mobile mentor

Intune Suite - An Introductory Guide

AMPLIFYING EFFICIENCY AND SECURITY WITH THE INTUNE SUITE

CONTENTS

What is Intune Suite?

Endpoint management can be complex and require many different tools with 'swivel-chair' integration. Intune Suite simplifies endpoint management and security by offering a modern integrated approach. It improves security and reduces cost and complexity by consolidating multiple tools. This results in more automation and intelligence for SysAdmins and a better experience for the end users.

Endpoint Privilege Management
Elevating user access privileges as needed

Enterprise App Management
Discovery, packaging, deployment and patching of Windows apps

Advanced Analytics – predict which machines, applications and users will have issues

Cloud PKI – publish and distribute certificates from Intune without complex PKI

Tunnel for MAM – secure access to LOB apps from unmanaged mobile devices

Remote Help – seamless interface between the Service Desk Agent and end user

Endpoint Privilege Management

What is Endpoint Privilege Management?

EPM is designed to elevate user access privileges as needed, effectively controlling application and administrative privileges following the **least privileged access** part of the Zero Trust framework.

Gaining full control of an endpoint is a hacker's dream scenario. By enforcing least privilege access, EPM reduces the ability of an attack to move laterally because all users are configured as **standard users** by default.

Standard user configuration significantly decreases the likelihood of security breaches but it increases friction because certain tasks like installing peripherals, applications, or running Windows diagnostics are restricted. This frustrates users, impacts productivity and increases support costs.

EPM addresses this challenge with easy addition or removal of rules, tenant-level enablement, and automatic, user-confirmed, or support-approved elevation. EPM streamlines IT workflows while enhancing security and providing a modern user experience.

Endpoint Privilege Management

How it works:

1 **Link applications to specific actions through two triggering methods. EPM identifies a process, and users can select "Run Elevated" to trigger elevation.**

2 **Three types of elevation actions are available: Automatic, User-confirmed, and Support-approved.**

- **Automatic** elevation rules are ideal for approved apps that need to elevate to run seamlessly, eliminating user friction.
- **User-confirmed** rules require validation from the user before elevation, providing an additional layer of security.
- **Support-approved** elevation is reserved apps for a trusted by IT, requiring approval from designated personnel for time-based elevation. By leveraging these rule types, you can effectively balance security, user experience, and trust according to specific requirements.

SysAdmins can turn on EPM in reporting mode to see what is happening before deploying in production. Rules can then be defined with child processes, assignment filters and based on Entra ID groups.

Endpoint Privilege Management

Scope and Timing

EPM is available for Windows 10 back as far as 21H2, and Windows 11 from 21H2.
EPM for macOS is coming soon!

How will EPM improve your overall endpoint management strategy?

By enforcing least privilege access, businesses can reduce the risk of local admin accounts. This not only enhances security but also enables businesses to maintain productivity by allowing controlled elevation of privileges when necessary.

Additionally, by monitoring elevations across the businesses, EPM empowers IT administrators with comprehensive visibility and control, ensuring a proactive approach to security management.

Learn more here: Learn about using Endpoint Privilege Management with Microsoft Intune

Enterprise App Management

What is Enterprise App Management?

Enterprise App Management is a comprehensive solution aimed at simplifying and streamlining the process of managing Windows EXE or MSI applications for deployment via Intune.

Traditionally, application packaging has been cumbersome, very time-consuming for SysAdmins, and prone to errors. However, with the introduction of the Enterprise App Catalog, SysAdmins can leverage a set of pre-packaged applications hosted by Microsoft.

This catalog includes both first-party and third-party applications, offering a guided deployment and patching experience for managed applications.

Enterprise App Management

How it works:

The Enterprise App Catalog contains Win32 apps that are prepared and hosted by Microsoft. Microsoft will wrap the installation files (EXE, or MSI) of those apps and create everything that is required to add the app as a Win32 app into Microsoft Intune.

When adding an app from the Enterprise App Catalog to Microsoft Intune, it will be pre-configured with the install and uninstall commands, the installation behavior, the return codes and detection rules. The SysAdmin can also modify these parameters as needed from the installation command line. As these apps are added as Win32 apps, the deployment is handled by the Intune Management Extension and the assignments and supersedence relationships can be created.

The SysAdmin can configure apps in the catalogue to automatically update when an update is detected to be available in the Enterprise App Catalogue. We expect Microsoft to iterate on the update process and provide IT Admin guided updates for non self-updating apps, where an update is available. This obviously works for apps that are enabled to auto-update and for other apps, the Catalogue enables precise version control.

Activate Enterprise App Management

Add Windows Catalog Apps

Assign apps to users/devices

Enterprise App Management

Scope and Timing

The average company has 130 applications and Microsoft is using telemetry across all Intune tenants to identify the most used applications, and then adding approximately 100 new applications to the Enterprise App Catalogue each month. Microsoft also has a priority list of applications based on requests from clients, partners and MSPs.

How will it improve your overall endpoint management strategy?

Enterprise application management reduces the effort required to package, deploy and manage Microsoft and third-party applications, leading to increased efficiency and productivity for IT teams.

You are able to stay current with vulnerability alerts and application patches, ensuring that applications are always up-to-date and secure. By proactively identifying and deploying app fixes to mitigate security risks, Enterprise Application Management helps minimize vulnerabilities and enhance overall security posture.

Microsoft is applying a rigorous testing process before each new application is added to the catalogue so this provides an additional layer of assurance for IT governance.

Learn more here: Microsoft Intune Enterprise Application Management

Microsoft Cloud PKI

What is Microsoft Cloud PKI?

Microsoft Cloud PKI in the Intune Suite is designed to streamline the management of certificate authorities and the lifecycle of certificates.

It enables SysAdmins to create, revoke, and manage certificates using Intune, eliminating the need for costly and complex on-premise PKI infrastructure.

Authentication with certificates offers a secure and seamless experience for users, establishing their identity as trustworthy, enabling them to request signed certificates for authentication purposes.

Microsoft Cloud PKI

How it works:

Deploying Microsoft Cloud PKI in the Intune Suite involves two models, **Greenfield and Brownfield**:

Greenfield: create a net new certificate authority in Intune.

- During the Cloud PKI root CA deployment, the Cloud PKI root certificate must be distributed to all relying parties.
- If an issuing CA certificate is absent on a relying party, it can automatically retrieve and install it through certificate discovery, known as the certificate chaining engine (CCE).
- This process, akin to CRL downloading, ensures the establishment of a trust chain by retrieving missing parent certificates.
- It is important to deploy the Cloud PKI certificate trust chain, comprising root and issuing CA public keys, to all relying parties, ensuring comprehensive coverage and trust across the infrastructure.
- There is a system limitation of 6 Certification Authorities, with a SCEP for each. You can also use RSA key or hash algorithms.

Microsoft Cloud PKI

Brownfield: leverage existing certificate authority and use Intune to issue the certs to devices

- When bring-your-own-CA deployment is initiated, Intune-managed devices are required to possess specific CA certificates.
- These include the private CA trust chain, encompassing root and issuing CA certificates responsible for signing the BYOCA CSR, along with the BYOCA-issuing CA certificate.
- With Cloud PKI BYOCA issuing CA using a private root CA, the trusted chain of private CA certificates, comprising the root CA and issuing CA, should already be deployed across the infrastructure.

Microsoft Cloud PKI

Scope and Timing

The Cloud PKI solution is already fairly mature and Microsoft is issuing thousands of new certificate authorities and tens of thousands of certificates each month.

How will it improve your overall endpoint management strategy?

Cloud PKI allows businesses to manage their cloud certificates alongside their endpoints, facilitating a migration from on-premises to cloud-managed certificates. This transition not only streamlines processes and reduces management costs but also drastically simplifies the delivery and management of certificates while enhancing security without requiring dedicated subject matter experts.

It reduces costs and complexities associated with traditional on-premise PKI solutions, enabling organizations to **deploy certificates in minutes** compared to weeks or months of planning, coordination, procurement, and deployment.

Learn more here: Microsoft Cloud PKI for Microsoft Intune - Microsoft Intune

Microsoft Tunnel for MAM

Tunnel for MAM extends the functionality of the Microsoft Tunnel VPN gateway to Android and iOS devices that are **not enrolled in Intune.**

This extension empowers users to securely access LOB (line of business) applications or data resources from unmanaged personal devices.

This enables employees to use their personal devices for both work and personal purposes without relinquishing management control.

Microsoft Tunnel for MAM

How it works:

1. SysAdmins can set up app configuration policies for Microsoft Edge and Microsoft Defender.

2. For Microsoft Edge, an app configuration policy should be configured to support identity-switch, enabling automatic connection to the VPN Tunnel when signing in or switching to a Microsoft Work or School account, and disconnection when switching to a personal account.

3. For Microsoft Defender, an app configuration policy is required to configure it for use as the tunnel client app on the device.

Configure Tenant
Activate Tunnel for MAM

Configure Apps
Deploy App Config Policy

Enable MAM Tunnel
Deploy App Protection Policy

Microsoft Tunnel for MAM

Scope and Timing

MAM Tunnel is available now for both iOS and Android. For Android the device needs to have the Company Portal app (sign-in not required), Microsoft Edge, and the Defender app installed. For iOS, no Company Portal or Defender for Endpoint app is required.

How will it improve your overall endpoint management strategy?

Tunnel for MAM can be considered part of a zero trust framework, providing secure network access from an unmanaged device.

Together with MAM, the MAM Tunnel provides flexibility for end-users, enabling them to work securely and efficiently without having to enroll their devices in an MDM system.

This facilitates the adoption of bring-your-own-device (BYOD) policies, embracing hybrid work trends without compromising data security.

Learn more here: Learn about using Microsoft Tunnel with Mobile Application Management

Interactive Demo for Android

Interactive Demo for iOS

Advanced Analytics

Advanced Analytics a significant enhancement to the current Endpoint Analytics experience in Intune to provide superior reporting, deeper insights and proactive management capabilities for SysAdmins.

Using Kusto queries and Device Query, SysAdmins can proactively detect and resolve endpoint issues, streamline troubleshooting process, and improve the users' technology experience.

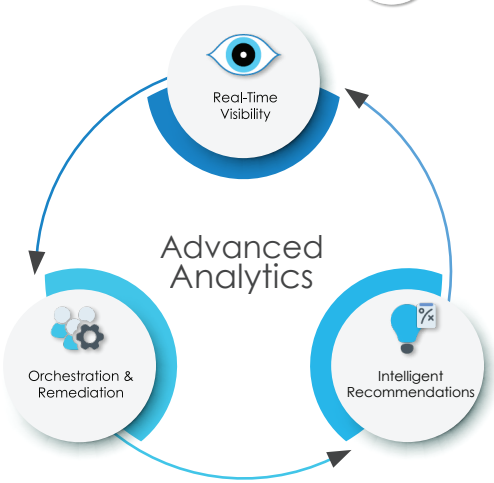
Advanced Analytics

How it works:

Custom Device Scopes allow you to use Scope Tags to slice endpoint reports to a specific subset of devices. You can see scores, insights, and recommendations for specific groups of devices.

For example, you can focus on devices that you manage, devices assigned to a specific business group, or devices located in a particular geographic region.

Anomalies monitor the health of devices in your organization for user experience and productivity regressions following configuration changes.



Enhanced device timeline includes more events and lower data latency to assist with troubleshooting device issues.

Device query enables SysAdmins to get near-real time access to data about the state and configuration of devices.

Battery health provides visibility into hardware performance issues impacting user technology experience.

Advanced Analytics

Scope and Timing

Devices need to be enrolled in Intune or co-managed with SCCM and visible in Endpoint Analytics to use Advanced Analytics. It may take up to 48 hours from license purchase to see Advanced Analytics features in the tenant.

How will it improve your overall endpoint management strategy?

The tool provides offering deeper insights and proactive management capabilities for IT teams. The tool allows administrators to shift their efforts from reactively responding to issues, to **proactively mitigating problems before they occur**. Additionally, there is integrated value (Entra/Conditional Access/Device Compliance) that helps to build trust and mitigate against using Support Methods for phishing attacks.

Microsoft is deploying Copilot capabilities across their entire range of products so it will be exciting to see the evolution from standard Endpoint Analytics to Advanced Analytics to AI-powered analytics.

Learn more here: What is Microsoft Intune Advanced Analytics - Microsoft Intune

Remote Help

The Intune Suite's Remote Help feature is designed to facilitate IT support for workers across various endpoints. It provides a secure platform for help desk agents to connect with users, allowing them to troubleshoot and resolve service issues efficiently.

With features like attended screen sharing, attended control, and unattended control for Android devices, Remote Help enables IT teams to offer timely assistance regardless of the user's location or device enrollment status.

Remote Help

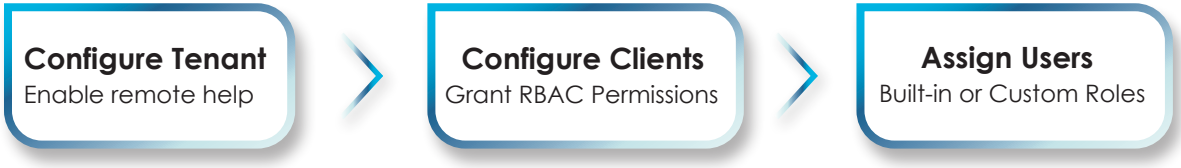
How it works:

Remote Help is a tenant-wide setting and must be enabled before users can be authenticated and supported.

Users can be supported on **both enrolled and unenrolled devices**, but they must be registered in **Entra ID**.The support agent and the end user must be both be signed-in to the same Microsoft tenant.

Remote Help uses Intune role-based access controls **(RBAC)** to set the level of access an agent is allowed. Through RBAC, a SysAdmin determines which agents can provide help, and what level of help they can provide e.g. elevation privileges etc.

Meta data from Remote Help sessions is logged for audit purposes but Microsoft **cannot** access a session or view actions taken during a session.



Remote Help

Scope and Timing

Remote Help is available on Windows 10, Windows 11 (also on ARM 64), Windows 365, Android Enterprise Dedicated (Samsung & Zebra) and macOS 12, 13 and 14. Remote Help is not (yet) available on iOS or iPadOS devices.

How will it improve your overall endpoint management strategy?

Remote Help enhances security by providing a secure platform for remote assistance, aligning with Zero Trust architecture principles and mitigating security risks associated with traditional support methods.

Remote Help in the Intune Suite reduces downtime and improves user satisfaction for workers anywhere, offering a seamless and trusted way to provide employees with the help they need, regardless of their geographical location.

Learn more here: Use Remote Help to assist users authenticated by your organization.

Remote Help Interactive Demo

Benefits of Intune Suite

The result of incorporating the Intune Suite into your endpoint management strategy is three-fold:

1. **Enhanced security** by making standard users the default setting, deploying certificates to all devices and automatically patching 3rd party applications.

2. **Improved user experience** by predicting which machines and users need help, then proactively intervening before the user is impacted, and using Remote Help to reduce downtime.

3. **Reducing costs** by consolidating multiple 3rd party tools, saving time for SysAdmins, and increasing efficiency for Service Desk agents.

Are You Ready?

Enterprises had an average of **80 security tools** in 2023. This fragmented approach is expensive and difficult to manage. Intune Suite provides a great opportunity to consolidate on one integrated platform and reduce the number of discrete tools in the environment.

Businesses can avoid painful data breaches due to inadequate device management, compliance violations resulting in hefty fines, and employee frustration stemming from inefficient workflows. Moreover, businesses can prepare for the future where AI enabled cybercrime is poised to wreak havoc.

Discover if your business qualifies for the Microsoft-Funded Intune Suite Pilot Program. Customers already using Intune may qualify for the Intune Suite Pilot program. Subject to specific criteria from Microsoft which change from time to time, this pilot program includes free trial licenses and assistance from a partner like Mobile Mentor to deploy the Intune Suite in the client's tenant to test and validate each of the features.

Discover if your business qualifies for the Microsoft-Funded Intune Suite Pilot Program.

mobile mentor