Microsoft Azure - Starter Kits for Partners

Introduction to Starter Kits

Enterprise Mobility

Last Update: April 2016





**MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.**

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2015 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

|  |
| --- |
| Enterprise Mobility Suite |
| WHAT IS IT |
| The **Microsoft Enterprise Mobility Suite (EMS)** helps give users a more secure and integrated productivity experience with Microsoft’s enterprise mobility solutions. Users can work anywhere, on any device, with easy and complete access to the apps—like Microsoft Office 365—and the data they need to be productive. Deliver all of this while giving IT peace of mind with tools that help secure company data. These tools also include integrated ways to manage the mobile workforce for user identity, devices, applications, and data. |
| VALUE PROPOSITION |
| |  | | --- | | Today’s workforce is highly mobile and business is conducted from almost anywhere, at any time. For businesses to be competitive, they need their employees to be productive on-the-go while keeping company data secure.  **Deep Microsoft Office integration**  Protecting email and other corporate collaboration data on mobile devices—without slowing down workers—is one of today’s biggest IT challenges. Other vendors address the problem with apps that compromise user experience and slow down productivity.  Microsoft enterprise mobility solutions integrate seamlessly with Microsoft Office, the gold standard of productivity on both mobile devices and PCs. Microsoft provides the only solution that can natively manage the Microsoft Office mobile apps to ensure that company data stays in company apps and not in personal apps to help give users rich productivity without compromising security.  **Flexibility of the cloud**  Architecture matters. That is why Microsoft’s enterprise mobility management solutions are designed to run in the cloud as enterprise-grade cloud services. These cloud services can also work seamlessly with existing on-premises infrastructures so that users can maximize their existing investments in the Active Directory directory service and the Microsoft System Center family of system management products.  Microsoft services are always up-to-date so that users do not have to manage patches or updates to more on-premises infrastructure. Additionally, with the rapid release schedule of Microsoft cloud services, users can take advantage of new trends and support the latest devices as soon as they are available. In short, Microsoft’s cloud-first approach to managing a mobile enterprise is one of the fastest, most cost-effective ways to meet new business challenges and accommodate new devices, new apps, and new hires—without worrying about scale, maintenance, or updates.  **Enterprise-grade security**  Only Microsoft offers enterprise-grade cloud identity and access management solutions designed to help secure the IT environment. Microsoft Azure Active Directory has hundreds of millions of users, is available in 35 data centers worldwide, and has processed more than **one trillion** authentications. Microsoft translates this scale into security insights by giving users advanced security reports showing the anomalous logon activity to the cloud directory.  In addition, the on-premises capabilities in Microsoft Advanced Threat Analytics (ATA) help protect an organization from advanced targeted attacks by user and entity behavioral analytics (UEBA). ATA also helps to identify known malware (malicious software) attacks, security issues, and risks using world-class security researchers’ work regionally and globally. Using behavioral analytics, ATA can help enterprises quickly focus on what is important and identify security breaches before they cause damage.  **C value**  Microsoft has the only enterprise mobility solution designed to help manage and protect users, devices, apps (PC or mobile), and data.  Microsoft not only provides the most comprehensive solution, it also offers a great value: The Microsoft Enterprise Mobility Suite is 58 percent less than stand-alone products from other vendors.  **Broad Gartner Magic Quadrant Coverage**  Microsoft is currently one of the only vendors featured in Gartner’s Magic Quadrants for Enterprise Mobility Suites, Identity and Access Management as a Service, and Client Management Tools validation. Microsoft provides a combined solution that empowers companies to manage computers, devices, and applications with identity at the center. | |
| WHAT’S NEW |
| Check out the cloud platform roadmap for the latest details at <http://www.microsoft.com/en-us/server-cloud/roadmap/>. |
| PRICING, LICENSING & OFFERS |
| Enterprise Mobility Suite is a per-user subscription that includes Microsoft Advanced Threat Analytics, Microsoft Azure Active Directory Premium, Microsoft Azure Rights Management Service, and Microsoft Intune cloud services. It is available as a complete User Subscription License (USL) or as an add-on for current customers licensing the Microsoft Core Client Access License (CAL), Microsoft Enterprise CAL (ECAL), or Bridge CAL. Learn more at <http://www.microsoft.com/en-us/server-cloud/enterprise-mobility/pricing.aspx>. |
| TARGET CUSTOMERS |
| **EMS customer needs/questions:** Customers dealing with identity management for multiple software as a service (SaaS) apps can benefit from Hybrid Identity features in Azure AD Premium. Customers with mobile devices can also benefit from MDM in Microsoft Intune.  **EMS customer targets:** Customers with Core, ECAL, and Bridge CAL plus existing Microsoft Office 365 deployments (or in-process deployments).  **EMS triggers:** Attach EMS to each anniversary or renewal. |
| COMPETE |
| Today, point solutions dominate the enterprise mobility space. However, more large IT vendors are integrating mobility into core offers (VMware’s recent acquisition of Airwatch demonstrates this). Microsoft differentiates in the following several key ways:  **It protects Microsoft Office better:** The only solution designed from the ground up to protect users’ Microsoft Office and Office 365 email, files, and apps, helping give users rich productivity and keep their company data safe.  **It is more secure:** Security is in Microsoft’s core. Its Enterprise Mobility solutions help users identify security breaches before they cause damage.  **It helps save money:** Up to 50 percent less than the cost of buying stand-alone solutions from other vendors.  **It just works:** Simple to set up, always up-to-date, and connects to an on-premises data center.  **It is integrated:** One integrated identity platform that protects users, devices, apps, and data.  **It is comprehensive:** Protects iOS, Android, the Windows operating system, and more than 2,500 popular SaaS apps. |
| FEATURES AND BENEFITS |
| **1,000s of apps, one identity**  Secure single sign-on to thousands of popular SaaS apps like Salesforce, Concur, and Workday. Use conditional access policies to prompt extra security (like multifactor authentication) to ensure access to apps has the right level of security. Provide self-service employee tools that save money by letting users accomplish tasks (like password resets or joining groups) without a call to the help desk.  **Detect and stop advanced threats**  Microsoft ATA helps you identify breaches and threats using behavioral analysis and provides a clear, actionable report on a simple attack timeline. Behavioral analytics uncovers suspicious activities and abnormal behavior, using machine-learning; detect known malicious attacks quickly; known security issues and risks are detected using world-class security researchers’ work.  **Manage iOS, Android, Windows—from one place**  Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Microsoft Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.  **Keep work at work**  Help maximize productivity with the Office mobile apps your employees know and love while preventing the leakage of company data by restricting actions such as copy, cut, paste, and “save as” between Microsoft Intune-managed apps and personal apps.  **Protect information at the source**  Encrypt important files and data to ensure only the right people have access. Manage and track it all from the cloud. Collaborate more securely by protecting virtually any file type on any device platform using Azure Rights Management. |
| CUSTOMER STORIES |
| Find all EMS case studies at <https://customers.microsoft.com/Pages/AdvancedSearch.aspx> search by the Enterprise Mobility Suite product filter. |
| FAQS |
| **Can a customer’s existing Azure Monetary Commitment be used for EMS or Azure AD Premium purchases?**  No. EMS is a net new per-user subscription purchased separately under the customers’ EA.  **If I license Office 365 Plan E3/Plan E4 (or A3/A4), what value does Azure RMS included in EMS provide?**  Azure RMS included in Office 365 provides access to enable RMS for office workloads. It does not enable RMS for on-premises Windows Server operating system file storage. Azure RMS also includes document tracking and revocation capabilities.  **If a customer licenses Office 365, what multifactor authentication additional value does EMS provide?**  Multifactor authentication for Office 365 user authentications are included in Office 365 subscriptions. However, enhanced security, fraud alert, the MFA software development kit (SDK), and MFA for other Azure AD workloads and on-premises workloads (like Microsoft Exchange Server, Remote Desktop Sessions, etc.) are part of Azure Active Directory Premium.  Microsoft is asking all sales to lead with EMS, which includes Azure AD Premium instead of point product of Azure AD Premium. It provides customers with the complete solution to enable enterprise mobility, aligns with Microsoft’s strategy of providing complete solutions to customers instead of point products, and retires more quota for sellers.  **How should I position EMS to Office 365 customers who get Azure AD as part of Office 365?**  The basic functionality of Azure that is needed for Office 365 is included with Office 365 plans. Customers need advanced identity management, enhanced security, and auditing capabilities as well as enterprise grade synchronization between on-premises Active Directory and Azure Active Directory that only become available with Azure AD Premium, which is part of EMS.  Lead with EMS, which includes Azure AD Premium instead of point product of Azure AD Premium. It provides customers with the complete solution to enable enterprise mobility, aligns with Microsoft’s strategy of providing complete solutions to customers instead of point products, and retires more quota for sellers. |
| ADDITIONAL RESOURCES |
| [**Microsoft Cloud and Enterprise Partner Resources - Enterprise Mobility Management**](http://aka.ms/EMSPartner)  [**EMS Customer**](http://www.microsoft.com/en-us/server-cloud/enterprise-mobility/Overview.aspx) |

Appendix

Introduction to Starter Kits

This concept is a set of deliverables, packaged as an offering that are named as a starter kit. Starter kits are designed to show a partner a specific scenario in Azure that could be possible for them to build and equip them in the technical sales cycle. Each kit will include:

1. A Description of the partner benefit for using and participating in the kit.
2. An assessment questionnaire and guidance that Partners could use with a customer.
3. An Architecture Topology presentation for a recommended way to implement the specified scenario.
4. A cost estimator (based on retail pricing) for implementing the recommended scenario on Azure.
5. A Statement of Work template for implementing the recommended scenario that a partner could use.
6. Hands on Labs a Partner can self-study to build technical skill implementing the recommended scenario.

Starter Kits - Partner Benefits

1. Reduce time in creating a proposal for a customer through a sale and deployment template
2. Reduce the learning curve cost by focusing on a proven scenario
3. Help assess and determine the technical requirements for implementing backup scenarios in the Cloud
4. Sell, estimate cost and deploy working solutions to your customer.
5. Get tools and templates to use when discussing a Backup deployment with your customers.
6. Receive a recommended set of topology diagrams for implementing an Archiving and Backup scenario on Azure.
7. Receive guidance for self-study for learning the recommended Archiving and Backup scenario at a technology level.