

Microsoft Endpoint Manager for Corporate Mobile Devices: Accelerated Deployment

Securely manage corporate mobile devices from anywhere

The digital landscape continues to evolve, and businesses need to adapt and ensure devices can be managed securely.

End users rely on a range of devices to operate seamlessly, achieve mobility and flexibility whilst maintaining productivity. Organisations face the challenge of managing and securing devices whilst ensuring security, data protection and visibility.

Microsoft Endpoint Manager (MEM) directly addresses these challenges, supports iOS, Android and macOS to ensure all devices are fully provisioned, secured and managed. MEM supports integration across operating systems to enable zero-touch cloud provisioning, downloading policies and applications your organisation has implemented within MEM.

Additionally, mobile devices can be managed without enrolment, policies on applications can be enforced on any device ensuring corporate data is safely accessed, whilst planning and implementing a migration strategy to MEM.

By adopting a modern management solution organisations can begin or continue their ongoing journey into a cloud-first ecosystem, alongside a Zero Trust security model.

For more information, please contact us: enquiries@itcsecure.com or 020 7517 3900

SOLUTION OVERVIEW

Typically conducted over a week, ITC Secure will help you with the installation and configuration of Microsoft Endpoint Manager (MEM), identifying through workshops, the key requirements to meet the goals of your business. Our experts will introduce MEM to your environment, working with you to identify key objectives and challenges, providing both a best practice solution for deployment as well as a demonstration of MEM.

This solution will demonstrate business benefits, device management improvements, time, money and resources savings, and how MEM complements other components of the Microsoft 365 security stack.

At the end of the engagement a documented roadmap is provided with details on next steps and continued deployment, so you can make the most of your investments.

KEY FEATURES AND BENEFITS



Organisational Discovery

- Agree current challenges and targets for device management
- Overview of MEM and how it meets the modern workplace challenges
- Outline specific requirements and formulate the optimum deployment plan



Configuring and Testing Device Policies

- Cloud-driven device policies and provisioning through Windows Autopilot
- Baseline device policies for Office apps, OneDrive and drive encryption plus any specific policies detailed during the discovery session



Roadmap for Further Automation

- Documentation on work achieved
- Proposed priorities for any follow-on work
- A key step in the longer cloud-first journey



Accelerated deployment to increase adoption and realise immediately tangible benefits



Pilot managing devices and users within MEM



Deploy Azure AD and hybrid Windows Autopilot with policies



Review and test deploying policies



Review deployment and discuss next steps

WHY ITC

ITC Secure is an advisory-led cyber security services company.

We have a 25+ year track record of delivering business-critical services to over 300 blue-chip organisations - bringing together the best minds in security, a relentless focus on customer service and advanced technological expertise to help businesses succeed.

With our integrated delivery model, proprietary platform and customer-first mindset, we work as an extension of your team throughout your cyber journey and always think not only about you, but also your customers and the reputation of your brand.

ITC Secure is headquartered in London, UK. With a dynamic balance of the best in people, technology and governance, we make cyber resilience your competitive advantage.

Gold
Microsoft Partner



Member of
Microsoft Intelligent
Security Association



For more information, please contact us: enquiries@itcsecure.com or 020 7517 3900