TECHNICAL WHITEPAPER

MICROLAND®
Extraordinary. Everyday.

TOP 10 THINGS YOU SHOULD KNOW IN YOUR JOURNEY TO SETUP MICROSOFT ENTERPRISE MOBILITY + SECURITY (EMS)

Products covered

Microsoft Enterprise Mobility + Security (EMS):

- Azure Active Directory
- System Center Configuration Manager (SCCM)
- Azure Information Protection
- Microsoft Intune
- Microsoft Cloud App Security
- Microsoft Advanced Threat Analytics
- Microsoft Identity Manager and Azure Rights Management

Top 10 Things to know when deploying Microsoft Enterprise Mobility + Security (EMS)

Abstract

Among the products available in the market for Enterprise Mobility Management (EMM), Microsoft's Enterprise Mobility + Security (EMS) offers a good suite of management capabilities for mobile landscapes. However, integrating Microsoft EMS with the current enterprise IT setup involves the following:

- Navigating the challenges of setting up Active Directory and Conditional Access
- Setting up the right data protection policies
- Understanding exactly what Microsoft EMS capabilities and restrictions are during the planning phase

Top 10 Things to know when deploying Microsoft Enterprise Mobility + Security (EMS)

Introduction

The threat landscape for Enterprise IT has become significantly complex as applications and data no longer reside behind a well-defined IT perimeter. It is estimated that over 75% of all network intrusions are due to compromised user credentials. Nowadays, a large percentage of IT services are consumed outside of this IT perimeter as mobility and cloud based services result in applications and data being consumed anywhere and on any device. As end users start using a variety of devices to perform their work, enterprises need to get their act together to provide a common identity across devices and the Cloud along with effective frameworks for PC and mobile device management. In addition, Enterprise IT needs a robust security framework for data protection and access control. In summary, the three major asks before enterprise IT in the end user computing space are

(a) Providing identity-driven access to IT resources
(b) Management of mobile devices and apps
(c) Data protection and secure collaboration

There are a variety of solutions addressing each of the above IT requirements. In 2014, Microsoft renamed its Enterprise Mobility Suite as Enterprise Mobility + Security comprising of the following products to address all the above.

Microsoft Enterprise Mobility + Security	Products
	Azure Active Directory
	Azure Information Protection
	Microsoft Intune
	Microsoft Cloud App Security
	Microsoft Advanced Threat Analytics
	Microsoft Identity Manager

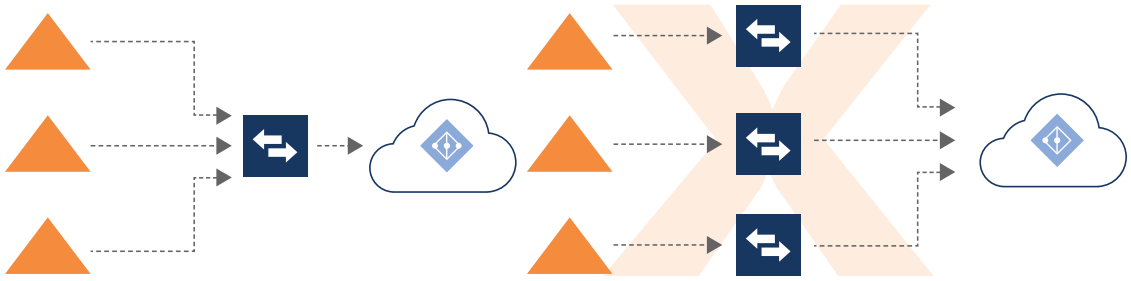
This paper is intended as a guide for avoiding common deployment issues across scenarios. This includes features available currently under Microsoft EMS, under the following sections:

(a) Configuring Active Directory and Conditional Access
(b) Setting up Data Protection (Advanced Threat Analytics (ATA) and Azure Rights Management Services (RMS) and Azure Information Protection (AIP))
(c) Wish list for Microsoft EMS

Configuring Active Directory and Conditional Access

(I) Active Directory topologies supported for EMS deployment

Enterprises cannot have multiple Azure AD Connect sync servers connected to the same Azure AD tenant, except for a staging server. This is not supported even if these servers are configured to synchronize with a mutually exclusive set of objects. The correct Active Directory topology is a pre-requisite for EMS deployment.



Supported	Unsupported
Single forest, single Azure AD tenant	Single forest, multiple sync servers to one Azure AD tenant
Multiple forests, single Azure AD tenant	Multiple forests, multiple sync servers to one Azure AD tenant

(II) Configuring Conditional Access policies

Conditional access is a feature in Azure Active Directory that enables enforcement of controls on the access to apps for specific conditions. This is implemented based on policies. For instance, access to Office 365 services can be restricted only to mobile devices that are domain-joined and enrolled on Microsoft Intune through conditional access policies. You have the option of configuring conditional access in multiple places and you can choose the right one that suits your enterprise needs.

a. Silverlight based conditional access is available for Exchange online, SharePoint online, Skype for Business online

b. AppCA policies are currently available for Exchange Online and SharePoint online only, not for Skype for Business. AppCA policies work mainly for Mobile Application Management (MAM) only scenarios, i.e. only for apps which operate using the modern authentication philosophy of Microsoft. Hence, conditional access policies will fail for Exchange Online. For instance, any email client app which uses legacy or basic authentication will continue to get access even if Outlook is whitelisted with App CA policy for Exchange Online.

   The workaround to prevent this is to block access by setting up ADFS claim rules separately. In this case, all Exchange Active Sync mail clients, including the built-in mail clients on iOS and Android that connect to Exchange Online, will be prevented from sending or receiving email as per the rule. Users will receive a single notification informing them that they need to use the Outlook mail app.

c. **Conditional access for Trusted domains:** In situations where there is a trusted domain outside and even if their ADs are trusted with each other, conditional access does not get implemented for trusted domains. Currently, there is no work around for this scenario.

d. **Microsoft Intune Device registration:** The initial device registration in Microsoft Intune happens when users log into any Office 365 application. For Android devices, this initial device registration is supported (i.e. done by logging into) only on the OneDrive app or the Outlook app) and not on other Office 365 apps currently. Hence, there is need for clear communication (emails etc.) to the users about the steps involved in enrolment to prevent user adoption issues.

(III) Configuring Azure Conditional Access for non-Windows 10 devices

Currently, not all enterprises have completely upgraded to the Window 10 platform. While configuring Azure conditional access for Windows devices, you need to watch out for the non-Windows 10 devices even if they are domain-joined. These devices need to be registered in Azure Device Registration service beforehand, to implement Azure Conditional Access.

Seamless Single Sign On: Azure Active Directory Seamless Single Sign-On (SSO) helps users to automatically sign in from their corporate devices on the corporate network to access their cloud-based applications without needing any additional on-premises components. This is a great feature and can be implemented for a non-federated environment. But when there is a federated* environment at an enterprise setting, this same feature needs to be implemented using ADFS claim rules.

(IV) Configuring authentication on mobile devices

Enterprises can have varying requirements when it comes to user authentication. For example, an organization may require that any user should be challenged only once on any app (i.e. when it is opened for the first time).

This can be implemented seamlessly within the MS office bundled products (Word, Excel, PowerPoint), but you need to watch out if there is any LoB or other apps (e.g. even Intune managed browser, Adobe Reader) as they do not pick up the MFA challenges from the recent past and prompt the user for authentication again. You may need to test the specific requirements around authentication in a test environment to set the expectations right with the users before deploying the suite.

(V) Conditional Access for specific services

Currently, SharePoint Online core services are used for access control to SharePoint Online content library, OneDrive for Business, Video (Stream) and Yammer. There is a caveat that conditional access cannot be implemented for specific services within this bundle, i.e. if a restriction is configured for SharePoint online, then it will take effect on all related services in the bundle.

On a related note, if SharePoint Online Limited Access conditional access policy is enabled, users are restricted from uploading documents into SharePoint as well (not just downloading).

* Federation services are software components that provide users with single-sign on access across organizational boundaries.

Setting Up Data Protection (Advanced Threat Analytics (ATA), Azure RMS and Azure Information Protection)

(VI) Active Directory Rights Management Service to Azure RMS migration

As Azure Information Protection comes as a part of the Office 365 E3 (or E5/EM+S/etc), migration of existing Active Directory RMS to Azure RMS is typically a required step. Azure Information Protection AIP enables secure collaboration with partners in the cloud. Before doing the migration steps provided in the documentation, it is advisable to examine the following:

a. Availability of Azure ExpressRoute:
Microsoft Azure ExpressRoute enables the extension of your on-premises networks into Azure over a private connection facilitated by a connectivity provider. This would facilitate the migration steps without much hassles. But do note that ExpressRoute is a separate Azure service that is charged separately.

b. Firewall configurations:
Microsoft as a policy does not expose the IP addresses for these RMS services due to security reasons. For migration, one would typically have a url with wildcard characters (e.g. *.sampledomain.com) which would be required to be added to the firewall. Sounds straightforward up to this point, however if your firewall does not allow wildcard URLs, then you would be faced with the costly option of upgrading your firewall to enable the migration to Azure RMS.

c. Web Proxy:
If neither of the above options are available due to cost / any operational reasons, you can use the standard web proxy server and add the url provided by Microsoft Azure RMS to the 'URL allowed' list on the proxy to enable the migration.

(VII) Change Management for Azure Information Protection

Azure Information Protection is a cloud-based solution that helps enterprises to label and protect their documents and emails, using Azure Right Management Services. This is deeply integrated with Office 365 and Azure Active Directory. With privacy laws and regulations such as General Data Protection Regulation (GDPR) coming into play, this solution gains significance for enterprises.

Unlike other aspects of implementing EMS, AIP requires significant change management when rolling out to end-users, since this fundamentally changes how the organization views its data by forcing them to classify and protect every document worked upon using Office 365. Hence AIP implementation should be done in different phases with different sets of users to reduce the impact on end users and support teams. A recommended approach to follow would be as follows:

a. Communication: Creating user awareness about data protection and classification.

b. Pilot with small teams: Pilot with an initial set of users and make them comfortable creating protected and appropriately labelled documents.

c. Classify existing data: A separate project needs to be launched to tackle and classify the existing documents residing within the organization (Public, Internal, Confidential, Secret etc.) This should start with a data discovery exercise (across file servers, Sharepoint document libraries etc.). It would be advisable to do this sizing properly and include the necessary resources before drawing up an AIP deployment plan.

d. Configure automatic controls: You also would be required to map your RMS templates with the appropriate labels within AIP.

(VIII) Use cases for Advanced Threat Analytics (ATA)

Microsoft Advanced Threat Analytics (ATA) is an on-premises platform that parses network traffic across multiple protocols as well as events/logs from existing tools to detect and report suspicious activities.

Setting up ATA needs to be carefully examined and a cost-benefit analysis done since it involves setting up of ATA / ATA Lightweight gateway infrastructure, storage and configuring port mirroring among other requirements. Typically, enterprises would already have an existing tool/solution which performs event correlation or user behavior analysis based on log files, events and other sources. You need to examine what would be the exact use cases for ATA and how it would fit into your overall security posture before proceeding with the ATA implementation.

Wishlist for Microsoft EMS:

(IX) Controlling Exchange On-Premise services (Exchange) from EMS

Typically enterprise mobility solutions will have connectors to control On-Premises Exchange services such as the Microsoft Intune on-premises Exchange Server connector. (e.g. to prevent data copy & paste from managed apps to other apps on mobile devices).

These controls work well for Microsoft Intune with Exchange Online, but not with Exchange On-Premises server despite the on-premises Exchange server connector.

While using Outlook (which is a MAM enabled app) with Exchange on-premises server, the controls configured in Intune will be ineffective and will not be implemented (as on 23 Aug 2017), despite the device being enroled in Intune.

(X) Microsoft Intune Wishlist:

Version Control: App developers who work on LoB apps to work with Microsoft EMS need to be aware off the following limitations. Within the Intune app store, there is currently no support for source control and version control for apps. i.e. you would need to upload a newer version or build of your app under a different name / build number without version control support. This could pose problems if you are planning beta / early access releases.

Download app bundles: Currently, if the developer needs to access the app bundle which has been uploaded into the Intune app store, there is currently no option to download the same as only uploads are supported. Developers better be alert with their source files as there is no option to get the source bundle back from the Intune app store.

Enabling "Install from Unknown Sources": When an enterprise's LoB app needs to be installed on an enrolled mobile device from the company portal, the setting for "Allow install from unknown sources" needs to be enabled. This setting to be reset later in order to meet the compliance and security requirements as this is enforced in most enterprises for security reasons. There is no elegant work around for this as of now.

Automatic upgrade notifications for LoB apps: The user experience for LoB apps deployed for enterprise use is not the same as the other apps on the user device since it misses the auto update option like in apps under Google Play Store or iOS app store.

Conclusion

The ten points listed above can serve as a guide for your Microsoft Enterprise Mobility + Security (EMS) solution. As with most IT initiatives, you can begin the journey from multiple approaches, from mobile device management to mobile application management to full-fledged mobile data protection integrated with your end point security solution. Microland services help your enterprise to address changing enterprise mobility challenges faster and more effectively.

Notices and Disclaimer

No part of this document may be reproduced or transmitted in any form without written permission from Microland Ltd. The data on the products mentioned in this document has been reviewed for accuracy as of the date of publication and is subject to change without notice.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. MICROLAND EXPRESSLY DISCLAIMS ANY WARRANTIES OF FITNESS FOR A SPECIFIC PURPOSE OR NON-INFRINGEMENT. Any data contained herein was obtained in a lab environments. Actual results that may be obtained in other production environments may vary significantly. While Microland has reviewed the observations in this paper for accuracy in a specific situation, there is no guarantee on the results that may be obtained elsewhere.

References

1. Microsoft (2017). Topologies for Azure AD Connect. Retrieved on 23 Aug 2017 from https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-topologies

2. Microsoft (2017). Azure Active Directory Seamless Single Sign-On. Retrieved on 23 Aug 2017 from https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso

3. Microsoft (2017). How to configure hybrid Azure Active Directory joined devices. Retrieved on 23 Aug 2017 from https://docs.microsoft.com/en-us/azure/active-directory/device-management-hybrid-azuread-joined-devices-setup

4. Microsoft (2017). Protect email access to Exchange on-premises and legacy Exchange Online Dedicated with Intune. Retrieved on 23 Aug 2017 from https://docs.microsoft.com/en-us/intune-classic/deploy-use/restrict-access-to-exchange-onpremises-with-microsoft-intune

Top 10 Things to know when deploying Microsoft Enterprise Mobility + Security (EMS)

About the author

Gokulan Subramani
Senior Lead Architect, EUS Practice

Gokulan Subramani, (Senior Lead Architect, EUS Practice) has over 14 years of experience in End User computing landscape focusing on enterprise mobility management (EMM) in addition to datacenter management and remote infrastructure management (RIM). He has worked with Fortune 100 enterprises on solution design, architecting and implementation of their EUC strategy. He has expertise across technologies such as Microsoft EMS, MobileIron, VMware AirWatch, Citrix XenMobile, VMware View, VMware vSphere and Citrix XenApp/XenDesktop.

Contributing author

Gokulakrishnan Sriram
Assoc. Director, EUS Practice

Gokulakrishnan Sriram, (Assoc. Director, EUS Practice) has over 10 years of experience in IT infrastructure & tech startups working in strategy and operations roles. In his role as the Business Leader, End User Services, he is responsible for all revenue growth initiatives. He also keeps track of market trends across the end user space to ensure that the service offerings keep pace with the latest developments and are in line with customer expectations

For further information
Contact us at: + **201 793 7052** or Email us at : **info@microland.com**

About Microland

Microland is a leading Hybrid IT Infrastructure Service Provider and a trusted partner to enterprises in their IT-as-a-Service journey. Incorporated in 1989 and headquartered in Bangalore, India, Microland has more than 3,700 professionals across its offices in Australia, Europe, India, Middle East and United States. Microland enables global enterprises to become more agile and innovative through a comprehensive portfolio of services that addresses hybrid IT transformation, workspace transformation, service transformation and end-to-end IT infrastructure management.

Learn more about us at:

www.microland.com