Microsoft Azure - Starter Kits for Partners

Azure Assessment

Enterprise Mobility

Last Update: September 2015





**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.

© 2014 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.

# Overview

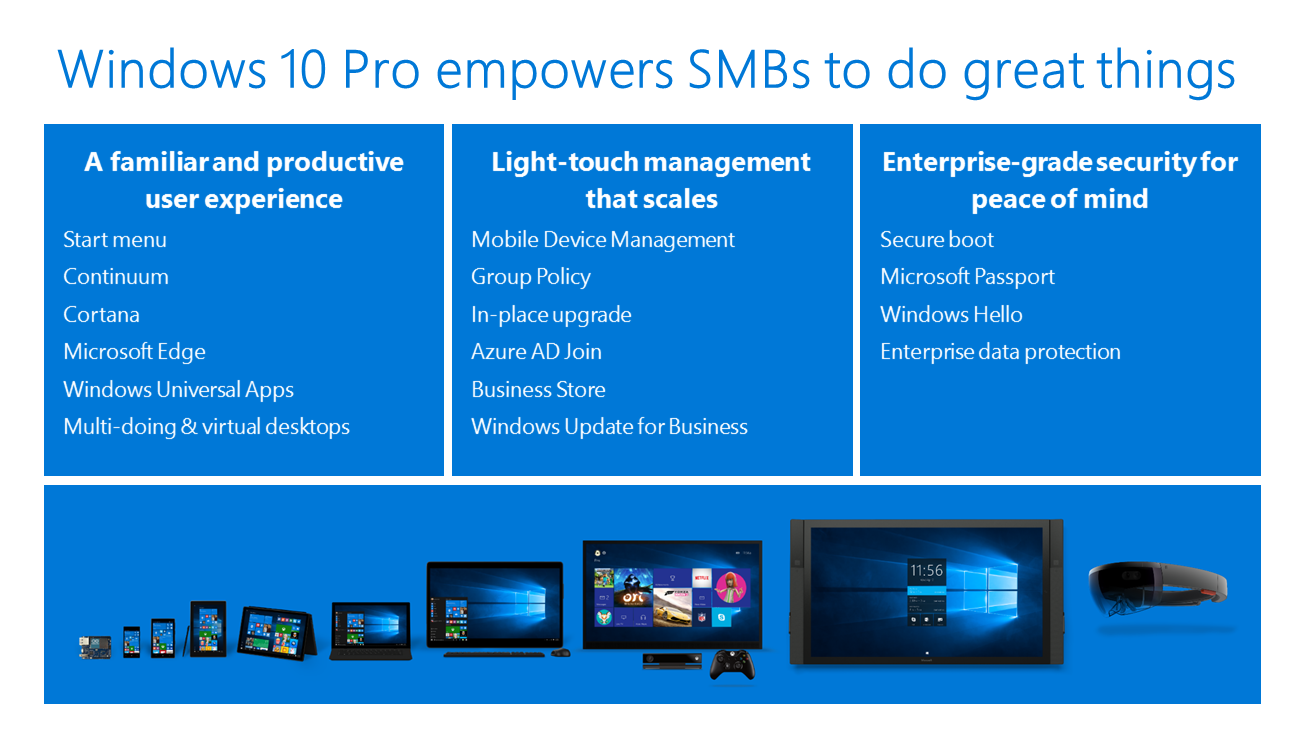
The purpose of this document is to provide Microsoft Partners an assessment to identify key components in customer scenarios and serve as a guide to the available resources. This will help partner to build an efficient architecture for the customer scenario and have an accurate cost proposal based in the customer needs.

In this document, we will cover the following topics:

* Deployment Scenarios
* Questionnaire
* Resources and Tools
* FAQ

# Azure Scenario Assessment

### Windows 10 and EMS



**Personal, productive, and always protected**

Windows 10 is the best Windows ever and provides a foundation for protection against modern threats and continuous management while enabling your users to be more productive. To get the most out of your mobile security and productivity strategy, integrate the Microsoft Enterprise Mobility Suite (EMS) with Windows 10 for greater protection of users, devices, apps, and data.

**Protect access to applications**

Windows 10 provides a foundation for secure user access with authentication options to protect identities and credentials. Azure Active Directory is built into Windows 10 to provide single sign-on for users, simplifying their experience and making it easy to set up company devices, access on-premises web apps, and access thousands of SaaS apps hosted in any public cloud. IT can use EMS to take advantage of unique Windows 10 device health data to help build conditional access policies to provide greater security when users access corporate applications.

**Flexible device and application management**

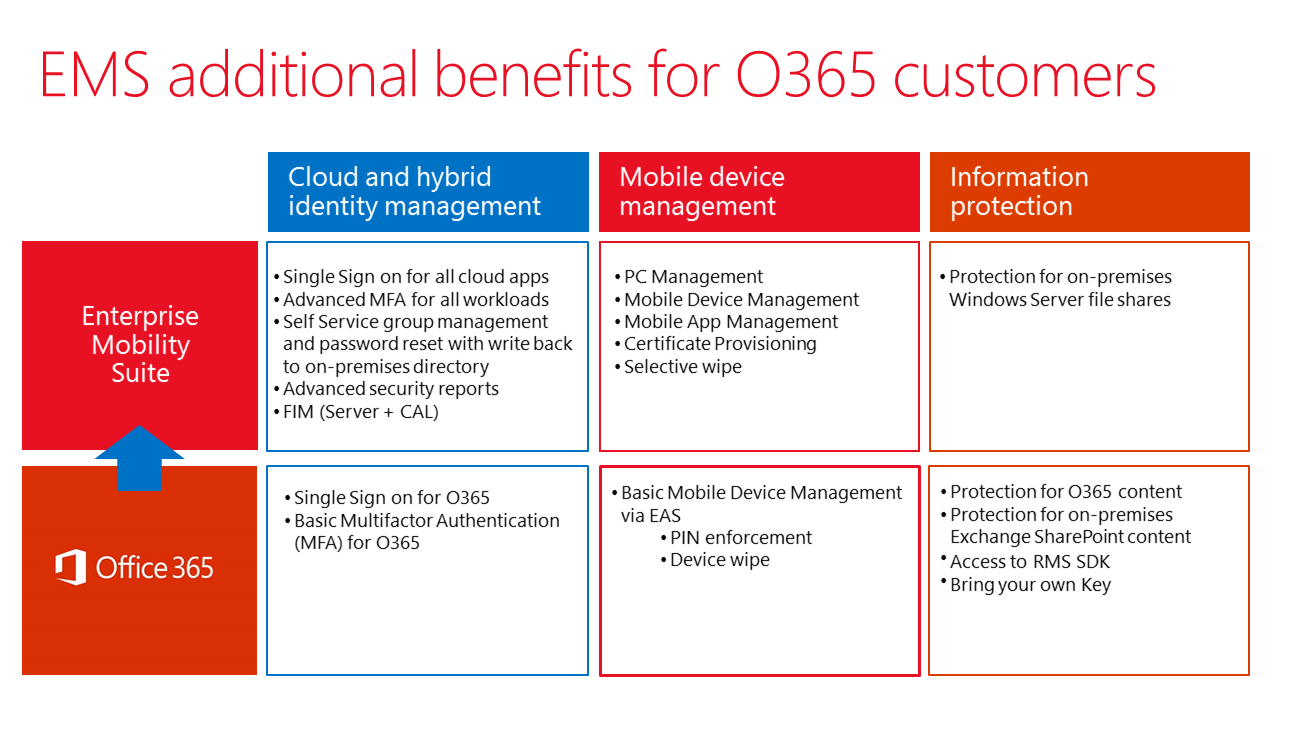
Continue to use System Center Configuration Manager (included in EMS) to deploy and manage Windows 10. In addition, you can take advantage of the mobile device management (MDM) capabilities in Windows 10 by automatically enrolling Windows 10 devices into MDM. EMS gives you a single tool to manage devices and applications across Windows, iOS, and Android. Mobile application management (MAM) for line-of-business and Office Mobile apps makes it possible to confine corporate information to use within corporate apps. Management flexibility with EMS and Windows 10 makes it possible for users to work with the tools they need, on the devices they trust, while meeting IT-defined security and compliance standards.

**Help secure data everywhere**

Extend Windows 10 security to protect your corporate data. Automatic encryption of data stored on the device gives your mobile employees a secure start. Make sure your sensitive information is always protected, even when employees share and work collaboratively. With EMS you can extend security capabilities beyond internal sharing to also protect data shared outside your organization. EMS includes data encryption with identity-based access policies for any file type for consistent performance across multiple device platforms. You can track and revoke access to files and run advanced security reports to detect threats and security issues. Now you can protect your data inside and outside your organization—and even in motion.

You have the option to host web applications on Azure Cloud Services or Azure Virtual Machines. These options are good choices when your web tier requires the additional level of control and customization that they provide; however, this increased control comes at a cost of increased complexity in application creation, management, and deployment. The following diagram illustrates the trade-offs among the three options.

### Office 365 and EMS



In a mobile-first, cloud-first world, access to corporate email, documents, and robust productivity tools is crucial for employees to stay productive while on the go. However, the amount of confidential data that is stored within corporate emails and documents can create a significant security risk for organizations, if the corporate data ends up in the wrong hands.

Enterprise Mobility Suite (EMS) helps to provide employees with secure and seamless access to corporate email and documents as well as familiar email and productivity experiences with Office mobile apps such, as Outlook, Word, Excel, and PowerPoint. EMS helps protect corporate data on the device itself and beyond with four layers of protection—all without affecting the personal data on the device. IT can even manage these apps without requiring the device to be enrolled for management.

Microsoft Outlook for iOS and Android brings together the core tools that employees need to get things done—e.g., email, calendar, contacts, and files—helping them to accomplish more, even on the smallest screen. Additionally, they can view and edit email attachments and documents using familiar productivity tools, such as Microsoft Word, Excel, PowerPoint, and OneDrive. With Office mobile apps and Enterprise Mobility Suite (EMS), employees get a consistent user experience and the ability to do more from virtually anywhere while EMS helps protect corporate data at the same time.

**A better way to manage access to email and documents**

Employees expect to have a seamless experience accessing corporate email and documents on the devices of their choice without going through several complex steps or calling the help desk. IT, on the other hand, wants to keep corporate data protected wherever it is.

With EMS organizations can enable conditional access to Office 365 (Exchange Online and SharePoint Online) as well as on-premises Exchange Server to help ensure that employees can only access corporate email and documents from devices that are managed and compliant based upon policies set by IT. When employees try to access corporate resources from unmanaged devices they are blocked and then provided with simple steps to quickly obtain access to email and other corporate resources. With the cloud architecture of EMS, IT does not need to install and configure email gateways or servers in the perimeter network nor do they need to develop custom scripts. EMS is directly integrated with Office 365 to give employees a seamless experience while also enabling IT to manage access to corporate resources.

**Extensive protection of corporate email and documents**

EMS has unique capabilities that help to protect corporate data, such as email and documents, across four layers: identity, device, application, and data.

***Identity***

EMS helps to ensure that only authorized users are permitted to access corporate email and documents by using security features, such as cloud-based authentication and authorization, multifactor authentication, and advanced security reports that leverage Microsoft Azure machine learning capabilities.

***Device***

Mobile device management (MDM) capabilities in EMS help organizations to manage and enforce device-level settings, such as encryption and password requirements, and resource access profiles, such as email, Wi-Fi, certificates, and VPN that enable seamless access to corporate resources.

***Application***

Mobile application management (MAM) capabilities in EMS help prevent corporate data leaks by restricting actions in Office mobile apps, such as cut, copy, paste, and save as. Employees can also use a single app (such as Outlook) for both personal and corporate use while EMS helps to ensure that the corporate data is separated and protected on devices that are both enrolled and not enrolled for management purposes.

***Data***

The information protection capabilities in EMS help to secure highly confidential documents at the file layer. Employees can encrypt virtually any type of a file, set granular permissions, and track usage to ensure that only the right people inside and outside of the organization can access email attachments and documents, wherever the files are.

# Environment Assessment for Enterprise Mobility Suite

# Azure Active Directory

## Azure Active Directory (Azure AD) is Microsoft’s multi-tenant cloud based directory and identity management service. For IT Admins, Azure AD provides an affordable, easy to use solution to give employees and business partners single sign-on (SSO) access to thousands of cloud SaaS Applications like Office365, Salesforce.com, DropBox, and Concur. For application developers, Azure AD lets you focus on building your application by making it fast and simple to integrate with a world class identity management solution used by millions of organizations around the world.

## Identity Integration

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the business require same sign-on or single sign-on? |  | * https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-user-signin/ |
| 1. Does the business have a single forest or multi-forest topology? |  | * https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-topologies/ |

## SaaS Application Integration

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the business have a complete list of SaaS applications? |  | * http://social.technet.microsoft.com/wiki/contents/articles/30962.getting-started-with-cloud-app-discovery.aspx |
| 1. Does the business need to enable single-sign on with SaaS applications? |  | * https://azure.microsoft.com/en-us/documentation/articles/active-directory-sso-integrate-saas-apps/ |

## Multi-Factor Authentication

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the business need to secure cloud or on-premises resources? |  | * https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-get-started/ |
| 1. Does the business need to integrate custom apps with MFA? |  | * https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-sdk/ |
| 1. Does the business need MFA for Office 365? |  | * https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6?ui=en-US&rs=en-US&ad=US |

## Self-Service

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the buiness require self-service password reset? |  | * https://azure.microsoft.com/en-us/documentation/articles/active-directory-passwords/ |

## On-premises Publishing

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the business have on-premises applications they wish to publish through Azure AD? |  | * https://azure.microsoft.com/en-us/documentation/articles/active-directory-appssoaccess-enable-hybrid-access/ |

# Azure Rights Management Service

Azure RMS protects sensitive corporate information using encryption, identity, and authorization policies to help secure files and email, and it works across multiple devices—phones, tablets, and PCs. Information can be protected both within an organization and outside the organization because that protection remains with the data, even when it leaves an organization’s boundaries. The persistent protection that Azure RMS provides not only helps to secure your company data, but might also be legally mandated for compliance, legal discovery requirements, or simply good information management practices.

## Encryption

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the business need to configure IRM for Office applications? |  | * https://technet.microsoft.com/en-us/library/jj585004.aspx |

## On-premises Investments

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the business need to migrate from AD RMS? |  | * https://technet.microsoft.com/en-us/library/dn858447.aspx |

## Tracking and Auditing

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Does the business need to track doccument usage? |  | * https://technet.microsoft.com/en-us/dn947488 |

# Microsoft Intune

There are several ways to enable enterprise mobility with Intune, depending on your company size, current management infrastructure, and need to scale. Intune is one part of the Enterprise Mobility Suite (EMS). You can use it by itself, or combine it with Azure Active Directory Premium, Azure Rights Management, and Microsoft Advanced Threat Analytics to provide comprehensive protection for your users and devices.

## Devices Management

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Do you need to enable mobile device management? |  | * https://technet.microsoft.com/library/dn646962(technet.10).aspx |
| 1. Do you need to manage settings and features on your devices? |  | * https://technet.microsoft.com/library/dn646984.aspx |
| 1. Do you need to manage PC’s. |  | * https://technet.microsoft.com/en-us/library/dn646959.aspx |

## Corporate Apps

Supported Application types: https://technet.microsoft.com/en-us/library/dn646955.aspx

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Do you need to deploy apps to mobile devices? |  | * https://technet.microsoft.com/en-us/library/dn646972.aspx |
| 1. Do you need to deploy apps to Windows PC’s? |  | * https://technet.microsoft.com/en-us/library/dn646961.aspx |

## Secure Applications

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Do you need to configure app settings on devices? Language, security, branding. |  | * https://technet.microsoft.com/en-us/library/mt481447.aspx |
| 1. Do you need to configure data loss prevention policies on published apps? |  | * https://technet.microsoft.com/en-us/library/mt627825.aspx |
| 1. Do you need to manage web browsing applications on devices? |  | * https://technet.microsoft.com/en-us/library/dn878029.aspx |

## Company Resources

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Do you need to publish certificates to enrolled devices? |  | * https://technet.microsoft.com/en-us/library/dn818904.aspx |
| 1. Do you need to publish wif-fi profiles to enrolled devices? |  | * https://technet.microsoft.com/en-us/library/dn818903.aspx |
| 1. Do you need to publish vpn profiles to enrolled devices? |  | * https://technet.microsoft.com/en-us/library/dn818905.aspx |
| 1. Do you need to publish email profiles to enrolled devices? |  | * https://technet.microsoft.com/en-us/library/dn800672.aspx |

## Configuration Manager Integration

|  |  |  |
| --- | --- | --- |
| Question | Answer | Read more |
| 1. Do you need to publish certificates to enrolled devices? |  | * https://technet.microsoft.com/en-us/library/dn818904.aspx |

# Resources and Tools

### Technical Documentation Library

Azure Active Directory Documentation Library:

https://azure.microsoft.com/en-us/documentation/services/active-directory/

Azure RMS Documentation Library:

https://technet.microsoft.com/library/jj585024.aspx

Microsoft Intune Documentation Library:

https://technet.microsoft.com/en-us/library/jj676587.aspx

## 

## Tools

Azure AD Connect

https://www.microsoft.com/en-us/download/details.aspx?id=47594

Getting Started with Cloud App Discovery

http://social.technet.microsoft.com/wiki/contents/articles/30962.getting-started-with-cloud-app-discovery.aspx

Rapid Deployment Guide for Azure Rights Management

https://technet.microsoft.com/en-us/library/mt634662.aspx

Mobile Device Management Design Guides

https://technet.microsoft.com/en-us/library/dn761724.aspx