ENCRYPTION CONSULTING

Microsoft Intune

Introduction

Microsoft Intune is the SaaS solution provided by Microsoft. A cloud-based utility for managing desktop and mobile devices is called Microsoft Intune. This works with Windows 10, Mac OS, iOS, and Android. This cloud solution is used as a modern management tool. It is possible to combine SCCM, Azure AD, and Active Directory with this MDM solution. UWP applications, Security policies, Configuration policies, Wi-Fi profiles, PKI certificates, and other things may all be deployed with this solution. Onboarding of new Hybrid MDM customers has been deprecated.

Microsoft's Intune is an enterprise mobility management (EMM) tool. The EMM provider supports managing mobile services, network configurations, and mobile devices. This solution is nothing but a combination of Device, Application, Information Protection, Endpoint Protection (antivirus software) and Security/Configuration policy management solution (SaaS) facilitated by Microsoft in Cloud.

Additionally, this solution has features called compliance policy which can be integrated with the Azure AD “Conditional Access” policy to restrict access to company resources.

License Requirement

Microsoft Intune is available for different customer needs and organization sizes, from a simple-to-use management experience for schools and small businesses, to more advanced functionality required by enterprise customers. As long as the subscription is active, the majority of licences that contain Microsoft Intune also permit the usage of Microsoft Endpoint Configuration Manager.

Intune is included in the following licenses: -

1. Microsoft 365 E5
2. Microsoft 365 E3
3. Enterprise Mobility + Security E5
4. Enterprise Mobility + Security E3
5. Microsoft 365 Business
6. Microsoft 365 F1

Lifecycle Of Intune

The Microsoft Intune app lifecycle begins when an app is added and progresses through additional phases.

Add: -

To manage and assign apps, you must first add them to Intune as the first step in the app deployment process. While you can work with many different app types, the basic procedures are the same. With Intune you can add different app types, including apps from the store, apps that are built in, and apps on the web.

Deploy: -

After you've uploaded the app to Intune, this process is simple, and once the app has been deployed, you can check the portal's Intune section to see if the deployment was successful. You can also buy app licences in bulk for your business in various app shops, like the Apple and Windows app stores. Intune can synchronize data with these stores so that you can deploy and track license usage for these types of apps right from the Intune administration console.

Configure: -

With the help of Intune, updating apps you've already deployed to a newer version is simple. For some apps, you can also set up additional functions, for instance:

- iOS/iPadOS app configuration policies provide settings that are used when an iOS/iPadOS app is launched.
- Managed browser policies assist you in configuring Microsoft Edge settings, which takes the place of the device's default browser and enables you to limit the websites that your users can access.

Protect: -

You have a lot of options with Intune to help safeguard the data in your apps. The primary techniques are:

- Conditional Access, which controls access to email and other services based on conditions that you specify. Conditions include device types or compliance with a device compliance policy that you deployed.

Key Features & Benefits

Some key features and benefits of Intune include:

- You have the ability to manage people and devices, both those owned by your business and those owned by you individually. Android, Android Open-Source Project (AOSP), iOS/iPadOS, macOS, and Windows client devices are all supported by Microsoft Intune. Utilizing the policies you establish; you can utilise these devices to safely access organisational resources with Intune.

- Intune simplifies app management with a built-in app experience, including app deployment, updates, and removal. You can connect to and distribute apps from your private app stores, enable Microsoft 365 apps, deploy Win32 apps, create app protection policies, and manage access to apps and their data..

- The implementation of policies for apps, security, device configuration, compliance, conditional access, and other areas is automated by Intune. You can distribute the policies to your user groups and device groups once they are ready. The gadgets just require internet access to receive these policies.

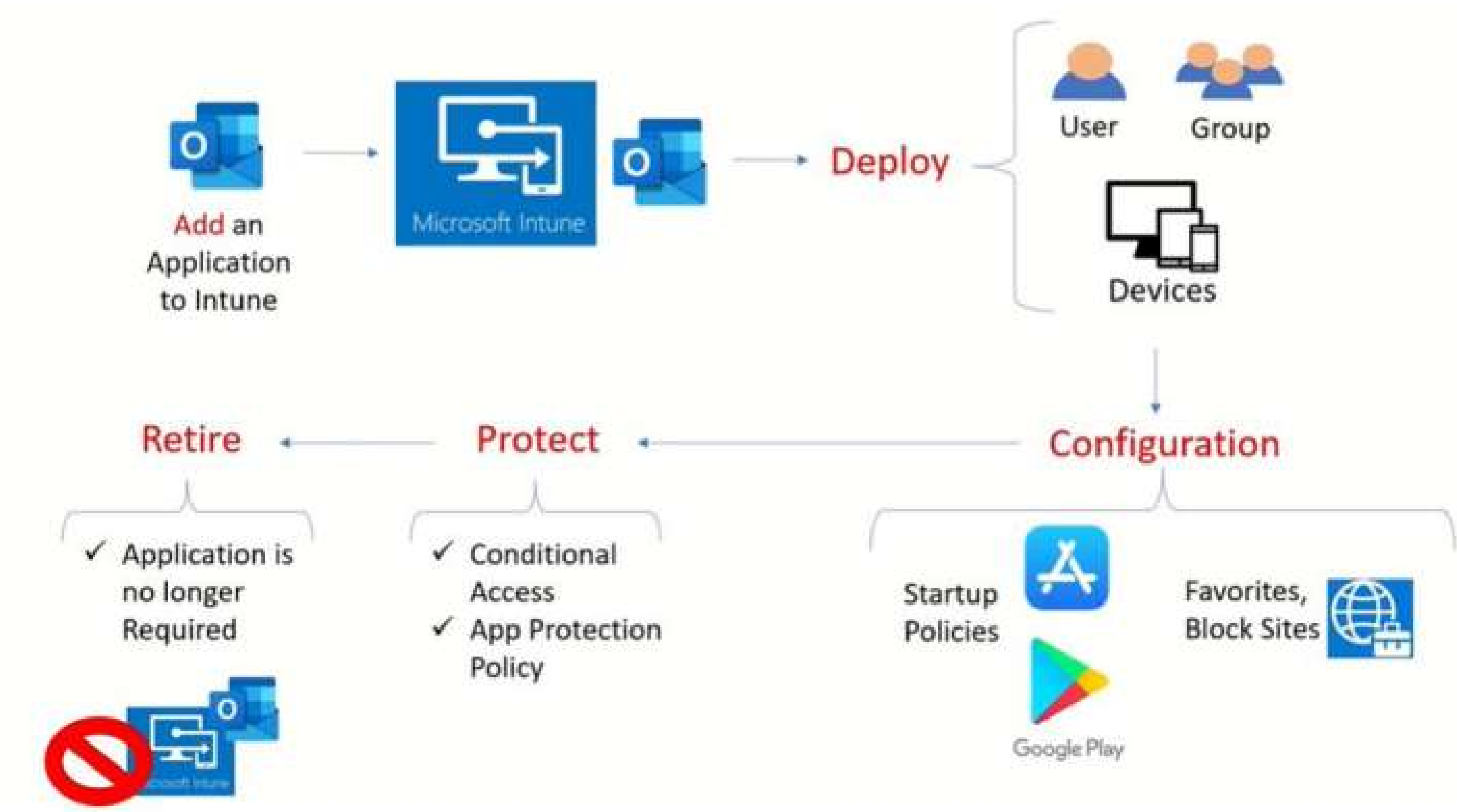
- The self-service features in the Company Portal app allow employees and students to reset a PIN or password, instal apps, join groups, and more. The Company Portal app can be customised to reduce support system calls.

- Intune integrates with mobile threat defense services. With these services, endpoint security is the focus, and you can develop threatresponse policies, perform real-time risk analysis, and automate remediation.

- App protection policies works with individual apps to help protect the company data that they use. For example, you can restrict copying data between unmanaged apps and apps that you manage, or you can prevent apps from running on devices that have been jailbroken or rooted.

Retire: -

It's likely that the apps you installed may eventually become out of date and it needs to be removed. Intune makes it easy to uninstall apps.



Intune App Lifecycle Management

How you can protect app data

Mobile devices are used by your staff for both personal and professional duties. You also want to protect company data that is accessed from devices that are not managed by you. Intune app protection policies can be used without a mobile device management (MDM) programme. With or without enrolling devices in a device management system, this independence helps you protect the data of your business. You can limit access to company resources and keep data under the control of your IT department by setting app-level controls.

Integrating Microsoft Services and Apps:

- **Endpoint Analytics:** Endpoint analytics can be used to find hardware problems or policies that are slowing down devices. Additionally, it offers advice that might proactively enhance end user experiences and reduces help desk requests.

- **Microsoft 365:** End-user productivity with Microsoft 365 includes Outlook, Teams, SharePoint, OneDrive, and other Office applications. You can deploy Microsoft 365 apps to users and devices in your organization. When users log in for the first time, you can also deploy these apps.

- **Windows Autopilot:** For modern OS deployment and provisioning. You can setup new devices with Windows Autopilot and send them from an OEM or device supplier directly to users. You can reimage old devices to instal the most recent version of Windows and enable Windows Autopilot on them.

Simplify Access

Intune helps organizations support employees who can work from anywhere. There are features you can configure that allow users to connect to an organization, wherever they might be. This section includes some common features that you can configure in Intune.

Use Windows Hello for Business instead of passwords:

To defend against phishing scams and other security risks, Windows Hello for Business is used. Additionally, it makes it simpler and faster for consumers to sign into their devices and apps. With the use of PINs or biometrics like fingerprint or face recognition, Windows Hello for Business replaces passwords. The devices themselves keep the biometric data locally; servers or other external devices are never accessed by this data.

Create a VPN connection for remote users:

VPN policies gives users secure remote access to your organization network. You may construct a VPN policy with your network settings using popular VPN connection partners including Check Point, Cisco, Microsoft Tunnel, Net Motion, Pulse Secure, and more. When the policy is prepared, you distribute it to your users and any equipment that needs to connect remotely to your network.

You can use certificates in the VPN policy to verify the VPN connection. Your end users won't have to enter usernames and passwords if you use certificates.

Strategic Technology Partnerships

We work with the industry's best technology providers and have broad experience deploying, managing, and integrating our integrating our solutions with their products and services. We also pride ourselves on our flexibility and are always open to help our clients achieve their data security success with the technology of their choice. If you have products and services already deployed or are considering, we'd be glad to help you evaluate these to get the most out of your investment.

ENTRUST

nCipher Security, a leader in the general purpose hardware security module market, is now an Entrust Datacard company, delivering trust, integrity and control to business critical information and applications.

THALES

Thales-e-Security is a leader in encryption, advanced key management, tokenization, priveleged user control and meets the highest standards of certification for high assurance solutions.

Fortanix

Fortanix is a leader in runtime encryption and it protects applications even when the infrastructure is compromised.

KEYFACTOR

Keyfactor has its roots in the trenches of IT security, deployment and operations. We understand how companies work because of our deep industry experience - we know firsthand the challenges of competing agendas, budget constraints and time pressures.

Microsoft

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington.

MICRO FOCUS

Micro Focus and HPE Software have joined to become one of the largest pure-play software companies in the world.

CRYPTOMATHIC

Cryptomathic is a global provider of secure server solutions to business across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile.

gemalto

For those shaping the digital interactions of tomorrow, we provide the digital security that enables the trusted connections of today.

FORNETIX

Fornetix Key Orchestration TM is a scalable and Aexible solution designed to simpligy key management. Granular ploicy tools, user access controls, and powerful automation enable organizations to manage hundreds of millions of encryption keys while integrating seamlessly with existing technology investments.

appviewX

AppviewX is revolutionizing the manner in which NetOps and SecOps team.

PrimeKey

PrimeKey's technology is used by organizations and enterprses to securely implement PKI solutions used for ePassports, eBanking, ePayment, mobile/Internet security, IoT and more.

UNBOUND

Unbound protects secrets such as cryptographic keys, credentials or private data by ensuring they never exist in complete form.

Venafi

Venafi Cloud helps organizations prevent outages and secure their keys and certificates.

PrimeFactors

Prime Factors software products help business leaders implement and manage enterprise-wide data protection policies to secure sensitive information being used by or stored in virtually any application or system.

utimaco

Utimaco is a leading manufacturer of Hardware Security Modules(HSMs) that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services to the public sector.

PROTEGRITY

The Only Data-First Security Solution. Protect sensitive enterprise data at rest, in motion, and in use with Protegrity's best-in-class data discovery, de-identification and governance capabilities.

comforte

Secure your data, minimise risk, and meet compliance and regulation requirements. Find out more about Comforte's Data Security Services.

Why Encryption Consulting LLC?

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized accees. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security for organizations.

Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates that provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure.

Hardware Security Module - HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.

Certificate Lifecycle Management

Certificates typically have a 4-phase lifecycle -Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases.

Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environment? Do you want to protect data without disruptive changes to applications or business practices?

Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations.

See it in action

Encryption Consulting LLC is a customer-focused cyber security consulting firm providing an array of services in all aspects of data protection.

Contact Us

encryptionconsulting.com

linkedin.com/company/encryptionconsulting

facebook.com/encryptionconsulting

twitter.com/encryptioncons