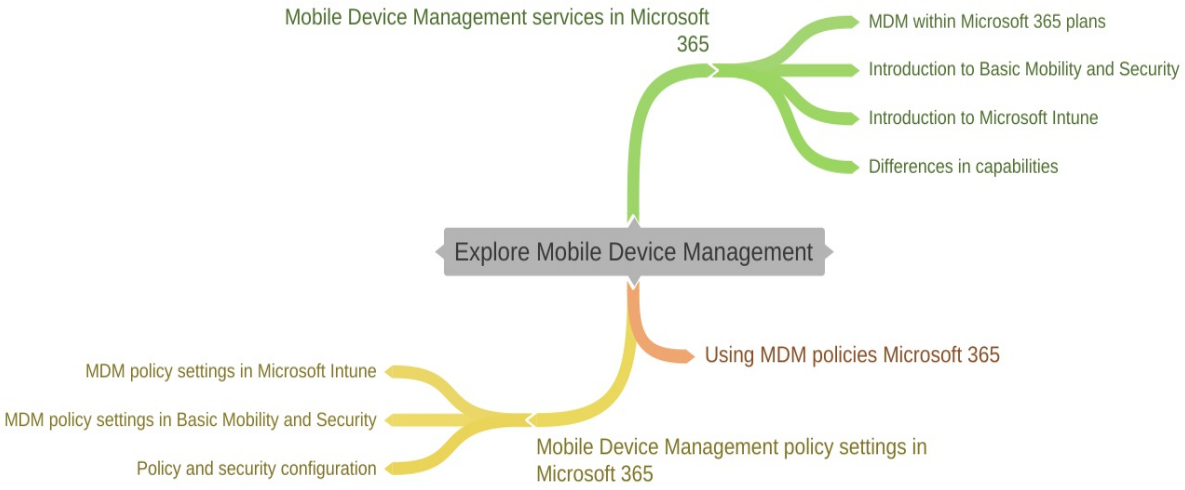
Using MDM policies, Microsoft 365

Organizations can define company policy using the Device Security policy in Microsoft 365. They can control access to email, documents, and other cloud apps by using Conditional Access policies. Compliance with company policy is just one criterion that can be evaluated in a Conditional Access policy. Organizations can also evaluate sign-in risk, device type, location, and client apps.

Devices that are not enrolled in MDM cannot have their compliance evaluated. However, organizations can still prevent access to mailboxes, documents, and cloud apps from such devices. If a user tries to access their mailbox from such a device, depending on how the policy is set up, they may experience one of the following outcomes:

- They are removed from accessing Microsoft 365 resources
- They are, redirected to enroll the device in MDM
- The user could have access, but Microsoft 365 would report a policy violation

Mind Map


Explore Mobile Device Management
Mobile Device Management services in Microsoft 365
MDM within Microsoft 365 plans
Introduction to Basic Mobility and Security
Introduction to Microsoft Intune
Differences in capabilities
Using MDM policies Microsoft 365
Mobile Device Management policy settings in Microsoft 365
MDM policy settings in Microsoft Intune
MDM policy settings in Basic Mobility and Security
Policy and security configuration

Deploy Mobile Device Management

This section examines how to deploy Mobile Device Management in Microsoft 365. Before organizations can start managing devices in Microsoft 365, they must first activate and configure MDM and then enroll their devices. Organizations can activate Microsoft Intune by choosing the MDM authority in Microsoft 365 Endpoint Manager. For Basic Mobility and Security, they must run a link to activate it.

Activate the Mobile Device Management services in Microsoft 365

While Microsoft has two solutions for MDM, Intune and Basic Mobility and Security, they do not have the exact prerequisites. Preparing your MDM environment will be slightly different depending on which solution you want.

- **Essential Mobility and Security -** Start by activating the Mobile Device Management service. Once you activate the MDM service, you must do several other steps to complete the deployment
- **Intune -** Choose the MDM authority before you can start managing devices

Basic Mobility and Security

In Microsoft 365, you activate the Basic Mobility and Security MDM service by running the following link:

https://admin.microsoft.com/EAdmin/Device/IntuneInventory.aspx#

It takes some time for the service to start, after which you will receive an email that explains the next steps for setting up Basic Mobility and Security. These steps include:

1. **Configure domains for Basic Mobility and Security.** If you do not have a domain

associated with Microsoft 365 or are not managing Windows devices, you can skip this step. Otherwise, you will need to add DNS records for the domain at your DNS host. This step is complete if you have already added the records to set up your domain with Microsoft 365.

After you add the records, the Microsoft 365 users who sign in on their Windows device with an email that uses your domain are redirected to enroll in Basic Mobility and Security.

2. **Configure an Apple Push Notification Service (APNS) certificate for iOS devices.** To operate iOS devices like iPad and iPhones, you must first create an APNS certificate.
3. **Set up multi-factor authentication.** MFA helps secure users sign in to Microsoft 365 for mobile device enrollment by requiring a second form of authentication.
4. **Manage device security policies.** Organizations should create and deploy device security policies to help protect their Microsoft 365 data.
5. **Make sure users enroll their devices.** After you have created and deployed an MDM policy, each licensed Microsoft 365 user in your organization will receive an enrollment message the next time they sign in to Microsoft 365 if the policy applies to their device.

Microsoft Intune

Organizations must configure the MDM authority to set up Microsoft Intune for device management. Device management in Intune is initially disabled, and MDM authority is unknown. Before an organization can start enrolling and managing devices, it must configure the MDM authority by selecting one of three available options:

- **Intune MDM Authority** - This option sets the MDM authority solely to Microsoft Intune. Intune is a cloud-only MDM solution, and it is managed by using a web browser. Microsoft recommends that organizations select this deployment option when using Intune
- **Configuration Manager MDM Authority** - This option is referred to as Hybrid MDM because it assumes the organization uses Configuration Manager for managing on-premises devices. This scenario integrates Intune's MDM capabilities into Configuration Manager in the following manner:
    - It uses Configuration Manager's on-premises infrastructure to administer content and manage the devices

- **None**. This option indicates that no MDM Authority has been chosen, and Intune can only manage devices if an MDM authority is chosen.

Configure Domains for Mobile Device Management

An organization can enable its users to enroll their Windows 10 devices in Mobile Device Management (MDM) using the Autodiscover service. Windows devices (Windows Phone 8.1 and 10 and Windows PCs 8.1 and 10) have a UI built into the operating system to enroll a device for management. The user enters a corporate email address that matches the User Principal Name (UPN) set for user identity. The device tries to auto-discover the enrollment server and start the enrollment process. If the Autodiscover service is not configured, the device enrollment server will not be found. In this case, the device presents a screen for the user to enter the server address.

The Autodiscover service is configured when you create an alias (CNAME resource record type) in the domain DNS zone that automatically redirects enrollment requests to Intune servers.

- **Autodiscover will not be configured if you do not add this CNAME record.** In this case, users can still enroll devices to MDM, but they will have to provide the address of the enrollment server manually
- **Autodiscover will be configured if you add this CNAME record.** With the Autodiscover service enabled, users just have to provide credentials when they want to enroll their devices to MDM

Manage Security Policies for Mobile Device-Managed Devices

Microsoft's two MDM solutions, the Basic Mobility and Security service, and Intune, enable organizations to configure and deploy different types of policies to manage their devices. Security policies can be implemented by configuring:

- Device Configuration Profiles
- Device Compliance Policies
- Conditional Access policies

Device security policies include:

- Password Settings
- Encryption Settings
- Settings that control the use of device features, such as a video camera

The following part offers a high-level overview of each of these policies.

Device configuration profiles

Microsoft Intune enables organizations to create and deploy different types of device configuration profiles, including:

- Device Restrictions
- Endpoint Protection
- Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)

A device configuration profile can specify how a specific device setting should be configured. For example, you can configure password settings, lock some device features, and limit access to cloud storage and the app store.

Device compliance policy

A device compliance policy specifies the device configuration that must be met for the device to be compliant, such as using a PIN or device encryption. A device compliance policy is not used for configuring a device. Instead, it is

used for defining whether devices are configured in a standard way. Based on that configuration, an organization can treat compliant devices differently from non-compliant ones. For example, you can allow access to Exchange Online only from compliant devices. A device compliance policy includes the following settings:

- Use a password to access devices
- Encryption
- Indicate whether the device is jail-broken or rooted
- Minimum OS version required
- Maximum OS version allowed
- Need the device to be at or under the Mobile Threat Defense level

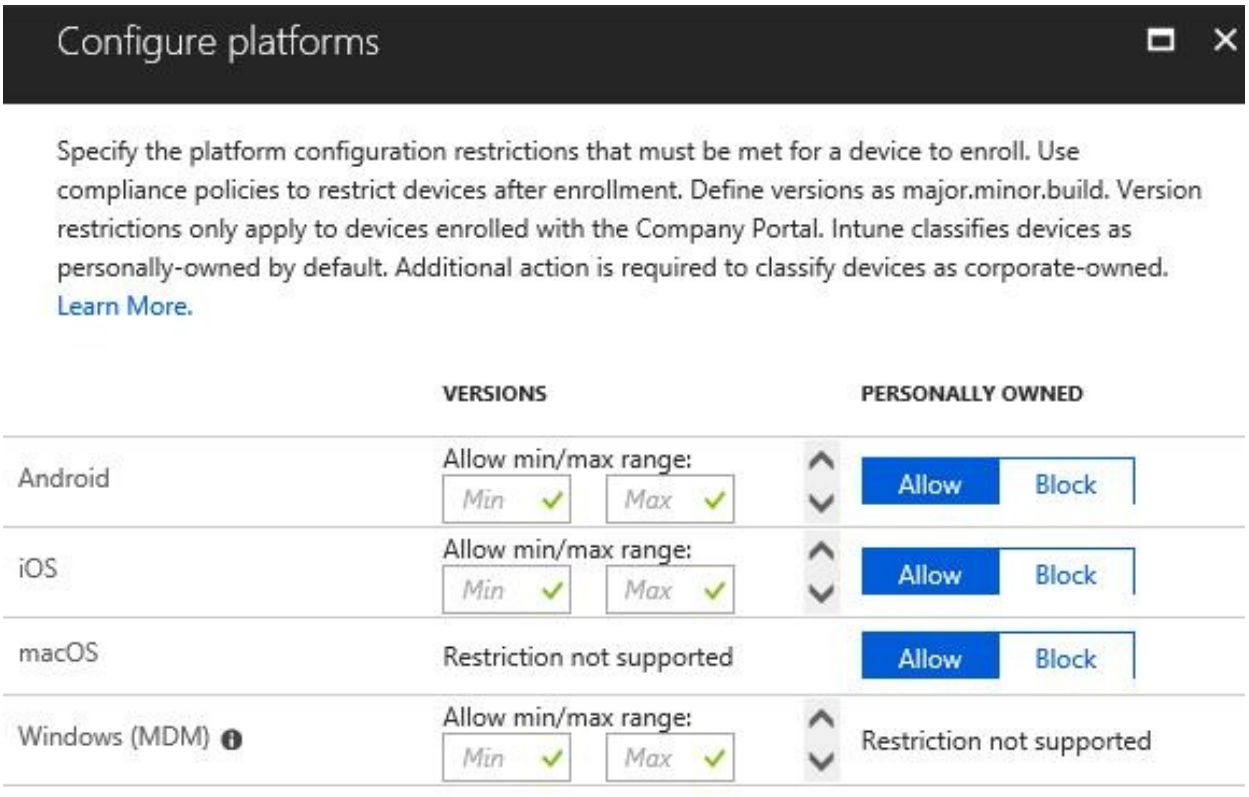
Define a Corporate Device Enrollment Policy

Microsoft Intune and Basic Mobility and Security enable organizations to manage known devices and apps and control access to company data. Using MDM to manage devices requires that they first be enrolled in Intune or Basic Mobility and Security.

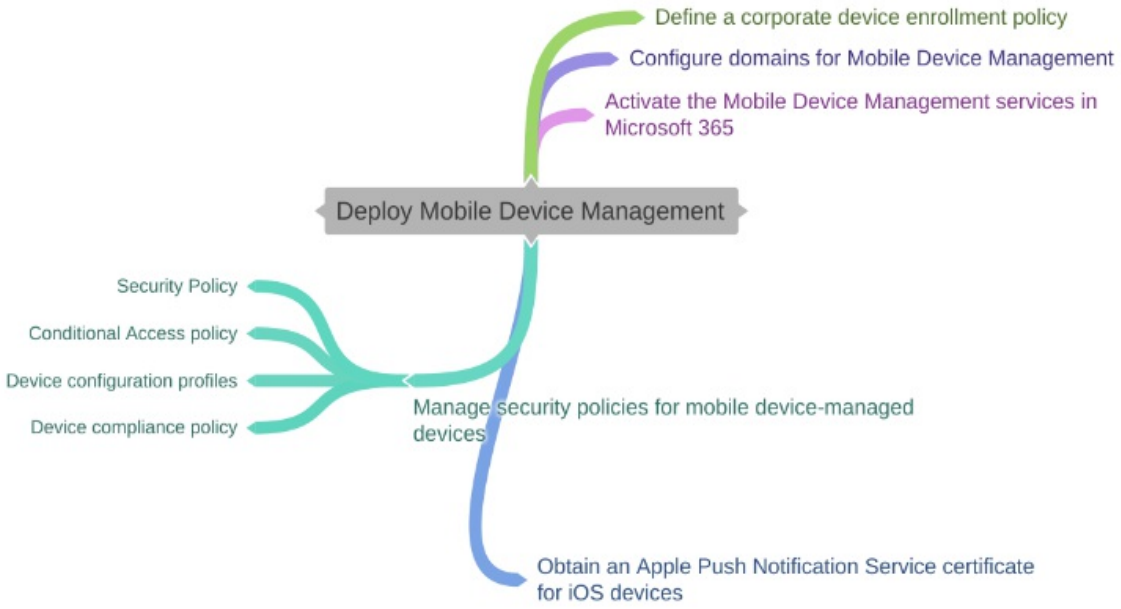
When a device is registered, it is issued an MDM certificate. This certificate is used to communicate with Intune, even if the organization uses Basic Mobility and Security as its MDM solution (remember, Basic Mobility and Security is hosted by the Intune service and includes a subset of Intune services). The certificate is renewed automatically when the device communicates with Intune. If the certificate expires, the device is no longer managed by MDM. The device is automatically removed from Intune after 180 days if the certificate is not renewed.

Intune's default setting allows users to enroll all supported device types. Organizations can optionally configure enrollment restrictions by using the following criteria:

- A maximum number of devices that a user can enroll in
- Device platforms that can be enrolled:
    - Android
    - Android work profile
    - iOS
    - macOS
    - Windows
- Required operating system version for Android, iOS, macOS, and Windows devices:
    - Minimum version
    - Maximum version
- Restrict enrollment of personally owned devices.



Mind Map


Define a corporate device enrollment policy
Configure domains for Mobile Device Management
Activate the Mobile Device Management services in Microsoft 365
Deploy Mobile Device Management
Security Policy
Conditional Access policy
Device configuration profiles
Device compliance policy
Manage security policies for mobile device-managed devices
Obtain an Apple Push Notification Service certificate for iOS devices

Enroll Devices in Mobile Device Management

Many devices today, such as Android, iOS, and Windows 10 S, cannot be joined to on-premises AD DS. But to manage devices centrally, they must trust the authority that defines configuration settings. In on-premises AD DS environments, such authorities were domain controllers; in today's cloud world, they are MDM authorities. You can manage a device only if it is enrolled in MDM, and an enrolled device means that it trusts the MDM authority, such as Intune or Basic Mobility and Security.

In this section, you will see the benefits of enrolling devices to MDM, how to enroll Windows 10, Android, and iOS devices, and how to create enrollment rules. And since Apple devices have their enrollment mechanism, you will be introduced to enrolling Apple devices using the Apple Device Enrollment Program (DEP).

Enroll in Windows 10 and Android devices

When a user enrolls a device to MDM, it creates trust between the device and the MDM authority. Once the device is enrolled, and the trust with MDM authority is established, the organization can then manage the device through MDM

There are several different ways to enroll Windows 10 devices to MDM, based on device type and the device's current state. These methods include:

- Group Policy can automatically enroll devices to MDM if the devices are already joined to the organization's on-premises AD DS
- Windows 10 devices linked to Azure AD can be automatically

enrolled to MDM if integration is configured between Azure AD and MDM

- Windows 10 devices can be manually enrolled to MDM by using a Settings app, provisioning packages, or the Company Portal app

Automatic enrollment to MDM only works for Windows 10 devices because only Windows 10 can be joined to an on-premises AD DS and Azure AD. Other devices, such as Android and iOS, can only be manually enrolled to MDM by using the Company Portal app.

The Company Portal app is not included on Android and iOS devices and is available as a free app in the Google Play and Apple app stores. If you want to enroll iOS devices, you must ensure that MDM is configured with a valid Apple Push Notification Service (APNS) certificate. iPhones, iPad, and macOS devices require an APNS certificate for secure communication with MDM, even if MDM is Intune, MDM for Microsoft 365, or a third-party MDM product.

Enroll iOS Devices using Apple's Device Enrollment Program

Apple DEP is only accessible for devices that an organization purchases through either Apple or authorized resellers to provide to employees.

iOS devices enrolled in DEP do not require manual configuration. Users never have to select MDM links or install the Company Portal app to enroll the device.

If an organization allows users to bring their own devices, they should complete the regular iOS device enrollment in Microsoft Intune.

But if the company provides employees with iOS devices that are part of the Device Enrollment Program, users can enroll those devices in MDM by

completing the following steps:

1. Turn on your iOS device.
2. After you select your **Language**, link your device to WiFi.
3. On the **Set-up iOS device** screen, choose whether you want to:
    - Set up as a new device
    - Restore from iCloud backup
    - Restore from iTunes backup
1. Once you have connected to WiFi, the **Configuration** screen will appear and a message will appear.
2. Agree to the **Terms and Conditions** and choose whether you need to send diagnostic information to Apple.
3. Once you finish your enrollment, your device may prompt you to take more action. These steps may include entering your password for email access or setting up a passcode.

Regulate Device Enrollment by Using Enrollment Rules

Organizations must first assign each user an Intune license before they can enroll their devices to Intune. Once users have been assigned an Intune license, organizations can optionally configure enrollment restrictions that users must meet before enrolling a device to Intune.

Examine How Users Enroll Their Devices in Mobile Device Management

As soon as users obtain their devices, they typically use them for personal leisure and work. This situation poses two problems for companies:

- Until the devices are enrolled in an MDM solution, the organization does not have control over them, nor can it manage them
- Device enrollment is usually a manual process, and users often forget to do it

As a result, most companies have resorted to making enrollment of personal

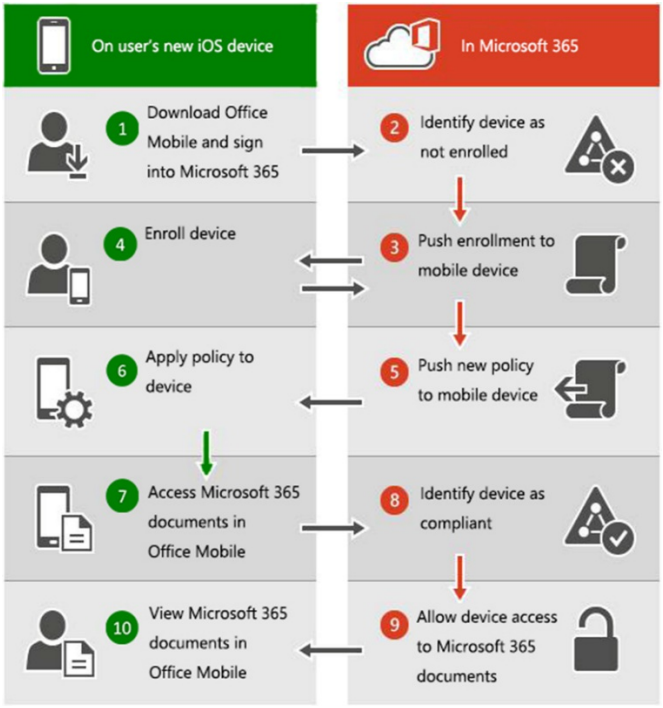
devices mandatory if users want to use them for work. Organizations also implement rules and policies to help manage these personal devices. For example:

- Users can only access company resources from enrolled devices that follow company policy
- Compliance policies are used to define how devices should be configured
- Conditional Access policies are used to control access to company resources

To control access to company resources, organizations can configure either a Security policy in Microsoft 365 or a Conditional Access policy in Intune. These policies can be configured only to allow access to company resources from enrolled devices.

For example, suppose such a policy is in place, and a user tries to access company resources, such as their Exchange Online mailbox. In that case, the user access will be blocked and redirected to enroll their device first. After the user enrolls the device, they can access their mailbox.

The following diagram displays what happens when a user with a new personal device tries to access Microsoft 365.



Enroll Devices Using the Device Enrollment Manager Account

In many companies, users enroll company-owned devices to MDM themselves. But there are scenarios where these same organizations prefer to have a device already enrolled when a user receives it. For example, when non-technical users use devices or if multiple users share the same device.

Every user can enroll only a limited number of devices to MDM. This limit does not apply to the DEM. The DEM account is a particular user account used to enroll devices. The features of this account include:

- It can be used to enroll up to 1000 devices in MDM
- It enables organizations to use Intune to manage large numbers of mobile devices with a single user account
- An organization can add multiple users to the DEM account to give them special capabilities. Only users that have been assigned an Intune license can be assigned to the DEM account

When a user enrolls a device, they are associated with that device. But when

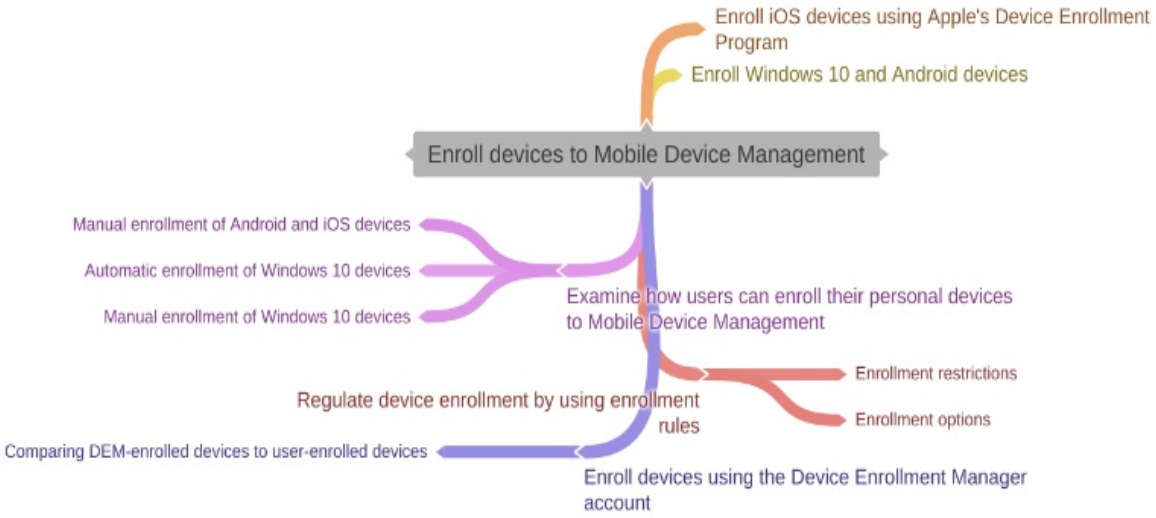
a DEM account enrolls the device, no user is associated with the device, and the device has no assigned user. Suppose an organization plans to bulk enroll many devices at one time. In that case, it can specify the users who will do the bulk enrollment as device enrollment managers on the Intune view in the Azure portal.

Examine the Need for Multi-Factor Authentication to Secure Mobile Device Enrollment

By default, a user must authenticate with a username and password when they want to enroll a device to MDM. In an environment where stronger authentication is required, organizations can include multi-factor authentication (MFA). MFA is a two-step verification process that needs that a user passes two or more of the following authentication methods:

- Something they know (typically a password)
- Something they have (a trusted device that is not easily duplicated, like a phone)
- Something they are (biometrics)

Mind Map


Enroll iOS devices using Apple's Device Enrollment Program
Enroll Windows 10 and Android devices
Enroll devices to Mobile Device Management
Manual enrollment of Android and iOS devices
Automatic enrollment of Windows 10 devices
Manual enrollment of Windows 10 devices
Examine how users can enroll their personal devices to Mobile Device Management
Enrollment restrictions
Enrollment options
Regulate device enrollment by using enrollment rules
Comparing DEM-enrolled devices to user-enrolled devices
Enroll devices using the Device Enrollment Manager account

CHAPTER 14: MICROSOFT 365 APPS

Introduction

Microsoft 365 Apps is a part of Office available through many Office 365 (and Microsoft 365) plans. It includes the applications you are familiar with. You can use these applications to link with Office 365 (or Microsoft 365) services.

Microsoft 365 Apps vs. Other versions of Office

Microsoft 365 Apps is quite similar to other versions of Office that you can deploy to your users. Here are some significant points:

- Its system needs are the same as other current versions of Office
- Microsoft 365 Apps is available in 32-bit and 64-bit versions
- When you deploy Microsoft 365 Apps, it is installed on the user's local computer. Users do not have to be linked to the internet all the time to use it

Reasons to choose the 64-bit version

Computers having 64-bit versions of Windows generally have more resources like processing power and memory than their 32-bit predecessors. Also, 64-bit applications can have more memory than 32-bit applications (up to 18.4 million Petabytes). Therefore, if your scenarios contain large files and working with large data sets and your computer has a 64-bit version of Windows, 64-bit is the right choice when:

- **You are supposed to work with complex data sets**, such as enterprise-scale Excel workbooks with complex calculations, many pivot tables, and data links to external databases. The 64-bit version of Office may perform well in these cases
- **You are supposed to work with huge pictures, videos, or animations in PowerPoint**. The 64-bit version of Office may be best suited to handle these complex slide decks

- **You are working with files over 2 GB in Project**, especially if the project has many sub-projects

Reasons to select the 32-bit version.

The below-mentioned computer systems can only install 32-bit Office:

- 64-bit OS with ARM-based processor
- 32-bit OS with an x86 (32-bit) processor
- Less than 4 GB RAM

If you are an IT professional or a developer, you must also review the below-mentioned cases where the 32-bit version of Office is still the best selection for you:

- **You run 32-bit COM Add-ins with no 64-bit alternative**. You can continue to have 32-bit COM add-ins in 32-bit Office on 64-bit Windows. You can also try connecting the COM Add-in vendor and asking for a 64-bit version
- **You have 32-bit controls with no 64-bit alternative**. You can continue to have 32-bit controls in 32-bit Office like Microsoft (Mscomctl.ocx, comctl.ocx) or any existing 3rd-party 32-bit controls
- **Your VBA code uses Declare statements**. Most VBA code does not need to change when used in 64-bit or 32-bit unless you use Declare statements to call
- **WindowsAPI.** WindowsAPI uses 32-bit data types such as long for pointers and handles. In most scenarios, adding PtrSafe to the Declare and substituting long with LongPtr will make the Declare statement works with both 32- and 64-bit
- **You are using SharePoint Server 2010 and want the Edit in Datasheet view.** You can continue to run the Edit in Datasheet view functionality in

Microsoft 365 Apps

Even though Microsoft 365 Apps is a bit similar to other versions of Office, there are differences, containing Deployment differences and Licensing

differences.

The main difference is that Microsoft 365 Apps is updated regularly, as often as monthly, with new features, unlike non-subscription versions of Office.

Microsoft 365 is a subscription in which you have updated productivity tools from Microsoft. There are Microsoft 365 subscriptions for home and personal use for small and mid-sized businesses, large enterprises, schools, and non-profits.

Microsoft 365 plans for home or business contain the robust Office desktop apps you are familiar with.

With a subscription, you will have the updated features, fixes, and security updates along with tech support at no added cost. You can select to pay for your subscription monthly or yearly. The Microsoft 365 Family plan also allows you to share these subscription benefits with up to 5 additional people.

Most of the Microsoft 365 plans for businesses, schools, and non-profits include fully updated desktop apps, but Microsoft also provides basic plans with the online versions of Office, file storage, and email. You choose what works best for you: Small business, Enterprise, School, or Non-profit.

Deployment differences

- By default, Microsoft 365 Apps updates as one package. This means that all Office apps are linked to the computer. But, you can create the deployment to exclude or delete specific Office applications
- Because Microsoft 365 Apps uses a separate installation technology, called Click-to-Run, there is an alternate way to apply software updates. Microsoft 365 Apps are configured to install updates from the Office CDN on the internet. But, you can form

Microsoft 365 Apps to install updates from a location within your network, or you can control updates to Microsoft 365 Apps with Microsoft Endpoint Configuration Manager

- Microsoft 365 Apps also offers the ability to manage how often users get feature updates. For example, users can have new features to Microsoft 365 Apps as soon as they are ready or once a month
- Office 365 (and Microsoft 365) offers a web-based portal where users can install Microsoft 365 Apps. If users are not local administrators, you will have to install Microsoft 365 Apps for them

Licensing differences

- Users can have Microsoft 365 Apps on up to 5 different computers with a single Office 365 license if a user can have Microsoft 365 Apps installed on a computer in Office, on a laptop to have when traveling, and on a home computer. Users can also install it on up to five tablets and five phones
- Microsoft 365 Apps is provided as a subscription. If you remove your subscription, Microsoft 365 Apps goes into smaller functionality mode. In smaller functionality mode, users can open and view existing Office files but cannot use most of the other Microsoft 365 apps' other features
- To use Microsoft 365 Apps, a user should have an Office 365 account and have been dedicated to a license. If the user's license or account is deleted, the user's installations of Microsoft 365 Apps go into smaller functionality mode

Microsoft 365 Apps for Business

With constantly updated desktop, mobile, and online versions of Word, Excel, PowerPoint, and Outlook, as well as business intelligence solutions to make your job more enjoyable and help your company develop, Microsoft 365 Apps for Business and Apps for Enterprise let you work how you want, practically anywhere.

- Download the desktop versions of Office programs such as Outlook, Word, Excel, PowerPoint, and OneNote (plus Access and Publisher for PC only).
- Each user gets 1 TB of OneDrive cloud storage for file storing and sharing.
- Use one license to cover five mobile devices, five tablets, and five PCs or Macs per user with fully installed Office programs.
- Every month, automatically add new features and functionalities to your apps.
- Access Microsoft's 24/7 phone and online support at any time.

Microsoft 365 Apps for Enterprise

The most efficient and secure Office experience for organizations is Microsoft 365 Apps for business, which enables your teams to collaborate easily from anywhere, at any time.

Built for Teamwork

With Microsoft 365 Apps for enterprise, you can enable your teams to collaborate easily across geographical boundaries. Give users the means to securely share files, collaborate in real time, and simply interact with coworkers.

Stay Connected

Utilize your iOS, Android, or Windows device from anywhere. From your tablet or phone, you may send emails and view, edit, and share documents.

Power of AI

Utilize technologies you already know and the intelligent cloud to complete more tasks. With the support of Microsoft 365 Apps for business, you can write better in Word and Outlook, get insights in Excel, and make presentations in PowerPoint.

Security

Protect your data and identities, recognize internal and external dangers sooner, and make sure that third-party apps and macros work with Microsoft 365 Apps for business.

Activating Microsoft 365

To get and activate a product key, Microsoft 365 Apps communicates with the Office Licensing Service and the Activation and Validation Service. The machine connects to the Activation and Validation Service every day or when the user logs on to check the licensing status and extend the product key. Microsoft 365 Apps continue to work flawlessly as long as the machine can connect to the internet at least once per 30 days. Microsoft 365 Apps enters a reduced functionality state until the next time a connection can be made if the computer is offline for longer than 30 days.

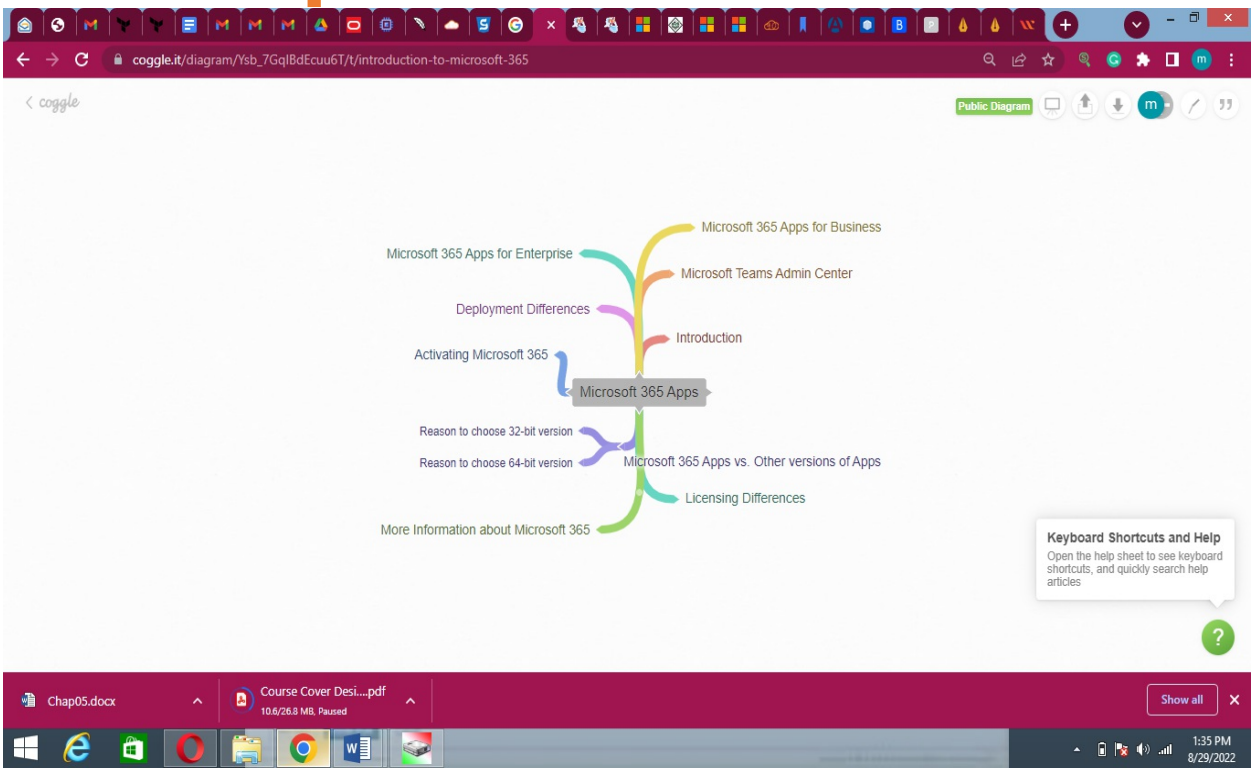
The user can connect to the internet and enable the Activation and Validation Service to reactivate the installation to make Microsoft 365 Apps fully functional. However, in some circumstances, the user must log in first.

Managing Activated Installations

A user is permitted to install Microsoft 365 Apps on a maximum of five desktop computers, five tablets, and five mobile devices per Microsoft 365 Apps license. Installments are managed by the user through the Office 365 site.

The device that has not been used the most often is disabled immediately if a user downloads Microsoft 365 Apps on more than 10 devices. On the inactive device, Microsoft 365 Apps enter a reduced capability mode. Please take note that, at this time, only Windows-based devices are supported for this automatic deactivation.

Mind Map


coggle.it/diagram/Ysb_7GqIBdEcuu6T/t/introduction-to-microsoft-365
coggle
Public Diagram
Microsoft 365 Apps for Business
Microsoft 365 Apps for Enterprise
Microsoft Teams Admin Center
Deployment Differences
Introduction
Activating Microsoft 365
Microsoft 365 Apps
Reason to choose 32-bit version
Reason to choose 64-bit version
Microsoft 365 Apps vs. Other versions of Apps
Licensing Differences
More Information about Microsoft 365
Keyboard Shortcuts and Help
Open the help sheet to see keyboard shortcuts, and quickly search help articles
Chap05.docx
Course Cover Desi....pdf
10.6/26.8 MB, Paused
Show all
1:35 PM
8/29/2022