1. **What is a cloud environment?**

◦ An all-cloud environment describes **a company, organization or individual that uses a Web-based application for every task** rather than installing software or storing data on a computer.

2. **Why we need Cloud Solutions?**

◦ Several reasons are there why we need **cloud computing** today! Here, not going into too deep, I have come up with few points that will be helpful for giving reason:

- One of the major reason why huge number of small scale and large scale business sectors from all over the world are using cloud today, is because of tremendous effect on **cost saving**. Yes, Cloud computing has made drastic change in the reduction of hardware and software cost and other server resources as well
- We can run all our workload data of applications and processes online over the internet remotely instead of using physical hardware and software
- Day to day issues related to server maintenance or installation of software/ hardware or whether it is renewal of license, all those factors are undertaken via cloud computing service providers
- With the help of cloud we can access any data, applications whenever and wherever we want to, over the internet. 100 of pre-configured applications can be install and updated
- Cloud not only handles data storage remotely but it also protects and recovers all crashed or loss data, so we don't have to worry about crashed or loss of data, it gives you high security

With the upcoming new technology in **cloud computing**, many providers offers accessing and paying option with the usability, where users can switch the applications easily according to the use and have pay only for the used resources. Ideally suitable for growing business, where the demand of bandwidth are high. Overall cloud computing can save your time and money!

3. **What are the categories of services provided in the Cloud?**

◦ In one statement, Cloud computing is the delivery of on-demand IT resources over the internet. The companies that offer these computing services are called **Cloud Service Providers** (CSPs). CSPs charge users/organizations based on Cloud resources used through a variety of billing models. Cloud resources are the resources that are abstracted from the underlying physical hardware with the help of a Hypervisor. But there is a lot of confusion about Cloud computing because there are multiple types of services and deployment models that fall under the umbrella that is Cloud computing. This article will help you clear the basic concepts of Cloud computing.

There are 4 types of Cloud deployment models:

- **Public Cloud**
- **Private Cloud**
- **Hybrid Cloud**
- **Community Cloud**

These deployment models differ on the basis of implementation type, hosting type and who has access to it. All Cloud deployment models are based on the same principle of Virtualization (abstraction of resources from bare metal hardware) but differ in terms of location, storage capacity, accessibility, and more. Depending on the type of data you are working with, you will want to compare Public, Private, Hybrid, and Community Clouds in terms of different levels of security they offer and the management required.

- **Public Cloud**

The entire computing infrastructure is located on the premises of the CSP that offers Cloud services over the internet. This is the most economical option for those individuals/organizations that do not wish to invest in IT infrastructure. In a Public Cloud environment, the resources are shared between multiple users who are also called 'Tenants' The cost of using Cloud services is determined through the usage of IT resources consumed.

- **Private Cloud**

Individuals/organizations that choose Private Cloud gets dedicated infrastructure that is not shared by any other individual/organization. The security and control level is highest while using a private network. The costs are born by an individual/organization and are not shared with any other individual/organization. Management of Private Cloud is taken care of by the user and the CSP does not provide any Cloud management services.

- **Hybrid Cloud**

This Cloud deployment model includes the characteristics of Public Cloud and Private Cloud. Hybrid Cloud allows the sharing of data and applications between Public and Private Cloud environments. Organizations mainly use Hybrid Cloud when their On-Premise infrastructure needs more scalability, so they make use of scalability on Public Cloud to meet fluctuating business demands. Organizations can keep their sensitive data on their Private Cloud when reaping the power of the Public Cloud.

- **Community Cloud**

A Community Cloud is a Cloud infrastructure that is shared by users of the same industry or by those who have common goals. This Cloud infrastructure is built after understanding the computing needs of a community as there are many factors including compliances and security policies which need to be included in the community Cloud infrastructure.

4. What is Web Role and Worker Role?

◦ What are Azure Cloud Services?

Azure Cloud Services is a classic Azure resource, originally introduced by Azure back in 2008. This technology was designed to support scalable web and worker role applications running on Windows. While Azure has been taking steps to move forward with its newer Azure VM Scale Sets, Classic Cloud Services still remains a popular deployment choice for many legacy environments in Azure.

What is an Azure Cloud Service Role?

In Azure, a Cloud Service Role is a collection of managed, load-balanced, Platform-as-a-Service virtual machines that work together to perform common tasks. Cloud Service Roles are managed by Azure fabric controller and provide the ultimate combination of scalability, control, and customization

What is a Web Role?

Web Role is a Cloud Service role in Azure that is configured and customized to run web applications developed on programming languages/technologies that are supported by Internet Information Services (IIS), such as ASP.NET, PHP, Windows Communication Foundation and Fast CGI.

What is a Worker Role?

Worker Role is any role in Azure that runs applications and services level tasks, which generally do not require IIS. In Worker Roles, IIS is not installed by default. They are mainly used to perform supporting background processes along with Web Roles and do tasks such as automatically compressing uploaded images, run scripts when something changes in the database, get new messages from queue and process and more.

Differences between the Web and Worker Roles

The main difference between the two is that:

- a Web Role automatically deploys and hosts your app through IIS
- a Worker Role does not use IIS and runs your app standalone

Being deployed and delivered through the Azure Service Platform, both can be managed in the same way and can be deployed on a same Azure Instance.

In most scenarios, Web Role and Worker Role instances work together and are often used by an application simultaneously. For example, a web role instance might accept requests from users, then pass them to a worker role instance for processing.

Monitoring performance of Web and Worker Roles

Azure Portal provides basic monitoring for Azure Web and Worker Roles. Users that require advanced monitoring, auto-scaling or self-healing features for their cloud role instances, should learn more about CloudMonix. Along with advanced features designed to keep Cloud Services stable, CloudMonix also provides powerful dashboards, historical reporting, various integrations to popular ITSM and other IT tools and much more. Check out this table for a detailed comparison of CloudMonix vs native Azure monitoring features.

5. What are Resource Groups?

◦ A resource group is **a container that holds related resources for an Azure solution**. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group.

6. What is a Virtual Machine?

◦ A virtual machine is **a program on a computer that works like it** is a separate computer inside the main computer. ... It is a simple way to run more than one operating system on the same computer. A very powerful server can be split into several smaller virtual machines to use its resources better.

7. What is an App Service?

◦ *Azure App Service* is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. You can develop in your favorite language, be it .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. Applications run and scale with ease on both Windows and Linux-based environments.

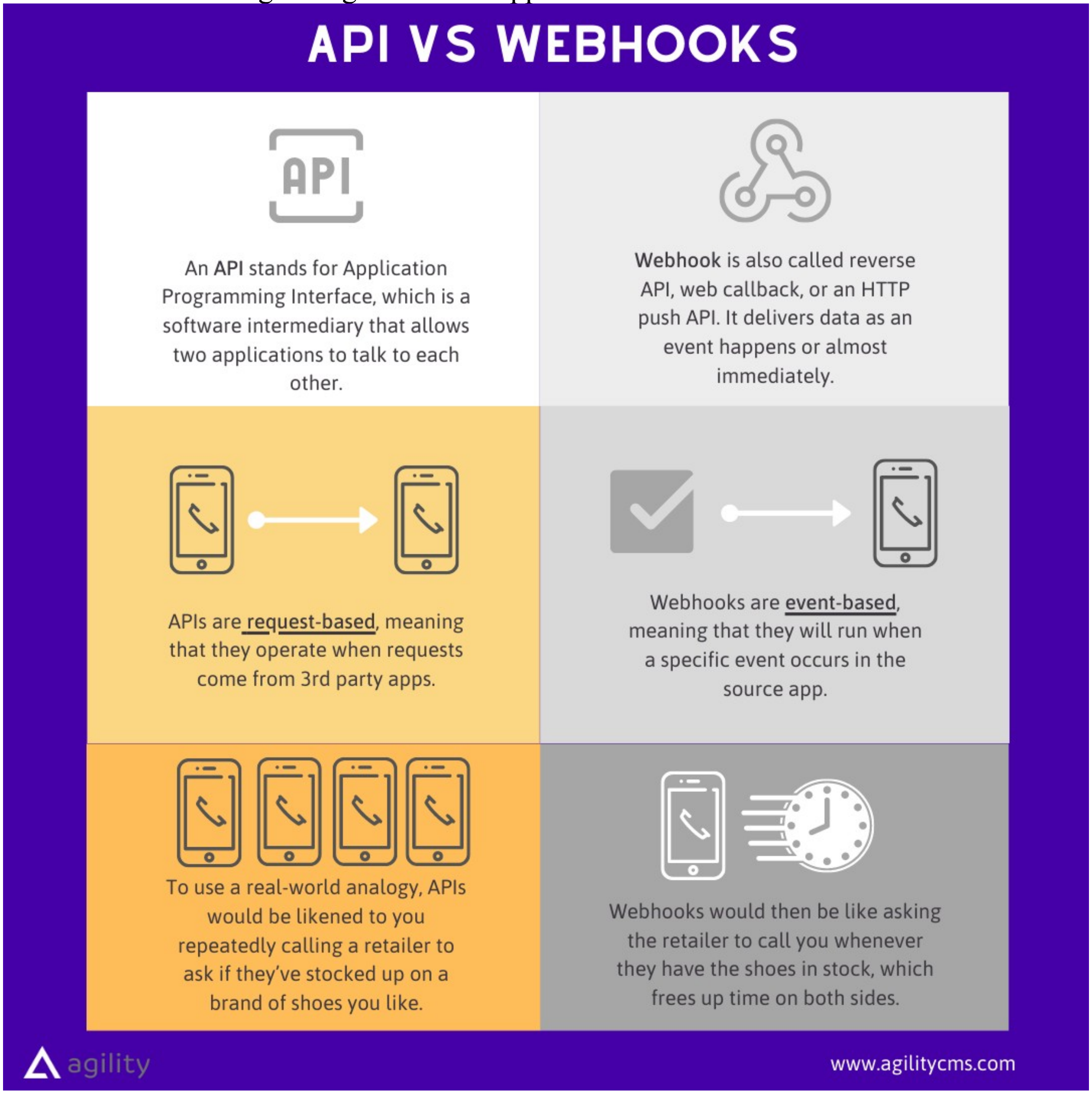
App Service not only adds the power of Microsoft Azure to your application, such as security, load balancing, autoscaling, and automated management. You can also take advantage of its

DevOps capabilities, such as continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domain, and TLS/SSL certificates.

With App Service, you pay for the Azure compute resources you use. The compute resources you use are determined by the *App Service plan* that you run your apps on. For more information, see Azure App Service plans overview.

8. What is a WebHook?

◦ A webhook in web development is a method of augmenting or altering the behavior of a web page or web application with custom callbacks. These callbacks may be maintained, modified, and managed by third-party users and developers who may not necessarily be affiliated with the originating website or application.



API VS WEBHOOKS

An **API** stands for Application Programming Interface, which is a software intermediary that allows two applications to talk to each other.

Webhook is also called reverse API, web callback, or an HTTP push API. It delivers data as an event happens or almost immediately.

APIs are **request-based**, meaning that they operate when requests come from 3rd party apps.

Webhooks are **event-based**, meaning that they will run when a specific event occurs in the source app.

To use a real-world analogy, APIs would be likened to you repeatedly calling a retailer to ask if they've stocked up on a brand of shoes you like.

Webhooks would then be like asking the retailer to call you whenever they have the shoes in stock, which frees up time on both sides.

9. What are Cloud computing benefits?

◦ **Benefits of cloud computing**

Cloud computing offers your business many benefits. It allows you to set up what is essentially a virtual office to give you the flexibility of connecting to your business anywhere, any time. With the growing number of web-enabled devices used in today's business environment (e.g. smartphones, tablets), access to your data is even easier.

There are many benefits to moving your business to the cloud:

Reduced IT costs

Moving to cloud computing may reduce the cost of managing and maintaining your IT systems. Rather than purchasing expensive systems and equipment for your business, you can reduce your costs by using the resources of your cloud computing service provider. You may be able to reduce your operating costs because:

- the cost of system upgrades, new hardware and software may be included in your contract
- you no longer need to pay wages for expert staff
- your energy consumption costs may be reduced
- there are fewer time delays.

Scalability

Your business can scale up or scale down your operation and storage needs quickly to suit your situation, allowing flexibility as your needs change. Rather than purchasing and installing expensive upgrades yourself, your cloud computer service provider can handle this for you. Using the cloud frees up your time so you can get on with running your business.

Business continuity

Protecting your data and systems is an important part of business continuity planning. Whether you experience a natural disaster, power failure or other crisis, having your data stored in the cloud ensures it is backed up and protected in a secure and safe location. Being able to access your data again quickly allows you to conduct business as usual, minimising any downtime and loss of productivity.

Collaboration efficiency

Collaboration in a cloud environment gives your business the ability to communicate and share more easily outside of the traditional methods. If you are working on a project across different locations, you could use cloud computing to give employees, contractors and third parties access to the same files. You could also choose a cloud computing model that makes it easy for you to share your records with your advisers (e.g. a quick and secure way to share accounting records with your accountant or financial adviser).

Flexibility of work practices

Cloud computing allows employees to be more flexible in their work practices. For example, you have the ability to access data from home, on holiday, or via the commute to and from work (providing you have an internet connection). If you need access to your data while you are off-site, you can connect to your virtual office, quickly and easily.

Access to automatic updates

Access to automatic updates for your IT requirements may be included in your service fee. Depending on your cloud computing service provider, your system will regularly be updated with the latest technology. This could include up-to-date versions of software, as well as upgrades to servers and computer processing power.

10. What is Public, Private and Hybrid cloud execution as for Azure or other platforms?

Basic Microsoft Intune Interview Questions

What is the difference between Cloud Based and on-Premise Mobility Solution?

On Premise vs. Cloud

It’s no surprise that cloud computing has grown in popularity as much as it has, as its allure and promise offer newfound flexibility for enterprises, everything from saving time and money to improving agility and scalability. On the other hand, on-premise software – installed on a company’s own servers and behind its firewall – was the only offering for organizations for a long time and may continue to adequately serve your business needs (think, “if it ain’t broke then don’t fix it”). Additionally, on-premise applications are reliable, secure, and allow enterprises to maintain a level of control that the cloud often cannot. But there's agreement among IT decision-makers that in addition to their on-premise and legacy systems, they'll need to leverage new cloud and SaaS applications to achieve their business goals.

On-Premise Software

Whether a company places its applications in the cloud or whether it decides to keep them on premises, data security will always be paramount. But for those businesses in highly regulated industries, the decision might already be made for them as to whether to house their applications on premise. And knowing your data is located within your in-house servers and IT infrastructure might also provide more peace of mind anyway.

On-premise software requires that an enterprise purchases a license or a copy of the software to use it. Because the software itself is licensed and the entire instance of software resides within an organization’s premises, there is generally greater protection than with a cloud computing infrastructure. So, if a company needs all this extra security, why would they dip its proverbial toes into the cloud?

The downside of on-premise environments is that costs associated with managing and maintaining all the solution entails can run exponentially higher than a cloud computing environment. An on-premise setup requires in-house server hardware, software licenses, integration capabilities, and IT employees on hand to support and manage potential issues that may arise. This doesn’t even factor in the amount of maintenance that a company is responsible for when something breaks or doesn’t work.

Cloud Computing

Cloud computing differs from on-premises software in one critical way. A company hosts everything in-house in an on-premise environment, while in a cloud environment, a third-party provider hosts all that for you. This allows companies to pay on an as-needed basis and effectively scale up or down depending on overall usage, user requirements, and the growth of a company.

A cloud-based server utilizes virtual technology to host a company's applications offsite. There are no capital expenses, data can be backed up regularly, and companies only have to pay for the resources they use. For those organizations that plan aggressive expansion on a global basis, the cloud has even greater appeal because it allows you to connect with customers, partners, and other businesses anywhere with minimal effort.

Additionally, cloud computing features nearly instant provisioning because everything is already configured. Thus, any new software that is integrated into your environment is ready to use immediately once a company has subscribed. With instant provisioning, any time spent on installation and configuration is eliminated and users are able to access the application right away.

As an example, EDI software has been traditionally been hosted on-premises, but recent cloud computing developments have allowed EDI providers to offer their services via an EDI SaaS model.

This development has saved installation costs for clients, but also enabled software companies to create a recurring revenue model charged on an annual basis.

Key Differences of On-Premise vs. Cloud

As outlined above, there are a number of fundamental differences between an on-premises and a cloud environment. Which path is the correct one for your enterprise depends entirely on your needs and what it is you're looking for in a solution.

Deployment

On Premises: In an on-premises environment, resources are deployed in-house and within an enterprise's IT infrastructure. An enterprise is responsible for maintaining the solution and all its related processes.

Cloud: While there are different forms of cloud computing (such as public cloud, private cloud, and a hybrid cloud), in a public cloud computing environment, resources are hosted on the premises of the service provider but enterprises are able to access those resources and use as much as they want at any given time.

Cost

On Premises: For enterprises that deploy software on premise, they are responsible for the ongoing costs of the server hardware, power consumption, and space.

Cloud: Enterprises that elect to use a cloud computing model only need to pay for the resources that they use, with none of the maintenance and upkeep costs, and the price adjusts up or down depending on how much is consumed.

Control

On Premises: In an on-premises environment, enterprises retain all their data and are fully in control of what happens to it, for better or worse. Companies in highly regulated industries with extra privacy concerns are more likely to hesitate to leap into the cloud before others because of this reason.

Cloud: In a cloud computing environment, the question of ownership of data is one that many companies – and vendors for that matter, have struggled with. Data and encryption keys reside within your third-party provider, so if the unexpected happens and there is downtime, you maybe be unable to access that data.

Security

On Premises: Companies that have extra sensitive information, such as government and banking industries must have a certain level of security and privacy that an on-premises environment provides. Despite the promise of the cloud, security is the primary concern for many industries, so an on-premises environment, despite some of its drawbacks and price tag, make more sense.

Cloud: Security concerns remain the number one barrier to cloud computing deployment. There have been many publicized cloud breaches, and IT departments around the world are concerned. From personal information of employees such as login credentials to a loss of intellectual property, the security threats are real.

Compliance

On Premises: Many companies these days operate under some form of regulatory control, regardless of the industry. Perhaps the most common one is the Health Insurance Portability and Accountability Act (HIPAA) for private health information, but there are many others, including the Family Educational Rights and Privacy Act (FERPA), which contains detailed student records, and other government and industry regulations. For companies that are subject to such regulations, it is imperative that they remain compliant and know where their data is at all times.

Cloud: Enterprises that do choose a cloud computing model must do their due diligence and ensure that their third-party provider is up to code and in fact compliant with all of the different regulatory mandates within their industry. Sensitive data must be secured, and customers, partners, and employees must have their privacy ensured.

Hybrid Cloud Solutions

While the debate of the pros and cons of an on-premises environment pitted against a cloud computing environment is a real one, and one that many enterprises are having within their offices right now, there is another model that offers the best of both worlds.

A hybrid cloud solution is a solution that features an element of different types of IT deployment models, ranging from on premises to private cloud and public cloud. A hybrid cloud infrastructure depends on the availability of a public cloud platform from a trusted third-party provider, a private cloud constructed either on premises or through a hosted private cloud provider, and effective WAN connectivity between both of those environments

1.

2. Explain the advantages and disadvantages of Cloud Based and on-Premise Mobility Solution.

◦ What is better: on-premises or cloud? Many established companies wonder if it's worth it to transition out of their on-premises technological infrastructure and move on to the cloud. In contrast, several newer companies wonder if they should invest their early capital in on-premises systems. To choose which option is right for your company, you need to be aware of the differences between on-premises and cloud-based services and infrastructure.

Anytime you do a cloud and on-premises comparison, it's important to think about the needs of your business. There are trade-offs to whatever option you choose, so you should be fully i nformed before you decide how many on-premises or cloud services you include at your company.

There are several elements that go into on-premises and cloud systems. To narrow it down, you should focus on the differences between two core elements to your solution: storage and software. Both storage and software are vital to a company's ability to function day-to-day. As such, there are several cloud and on-premises offerings for storage and software applications.

Cloud Storage vs. On-Premises Storage

Choosing to store your data on external servers or in-house servers is a major decision that companies must consider. As you look at the pros and cons of on-premise and cloud storage, you should be knowledgeable about their most important qualities.

ADVANTAGES OF CLOUD STORAGE

One of the primary ways the cloud interacts with your company is in the way it stores data. Unlike an on-premises servers with storage, cloud storage uses external servers managed by another company.

A primary function of any business is the ability to store data in servers. After all, servers are the lifeblood of your organization. They store your information, connect your employees and allow you to connect with others around the world. In the past, on-site servers were the only options available to you, but now, cloud-based servers are a viable option as well.

Cloud storage is a great option for many companies, as it provides cost-saving benefits along with functional ones like regular data backups and the ability to scale easily. Cloud storage is a great option for your company because it can:

- **Reduce IT staff's responsibilities:** As your cloud storage will be managed by another company, your IT staff won't have to take the time to install new software patches or updates, freeing up their time for other tasks.
- **Eliminate capital expenses:**While on-premises storage is considered a capital expense, cloud storage is considered an operational expense. Typically, on-premises storage requires a large initial investment to purchase equipment and install it in the office. As cloud storage is taken care of externally, there is no need for capital investment. Instead, companies will pay an affordable monthly subscription.
- **Adjust to your budget:** To help companies keep their initial costs low, organizations regularly pay for cloud-storage on a month by month basis. No matter if you're scaling up or scaling down, most cloud-based storage companies can adjust their prices to meet your budget. Additionally, cloud storage features can be adjusted, added or left out of plans altogether. This sort of flexibility is great for companies who expect change and don't want to get locked into paying for services they don't need.
- **Perform regular data backups:**The cloud offers easier data backup than on-premises servers ever could. Cloud-based servers give users peace of mind because they know if their computer goes haywire or their local files are deleted, they can find the

information again. This ability to access information that would otherwise be lost means your company can minimize the risk of losing critical information.

- **Adjust to your company's needs:** Cloud-based storage is built to scale. Need a few extra terabytes of data to store more data? Simply upgrade your plan with a click or two. Unlike a company's own servers that would need to have new hardware installed, cloud-based servers can quickly be expanded to meet the needs of your company. For those companies growing quickly, it means that you'll never have to worry about slowing down because your equipment can't keep up.

WHY CLOUD STORAGE MAY NOT BE THE BEST OPTION

Though there are several benefits to using the cloud for your storage needs, it also comes with some drawbacks. Cloud storage may not be the best choice for your company because:

- **Internet determines user experience:** When you use cloud storage, a fast and reliable internet connection is a must-have. A redundant Internet connection should also be considered if a majority of the workload will be hosted in the Cloud. If you have a slow connection, accessing your files or downloading them can be a tedious experience. For those who need to work quickly, a slow internet connection can provide a horrible user experience while they access your cloud servers.
- **Costs can balloon with little warning:** The rapid scalability of cloud storage, while an advantage listed above, can also be a costly determent if left unmanaged. Cloud services are consumption models, so the more storage your Company requires, the higher the monthly cost. Companies should adopt policy and process to avoid the surprise of a costly invoice. A single point of contact should be identified within the Company, one who is accountable for the Cloud relationship and lap-lanes should be established for consumption with anticipated cost increases when lap-lanes are exceeded.
- **Access is based on connection:** A downside of relying on the internet to store your files is that an internet outage can totally knock out your access to important files. Losing access to your data during a connection outage can delay your operations and make it impossible for some staff members to be productive. While the reliability of the internet has come a long way over the years, companies need to be confident in their connection before they switch to cloud storage.
- **Litigation – search warrant:** If your company is the focus of an investigation, law enforcement could issue a search warrant to your cloud supplier. Forcing access to your Company storage without your consent to search for artifacts that support an investigation. Electronic materials that are strategic to the Company operation, may not be appropriate for Cloud storage. Companies should have written guidelines and acceptable use policy to accompany the cloud storage service
- **Data is less secure:** Whenever you work with a cloud storage company, you are entrusting the management of your data to another party for them to manage and keep secure. Whenever an outside-party is trusted with your company data, you run the risk of unauthorized personnel accessing it. To avoid this, you'll want to ask about security practices

and procedures of the Cloud company and how they encrypt your data while it's in transit and at rest.

ADVANTAGES OF ON-PREMISES STORAGE

Unlike cloud storage, on-premises storage relies on infrastructure at your Company's brick and mortar office to manage your data. You'll own all of the equipment and you will be responsible for the lifecycle management. As you might guess, there are several pros and cons of on-premises solutions for data storage.

Though cloud-storage has been all the rage lately, some companies still believe that on-premises solutions are best suited for their business needs. For example, many enjoy the greater security that on-premises solutions and storage give their data. On-premises storage is a great option for your business because it can:

- **Operate without internet:**One of the major upsides to on-premises storage is that it doesn't require users to have an internet connection to access data. Though most businesses rely on the internet to conduct business, there's always a fear that the loss of a connection could harm productivity and make it impossible to access crucial data. On-premises servers will provide you with an internal network that is accessible anytime, no matter your internet connection.
- **Lower monthly internet costs:** If your business doesn't rely on the internet or cloud-based services, you may not need to pay for such a high-speed connection. For those with on-premises storage, the need for a strong connection with fast download speeds is reduced even further. Based on your needs, you may not have to pay for a more expensive internet plan if you don't have to access the cloud to view files.
- **Provide greater security:** Unlike cloud-storage, which is more vulnerable to third parties and prying eyes, on-premises storage is completely restricted from anyone other than authorized personnel. On-premises servers are not accessible to those outside the network, as they are not storing the data online. For companies who handle sensitive data, like those in the financial industry, on-premises storage may be a preferred option.
- **Offer control over server hardware:**Some companies enjoy having dedicated servers within their building to handle all their needs. Instead of having to ask a cloud storage company to upgrade their storage plan or add new features, the company can simply do the upgrades themselves. Potentially, being able to modify the server's hardware can give savvy companies greater flexibility and customization for their storage needs.

WHY ON-PREMISES STORAGE MAY NOT BE THE BEST OPTION

Despite the many advantages that come with on-premises storage, there are some drawbacks companies should be aware of. On-premises storage may not be the best choice for your business because it can:

- **Require extra IT support:** If you decide you want to use on-premises storage, you'll also need to have IT staff to maintain and manage your servers. This could mean you have to hire new staff members or devote more of your current staff's time to maintaining the servers. This extra support can add to your costs and reduce the efficiency of your IT department as they will have increased responsibilities associated with the on-premises servers.

- **Adherence to industry compliance:** If your Company operates within a regulated industry such as Finance or HealthCare, the responsibility to abide by the governing regulations will fall squarely on your Company as you are the owner and operator of the servers and on-premise storage. Compliance can require the attention of many employees, additional money for outside audits and potential fines if the infrastructure is found to be out of compliance.
- **Increase maintenance costs:** Along with the initial capital investment required to purchase servers and other hardware, you'll also need to continue to buy hardware, software and licenses to upgrade the system or repair it. Oftentimes, a piece of hardware will malfunction and need to be replaced. Additionally, in order to realize the most from your server investment, you will want to upgrade your equipment, which will likely be annually (at least), and will require an investment of more money.
- **Require a greater capital investment:** When you first set up on-premises storage, you'll have to invest a significant amount of capital to purchase the servers and other pieces of hardware to get it running. For companies just trying to get off the ground, this level of capital investment can be a huge disadvantage. Along with purchasing the equipment, you'll also need to devote time and money to make sure it's properly installed.
- **Increase the risk of data loss:** Data is the backbone of your business. Losing it can be crippling, both for your efficiency and your reputation. With on-premises storage, a malfunction in the system or a compromised system held for ransom can cause you to lose your data permanently. While a cloud-based system will keep your data backed up, on-premises storage systems have all the data stored on an internal server, meaning you assume a greater amount of risk. A best practice for on-premise storage, to avoid the loss of data, is to include an off site backup service that replicates the data to another site or media.
- **Limit your company's ability to scale:**If your company scales up and needs more storage space or other capabilities, it's more difficult to scale your on-premises servers quickly. Unlike cloud-storage, where companies can simply pick a more expansive plan with a click, on-premises storage requires you to install new hardware and devote manpower to building the new systems.

When you are comparing your options of on-premise and cloud storage, make sure to weigh the pros and cons of each. As you are selecting your provider for the services, ask the right questions to make sure you get the best option for your organization.

Cloud-Based Software vs. On-Premises Software

Is on-premises or cloud better for your business? Whenever a company looks to add new software to their business, it's important for them to know about whether cloud computing or on-premises software is a better option for their needs.

ADVANTAGES OF CLOUD-BASED SOFTWARE

If you're interested in cloud-based software, you'll be happy to know that there are plenty of advantages to using it. Some of the top benefits include:

- **Affordability:** Generally, costs are lower for cloud-based applications. Instead of having to pay a large licensing fee upfront, you'll have much lower monthly costs. Often times, these monthly costs take the form of subscription fees. Along with the lower initial costs that make them more affordable, the companies offering these subscriptions often include maintenance and support, saving you manpower and the financial cost of having to troubleshoot problems yourself.
- **Ease of deployment:** One of the biggest advantages of cloud computing is its ability to be deployed quickly without long installation processes. Customers of cloud software vendors will be able to start using the vendors' application within minutes. Quick deployment gives companies an edge over the competition, and as such, is very popular among competitive companies.
- **Management services:** One major aspect of cloud computing is the management services that vendors will typically offer clients. Instead of having to host the software or purchase hardware themselves, a customer can work with a vendor who will take care of it all externally, freeing up staff and reducing costs. The business won't ever have to worry about upgrades or network monitoring, as the vendor will manage it all.

WHY CLOUD-BASED SOFTWARE MAY NOT BE THE BEST OPTION

As you can see, cloud-based computing has several benefits. However, before you sign up for it, there are a few disadvantages you'll need to be mindful of, including:

- **Long term costs**: One drawback to cloud-based software is that, in the long-term, subscription costs can end up costing more in total than if a company would have paid for a licensing fee from the very beginning. This is especially true if your organization does not rely on the latest version of software. Cloud based software provides the latest version to the user and those development costs are reflected in the monthly subscription.
- **Less flexibility:** Flexibility and customizability is often an issue for companies that use cloud-based software. The suppliers that provide software to companies via the cloud often don't include widely customizable options. All consumers are provided the same off the shelf application. The service is often designed for the industry rather than the specific needs of a company, meaning that customers may not receive a service that is convenient for everything they do.
- **Security concerns:** Like the security issues that affect cloud storage, cloud software also has comparable problems with security. Though security has gotten better, the cloud can still be hacked into by outside forces that look to extract data from these online programs. If you go with the cloud, seek out suppliers who support single sign on and multi-factor authentication. Onboarding / offboarding processes should be adopted to manage employee access via a common company directory server.

ADVANTAGES OF ON-PREMISES SOFTWARE

On-premises software comes with advantages that are sure to provide value to your business. The following are some of the top ways on-premises software can be of assistance:

- **Greater customization:** Since you'll handle all of the on-premises software yourself, you'll likely be able to customize it much more than if you were subscribing to a cloud-based system. If your company has niche needs that aren't regularly covered by options in the industry, then on-premises software may be right for you.
- **License purchase versus subscription:** licensing models for premise system are usually tied to the host hardware vs. the employee. A company has greater discression for reallocating licenses within this concurrent seat model. It is usually a best practice to purchase 10-15% more licenses to accommodate growth during the lifecycle of the platform.
- **Greater security:** Better security is commonly cited as the main reason businesses stick with on-premises security. Like with storage, it's less likely that anyone will be able to access your programs and siphon data if you keep everything in-house. Additionally, it's typically easier to install extra data protection tools to data and programs based on an on-premises system rather than a cloud-based one.

WHY ON-PREMISES SOFTWARE MAY NOT BE THE BEST OPTION

Even with the many advantages on-premises software provides, you'll also need to take into account the downsides, including:

- **Long deployment times:** One major issue affecting companies that use on-premises software is its inability to be deployed quickly. When you purchase a piece of software, you'll have to configure the hardware, test the program to see if its working and then roll it out to every employee. This can be incredibly time consuming and can put you at a disadvantage.
- **Scalability:** Another common issue with on-premises software is that it doesn't scale as well as cloud-based software. For example, if you increase the number of users in a program, your IT staff will have to manually install the software or hardware to let your new employees use it. Additionally, old software can go out of date and saddle you with programs that you no longer have any use for.
- **Remote offices and mobile workforce:** If your company has multiple offices or a large mobile workforce, on premise software can introduce new challenges in providing access to these remote employees. Additional network or carrier services must be included, increasing the operational costs and overall complexity for the Company.
- **Upfront costs:**When you decide to purchase software and integrate it into your on-premises system, you'll need to pay a higher initial cost for the services. While these costs may even out over time, it's likely that new, updated programs will hit the market, meaning you may not use a program long enough to make back the money you spent at the beginning. For companies that don't have a lot of capital on hand, a cloud-based subscription may be better.

4. What is Microsoft Intune?

◦ Microsoft Intune, which is a part of Microsoft Endpoint Manager, is a Microsoft cloud-based management tool for mobile devices that aims to provide unified endpoint management of both corporate and BYOD equipment in a way that protects corporate data.

5. How Microsoft Intune works?

If you've been looking at **the benefits of Microsoft 365 for business**, you may have noticed something called **Intune** listed as one of the secure cloud services included. Intune's something I hadn't used a lot and I don't think there's a lot of awareness about it, so I decided to research and write this post.

Microsoft Intune is a secure cloud service that enables mobile device management and mobile application management. With Intune you can manage how devices are used and enforce policies that allow you to control applications.

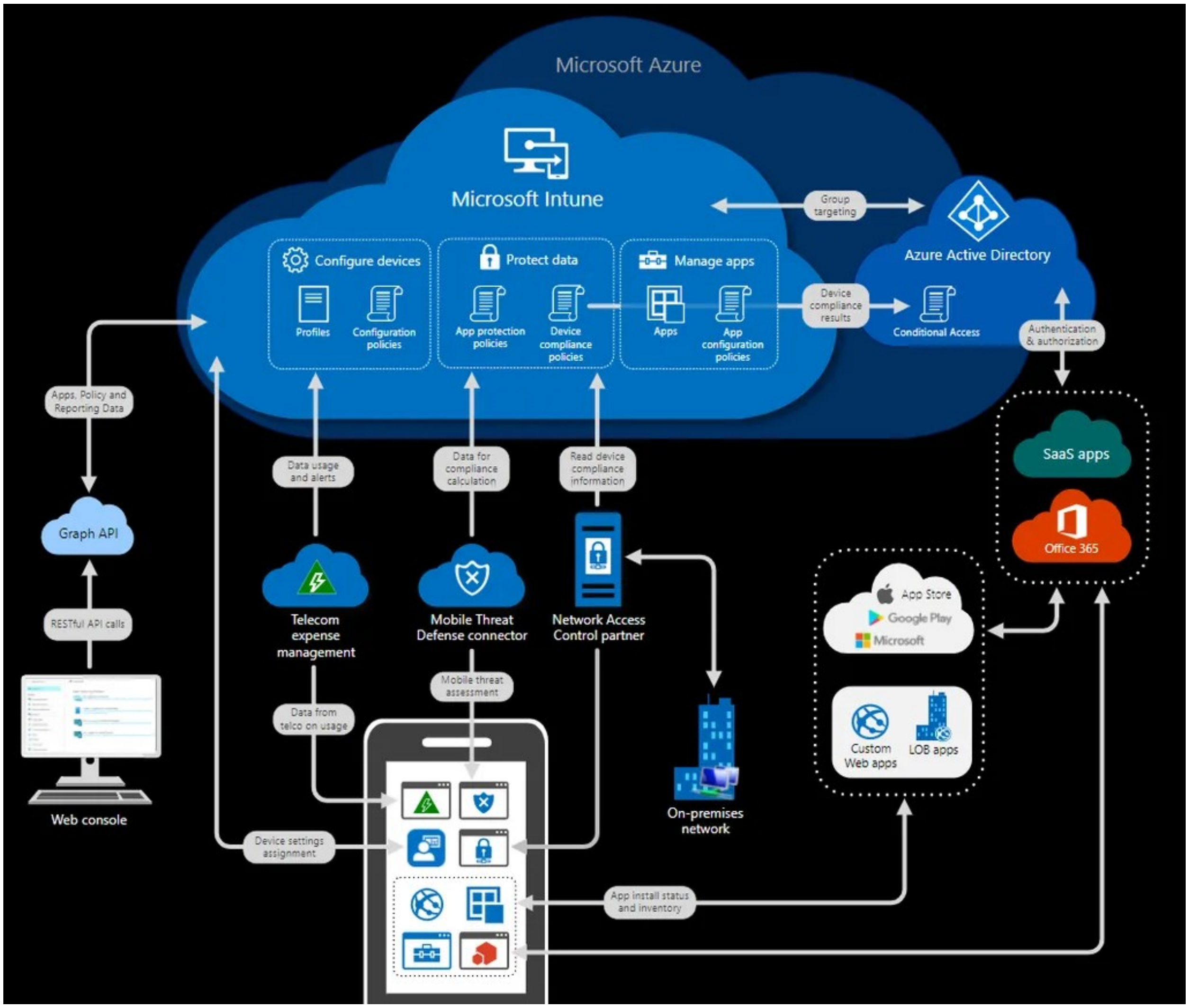
Intune is an advanced cloud-based service that integrates with other Microsoft services to provide comprehensive management of mobile devices. This blog post is going to be a bit of an overall look at Intune, including:

- How Does Microsoft Intune Work?
- What Can You Do With Microsoft Intune?
- How Does Microsoft Intune Integrate With Other Microsoft Services?
- Why Use Microsoft Intune?
- What Licences Do I Need To Use Microsoft Intune?

By the end of this blog post, you should know how Intune works and how your organisation would benefit from using it.

How Does Microsoft Intune Work?

As I said, Microsoft Intune is a cloud-based service that allows you to remotely manage mobile devices and mobile applications. One of the biggest benefits of Intune is that you can have an ultra-productive mobile workforce without worrying about the security of your organisation's data.



Microsoft Intune architecture. *Image: docs.microsoft.com*

You can do a lot with Intune, making it possible for your teams to work anywhere using their mobile devices. You can:

- **Set rules and configure policies for a range of devices, whether they're personal or organisation-owned.** This means your company can have a BYOD (Bring Your Own Device) policy without major concerns about security.
- **Deploy apps to mobile devices from any location to several devices concurrently.** For example, you can deploy apps such as Microsoft Teams, Word, and Outlook to the devices you manage using Intune.
- **Control what users and devices can access.** Protect your organisation's data by controlling the information that users can access and share.

- **Ensure that the devices your team members are using are compliant with your security requirements.** If devices aren't compliant, this will be flagged up and you can resolve the issue.

Intune is an excellent cloud-based service to use for both organisation-owned and personal mobile devices. However, I think it's particularly useful for businesses that embrace a **Bring Your Own Device** policy.

If your team members are using their own devices (mobile phones, laptops, and tablets to give 3 examples) for work, you must do everything within your power to protect your organisation's devices. **Microsoft Intune is massively beneficial here, as it lets you prevent users from accessing certain data on certain devices. You can also prevent users from sharing your organisation's data and isolate organisation data from personal data.**

Intune is actually part of Microsoft's Enterprise Mobility + Security Suite and it also integrates with several other Microsoft services. For example, Microsoft Intune integrates with:

- **Azure AD (Azure Active Directory)**
- **Azure Information Protection**
- **Microsoft 365 Applications**

Microsoft Enterprise Mobility + Security Suite (EMS) is made up of a range of applications and services:

- Azure Active Directory
- Microsoft Endpoint Configuration Manager
- Microsoft Intune
- Azure Information Protection
- Microsoft Cloud App Security
- Microsoft Advanced Threat Analytics
- Microsoft Defender for Identity
- Microsoft Secure Score

As you can see, Microsoft Intune is a small part of Microsoft Enterprise Mobility + Security (EMS). The EMS Suite is designed to offer businesses excellent, best-in-class protection, detection, and response capabilities.

To fully appreciate Microsoft Intune and make the most of it, you need to fully understand what you can do with it. Here's what you can do with Microsoft Intune.

What Can You Do With Microsoft Intune?

Microsoft Intune is an excellent cloud-based service for MDM (mobile device management) and MAM (mobile application management). Here's a quick overview of everything you can do with it.

There are 3 main things you can do with Microsoft Intune:

- **Set rules and configure policies for devices**
- **Deploy apps to mobile devices remotely**

- **Control what users can access and share**

I think those points give you a really good idea of how you can use Intune and how doing so would advantage your business. However, I'm going to break down each point and give you some real-world examples of what you can do.

Set rules and configure policies for devices

Microsoft Intune enables you to set rules and policies for enrolled devices. Your organisation can control how team members can use the devices, ultimately protecting your business and its data.

In Microsoft Intune, you can create several configuration profiles that you can apply to mobile devices used by your team members. There are numerous features and settings that you can enable and disable on devices that are enrolled in Intune.

Configuration profiles can be created for a range of devices and operating systems, such as iOS, Android, and Windows. Configuration profiles contain a range of settings and rules that can be applied to any device within your organisation. For example, here are some of the functions Intune will allow you to control:

- Block access to Bluetooth settings on devices
- Block/allow access to certain devices on the network, such as printers
- Create VPN profiles, enabling the devices to remotely access your organisation's network
- The installation of updates

There are literally hundreds of configuration profile templates ready to go. Pick and choose between the templates you want to use to create profiles that are tailored to the requirements of your organisation.

Deploy apps to mobile devices remotely

A part of Microsoft Intune is mobile application management (MAM). **Mobile application management within Intune allows you to deploy and control apps, as well as monitor usage.**

For enrolled devices (personal or organisation-owned), you can:

- **Remotely configure apps**, controlling when the device user can open apps or force them to open at a certain time
- **Assign devices and users to fully-configurable groups**, making deploying apps, policies, and rules simple
- **See reports on when and how devices are used**
- **Wipe data from apps remotely**, which is ideal if a device is stolen or you suspect malcontent

- **Control actions that users can take in apps**, such as preventing sharing, screenshotting, and copy & pasting

You can give users as much flexibility as required to enhance productivity while still controlling your organisation's data.

Control what users can access and share

With Microsoft Intune, you have complete control over what users can access and share on enrolled devices.

Controlling what users can access and share can be much more advanced than just allowing or restricting access. **You can micromanage access and sharing with app protection policies, preventing users from performing certain actions within apps.**

For example, you can restrict users by preventing them using copy and paste functionality within certain apps. You can also control whether or not users can send emails to email addresses outside of your organisation's control, or prevent certain types of data from being transmitted via email.

Using user groups, you can assign certain policies and rules to groups of users and devices. Alternatively, you can assign policies and rules per user and per device should you wish to. However, using groups you can rapidly push policies and rules to large numbers of devices and users.

How Does Microsoft Intune Integrate With Other Microsoft Services?

Microsoft Intune integrates with a number of other Microsoft services as I mentioned earlier in this blog post.

Intune integrates with Azure Active Directory for access control and Azure Information Protection for data protection purposes.

Microsoft Intune also integrates with the Microsoft Office suite of products. With Intune, you can remotely install applications such as Outlook and Word on devices and for certain users. You can also control how these applications work for certain devices and users.

As one of the cloud-based services that makes up Microsoft's Enterprise Mobility + Security (EMS) suite, Intune is also closely integrated with the other services that make up the suite. EMS is a mobility management and security platform, so all the services within the platform are designed to empower your organisation's team members to work productivity anywhere while ensuring your organisation is kept secure.

Are you still wondering why you should use Microsoft Intune? Here's why Intune is beneficial for organisations and their employees.

Why Use Microsoft Intune?

The workforce, or labor force, is becoming increasingly mobile worldwide. More organisations than ever have people working on the move, which is enabled by the number of cloud services available to us. However, security is a big concern when users are working remotely or on the go. Intune is one of the Microsoft services that makes working on the go secure and accessible for all organisations.

Microsoft Intune lets you give your team everything they need to work on their mobile devices without sacrificing security. Essentially, you get the best of both worlds. Users can remain productive regardless of the device they are using without having to worry about the security of your organisation's data.

What Licences Do I Need To Use Microsoft Intune?

There are three primary ways to get access to Microsoft Intune. They are:

- **As a standalone Azure service.** Intune is available as a standalone add-on within Azure. You will pay a subscription fee per user.
- **As part of a Microsoft 365 licence.** Microsoft Intune is available to users with any of the following M365 licences:
- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Microsoft 365 Government
- **As part of Mobile Device Management for Microsoft 365.** Mobile Device Management for Microsoft 365/Basic Mobility and Security is essentially a more basic version of Intune. This is available to users of all M365 plans.

6.Explain end to end setup of Microsoft Intune?

https://docs.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-intune-setup
https://www.thelazyadministrator.com/2018/11/19/configure-and-deploy-intune-mdm/
https://www.anoopcnair.com/learn-microsoft-intune/
https://tminus365.com/wp-content/uploads/2019/04/Intune-Implementation-TMINUS.pdf
https://tminus365.com/wp-content/uploads/2019/04/Intune-Implementation-TMINUS.pdf
https://systemcenterdudes.com/setup-microsoft-intune-and-manage-it-in-endpoint-manager/

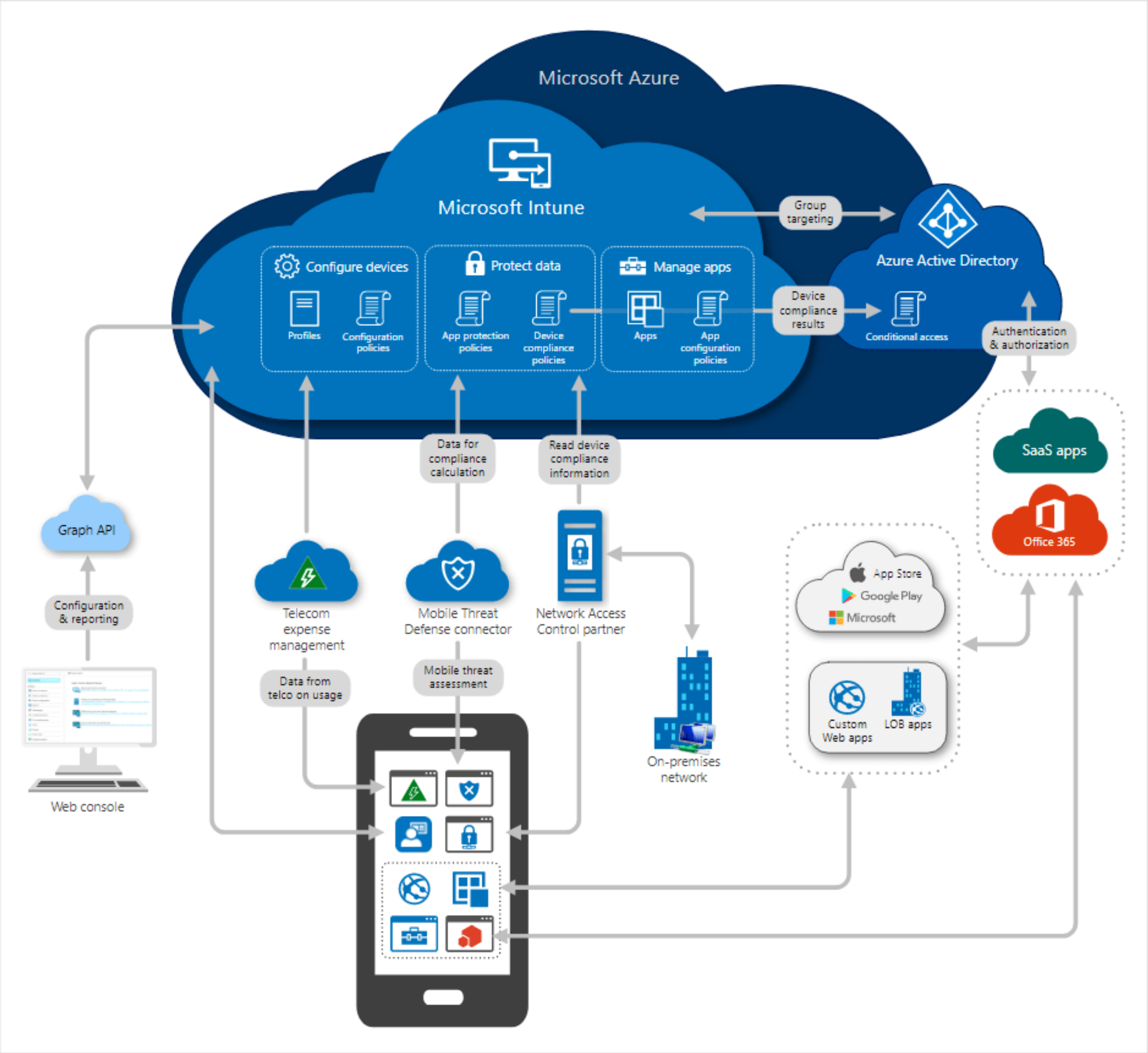
7.Explain the differences between Microsoft MDM for Office 365 and Microsoft Intune.

Mobile Device Management (MDM) for Office 365 is a useful solution for many organizations who want to to securely manage their mobile devices (Android, iOS, and Windows devices). Luckily, many Office 365 subscriptions include MDM. In addition to MDM for Office 365, you can also use Microsoft Intune to manage your mobile devices. Unlike MDM, Intune is not a built-in feature of Office 365. It's a paid subscription, or you can purchase it with Enterprise Mobility + Security (EMS). They both include MDM, so what is the difference between them and which one should you use? Let me give you my take on how I see these two Microsoft offerings and then I will compare the two.

MDM is a built-in feature included in Office 365, while Intune is a stand-alone platform that integrates nicely with Office 365. To better understand the difference between them, you might want to think of MDM as a subset of Microsoft Intune. Technically speaking, MDM is not related to Intune and it's not really a subset of Intune. The only reason I said to think that way is that Intune offers everything that MDM for Office 365 offers plus more. Intune is a cloud-based mobile management platform. It's a feature-rich solution that offers not only MDM, but also Mobility Application Management (MAM). MAM is especially useful for companies that support Bring Your Own Device (BYOD) because it lets you deploy and manage mobile apps. Here's how I look at the two.

MDM for Office 365	**Microsoft Intune**
MDM	MDM + MAM + more

Because Intune integrates in many ways with many Office 365 services, it gives you much more control over your mobile devices. It can be used to deploy business apps, Microsoft store apps, and even certificates, Wi-Fi, VPN, and email profiles. Intune also includes the Intune Managed Browser, which allows users to securely browse the Web. The following architecture shows how Microsoft Intune integrates with Microsoft Azure.



(Source: Microsoft Corporation)

Let’s compare the features offered by MDM for Office 365 and Intune. The following table is based on information provided by Microsoft and will give you a much better idea as to which one is the right solution for you.

Feature	**MDM for Office 365**	**Microsoft Intune**
Price	Included at no additional cost with many Office 365 Enterprise and Business subscriptions	Can be purchased with EMS, or as a paid subscription
Device Management	Manage through Security and Compliance Center in Office 365	Manage with Intune’s admin console if you are using Intune by itself, otherwise you can use

		Azure Active Directory, Microsoft 365 admin center, etc.
Types of Devices You Can Manage	Android, iOS, and Windows	Android, iOS, Windows 8.1 (phone and PC), Mac OS X, Windows 10
Key Functionalities	Restrict users from accessing company email and documents only from phones and tablets that are managed by your company and comply with your policies. Manage security policies (e.g. jailbreak detection, device level pin lock, encryption) to prevent unauthorized access to company data if a device is lost or stolen. Remotely wipe out company data from an employee's device, while leaving employee's personal data in place. Visit Capabilities of Built-in Mobile Device Management for Office 365 for more specific information, including the device versions that are supported.	All features included with MDM for Office 365, plus the following: Deploy internal business apps and Microsoft store apps. Enroll and manage company devices in groups to better organize and simplify policy and app deployment. Provide secure access to business resources by deploying certificates, Wi-Fi, VPN, and email policies for users. Enhance security by restricting users' actions like copy, cut, paste, and save as, to only those apps that are managed by Intune. Enable secure Web browsing for users through Intune Managed Browser app. Setup MAM policies through Azure portal, even if employees devices are not enrolled in Intune. Visit Protect app data using MAM policies for more information.

For licensing or other reasons, you may be interested in taking advantage of both MDM for Office 365 and Microsoft Intune. Because they don't step over each other, you can manage some devices with MDM for Office 365 and others with Microsoft Intune.

(Or)

By

- **Peter van der Woude,** KPN ICT Consulting

Published: **10 Mar 2020**

Microsoft offers two ways to handle mobile device management: MDM for Office 365 and Microsoft Intune.

The enterprise mobility industry has changed significantly in the past few years. Mobile device management (MDM) platforms such as MDM for Office 365 was once enough for most organizations. As devices such as iPads, wearables and IoT devices became prevalent in the enterprise, however, many organizations needed advanced management capabilities and a unified console. Unified endpoint management (UEM) products such as Intune entered the market, which provided a way for IT admins to manage a range of different devices under a single console.

MDM still has use cases today, however. MDM for Office 365 provides a limited feature set, but it is included in the price of many Office 365 subscriptions. This built-in tool offers organizations an integrated, inexpensive way to manage mobile devices. Microsoft Intune, on the other hand, provides a rich feature set and comes with additional costs.

MDM for Office 365 capabilities

MDM for Office 365 provides a lightweight version of MDM that does not include mobile application management (MAM). It provides organizations with MDM policies and settings that will help to control access to Office 365 data for supported mobile devices and apps. For stolen or lost devices, it offers the ability to remotely wipe the device to remove corporate data.

Supported platforms

MDM for Office 365 provides support for the following platforms:

- iOS 10.0 or later
- Android 4.4 or later
- Windows 8.1 (limited to Exchange ActiveSync functionality)
- Windows 10 (requires the device to be Azure Active Directory joined)

Supported access control scenarios

MDM for Office 365 provides a few scenarios that will prompt the user to enroll their device. When the user's device doesn't comply with the policy, the user might be blocked from accessing Office 365 data, depending on the policy configuration.

These are the following scenarios:

- Access to **Exchange** by using the built-in mail app on iOS 10 or later
- Access to **Exchange** by using the built-in mail app on Android 4.4 or later
- Access to **Office** and **OneDrive for Business** by using the Outlook, OneDrive, Word, Excel or PowerPoint app on iOS 10 or later
- Access to **Office** and **OneDrive for Business** by using the Outlook, OneDrive, Word, Excel, PowerPoint or the Office Mobile (phones only) app on Android 4.4 or later

People who are using mobile browsers to access Office 365 data will not be prompted to enroll their devices and will not be blocked.

Supported policy settings

With MDM for Office 365, IT can enable certain settings as requirements to access Office 365 data. IT can use these settings in the supported access control scenarios to block users from accessing Office 365 data. These settings are divided into the following categories:

- Security - Require password settings
- Encryption - Require encryption settings
- Jailbroken - Require non-jailbroken devices
- Managed email profile - Require managed email profile

MDM for Office 365 also provides a limited set of policies that IT can use to configure settings on the user's device, such as policies to prevent data loss on devices, access public clouds, make screen captures and access the store.

Microsoft Intune capabilities

Microsoft Intune is a UEM platform that provides MDM and MAM functionality and comes with additional costs, as it's not part of the different Office 365 subscriptions. It requires an organization to have licenses that include the rights for using Microsoft Intune. These licenses include Microsoft Intune standalone, the Enterprise Mobility + Security and the Microsoft 365 subscriptions.

Microsoft Intune helps organizations to provide MDM and MAM policies and settings that will help with controlling access to corporate data. This includes not just data in Office 365, but nearly all corporate data that is available from apps that are exposed via Azure Active Directory (AAD). For stolen or lost devices, Intune provides the ability to remotely wipe the device or app to remove corporate data. It provides organizations with a strong method to secure and manage mobile devices, apps and corporate data.

Supported platforms

Microsoft Intune provides support for the following platforms:

- iOS and iPadOS 11.0 and later
- Mac OS X 10.0.12 and later
- Android 5.0 and later, including Android Enterprise
- Windows 8.1, including Windows 8.1 RT
- Windows 10, including Windows 10 Teams, Windows 10 IoT and Windows Holographic for Business

Supported access scenarios

Microsoft Intune supports many scenarios. The main difference of MDM for Office 365 vs Intune is that Intune is not limited to Office 365-related scenarios. For most organizations, the management boundaries must expand to include all apps and data that can be exposed via AAD and all apps on the devices that can use modern authentication. Intune integrates well within a Microsoft ecosystem, including Office 365.

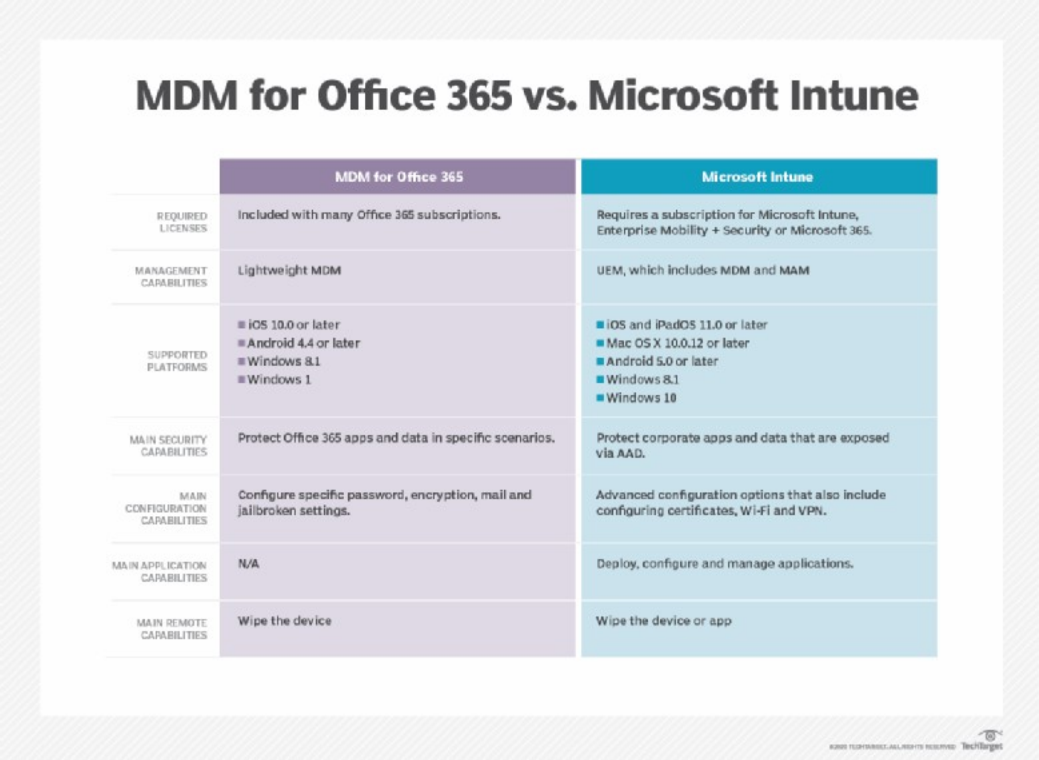
Microsoft Intune can do more than just control access to corporate apps and data. IT can use Intune to verify compliance of devices, deploy applications, assign advanced configurations including Wi-Fi configuration, push certificates and VPN configurations, provide inventory information and more. And that's only mentioning MDM scenarios. Besides that, it also provides MAM scenarios, including the ability to limit access to corporate apps and data and the ability to perform a selective wipe of only the app.

Supported policy settings

Microsoft Intune provides many policy settings and it's nearly impossible to list all the possibilities. It provides the policy settings that are available with MDM for Office 365 and many more. These policy settings are categorized to provide functionality to address the supported access scenarios – for example, policies to verify access requirements, policies to verify compliance, policies to configure settings, policies to configure updates and the ability to deploy, configure and manage apps.

MDM for Office 365 vs. Microsoft Intune

The following table provides an overview of the main capabilities of MDM for Office 365 vs Microsoft Intune.



MDM for Office 365 vs. Microsoft Intune

	MDM for Office 365	Microsoft Intune
REQUIRED LICENSES	Included with many Office 365 subscriptions.	Requires a subscription for Microsoft Intune, Enterprise Mobility + Security or Microsoft 365.
MANAGEMENT CAPABILITIES	Lightweight MDM	UEM, which includes MDM and MAM
SUPPORTED PLATFORMS	■ iOS 10.0 or later ■ Android 4.4 or later ■ Windows 8.1 ■ Windows 1	■ iOS and iPadOS 11.0 or later ■ Mac OS X 10.0.12 or later ■ Android 5.0 or later ■ Windows 8.1 ■ Windows 10
MAIN SECURITY CAPABILITIES	Protect Office 365 apps and data in specific scenarios.	Protect corporate apps and data that are exposed via AAD.
MAIN CONFIGURATION CAPABILITIES	Configure specific password, encryption, mail and jailbroken settings.	Advanced configuration options that also include configuring certificates, Wi-Fi and VPN.
MAIN APPLICATION CAPABILITIES	N/A	Deploy, configure and manage applications.
MAIN REMOTE CAPABILITIES	Wipe the device	Wipe the device or app

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

It should be clear that Microsoft Intune is the most logical choice from a security and management perspective. That doesn't that mean there is no use case for MDM for Office 365. For smaller organizations, or organizations that only use Office 365, this could be enough. That does require strong agreements with the employees, however, as MDM for Office 365 only provides basic security for accessing Office 365 data.

MDM for Office 365 is a good starting point for any organization beginning to deploy MDM. To provide real security and management capabilities, however, any organization should eventually look at using Microsoft Intune when using more than just Office 365.

To support a migration path from MDM for Office 365 and Microsoft Intune, organizations can run both products alongside each other. When a user gets a Microsoft Intune license, the enrollment process will automatically prefer the Microsoft Intune enrollment above the MDM for Office 365 enrollment.

Autopilot —> https://tech24online.com/windows-10-autopilot-with-intune/

8.Explain briefly the difference between Microsoft System Centre Configuration Manager and Microsoft Intune.

Many IT departments are currently facing specific challenges in the management of their systems. Traditional tools such as the System Center Configuration Manager (SCCM) are often used for this purpose. Others like Intune and Autopilot are already based around cloud technologies. A few still rely on old-fashioned '**sneaker networks**'. It is becoming increasingly important for all companies to consider computer devices over their entire life cycle. Updates must be installed regularly to close security vulnerabilities. New Windows 10 versions need to be distributed twice a year. Inventory and compliance management, also beyond the proprietary Active Directory forest, are playing an increasingly important role.

But which is the right solution for my company? Typically for IT, the answer is quite simply '*it depends*'. We will talk about the reasons for using the traditional method via SCCM and the reasons for choosing a modern approach using Intune. It is not intended as a detailed technical comparison, but merely as a description of the most important aspects.

System Center Configuration Manager

The System Center Configuration Manager is the classic solution for managing computer systems. Originally released in 1994 under the name Systems Management Server (SMS), it now runs as the System Center Configuration Manager Current Branch 1902. Like Windows 10, upgrades are released several times a year to fix bugs and introduce new features. The SCCM offers almost everything that admins could possibly want:

- Inventory rationalization
- Application distribution
- Distribution of software updates
- Distribution of operating systems
- Compliance management
- Remote maintenance
- Control of Windows Defender Antivirus
- Reporting
- And much, much more …

The SCCM runs on servers in the company network, and a single server is often sufficient for small environments. But scaling across multiple servers and multiple locations is no problem for larger setups. Connections to services in Microsoft Azure also work perfectly.

But what precisely are its strengths compared to Microsoft Intune?

Use of the Microsoft Cloud is not mandatory. It is also not necessary to synchronize Active Directory with Azure. Bear in mind, though, that SCCM supports this option as well.

Windows Server can be managed, while Intune only supports Windows Client systems.

SCCM can be used to manage systems without Internet connection.

Administrators decide which changes to the SCCM environment are implemented.

Intune

Microsoft launched Intune in 2011. Starting with a very weak feature set, it has since evolved into one of the most important components in the Enterprise & Mobility Suite (EMS). In places, Intune offers the same features as SCCM. Here are a few of them:

- Inventoriy rationalization
- Application distribution
- Distribution of software updates
- Compliance management
- Control of Windows Defender Antivirus
- Reporting

Some may be surprised to note that the provisioning of operating systems is missing from the list. But that is correct. Modern client management uses a different technology called Windows Autopilot. The devices must be registered in Intune, and ideally the hardware distributor will take care of this when ordering new systems. During commissioning, the device is then automatically configured according to the specifications of the IT department and supplied with the required applications. The truly ingenious aspect of this method is that it does not require an admin. The system is simply handed over to the user in its original packaging, because everything will run automatically. Only an Internet connection is required.

Intune and associated services like Windows Autopilot are exclusively cloud-based systems. There is no need to provide an on-premises infrastructure. But they do require an Azure Active Directory. Mostly the data from the local Active Directory is synchronized here. The positive aspect is that users who already run Office 365 today can also benefit from Intune and co. with relatively little effort.

The following describes the strengths of Intune, compared to SCCM:

- Complete MDM solution iPhones and Android devices
- No local infrastructure is needed
- Infrastructure does not require maintenance. Microsoft deals with this because it is a cloud application
- Windows Autopilot
- Extensive integration with other features from the Enterprise & Mobility Suite

I Want It All & I Want It Now

Microsoft also has a solution up its sleeve for anyone keen to benefit from the best of both worlds. Co-management enables synchronous administration by both SCCM and Intune. This requires a Cloud Management Gateway on the SCCM side. The Cloud Management Gateway is a virtual instance within Azure that enables the management of SCCM clients that are not located in the local network. It is necessary to define which management system is in charge of particular areas in order to prevent SCCM and Intune from getting in each other’s due to different configurations.

Summary

As I mentioned in the introduction, a one-size-fits-all solution does not exist. It is vital that you take a good look at the infrastructure you are currently running, but also at the infrastructure you want to operate in the future. Both SCCM and Intune offer many, often overlapping features. So the right choice will always depend on your own strategic approach.

Or

In today’s mobile-first, cloud-first world, every organization needs some mobile device management solution. Depending on business needs, some organizations prefer SaaS Cloud MDM solution whereas some organization needs on-premises customized MDM solution for them. Microsoft has both for its customers: Intune and SCCM. Organizations are often confused on whether to use Microsoft Windows Intune, SCCM or both together known as the Hybrid approach. Microsoft has retired the hybrid MDM service offering from September 01, 2019.

You need to remove the Microsoft Intune subscription from Configuration Manager. Microsoft also wrote a very nice article on it.
In this blog, we'll talk about features of Microsoft Windows Intune and SCCM and their comparison in detail that would help you to choose the best approach that fits your business's cloud computing needs.

Do You Know? 43% Of Breaches Take Place At Small Business

Go Passwordless! The future is here for your Microsoft account, and it no longer requires a password! No more worrying about a breach happening to your business. This Free Inforgraphic will list everything that is potentially at risk and how to protect it.

System Center Configuration Manager

System Center Configuration Manager (SCCM) is a PC and Server Management solution that helps you manage devices. The SCCM integrated console enables the management feature of Microsoft Application Virtualization (App-V), Microsoft Enterprise Desktop Virtualization (Med-V), Citrix XenApp, Microsoft Forefront, and Windows Phone applications from a single.

System Center Configuration Manager Features

Some basic enhancement features of SCCM are as follows: Windows 10 Management
In-Console UpdatesApplication Delivery
Device ManagementVirtual Desktop ManagementEndpoint Protection
Compliance And Settings Management
Power Management
Operating System DeploymentSoftware Update Management
Client Health And Monitoring
Asset Intelligence
InventoryPatch Management
Mobile ManagementVirtual Desktop Infrastructure
Reporting Productivity

Microsoft Windows Intune

Microsoft Intune is solely a cloud technology by Office 365. It is also known as cloud variant of SCCM but it is NOT equivalent to SCCM. As SCCM is a much more powerful tool than Intune as a service for business users. You could always find help to set things up and detailed reporting with help from Intune Consultants.

Microsoft Intune Features

Some basic features of Microsoft Intune are as follows:
Bring Your Own Device (BYOD)Application Level ManagementNo Infrastructure Required Data ProtectionEasy Administration

Microsoft Intune vs SCCM Comparison

There are multiple different ways of managing mobile devices. The device and application Management capabilities often differ depending on the device platform under use for managing functionality-related needs in modern management. For your better understanding of enterprise mobility and security, a basic comparison of the capabilities of Intune and Configuration Manager On-premises is as below for a smoother user experience:

Capabilities	**Microsoft Windows Intune**	**System Center Configuration Manager**
Platform		
Microsoft Windows	Yes	Yes
Microsoft Windows Server	No	Yes
Windows Phone	Yes	Windows 10 only
iOS	Yes	No
Windows RT	Yes	No
Android	Yes	No
Compliance Settings		
Deploy and customize Windows PC device configuration settings (e.g., WMI, registry)	No	Yes
Deploy configuration settings to mobile devices.	Yes	No
Deployment		
Deploy apps to devices and Windows PCs	Yes	Yes
Deploy Windows operating systems	No	Yes
Security and Privacy		
Manage Windows software updates	Yes	Yes

Administration and Reporting		
Monitor and report on how often software is being used with software metering	No	Yes
Hardware and software inventory	Yes	Yes
Use role-based administration and reporting to control who has access to product capabilities	No	Yes
Data Protection for mobile devices		
Deploy security settings to mobile devices	Yes	Yes
Remote lock	Yes	Yes
Company resource access		
Email profiles	Yes	Yes
Mobile application management	Yes	Yes
Manage access to Exchange email and SharePoint with conditional access	Yes	Yes
Managed Internet browser policy	Yes	Yes

9.Explain the functionalities that gets extended from on premise to cloud, in case of Mobility Services.?

When organizations move workloads and data to the cloud, their on-premises datacenters often continue to play an important role. The term *hybrid cloud* refers to a combination of public cloud and on-premises datacenters, to create an integrated IT environment that spans both. Some organizations use hybrid cloud as a path to migrate their entire datacenter to the cloud over time. Other organizations use cloud services to extend their existing on-premises infrastructure.

This article describes some considerations and best practices for managing data in a hybrid cloud solution,

When to use a hybrid solution

Consider using a hybrid solution in the following scenarios:

- As a transition strategy during a longer-term migration to a fully cloud-native solution.
- When regulations or policies do not permit moving specific data or workloads to the cloud.
- For disaster recovery and fault tolerance, by replicating data and services between on-premises and cloud environments.
- To reduce latency between your on-premises datacenter and remote locations, by hosting part of your architecture in Azure.

Challenges

- Creating a consistent environment in terms of security, management, and development, and avoiding duplication of work.
- Creating a reliable, low latency and secure data connection between your on-premises and cloud environments.
- Replicating your data and modifying applications and tools to use the correct data stores within each environment.
- Securing and encrypting data that is hosted in the cloud but accessed from on-premises, or vice versa.

On-premises data stores

On-premises data stores include databases and files. There may be several reasons to keep these data stores local. There may be regulations or policies that do not permit moving specific data or workloads to the cloud. Data sovereignty, privacy, or security concerns may favor on-premises placement. During a migration, you may want to keep some data local to an application that hasn't been migrated yet.

Considerations in placing application data in a public cloud include:

- **Cost**. The cost of storage in Azure can be significantly lower than the cost of maintaining storage with similar characteristics in an on-premises datacenter. Of course, many companies have existing investments in high-end SANs, so these cost advantages may not reach full fruition until existing hardware ages out.
- **Elastic scale**. Planning and managing data capacity growth in an on-premises environment can be challenging, particularly when data growth is difficult to predict. These applications can take advantage of the capacity-on-demand and virtually unlimited storage available in the cloud. This consideration is less relevant for applications that consist of relatively static-sized datasets.

- **Disaster recovery**. Data stored in Azure can be automatically replicated within an Azure region and across geographic regions. In hybrid environments, these same technologies can be used to replicate between on-premises and cloud-based data stores.

Extending data stores to the cloud

There are several options for extending on-premises data stores to the cloud. One option is to have on-premises and cloud replicas. This can help achieve a high level of fault tolerance, but may require making changes to applications to connect to the appropriate data store in the event of a failover.

Another option is to move a portion of the data to cloud storage, while keeping the more current or more highly accessed data on-premises. This method can provide a more cost-effective option for long-term storage, as well as improve data access response times by reducing your operational data set.

A third option is to keep all data on-premises, but use cloud computing to host applications. To do this, you would host your application in the cloud and connect it to your on-premises data store over a secure connection.

Azure Stack

For a complete hybrid cloud solution, consider using Microsoft Azure Stack. Azure Stack is a hybrid cloud platform that lets you provide Azure services from your datacenter. This helps maintain consistency between on-premises and Azure, by using identical tools and requiring no code changes.

The following are some use cases for Azure and Azure Stack:

- **Edge and disconnected solutions**. Address latency and connectivity requirements by processing data locally in Azure Stack and then aggregating in Azure for further analytics, with common application logic across both.
- **Cloud applications that meet varied regulations**. Develop and deploy applications in Azure, with the flexibility to deploy the same applications on-premises on Azure Stack to meet regulatory or policy requirements.
- **Cloud application model on-premises**. Use Azure to update and extend existing applications or build new ones. Use consistent DevOps processes across Azure in the cloud and Azure Stack on-premises.

SQL Server data stores

If you are running SQL Server on-premises, you can use Microsoft Azure Blob Storage service for backup and restore. For more information, see SQL Server Backup and Restore with Microsoft Azure Blob Storage Service. This capability gives you limitless offsite storage, and the ability to share the same backups between SQL Server running on-premises and SQL Server running in a virtual machine in Azure.

Azure SQL Database is a managed relational database-as-a service. Because Azure SQL Database uses the Microsoft SQL Server Engine, applications can access data in the same way with both technologies. Azure SQL Database can also be combined with SQL Server in useful ways. For example, the SQL Server Stretch Database feature lets an application access what looks like a single table in a SQL Server database while some or all rows of that table might be stored in Azure SQL Database. This technology automatically moves data that's not accessed for a defined period of time to the cloud. Applications reading this data are unaware that any data has been moved to the cloud.

Maintaining data stores on-premises and in the cloud can be challenging when you desire to keep the data synchronized. You can address this with SQL Data Sync, a service built on Azure SQL Database that lets you synchronize the data you select, bi-directionally across multiple Azure SQL databases and SQL Server instances. While Data Sync makes it easy to keep your data up-to-date across these various data stores, it should not be used for disaster recovery or for migrating from on-premises SQL Server to Azure SQL Database.

For disaster recovery and business continuity, you can use AlwaysOn Availability Groups to replicate data across two or more instances of SQL Server, some of which can be running on Azure virtual machines in another geographic region.

Network shares and file-based data stores

In a hybrid cloud architecture, it is common for an organization to keep newer files on-premises while archiving older files to the cloud. This is sometimes called file tiering, where there is seamless access to both sets of files, on-premises and cloud-hosted. This approach helps to minimize network bandwidth usage and access times for newer files, which are likely to be accessed the most often. At the same time, you get the benefits of cloud-based storage for archived data.

Organizations may also wish to move their network shares entirely to the cloud. This would be desirable, for example, if the applications that access them are also located in the cloud. This procedure can be done using data orchestration tools.

Azure StorSimple offers the most complete integrated storage solution for managing storage tasks between your on-premises devices and Azure cloud storage. StorSimple is an efficient, cost-effective, and easily manageable storage area network (SAN) solution that eliminates many of the issues and expenses associated with enterprise storage and data protection. It uses the proprietary StorSimple 8000 series device, integrates with cloud services, and provides a set of integrated management tools.

Another way to use on-premises network shares alongside cloud-based file storage is with Azure Files. Azure Files offers fully managed file shares that you can access with the standard Server Message Block (SMB) protocol (sometimes referred to as CIFS). You can mount Azure Files as a file share on your local computer, or use them with existing applications that access local or network share files.

To synchronize file shares in Azure Files with your on-premises Windows Servers, use Azure File Sync. One major benefit of Azure File Sync is the ability to tier files between your on-premises file server and Azure Files. This lets you keep only the newest and most recently accessed files locally.

For more information, see Deciding when to use Azure Blob storage, Azure Files, or Azure Disks.

Hybrid networking

This article focused on hybrid data solutions, but another consideration is how to extend your on-premises network to Azure. For more information about this aspect of hybrid solutions, see:

- Choose a solution for connecting an on-premises network to Azure
- Hybrid network reference architectures

1.How UEM (and Intune) fits into the EMM market.

Microsoft Endpoint Manager is Microsoft's unified endpoint management platform with numerous uses for device management and data security tasks in the cloud and on premises.

MEM contains all the different services and tools that IT can use to manage and monitor endpoint devices such as smartphones, tablets, desktops, laptops, virtual machines and even servers. These different management services and tools combine the strength of existing products, including Microsoft Intune, Configuration Manager, Desktop Analytics, Windows Autopilot, and the other services that were available via the Device Management Admin Console.

The offering is an extremely broad mix of mostly existing Microsoft tools and services, but the rebranding and renaming of these components can confuse Microsoft customers.

What does Microsoft Endpoint Manager include?

Microsoft Endpoint Manager is a rebrand of Microsoft services, which brings these existing products together in a single platform and a single management interface. This admin interface is available via the Microsoft Endpoint Manager admin center, which Microsoft previously provided via the Device Management Admin Console.

In addition to simplifying the admin experience, MEM makes the licensing process easier for customers. For example, a license for Configuration Manager also includes a license for Intune for MEM customers. This simplifies the path for organizations with all types of environments -- on premises, in the cloud or a hybrid model.

Here is a closer look at the products and tools that are part of Microsoft Endpoint Manager.

Microsoft Intune

Microsoft Intune still exists -- both in name and product -- and is now part of MEM. Even as part of Microsoft Endpoint Manager, IT administrators can still use Intune as a separate management platform for mobile device management (MDM) and unified endpoint management (UEM).

IT administrators can manage configurations and verify compliance on Android, iOS, iPadOS, macOS and Windows 10 devices. IT can also configure apps and protect data in apps on Android, iOS, iPadOS and Windows 10 devices based on Windows Information Protection (WIP). Besides these built-in functionalities, Intune also provides many integrations with third-party products and, of course, other Microsoft products. The integrations can go a long way for organizations trying to meet industry compliance standards.

Bottom line: IT can use Intune as a standalone device management and app management platform without using the other products that are part of the MEM offering.

Configuration Manager

Previously known as System Center Configuration Manager, Configuration Manager is now part of Microsoft Endpoint Manager and Microsoft rebranded it to Microsoft Endpoint Configuration Manager. Even as part of Endpoint Manager, IT administrators can use Configuration Manager separate from MEM.

Configuration Manager is Microsoft's on-premises device management platform. IT administrators can use it to manage laptops, desktops and servers for organizations. IT can manage those devices on the intranet and the internet. It enables IT administrators to deploy apps, software updates and OSes. IT can also monitor compliance and query devices, among other tasks. To initiate a cloud migration, IT can attach Configuration Manager to the cloud provider, add more functionalities and move to the single administrative interface in the Microsoft Endpoint Manager admin center.

Desktop Analytics

Microsoft's Desktop Analytics is a cloud-based platform that integrates directly with Configuration Manager to provide information about the update readiness of Windows 10 devices. IT can use this information to identify compatibility issues with apps and drivers and provide insights about security updates, apps and devices within the organization.

Co-management

With the co-management service from Microsoft, IT admins have a bridge from an on-premises environment to a cloud environment. It enables IT administrators to combine Configuration Manager with Intune for Windows 10 endpoint management. With the simplified licensing that comes with Microsoft Endpoint Manager, this doesn't require any additional licenses.

Co-management means that IT manages devices with both Configuration Manager and Intune. That combination enables the patch to the cloud for organizations by switching workloads from Configuration Manager to Intune. Those workloads are simply groups of configuration options that IT switches from one device management product to another.

Windows Autopilot

Windows Autopilot is a cloud-based platform that IT admins can use to configure Windows 10 devices for an out-of-the-box experience for end users. This way, organizations can quickly get devices up and running without manually imaging them.

During that experience, Windows Autopilot takes care of installing apps and applying configurations. Those configurations include options to join the devices to Azure Active Directory (Azure AD) and automatically enroll the devices to Intune or Configuration Manager.

One of the most important configurations that IT will need to set via Windows Autopilot is the end-user device's account type -- standard or administrator.

What happened to Microsoft Intune?

The arrival of Endpoint Manager doesn't affect the position or usage of Intune. Intune is now part of the Endpoint Manager platform, but the standalone product has the same focus. Almost nothing changes for organizations that have deployed Intune before the arrival of Microsoft Endpoint Manager.

The main difference for the Intune administrators is the administrator experience. The IT administrator will now use the Microsoft Endpoint Manager admin center instead of the Device Management Admin Console, the Azure portal or, from even further back, the Silverlight portal. All the different configuration options are still available.

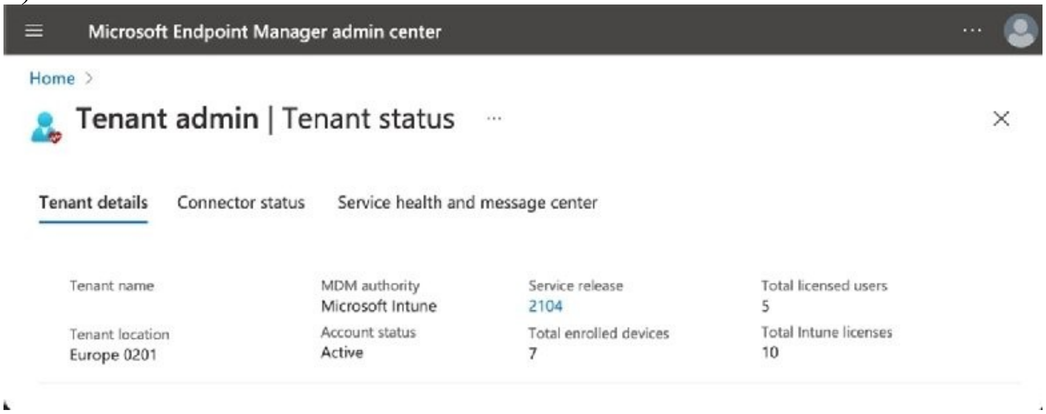
Bottom line: IT can use Intune as a standalone device management and app management platform without using the other products that are part of the MEM offering.

How can IT perform Intune management tasks?

The best thing about MEM for IT administrators is that it brings all of Microsoft's endpoint management tools and services into a single admin console with the Microsoft Endpoint Manager admin center. This offers a unified experience, especially once all the different management features become available via that same single admin console.

When IT administrators use Intune in combination with Configuration Manager, they can also access the information from the Configuration Manager managed devices via that same console. This way, IT can retrieve inventory information and configuration options from those devices through the admin interface.

At this moment, most Configuration Manager-related configuration options only require the Configuration Manager admin console. However, when looking at Intune specifically, all of its management tasks are available via the Microsoft Endpoint Manager admin center. It may be difficult for IT to find evidence of Intune within this console, but Intune is still the designated MDM and mobile application management (MAM) provider. The best place to verify that information is in the **Tenant admin** node under the **Tenant status** option. This will display information referring to Intune with the **MDM authority** and the **Total Intune licenses** (figure 1).



Microsoft Endpoint Manager admin center
Home >
Tenant admin | Tenant status
Tenant details
Connector status
Service health and message center

Tenant name

Tenant location
Europe 0201

MDM authority
Microsoft Intune

Account status
Active

Service release
2104

Total enrolled devices
7

Total licensed users
5

Total Intune licenses
10

PETER VAN DER WOUDE

The tenant status of deployed endpoint devices in the MEM admin center

The main features of Intune focus on device management, app management and reporting, and each of them are critical for IT administrators to know.

Device management

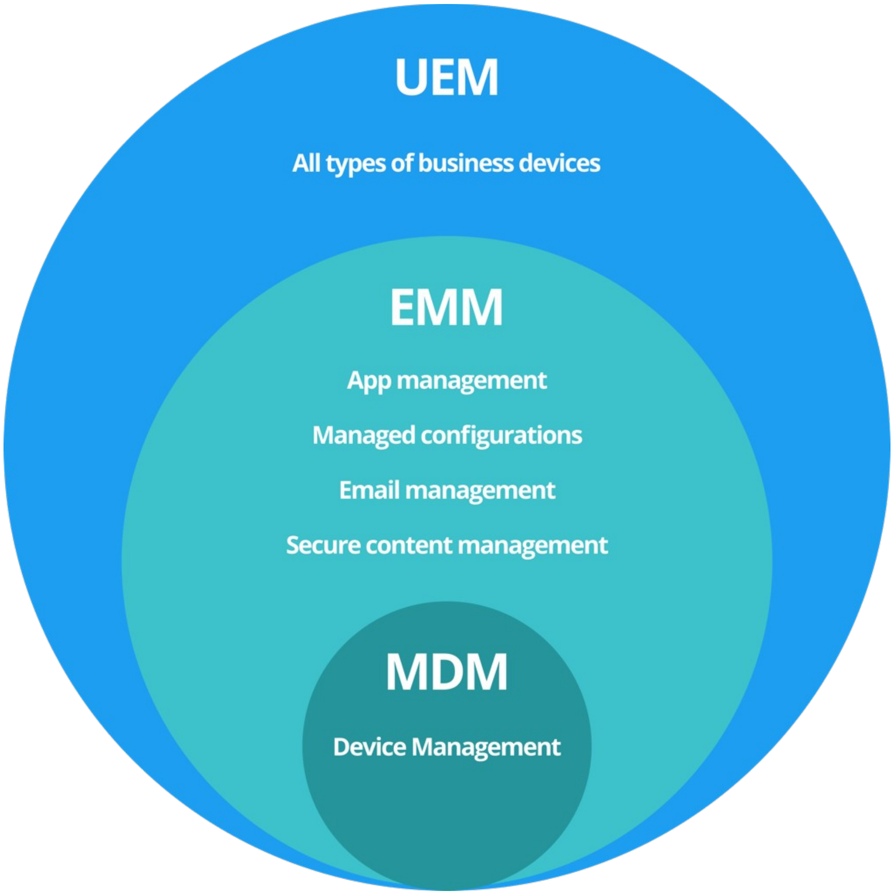
IT can manage devices using the **Devices** node in the Microsoft Endpoint Manager admin center. That node includes configuring devices with restriction profiles, certificate profiles, VPN profiles, Wi-Fi profiles and much more. IT can also use this for device compliance policies that verify the device compared to the compliance baseline of the organization before granting access to company resources and data. The **Endpoint Security** node also contains nearly all security-related device configuration options. This currently overlaps with many settings that are available in the device restriction profiles as well.

Application management

IT can perform app management using the **Apps** node in the Microsoft Endpoint Manager admin center. From this node, IT can deploy, configure and protect apps. More specifically, IT can deploy company-specific apps to managed devices and to control apps on company and personal devices. That includes both managed and unmanaged devices. In the latter case, only the app is managed based on the identity of the user. That identity must exist in Azure AD.

Reporting

MEM's reporting information is available via the **Reports** node in the admin center. IT can use this node to retrieve information about device compliance, updates, endpoint security and endpoint analytics. The latter is a very helpful Intune feature that provides insights into the device's performance and the app's performance on those devices. Besides that, the different nodes for **Devices** and **Apps** also contain the subnode **Monitor** for configuration and compliance information of the different policies and the status information for the app deployments.



2.Explain all the given Management operation

Device

Mobile

Email

BYOD (Bring Your Own Device)

What is mobile device management?

Mobile device management is the process of securing, monitoring and supporting the use of mobile devices, such as smartphones and tablets, in the workplace. The function of MDM is to control data, configuration settings and applications on all mobile devices used within a company or organization.

Businesses use third-party software to implement MDM. By regulating and securing the configuration settings and data for all mobile devices in a network, MDM reduces security risks and associated costs. These solutions form a core component of a company's enterprise mobility management — the set of processes, people and technology that control mobile devices, computers and wireless networks.

Related: How Employers Enforce Cell Phone Policies in the Workplace

An increasing number of employers are giving their employees a company device. Some companies are implementing bring your own device (BYOD) policies to save on costs. These policies allow employees to use their personal devices to access company resources such as email, calendars and contacts. BYOD policies increase productivity and flexibility while reducing costs. To prevent any security risks, MDM is essential for any workplace that uses BYOD policies.

Why is mobile device management important?

MDM allows employees to use company or personal devices to complete work while staying secure. These devices are essential to workplace productivity, so IT departments need to manage them, especially when issues arise, like viruses or malware. MDM can also give an IT department the ability to wipe your device completely if it is lost or stolen, then set up a new device from a company backup.

How mobile device management works

MDM solutions use various combinations of corporate policies, software, infrastructure and device applications to manage all devices on a network. These solutions work even if mobile devices have different service providers or operating systems.

Mobile device management systems usually include two components:

- **Server component:** This part includes a centralized system that sends out commands to all devices on the server. Some solutions implement an over-the-air system to send out commands remotely.
- **Client component:** This is the part the user sees. This component receives commands from the server and implements them. Data from clients is sent back to the server component.

To initialize mobile device management, an application is installed on the smartphone or other mobile device. This gives an IT department the ability to monitor and control activity. Simple mobile device management can allow an IT department to lock a device remotely, monitor internet activity or unlock a device. These services can also prevent you from downloading certain applications or visiting unauthorized websites on a work device. Your employer may prohibit you from using a work device for personal use.

Advantages of mobile device management

Some of the benefits of MDM include:

Support for BYOD policies

BYOD policies increase employee productivity and make for a flexible environment. Employees are easily able to access company emails, calendars and other resources from their own devices. Additionally, the company does not need to provide employees with a device, reducing costs. A thorough MDM policy reduces the risks associated with BYOD.

Application management

MDM services allow companies to regulate and control the applications used for work processes. Centralized control processes install specific applications for each employee. For example, businesses can provide a salesperson with applications that are different from an office assistant's applications.

Remote control

IT departments can monitor the security of devices at all times with remote control. If needed, they can prohibit unauthorized access to company data instantly.

Orderly software updates

It is essential to make sure that all systems are up to date for security purposes. MDM solutions allow companies to update all devices in a coordinated manner.

Data backup

Devices with MDM software automatically back up data based on company policy. For example, an employer could request backups daily or weekly. This allows you to access your information from any device when you need it. It also helps you save your data if any of your devices are lost or stolen.

Different profiles

More complex MDM solutions can split your personal mobile device into work and personal sections, meaning you can switch in between different profiles. The MDM monitors your work programs but not your personal apps.

Increased productivity

Whether you participate in BYOD or use a company-issued device, you'll likely have more access to company resources. Having a device near you can make it easier to respond to emails or complete other tasks quickly.

Related: How To Get Motivated at Work

How does mobile device management affect you?

Your company's use of MDM can affect you in the following ways:

Signing agreements

You need to be aware of your company's MDM policies since you usually need to sign an agreement before receiving a device or participating in BYOD. Read any forms or policies carefully and ask your manager or IT department any questions you have.

Privacy issues

In some cases, if you agree to a BYOD policy, it means that the employer could have access to all of the data on that device. Read what kinds of information the employer can access and how they may monitor your activity. If it's an option, create a separate work profile on your device so employers only track that profile.

You could also see if getting a company-issued device is possible to prevent any privacy concerns. Having a company device allows you to easily separate your work and personal information. If BYOD is your only option, see if your employer offers reimbursement for part of your data plan, which could be an added financial benefit.

Work-life balance

If you are issued a company device, you can turn it off when you want, which can improve your work-life balance. Read any guidelines about the applications you can download on a company device and websites you can visit, so you know which ones are better reserved for your personal device at home.

MDM

In the early 2000, the use of mobile devices started to increase in businesses. Since then, it has been steadily growing, and mobile devices have become essential tools in today's modern workplaces.

Mobile devices help increase flexibility and productivity, but when unmanaged, they can pose various challenges to organizations. The lack of control and visibility over mobile endpoints and non-standardized ways of managing these devices can cause inefficiencies and security risks.

Mobile Device Management (MDM) is a great way to create the foundation for secure enterprise mobility, and in this article, we cover all the essential things you need to know about MDM:

- What is MDM?
- How does MDM work?
- Benefits
- Most essential MDM features
- Managing different devices
- Use cases
- What is the best MDM software?

What is MDM?

MDM is an abbreviation of Mobile Device Management and refers to the administration of mobile endpoints, such as smartphones, tablets, and laptops, as part of the broader scope of Enterprise Mobility Management (EMM). It is the process of managing the entire lifecycle of mobile devices used in the workplace.

Mobile Device Management is implemented through MDM software with suitable management features for one or more operating systems. With MDM software, companies can monitor, manage, and secure their mobile devices to ensure device performance and the safe use of devices.

MDM, EMM, or UEM?

Today, all three terms, MDM, EMM, and UEM, are used when talking about mobile device management. Thus, getting the hang of the terminology can be difficult.

In early 2000, the use of mobile devices for corporate use started to boom. However, it took about ten years before the first mobile device management solutions were launched and Mobile Device Management (MDM) became a commonly used term. Over the years, the management capabilities improved, and companies could manage the entire device lifecycle with a single solution, including device inventory, configuration management, and remote wipe.

Gradually, companies began to have more complex mobility and device management requirements and Enterprise Mobility Management (EMM) emerged as a new industry term.

EMM covers the entire suite of mobility management solutions, including application, content, and identity management, whereas MDM focuses solely on mobile devices and their security. As EMM was explicitly designed for managing the apps and content on mobile devices, it was not suitable for Windows and Mac management. After a while, Unified Endpoint Management (UEM), which combines EMM and PC management into one solution, was born.

Today, all three terms, MDM, EMM, and UEM, are used when talking about mobile device management. Thus, getting the hang of the terminology can be difficult. However, among end-users, MDM is still the most used, even when talking about EMM or UEM solutions, and therefore, we chose to use the term “MDM” in this blog post as well.

How do MDM solutions work?

Mobile Device Management software typically runs either on-premise or in the cloud. Through MDM’s management console, IT admins can remotely configure and manage devices. But before that, devices need to be enrolled in the MDM software, or in other words, the MDM server. This can be done through vendor-specific enrollment programs that Apple, Google, Samsung, and Microsoft offer, or by adding devices manually with a token, QR code, or NFC, or via email/SMS.

IT admins can use the management console to push configurations and applications to mobile devices over the air (OTA). Technically speaking, the MDM server (software) sends out a set of commands that are applied to devices through application programming interfaces (APIs) built in the operating system.

MDM software sends out a set of commands that are applied to devices through application programming interfaces (APIs) built in the operating system.

Some MDM vendors offer both cloud-based Software-as-a-Service (SaaS) and on-premise models. However, SaaS solutions are typically quicker and more cost-efficient to implement as they don’t require additional hardware. Furthermore, on-premise solutions require management, monitoring, maintenance, and updates, which all come included in SaaS solutions.

Benefits of using MDM software

While mobile devices help increase efficiency and flexibility, a large number of devices and their use outside the office can sometimes cause challenges for the IT team — especially when employees are using various operating systems and device models.

No matter what size of the company you have, MDM provides indisputable benefits, including reduced support costs, increased employee productivity, and data security.

Therefore, many organizations rely on MDM tools that bring flexibility to both the IT department and end-users. With MDM, IT admins can securely manage all devices from a single portal, while employees can choose the devices they prefer to use.

No matter what size of the company you have, MDM provides indisputable benefits, including reduced support costs, increased employee productivity, and data security. Here are a few reasons why you should invest in MDM:

1. Control over all corporate mobile devices

When a wide range of devices and operating systems are in use, it can be hard to keep track of them and establish unified device management processes. With MDM, organizations have better visibility over their devices as the software pulls valuable data from managed devices. IT teams know which devices are in use and what's their security level and organizations can more easily manage security risks.

MDM also gives full control over the use of devices and the entire device lifecycle. IT admins can configure devices remotely and handle updates and device replacements on time. And when an employee leaves the company, all business-related information can be wiped from the device, and the device can be assigned to a new employee.

2. Data and device security

Unmanaged mobile devices pose various cybersecurity risks. Whereas PCs and laptops typically have pre-installed malware protection in them, tablets and mobile phones are more vulnerable to cyber-attacks. MDM offers an effective way to safeguard devices and data and stay compliant with prevailing data protection regulations, such as GDPR, HIPAA, ELD, and CJIS.

Data and device security can be ensured with several configurations and restriction options. The use of certain device functionalities or apps can be prohibited, and the use of strong passcodes can be enforced on devices. And in case the same device is used both at work and in the free time, the user's personal data can be separated from work data with secure containers. With these encrypted containers, companies can ensure that sensitive data does not leak to third parties, for example, through instant messaging apps.

3. Increased productivity and lower costs

With MDM, organizations can manage every step of device management efficiently from a single platform and automate device enrollments and configurations, which helps save time and, ultimately, money.

Especially if you're managing multiple devices, automation can bring valuable benefits: human errors decrease, and devices can be setup up to 30 minutes faster. For small and medium-sized organizations, MDM provides a great way to secure devices without huge investments or the need to hire an in-house IT specialist. MDM also makes it easier to allow for BYOD/CYOD policies.

Furthermore, MDM helps increase employee productivity when end-users don't have to waste time setting up devices themselves or visit the IT department. Instead, they get pre-configured devices and access to necessary data and applications from day one.

Most essential MDM features

Features and supported operating systems vary a lot between different MDM tools. Typically, you can view your device inventory, secure devices and data, manage apps and configurations, enforce standardized device policies, and update software remotely. Some solutions even provide identity, access, and expense management.

When choosing an MDM software, it's good to compare different options to make sure that you find the right one for your organization's needs. Here's an overview of the seven most common MDM capabilities:

Device inventory

MDM software collects various hardware and software information on devices, which helps companies monitor and track company-owned and BYOD devices. You can, for example, view ownership information, installed configurations and applications, warranty and security status, and current location, among other data.

Restrictions and configurations

One of the most significant benefits of MDM is the possibility to configure devices remotely. With different configuration and restriction possibilities, organizations can easily ensure data security and compliance and provide employees with the tools they need. MDM makes it possible to install all necessary settings (e.g., VPN, Wi-Fi) to devices and set restrictions for device usage (e.g., Single-App Kiosk mode).

Application and content management

To be productive, employees need to have easy access to the right applications and files. With MDM, companies can manage all mobile content centrally and keep applications updated. Apps can also be whitelisted/blacklisted or removed from the device.

Device and data security

Various security actions can be taken to safeguard both the device and the sensitive data in it. MDM allows companies to, for example, enforce disk encryption and the use of strong passcodes and create secure containers that separate company data from personal data. And in case a device gets lost, it can be tracked and wiped remotely.

Policy enforcement

Unified device policies help companies standardize device management, and ultimately increase efficiency and stay compliant with prevailing regulations. With different policies, companies can pre-determine which configurations, restrictions, and applications should be installed on devices, and mass-deploy these policies to a group of devices.

Automation

When a company is managing multiple devices, automation comes in handy. Most MDM solutions support automated device enrollments through Apple Business Manager / Apple School Manager, Android Zero-Touch Enrollment, or Samsung Knox Mobile Enrollment. And when these built-in programs are connected to a mobile device management software, companies can use MDM to deploy all necessary settings and applications to devices automatically with business policies.

Remote maintenance

With MDM, devices can be updated and serviced remotely, which means that employees don't have to visit the IT department in person. Companies can save a significant amount of time as all software updates and configurations, device diagnostics, and troubleshooting can be done over the air.

Managing different devices with MDM

Mobile device management solutions primarily support the management of smartphones and tablets. You can also find solutions that enable you to manage laptops, desktops, and other devices, such as printers and POS devices, from the same portal.

Supported operating systems vary between MDM solutions. Some vendors specialize in Apple or Android devices, while some support a more diverse mix of devices and operating systems, including Windows, Chromebook, and Linux.

Solutions that offer multi-platform support are often referred to as EMM or UEM. They're a great option if you want to manage all your devices centrally without having to depend on multiple systems.

Regardless of the mobile device management software you choose, device manufacturers have their own special device enrollment and management programs that you can connect to your MDM software. Here's a summary of the programs that Apple, Android, and Windows offer:

iPhone, iPad, and Mac management

Whether you're managing iOS, iPadOS, and macOS devices, you will come across Apple Business Manager and Apple School Manager that include Device Enrollment (formerly known as DEP) and Volume Purchase Program (VPP). Apple Business/School Manager is Apple's web portal, where IT admins can enroll their Apple devices and manage applications and licenses through VPP.

Android device management

To automate the enrollment of Android smartphones and tablets, you can utilize Android Zero Touch and Samsung Knox Mobile Enrollment (for Samsung devices) that are both built-in device management platforms. For managing software licenses and app installations, organizations can use the Managed Google Play Store.

Windows device management

Azure Active Directory is Microsoft's identity and access management platform, which organizations can use to provide their employees with seamless access to all necessary apps. It can also be used for automating Windows device enrollments by connecting Azure AD to an MDM software and adding Azure AD workplace accounts to managed devices.

MDM use cases

Using mobile devices in an office environment is just one example of their diverse use. Today, mobile devices are often used as point-of-sale (POS) terminals and info screens, and they have also become invaluable tools in telemedicine, logistics, and education. Here are some examples of how Mobile Device Management benefits various industries.

Healthcare and telemedicine

A surge in-home health aides and remote patient monitoring has fueled the need for reliable, secure mobile device management. As mobile devices are often used for storing and handling highly sensitive patient data, MDM helps healthcare organizations secure their devices and data and comply with industry regulations, like HIPAA. MDM also makes it easier to take devices into use and configure them according to company policies.

Transportation and logistics

Smartphones and tablets assist in various tasks throughout the entire supply chain: accessing custom applications, scanning bar codes, locating deliveries, sending notifications, and making quality controls. With MDM, transportation and logistics companies can enroll devices in minutes and ensure that they are always functioning correctly. And when there's a need to restrict device functionalities, devices can be turned into Single App Kiosk mode. MDM also helps in becoming compliant with regulations, such as the U.S. congressionally mandated electronic logging device (ELD) rule.

Education

Schools and other educational institutions are gradually adopting tablet-based teaching methods to facilitate teaching and learning. Tablets and laptops need to be correctly configured and have all the essential apps installed before they can be used in teaching. With Mobile Device Management, IT can configure the entire device fleet remotely and set restrictions for device usage, such as blacklist harmful applications or block access to specific websites. Some MDM vendors also offer flexible licensing, which makes those solutions suitable for every budget.

Retail and service industry

Mobile devices are widely used in the retail and service industry. They serve as point-of-sale (POS) terminals, info screens, and self-service checkouts. And in restaurants, tablets can be used for ordering food or viewing seating charts. When devices have multiple users, their secure use can be ensured by turning them into Single-App Kiosk mode or setting other device restrictions. Devices can also be customized with wallpapers to achieve a consistent brand experience.

Government

Governments must often comply with even stricter security standards than big corporations and securing devices and sensitive data is paramount. MDM helps public-sector organizations comply with regulations and increase operational efficiency with automation tools.

MDM for small business

Cloud-based MDM tools are excellent options for small and medium-sized businesses (SMBs). They help SMBs to track their device fleet and manage devices remotely without the need to hire an in-house IT specialist. Being able to administer devices through a single portal increases efficiency and makes it easier to manage security risks.

Managed Service Providers

Mobile Device Management helps Managed Service Providers (MSPs) establish automated, secure, and legislation-compliant processes that enable seamless IT service. In one centralized MDM portal, IT service providers can view all their customers' devices and manage them proactively. To customers, this means, among other things, faster device setups and less time spent on the phone with IT.

What is the best MDM software for you?

The number of devices, and the way they are used, set requirements for device management software. Even though some MDM tools have gained popularity, there is no single solution that perfectly fits every organization. To help you choose the right software for your company, use the checklist below, and take your time to compare different platforms.

1. Supported operating systems

The most important thing when choosing an MDM software is to ensure that it supports the devices and operating systems used in your organization. Some solutions only support a specific operating system, while others enable the management of multiple OSs. With multi-platform support, businesses can manage all their devices with the same software, and employees can more freely choose the device they want to use.

2. Feature requirements

Companies who are looking for their first MDM software typically want a simple device inventory to keep track of their devices. Additionally, basic configuration and restriction capabilities, such as email account and Wi-Fi/VPN settings, and passcode and drive encryption enforcement, are essential. Device enrollment automation and remote software updates typically become necessary as the number of manageable devices grows. Compare different vendors and supported features for each OS to find the right one for your needs.

3. On-premise or cloud

Most MDM solutions are cloud-based, and you can get started smoothly without investing in additional hardware. Cloud-based solutions also provide scalability, which means that you can enroll more devices as your business grows and upgrade your plan to take additional features into use. However, if your company prefers to run the MDM system in your own data center, which is sometimes the case in highly regulated industries, there are on-premise and hybrid solutions available.

In most cases, cloud-based MDM is an excellent option as on-premise solutions require a dedicated person who takes care of its implementation, monitoring, maintenance, and updates. Moreover, they might not always be as scalable as SaaS solutions.

4. Usability

If you are new to device management, choosing a solution with a user-friendly user interface facilitates its adoption. If there are multiple features that you don’t need, a large number of options can be confusing and affect usability negatively. There are many review sites, such as G2 or Capterra, that you can browse to see how others rate different MDM tools and their user experience.

5. Budget

Budget is typically one of the biggest factors when choosing an MDM software. Luckily, you can find MDM vendors that offer great features at an affordable price and different plan options that enable you to scale up and down when needed. The most expensive option is not always the best one for your organization’s needs, but if you require highly specific features, you might want to consider the biggest players in the market.

Some of the better-known MDM solutions

- Miradore
- Addigy (Apple only)
- Citrix Endpoint Management

- Cisco Meraki
- Hexnode
- IBM MaaS360
- Jamf Pro (Apple only)
- ManageEngine
- Microsoft Intune
- MobileIron
- Quest KACE
- Scalefusion (formerly known as MobiLock)
- SimpleMDM (Apple only)
- Sophos Mobile
- SOTI MobiControl
- VMware Workspace ONE (formerly known as AirWatch)

How can Miradore help?

Miradore is a cloud-based MDM/UEM software that makes it easy to manage a diverse mix of Android, Windows, iOS, and macOS devices, even if you're new to MDM. You can create a site in minutes and start managing your devices the same day without a lengthy purchase process or the need to install the software on your company's servers. Here are some examples of what you can do with Miradore MDM:

Device and data security

Miradore's features enable you to ensure device and data security easily. You can enforce the use of passcodes, encrypt your devices, and create a secure container for work data. And in case a device gets lost, you can lock and wipe it remotely.

Device settings and restrictions

Managing device settings and restrictions is easy with configuration profiles that you can save and deploy to your devices. You can, for example, set devices' Wi-Fi, data roaming, or email settings, and limit the use of specific applications, content, services, and device features.

Application management

Application management enables you to get the right software into the hands of device users. You can deploy, remove, and blacklist/whitelist applications, and manage software licenses.

Dashboard and reports

You can view device-related data easily through Miradore's dashboard and reports. The dashboard gives you a quick overview of all the managed devices, but you can also create custom reports that allow you to dive deeper into specific data.

Automation of manual tasks

You can save time by automating various manual tasks, such as device enrollments and configurations. With Miradore's business policies, you can define which settings and apps should be installed automatically on devices that meet certain conditions.

1. What is MAM?
2. What are the benefits of MAM app protection?

3. What device configurations does MAM support?
4. What are app protection policies?

Adding Office 365 App Protection policies

Policies use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.
2. Go to **Services** > **Microsoft Graph** > **Policies** > **Add**.
3. Complete the **App protection policies** form.Refer to Add Office 365 App Protection policies window for details.
4. In the Compliance Actions section, select a Setting, enter the value, and select an Action. Refer to the App protection policies fields table.
5. Click **+Add** to configure additional compliance actions.
6. Click **Save** to add the policy to the list of DLP policies on the **Policies** table.

Editing Office 365 App Protection policies

Policies use data populated from Azure Active Directory during real-time syncs.

Procedure

1. Log into the Admin Portal.
2. Go to **Services** > **Microsoft Graph** > **Policies**.
3. Click the name of a policy you want to edit.
4. Complete the **App protection policies** form.Refer to Add Office 365 App Protection policies window for details.
5. In the Compliance Actions section, select a Setting, enter the value, and select an Action. Refer to the App protection policies fields table.
6. Click **+Add** to configure additional compliance actions.
7. Click **Save** to save the policy edits.

Managing Office 365 App Protection policies

You can take any of the following actions on each Office 365 App Protection policy:

- Assign User Groups
- Assign Apps
- Delete Policies

Procedure

1. Log into the Admin Portal.
2. Go to **Services** > **Microsoft Graph** > **Policies**.
3. Locate a policy you want to manage and go to the **Actions** column.
4. Assign user groups to the App Protection policy.

- Click the **Assign User Groups** icon.
- Search for user groups.
- Select one or more user groups to add to the policy.
- Click **Save**.

5. Assign Office 365 apps to the app protection policy.

- Click the **Assign Apps** icon.
- Search for apps.

- Select one or more apps to add to the policy.
- Click **Save**.

6. Delete an Office 365 App Protection policy.

- Click the **Delete Policy** icon.
- Click **Yes** to confirm deletion of the policy.

The Office 365 App Protection policies take affect:

- After assigning the policy to a user group.
- A user from the assigned user group logs into an Office 365 app using AAD credentials.

Add Office 365 App Protection policies window

Access this window by logging into the Admin Portal and selecting **Services > Microsoft Graph > Policy** and clicking **Add** or clicking a policy to edit.

The following table summarizes fields and descriptions in the **Add App Policies** window. Also, refer to the App protection policies fields table.

Table 80. App protection policies fields

Fields	**Description**
Name	This required field is the name used to track the Office 365 App Protection policy in Core.
Description	Describes the profile's purpose (optional).
Platform	Select the platform for the Office 365 apps. The options are: **iOS** or **Android**. Some of the other options on this form will change depending on which platform you select. Refer to the relevant platform's Device Management Guide.
Data Relocation	
Prevent Android backups	Choose **Yes** to prevent this app from backing up data to the Android Backup Service Choose **No** to allow this app to back up data. (The default is **Yes**.)
Allow app to transfer data to other apps	Use this option to specify what apps can receive data from this app. The options are listed below. • **Policy managed apps**: Allow transfer only to other policy-managed apps. • **All apps**: Allow transfer to any app (default.) • **None**: Do not allow data transfer to any app, including other policy-managed apps. When any of the above options except *All apps* are selected, the exempted apps are listed to the right of the *Allow app to receive data from other apps* field. Modifying these settings changes how data is

	transferred to other applications.
Allow app to receive data from other apps	Select an option to specify what apps can transfer data to this app. • **Policy managed apps** - Allow app to receive data from only other policy-managed apps. • **All apps** Allow app to receive data from other apps (default.) • **None** - Do not allow app to receive data from any app, including other policy-managed apps.
Prevent "Save As "	Select to disable the use of the Save As (a new document) option in any app that uses this policy. De-select if you want to allow the use of Save As. (Default is unchecked.) Selecting Prevent Save As activates the **Select which storage services corporate data can be saved to field**. The options are: • OneDrive for Business • SharePoint • Local Storage
Restrict cut, copy and paste with other apps	Specifies when cut, copy, and paste actions can be used with this app. The options are listed below. • **Blocked**: Do not allow cut, copy, and paste actions between this app and any other app. • **Policy managed apps**: Allow cut, copy, and paste actions between this app and other policy-managed apps. • **Policy managed with paste in**: Allow cut or copy between this app and other policy-managed apps. Allow data from any app to be pasted into this app. • **Any app**: No restrictions for cut, copy, and paste to and from this app. (This is the default.)
Block screen capture and Android assistant	Check this to block the ability to use screen captures and block Android assistant. Default is allowed.
Encrypt app data	Select to encrypt app data that is associated with an Intune mobile application management policy. Encryption is provided by Microsoft. Data is encrypted synchronously during file I/O operations according to the setting in the mobile application management policy. Managed apps on Android use AES-128

	encryption in CBC mode utilizing the platform cryptography libraries. The encryption method is not FIPS 140-2 certified. SHA-256 encryption is supported as an explicit instruction using the SigAlg parameter and will only work on devices 4.2 and above. Content on the device storage is always encrypted.
Disable app encryption when device encryption is enabled	This field activates when the *Encrypt app data* field is selected. Disables app encryption when the device encryption is enabled . Default is de-selected.
Disable contact sync	When this setting is enabled, users cannot sync contacts to the native address book. Default is un-checked.
Disable printing	Select this to block printing protected data from the app. Default is un-checked.
Restrict web content to display in the Managed Browser	Check this to enforce web links in the app to be opened in the Managed Browser app. Uncheck this to open web links in Chrome. Default is de-selected.
Block third party keyboards	When this setting is enabled, a third-party keyboard cannot be used with protected apps.
Access	
Require PIN for access	Select this to require users to enter a PIN to access this app. The user is prompted to set up this PIN the first time the app is run. Default is selected, which activates all the fields in the Access section of this page.
Allow simple PIN	**Allow simple PIN**: Check this to allow users to use simple PIN sequences like 1234 or 1111. Choose No to prevent them from using simple sequences. (The default value is checked.) • **PIN length**: Specify the minimum number of digits in a PIN sequence. (The default value is **4**.) When the *Require PIN for access* field is de-selected, this field is deactivated.
Allow fingerprint of PIN (Android 6.0+)	Select this to allow the user to use Touch ID instead of a PIN for app access. (The default is checked.) When the *Require PIN for access* field is de-selected, this field is deactivated.

Override fingerprint with PIN after timeout (minutes)	If required, depending on the timeout (minutes of inactivity), a PIN prompt will override Touch ID prompts. If this timeout value is not met, the Touch ID prompt will continue to show. This timeout value specified under "Recheck the access requirements after (minutes of Activity)". On iOS, this feature requires the app to have Intune SDK version 8.1.1 or above. **Inactivity timeout**: Specify a time in minutes after which the PIN will override the use of a fingerprint. When the *Require PIN for access* field is de-selected, this field is deactivated.
Disable app PIN when device PIN is managed	Select to disable the app PIN when a device lock is detected on an enrolled device. If you select this option, it overrides the requirements for PIN or Touch ID. (The default is unchecked.) When the *Require PIN for access* field is de-selected, this field is deactivated.
Require corporate credentials for access	Select to require corporate credentials instead of a PIN for app access. Not selecting this option overrides the requirements for PIN or Touch ID. The user will be prompted to provide their corporate credentials. (The default is unchecked.)
Recheck the access requirements after (minutes)	Timeout for access requirements is measured in terms of the time of inactivity between any policy-managed application. • **Timeout**: Enter the number of minutes before the access requirements (defined earlier in the policy) are rechecked. For example, an administrator turns on PIN in the policy, which means a when device user opens a app, a PIN must be entered. When using the Recheck the access requirements setting, the device user would not have to re-enter the PIN on any app for another 30 minutes. (The default is 30.)

Compliance Actions

Use the Compliance Actions Settings to set the security requirements for your access protection policy. Several settings are provided with pre-configured values and actions.

Procedure

1. Select a Setting, enter the value, and select an Action. Refer to the table below.
2. Click **+Add** to configure additional compliance actions.
3. At the top of the Policies tab, click **Save**.

Table 81. Compliance Action Settings

Setting	Description
Max PIN attempts (default)	Specify the number of tries the device user has to successfully enter the correct PIN before the configured action is taken. (Default value is 30 minutes.) Actions include: • **Reset PIN** - The user must reset their PIN. • **Wipe data** - The user account that is associated with the application is wiped from the device.
Offline grace period (default)	This is the number of minutes that apps can run offline. Specify the time (in minutes) before the access requirements for the app are rechecked. After this period is expired, the app will **Block Access**. The default is 720 minutes (12 hours.)
Offline grace period (default)	This is the number of minutes that apps can run offline. Specify the time (in days) before the access requirements for the app are rechecked. After this period is expired, the app will **Wipe data**. The default is 90 days.
Jailbroken/rooted device	• **Block access** - Prevent this app from running on jailbroken or rooted devices. The device user continues to be able to use this app for personal tasks, but will have to use a different device to access data in this app. • **Wipe data** - The device user account that is associated with the application is wiped from the device
Min OS version	Select this to require a minimum operating system to use this app. Enter the value in the following format [major].[minor] and select one of the following actions: • **Block access** - The device user will be blocked from access if the version on the device does not meet the requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device. • **Warn** - The user will see a notification if the operating system version on the

	device does not meet the requirement. This notification can be dismissed.
Min App version	Check this option to require a minimum app version to use the app. The user will be blocked from access if the app version on the device does not meet the requirement. • **Block access** - The device user will be blocked from access if the app version on the device does not meet this requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device. • **Warn** - The user will see a notification if the app version on the device does not meet the requirement. This notification can be dismissed.
Min Patch version	Select to require devices have a minimum Android security patch released by Google. Click the calendar icon to select the date for the action below to occur: • **Block access** - The device user will be blocked from access if the Android version on the device does not meet this requirement. • **Wipe data** - The device user account that is associated with the application is wiped from the device. • **Warn** - The user will see a notification if the Android version on the device does not meet the requirement. This notification can be dismissed.
Device manufacturer(s)	Specify a device manufacturer that is required to use this app. Actions include: • **Block access** - Only devices that match the specified manufacturer can use the app. All other devices are blocked. • **Wipe data** - The user account that is associated with the application is wiped from the device.

1. What are examples of app protection policies?

- Data relocation policies like Save copies of org data, and Restrict cut, copy, and paste.
- Access policy settings like Require simple PIN for access, and Block managed apps from running on jailbroken or rooted devices.

1. Which apps can be managed by app protection policies?
https://docs.microsoft.com/en-us/mem/intune/apps/apps-supported-intune-apps

——————————————————————INTUNE Microsoft Site Questions

What is MAM?

Intune mobile application management refers to the suite of Intune management features that lets you publish, push, configure, secure, monitor, and update mobile apps for your users.

What are the benefits of MAM app protection?

MAM protects an organization's data within an application. With MAM without enrollment (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any device, including personal devices in bring-your-own-device (BYOD) scenarios. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM. See the official list of Intune-managed apps available for public use.

What device configurations does MAM support?

Intune MAM supports two configurations:

- **Intune MDM + MAM**: IT administrators can only manage apps using MAM and app protection policies on devices that are enrolled with Intune mobile device management (MDM). To manage apps using MDM + MAM, customers should use the Microsoft Endpoint Manager admin center.
- **MAM without device enrollment**: MAM without device enrollment, or MAM-WE, allows IT administrators to manage apps using MAM and app protection policies on devices not enrolled with Intune MDM. This means apps can be managed by Intune on devices enrolled with third-party EMM providers. To manage apps using MAM-WE, customers should use the Microsoft Endpoint Manager admin center. Also, apps can be managed by Intune on devices enrolled with third-party Enterprise Mobility Management (EMM) providers or not enrolled with an MDM at all.

App protection policies

What are app protection policies?

App protection policies are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app.

What are examples of app protection policies?

See the Android app protection policy settings and iOS/iPadOS app protection policy settings for detailed information on each app protection policy setting.

Is it possible to have both MDM and MAM policies applied to the same user at the same time, for different devices? For example, if a user could be able to access their work resources from their own MAM-enabled machine, but also come to work and use an Intune MDM-managed device. Are there any caveats to this idea?

If you apply a MAM policy to the user without setting the device state, the user will get the MAM policy on both the BYOD device and the Intune-managed device. You can also apply a MAM policy based on the managed state. So when you create an app protection policy, next to Target to all app types, you'd select No. Then do any of the following:

- Apply a less strict MAM policy to Intune managed devices, and apply a more restrictive MAM policy to non MDM-enrolled devices.
- Apply an equally strict MAM policy to Intune managed devices as to 3rd party managed devices.
- Apply a MAM policy to unenrolled devices only.

For more information, see How to monitor app protection policies.

Apps you can manage with app protection policies

Which apps can be managed by app protection policies?

Any app that has been integrated with the Intune App SDK or wrapped by the Intune App Wrapping Tool can be managed using Intune app protection policies. See the official list of Intune-managed apps available for public use.

What are the baseline requirements to use app protection policies on an Intune-managed app?

- The end user must have an Azure Active Directory (Azure AD) account.

See Add users and give administrative permission to Intune to learn how to create Intune users in Azure Active Directory.

- The end user must have a license for Microsoft Intune assigned to their Azure Active Directory account. See Manage Intune licenses to learn how to assign Intune licenses to end users.
- The end user must belong to a security group that is targeted by an app protection policy. The same app protection policy must target the specific app being used. App protection policies can be created and deployed in the Microsoft Endpoint Manager admin center. Security groups can currently be created in the Microsoft 365 admin center.
- The end user must sign into the app using their Azure AD account.

What if I want to enable an app with Intune App Protection but it is not using a supported app development platform?

The Intune SDK development team actively tests and maintains support for apps built with the native Android, iOS/iPadOS (Obj-C, Swift), Xamarin, and Xamarin.Forms platforms. While some customers have had success with Intune SDK integration with other platforms such as React Native and NativeScript, we do not provide explicit guidance or plugins for app developers using anything other than our supported platforms.

Does the Intune APP SDK support Microsoft Authentication Library (MSAL)?

The Intune App SDK can use the Microsoft Authentication Library for its authentication and conditional launch scenarios. It also relies on MSAL to register the user identity with the MAM service for management without device enrollment scenarios.

What are the additional requirements to use the Outlook mobile app?

- The end user must have the Outlook mobile app installed to their device.
- The end user must have a Microsoft 365 Exchange Online mailbox and license linked to their Azure Active Directory account. **Note**The Outlook mobile app currently only supports Intune App Protection for Microsoft Exchange Online and **Exchange Server with hybrid modern authentication** and does not support Exchange in Office 365 Dedicated.

What are the additional requirements to use the Word, Excel, and PowerPoint apps?

- The end user must have a license for Microsoft 365 Apps for business or enterprise linked to their Azure Active Directory account. The subscription must include the Office apps on mobile devices and can include a cloud storage account with OneDrive for Business. Microsoft 365 licenses can be assigned in the Microsoft 365 admin center following these instructions.
- The end user must have a managed location configured using the granular save as functionality under the "Save copies of org data" application protection policy setting. For example, if the managed location is OneDrive, the OneDrive app should be configured in the end user's Word, Excel, or PowerPoint app.

- If the managed location is OneDrive, the app must be targeted by the app protection policy deployed to the end user. **Note**The Office mobile apps currently only support SharePoint Online and not SharePoint on-premises.

Why is a managed location (i.e. OneDrive) needed for Office?

Intune marks all data in the app as either "corporate" or "personal." Data is considered "corporate" when it originates from a business location. For the Office apps, Intune considers the following as business locations: email (Exchange) or cloud storage (OneDrive app with a OneDrive for Business account).

What are the additional requirements to use Skype for Business?

See Skype for Business license requirements. For Skype for Business (SfB) hybrid and on-prem configurations, see Hybrid Modern Auth for SfB and Exchange goes GA and Modern Auth for SfB OnPrem with Azure AD, respectively.

App protection features

What is multi-identity support?

Multi-identity support is the ability for the Intune App SDK to only apply app protection policies to the work or school account signed into the app. If a personal account is signed into the app, the data is untouched.

What is the purpose of multi-identity support?

Multi-identity support allows apps with both "corporate" and consumer audiences (i.e. the Office apps) to be released publicly with Intune app protection capabilities for the "corporate" accounts.

What about Outlook and multi-identity?

Because Outlook has a combined email view of both personal and "corporate" emails, the Outlook app prompts for the Intune PIN on launch.

What is the Intune app PIN?

The Personal Identification Number (PIN) is a passcode used to verify that the correct user is accessing the organization's data in an application.

When is the user prompted to enter their PIN?

Intune prompts for the user's app PIN when the user is about to access "corporate" data. In multi-identity apps such as Word/Excel/PowerPoint, the user is prompted for their PIN when they try to open a "corporate" document or file. In single-identity apps, such as line-of-business apps managed using the Intune App Wrapping Tool, the PIN is prompted at launch, because the Intune App SDK knows the user's experience in the app is always "corporate."

How often will the user be prompted for the Intune PIN?

The IT admin can define the Intune app protection policy setting 'Recheck the access requirements after (minutes)' in the Intune admin console. This setting specifies the amount of time before the access requirements are checked on the device, and the application PIN screen is shown again. However, important details about PIN that affect how often the user will be prompted are:

- **The PIN is shared among apps of the same publisher to improve usability:** On iOS/iPadOS, one app PIN is shared amongst all apps **of the same app publisher**. On Android, one app PIN is shared amongst all apps.
- **The 'Recheck the access requirements after (minutes)' behavior after a device reboot:** A "PIN timer" tracks the number of minutes of inactivity that determine when to show the Intune app PIN next. On iOS/iPadOS, the PIN timer is unaffected by device reboot. Thus, device restart has no effect on the number of minutes the user has been inactive from an iOS/iPadOS app with Intune PIN policy. On Android, the PIN timer is reset on device reboot. As such, Android apps with Intune PIN policy will likely prompt for an app PIN regardless of the 'Recheck the access requirements after (minutes)' setting value **after a device reboot**.
- **The rolling nature of the timer associated with the PIN:** Once a PIN is entered to access an app (app A), and the app leaves the foreground (main input focus) on the device, the PIN timer gets reset for that PIN. Any app (app B) that shares this PIN will not prompt the user for PIN entry because the timer has reset. The prompt will show up again once the 'Recheck the access requirements after (minutes)' value is met again.

For iOS/iPadOS devices, even if the PIN is shared between apps from different publishers, the prompt will show up again when the **Recheck the access requirements after (minutes)** value is met again for the app that is not the main input focus. So, for example, a user has app *A* from publisher *X* and app *B* from publisher *Y*, and those two apps share the same PIN. The user is focused on app *A* (foreground), and app *B* is minimized. After the **Recheck the access requirements after (minutes)** value is met and the user switches to app *B*, the PIN would be required.

Note

In order to verify the user's access requirements more often (i.e. PIN prompt), especially for a frequently used app, it is recommended to reduce the value of the 'Recheck the access requirements after (minutes)' setting.

How does the Intune PIN work with built-in app PINs for Outlook and OneDrive?

The Intune PIN works based on an inactivity-based timer (the value of 'Recheck the access requirements after (minutes)'). As such, Intune PIN prompts show up independently from the built-in app PIN prompts for Outlook and OneDrive which often are tied to app launch by default. If the user receives both PIN prompts at the same time, the expected behavior should be that the Intune PIN takes precedence.

Is the PIN secure?

The PIN serves to allow only the correct user to access their organization's data in the app. Therefore, an end user must sign in with their work or school account before they can set or reset their Intune app PIN. This authentication is handled by Azure Active Directory via secure token exchange and is not transparent to the Intune App SDK. From a security perspective, the best way to protect work or school data is to encrypt it. Encryption is not related to the app PIN but is its own app protection policy.

How does Intune protect the PIN against brute force attacks?

As part of the app PIN policy, the IT administrator can set the maximum number of times a user can try to authenticate their PIN before locking the app. After the number of attempts has been met, the Intune App SDK can wipe the "corporate" data in the app.

Why do I have to set a PIN twice on apps from same publisher?

MAM (on iOS/iPadOS) currently allows application-level PIN with alphanumeric and special characters (called 'passcode') which requires the participation of applications (i.e. WXP, Outlook, Managed Browser, Yammer) to integrate the Intune APP SDK for iOS/iPadOS. Without this, the passcode settings are not properly enforced for the targeted applications. This was a feature released in the Intune SDK for iOS/iPadOS v. 7.1.12.In order to support this feature and ensure backward compatibility with previous versions of the Intune SDK for iOS/iPadOS, all PINs (either numeric or passcode) in 7.1.12+ are handled separately from the numeric PIN in previous versions of the SDK. Therefore, if a device has applications with Intune SDK for iOS/iPadOS versions before 7.1.12 AND after 7.1.12 from the same publisher, they will have to set up two PINs.That being said, the two PINs (for each app) are not related in any way i.e. they must adhere to the app protection policy that's applied to the app. As such, *only* if apps A and B have the same policies applied (with respect to PIN), user may setup the same PIN twice.This behavior is specific to the PIN on iOS/iPadOS applications that are enabled with Intune Mobile App Management. Over time, as applications adopt later versions of the Intune SDK for iOS/iPadOS, having to set a PIN twice on apps from the same publisher becomes less of an issue. Please see the note below for an example.

Note

For example, if app A is built with a version prior to 7.1.12 and app B is built with a version greater than or equal to 7.1.12 from the same publisher, the end user will need to set up PINs separately for A and B if both are installed on an iOS/iPadOS device.If an app C that has SDK version 7.1.9 is installed on the device, it will share the same PIN as app A.An app D built with 7.1.14 will share the same PIN as app B.If only apps A and C are installed on a device, then one PIN will need to be set. The same applies to if only apps B and D are installed on a device.

What about encryption?

IT administrators can deploy an app protection policy that requires app data to be encrypted. As part of the policy, the IT administrator can also specify when the content is encrypted.

How does Intune encrypt data?

See the Android app protection policy settings and iOS/iPadOS app protection policy settings for detailed information on the encryption app protection policy setting.

What gets encrypted?

Only data marked as "corporate" is encrypted according to the IT administrator's app protection policy. Data is considered "corporate" when it originates from a business location. For the Office apps, Intune considers the following as business locations: email (Exchange) or cloud storage (OneDrive app with a OneDrive for Business account). For line-of-business apps managed by the Intune App Wrapping Tool, all app data is considered "corporate."

How does Intune remotely wipe data?

Intune can wipe app data in three different ways: full device wipe, selective wipe for MDM, and MAM selective wipe. For more information about remote wipe for MDM, see Remove devices by using wipe or retire. For more information about selective wipe using MAM, see the Retire action and How to wipe only corporate data from apps.

What is wipe?

Wipe removes all user data and settings from **the device** by restoring the device to its factory default settings. The device is removed from Intune.

Note

Wipe can only be achieved on devices enrolled with Intune mobile device management (MDM).

What is selective wipe for MDM?

See Remove devices - retire to read about removing company data.

What is selective wipe for MAM?

Selective wipe for MAM simply removes company app data from an app. The request is initiated using the Microsoft Endpoint Manager admin center. To learn how to initiate a wipe request, see How to wipe only corporate data from apps.

How quickly does selective wipe for MAM happen?

If the user is using the app when selective wipe is initiated, the Intune App SDK checks every 30 minutes for a selective wipe request from the Intune MAM service. It also checks for selective wipe when the user launches the app for the first time and signs in with their work or school account.

Why don't On-Premises (on-prem) services work with Intune protected apps?

Intune app protection depends on the identity of the user to be consistent between the application and the Intune App SDK. The only way to guarantee that is through modern authentication. There are scenarios in which apps may work with an on-prem configuration, but they are neither consistent nor guaranteed.

Is there a secure way to open web links from managed apps?

Yes! The IT administrator can deploy and set app protection policy for the Microsoft Edge app. The IT administrator can require all web links in Intune-managed apps to be opened using the Microsoft Edge app.

App experience on Android

Why is the Company Portal app needed for Intune app protection to work on Android devices?

Much of app protection functionality is built into the Company Portal app. Device enrollment is *not required* even though the Company Portal app is always required. For MAM-WE, the end user just needs to have the Company Portal app installed on the device.

How do multiple Intune app protection access settings that are configured to the same set of apps and users work on Android?

Intune app protection policies for access will be applied in a specific order on end user devices as they try to access a targeted app from their corporate account. In general, a block would take precedence, then a dismissible warning. For example, if applicable to the specific user/app, a minimum Android patch version setting that warns a user to take a patch upgrade will be applied after the minimum Android patch version setting that blocks the user from access. So, in the scenario where the IT admin configures the min Android patch version to 2018-03-01 and the min Android patch version (Warning only) to 2018-02-01, while the device trying to access the app was on a patch version 2018-01-01, the end user would be blocked based on the more restrictive setting for min Android patch version that results in blocked access.

When dealing with different types of settings, an app version requirement would take precedence, followed by Android operating system version requirement and Android patch version requirement. Then, any warnings for all types of settings in the same order are checked.

Intune App Protection Policies provide the capability for admins to require end user devices to pass Google's SafetyNet Attestation for Android devices. How often is a new SafetyNet Attestation result sent to the service?

A new Google Play service determination will be reported to the IT admin at an interval determined by the Intune service. How often the service call is made is throttled due to load, thus this value is maintained internally and is not configurable. Any IT admin configured action for the Google SafetyNet Attestation setting will be taken based on the last reported result to the Intune service at the time of conditional launch. If there is no data, access will be allowed depending on no other conditional launch checks failing, and Google Play Service "roundtrip" for determining attestation results will begin in the backend and prompt the user asynchronously if the device has failed. If there is stale data, access will be blocked or allowed depending on the last reported result, and similarly, a Google Play Service "roundtrip" for determining attestation results will begin and prompt the user asynchronously if the device has failed.

Intune App Protection Policies provide the capability for admins to require end user devices to send signals via Google's Verify Apps API for Android devices. How can an end user turn on the app scan so that they are not blocked from access due to this?

The instructions on how to do this vary slightly by device. The general process involves going to the Google Play Store, then clicking on **My apps & games**, clicking on the result of the last app scan which will take you into the Play Protect menu. Ensure the toggle for **Scan device for security threats** is switched to on.

What does Google's SafetyNet Attestation API actually check on Android devices? What is the difference between the configurable values of 'Check basic integrity' and 'Check basic integrity & certified devices'?

Intune leverages Google Play Protect SafetyNet APIs to add to our existing root detection checks for unenrolled devices. Google has developed and maintained this API set for Android apps to adopt if they do not want their apps to run on rooted devices. The Android Pay app has incorporated this, for example. While Google does not share publicly the entirety of the root detection checks that occur, we expect these APIs to detect users who have rooted their devices. These users can then be blocked from accessing, or their corporate accounts wiped from their policy enabled apps. 'Check basic integrity' tells you about the general integrity of the device. Rooted devices, emulators, virtual devices, and devices with signs of tampering fail basic integrity. 'Check basic integrity & certified devices' tells you about the compatibility of the device with Google's services. Only unmodified devices that have been certified by Google can pass this check. Devices that will fail include the following:

- Devices that fail basic integrity
- Devices with an unlocked bootloader
- Devices with a custom system image/ROM
- Devices for which the manufacturer didn't apply for, or pass, Google certification
- Devices with a system image built directly from the Android Open Source Program source files

- Devices with a beta/developer preview system image

See Google's documentation on the SafetyNet Attestation for technical details.

There are two similar checks in the Conditional Launch section when creating an Intune App Protection Policy for Android devices. Should I be requiring the 'SafetyNet device attestation' setting or the 'jailbroken/rooted devices' setting?

Google Play Protect's SafetyNet API checks require the end user being online, atleast for the duration of the time when the "roundtrip" for determining attestation results executes. If end user is offline, IT admin can still expect a result to be enforced from the 'jailbroken/rooted devices' setting. That being said, if the end user has been offline too long, the 'Offline grace period' value comes into play, and all access to work or school data is blocked once that timer value is reached, until network access is available. Turning on both settings allows for a layered approach to keeping end user devices healthy which is important when end users access work or school data on mobile.

The app protection policy settings that leverage Google Play Protect APIs require Google Play Services to function. What if Google Play Services are not allowed in the location where the end user may be?

Both the 'SafetyNet device attestation', and 'Threat scan on apps' settings require Google determined version of Google Play Services to function correctly. Since these are settings that fall in the area of security, the end user will be blocked if they have been targeted with these settings and are not meeting the appropriate version of Google Play Services or have no access to Google Play Services.

App experience on iOS

What happens if I add or remove a fingerprint or face to my device?

Intune app protection policies allow control over app access to only the Intune licensed user. One of the ways to control access to the app is to require either Apple's Touch ID or Face ID on supported devices. Intune implements a behavior where if there is any change to the device's biometric database, Intune prompts the user for a PIN when the next inactivity timeout value is met. Changes to biometric data include the addition or removal of a fingerprint, or face. If the Intune user does not have a PIN set, they are led to set up an Intune PIN.

The intent of this is to continue keeping your organization's data within the app secure and protected at the app level. This feature is only available for iOS/iPadOS, and requires the participation of applications that integrate the Intune APP SDK for iOS/iPadOS, version 9.0.1 or later. Integration of the SDK is necessary so that the behavior can be enforced on the targeted applications. This integration happens on a rolling basis and is dependent on the specific application teams. Some apps that participate include WXP, Outlook, Managed Browser, and Yammer.

I am able to use the iOS share extension to open work or school data in unmanaged apps, even with the data transfer policy set to "managed apps only" or "no apps." Doesn't this leak data?

Intune app protection policy cannot control the iOS share extension without managing the device. Therefore, Intune ***encrypts "corporate" data before it is shared outside the app***. You can validate this by attempting to open the "corporate" file outside of the managed app. The file should be encrypted and unable to be opened outside the managed app.

How do multiple Intune app protection access settings that are configured to the same set of apps and users work on iOS?

Intune app protection policies for access will be applied in a specific order on end user devices as they try to access a targeted app from their corporate account. In general, a wipe would take precedence, followed by a block, then a dismissible warning. For example, if applicable to the specific user/app, a minimum iOS/iPadOS operating system setting that warns a user to update their iOS/iPadOS version will be applied after the minimum iOS/iPadOS operating system setting that blocks the user from access. So, in the scenario where the IT admin configures the min iOS/iPadOS operating system to 11.0.0.0 and the min iOS/iPadOS operating system (Warning only) to 11.1.0.0, while the device trying to access the app was on iOS/iPadOS 10, the end user would be blocked based on the more restrictive setting for min iOS/iPadOS operating system version that results in blocked access.

When dealing with different types of settings, an Intune App SDK version requirement would take precedence, then an app version requirement, followed by the iOS/iPadOS operating system version requirement. Then, any warnings for all types of settings in the same order are checked. We recommend the Intune App SDK version requirement be configured only upon guidance from the Intune product team for essential blocking scenarios.