Managing Access and Help Protect Corporate Email Data on Mobile Devices with Enterprise Mobile Suite

Last updated: 7/15/15

Balancing productivity and security

Employees want to be able to use their own devices to access company resources and productivity tools. IT needs to make sure that employees have this ability but sensitive company data is protected. BYOD (Bring your own device) poses a specific challenge in that there needs to be a separation of personal and work data on personal devices and prevent intentional or unintentional sharing of company data.

Studies show that:

37% of the world's workforce is mobile*

53% of total email opens occurred on a mobile phone or tablet in Q3 2014**

61% of workers mix personal and work tasks in their devices***

Consider this:

- Email is often the most used application on any device.
- Content in email and email attachments can be copied, shared, or moved to other locations outside of your IT department purview, which can lead to compromising your company's security.

Since end-users want to do company work using their own personal devices and email is the most often accessed application, the first step for your IT is to make sure that end-users can access corporate email on their devices while making sure that sensitive data in email is not compromised.

What this article covers

This article starts with an overview of how you can provide data protection for your company while ensuring that the end-user experience is simple and does not impact productivity. Then, we will focus specifically on how you can help provide secure access to your corporate email and help protect company data in email and attachments using the Microsoft Enterprise Mobility Suite solution.

Overview

Microsoft offers the Enterprise Mobility Suite (EMS), a comprehensive solution for identity, mobile device management, app management, and data protection. EMS provides a layered security model which allows your IT department to manage access to email, data, and corporate applications from almost any device.

EMS is composed of the following cloud services:

Using EMS, data is protected both inside and outside of your corporate network:

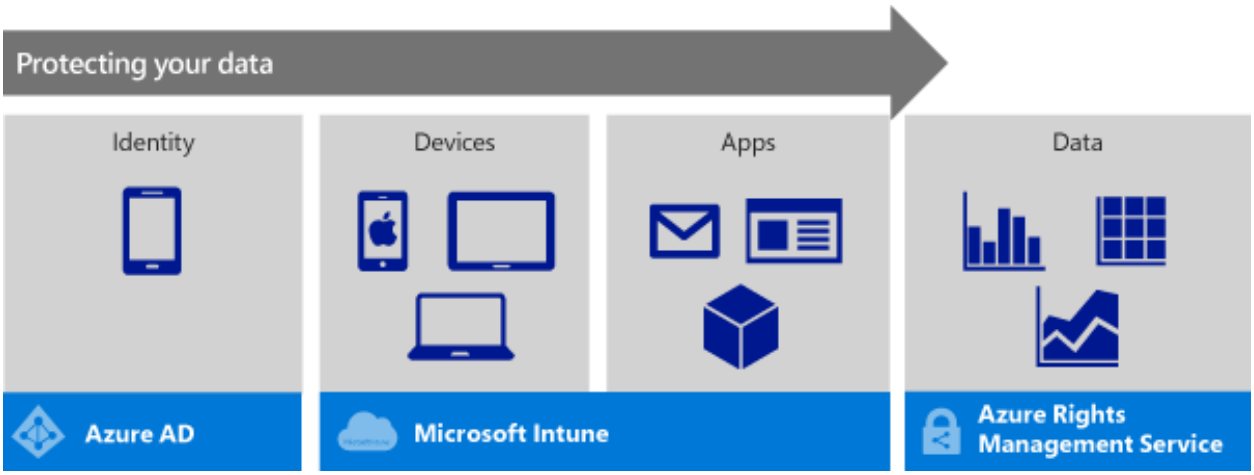
- **Employees** have access to corporate email, work-related applications, and company data on the device of their choice without worrying about compromising sensitive company information.
- Company data is protected at every level: **user**, **device**, **application** and finally, at the level of the **data** itself.
- **Your IT admin** can make sure that corporate data is accessed only by trusted users on managed and compliant devices, and in the context of managed applications.

Intune-managed apps include **Office mobile apps**, which are central to this solution. With Office mobile apps, you can help **maximize employee productivity** while preventing data leakage. For example, your IT admin can set policies that prevent copying company data to personal cloud storage like Dropbox.

When employees move or change jobs, or lose their device, EMS provides the option to remotely and **selectively wipe corporate data** from the device. This can be done by the end-user or by your IT admin.

How EMS can help protect your data

The 4 layered security model for identity, devices, apps, and data is about making sure that your company resources are only accessed by the intended user, on a device that meets a set of compliance policies configured by you, and within the boundaries of managed apps.



Protecting your data starts with establishing and validating the user identity. *Azure AD*, an enterprise-grade identity and access management tool delivers single sign-on, multi-factor authentication, self-service passwords, and more. It provides the functionality for the **identity layer** of the security model.

Building on the identity baseline, your IT admin can use *Microsoft Intune* to make sure that mobile devices are enrolled, managed and compliant with your corporate policies. This is the **device layer**.

The third layer is the **app management layer** with the *Intune*-managed app ecosystem. This ecosystem, while enabling users to be productive and use the tools that they need and know like Office, also enables your IT to keep sensitive data within the managed app ecosystem.

Azure Rights Management (Azure RMS) completes the security model by protecting data at the file level. The security policies that are applied to the data, travel with the data, help keep the data secure in transit and at rest, regardless of the device that is used to access it. This is the **data layer** of the security model.

Managing access to corporate email and help protect email content:

Protecting corporate email involves two main objectives:

- **Allow only compliant devices to access your company's email**

- **Protecting the content in email and attachments**

Allow only compliant devices to access your company's email

An important step to protecting corporate data is restricting access to devices that don't use a strong password, are not jailbroken, or not encrypted. Microsoft Intune gives you the ability to set conditions that your users have to meet to gain access to your company resources. This is known as conditional access.

Conditional access is determined by **two types of policies** you can set in Intune:

Compliance policies determine the compliance of a device. They evaluate settings and conditions like:

- **PIN and passwords:** Your IT can create rules to require passwords before unlocking a device, the complexity of the password, password expiration, and other password settings.
- **Encryption:** Your IT can restrict access to devices that are encrypted.
- **Device is not jailbroken or rooted:** Intune can detect if an enrolled device is jailbroken, and your IT can set the policy to block access on such devices.

Conditional access policies are configured for a particular service like Exchange Online or SharePoint Online. For each service, you can define which groups of users these policies should apply to. For example, you can make sure that everyone in the finance department can only access company email from enrolled and compliant devices.

Watch this four minute video to see how conditional access affects your end users.

Why Architecture Matters

The different components of EMS and Office 365 are built for and designed to run in the cloud. This brings all the benefits that the cloud offers: scalability, flexibility, and ease of management.

Since different businesses have different requirements, EMS is designed to integrate with **existing on-premises infrastructure** such as Active Directory, Exchange Server, or System Center Configuration Manager. This allows you to use the credentials already established in your network for both on-premises and cloud resources.

The following sections describe the architecture as designed to run in the cloud, and touch briefly on the on-premises option.

Email Access Flow

Depending on the type of email application that you use to access Exchange online, the path to establishing secured access to email can be slightly different. However, the key components: Azure Active Directory (Azure AD), Office 365/Exchange Online, and Microsoft Intune, are the same. The IT experience, and end-user experience also are similar. EMS currently supports native email apps and the Microsoft Outlook app for iOS and Android.

Access control flow for native email applications

Exchange ActiveSync (EAS) clients attempting to access email in Exchange Online will be evaluated for the following properties:

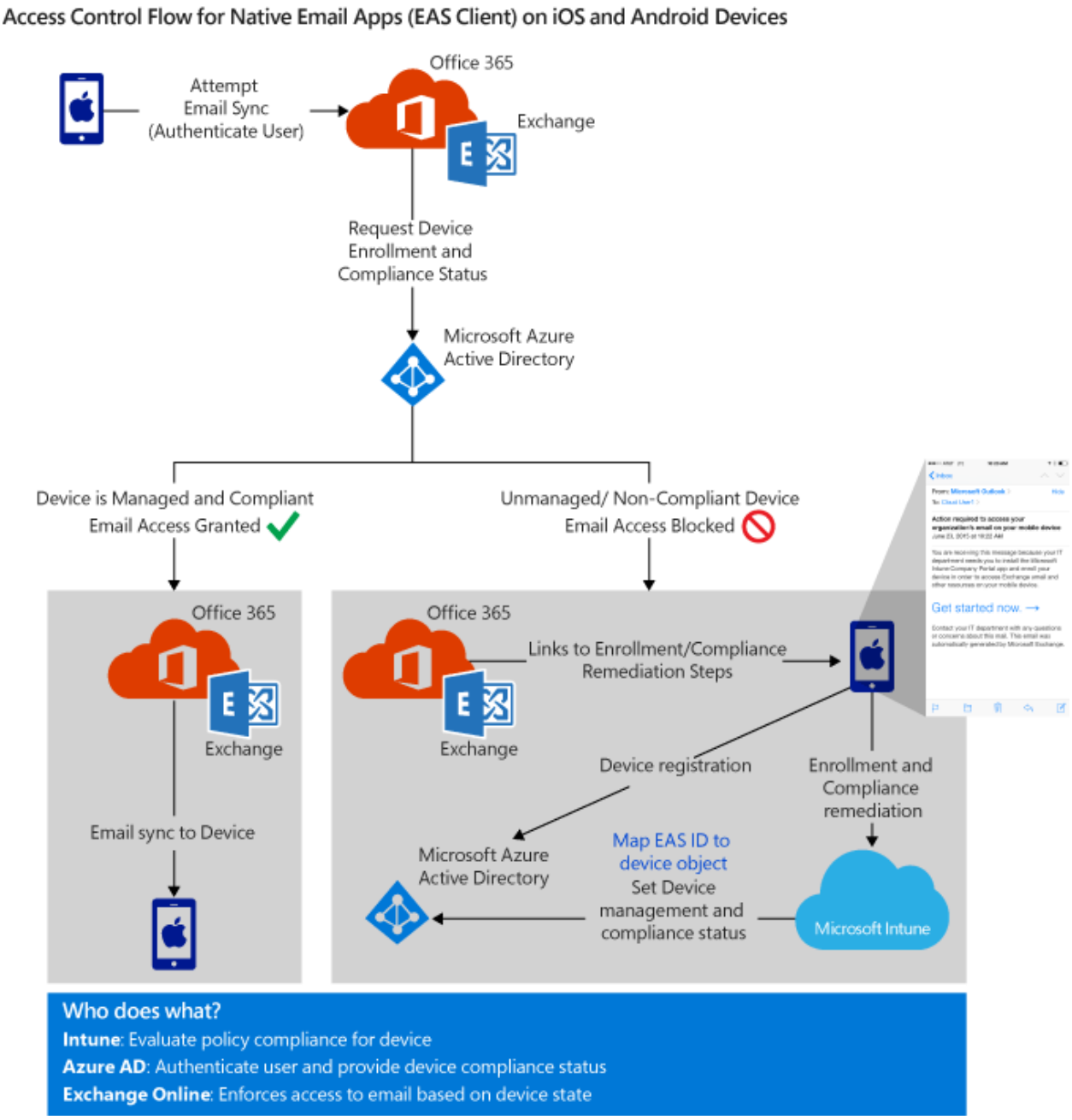
- Is the device managed by Intune?
- Is the device registered with Azure Active Directory?
- Is the device compliant?
- Is the client EAS ID mapped to a registered device?

To get to a compliant state, the device on which the **EAS client** is running needs to:

- **Enroll** with Intune
- Register with **Azure Active Directory**, and
- Be **compliant** with the device policies set by your IT admin.

On most platforms, the Azure Active Directory device registration happens automatically during enrollment. The device states are written by Intune into Azure Active Directory, and then read by Exchange Online the next time the EAS client tries to get email. If the device is not registered, the user will get a message in their inbox with instructions on how to register (also known as enrolling). If the device is not compliant, the user will get a different email that redirects them to the Intune web portal where they can get more information on the compliance problem and how to remediate it.

Azure AD, authenticates the user and the device**,** Microsoft **Intune** manages the compliance and conditional access policies, and **Exchange Online** manages access to email based on the device state.



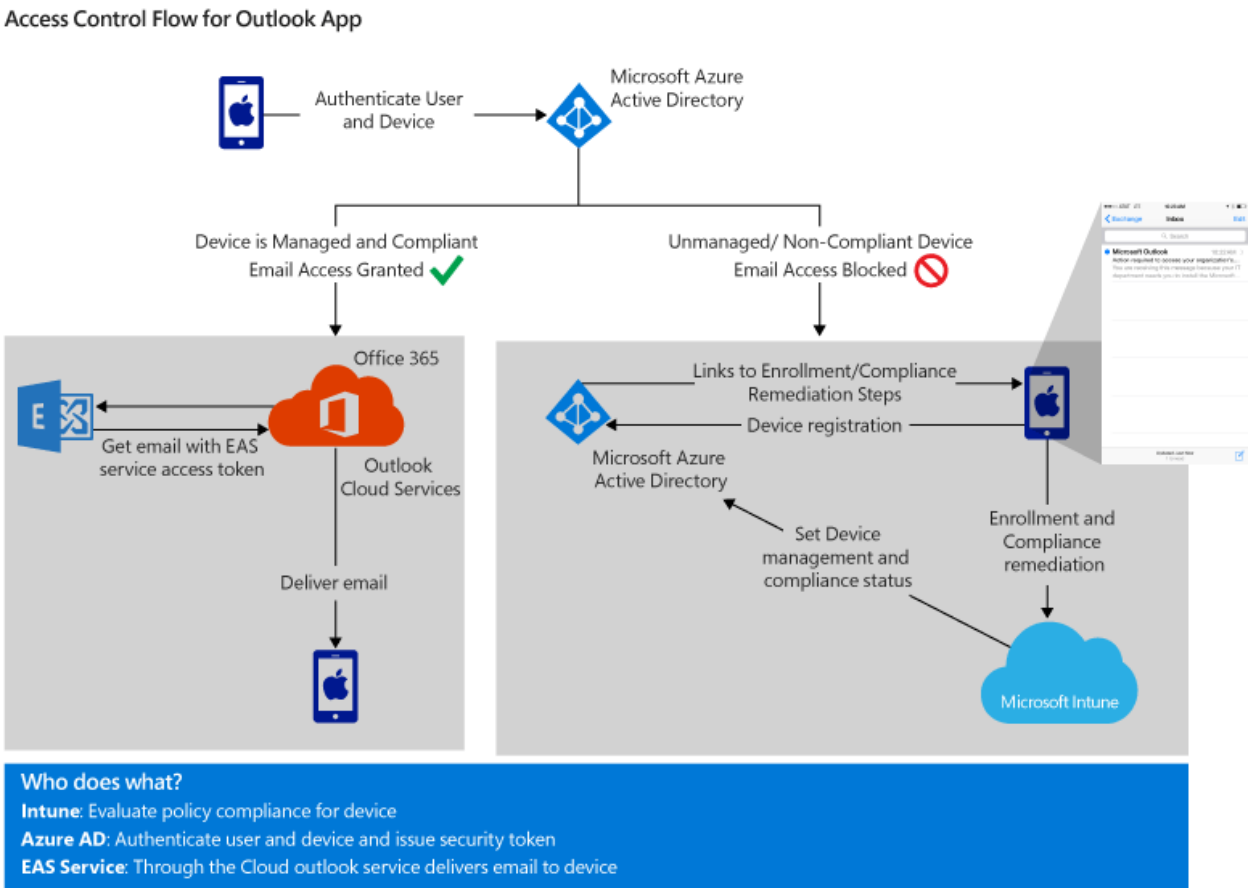
Access control flow for Outlook applications

Similar to the EAS client, the Outlook email app attempting to access mail in Exchange Online will be evaluated for the following properties:

- Is the device managed by Intune?
- Is the device registered with Azure Active Directory?

- Is the device compliant?

The device compliance is established in much in the same way as described in the EAS client access control flow. However, for Outlook apps, the flow between the components is slightly different. When the Outlook app attempts to get email, it is redirected to Azure AD. Azure AD issues a security token if the device is successfully evaluated to be enrolled and compliant. The security token is then used to get corporate email from Exchange Online. The email sync is actually brokered through the Outlook cloud service, which gets an EAS service access token on behalf of the user to complete the authentication and delivers the email.



The IT admin experience:

There is no complex infrastructure setup required for Azure AD or Exchange to make this happen. Your IT admins:

- Configure and deploy the compliance polices that are used to evaluate the compliance status of the device.
- Configure the Exchange Online conditional access policy, and specify which Azure AD security groups will be affected by, or exempted from these policies.

- Choose to allow or block devices that are not capable of enrolling in Intune. The list of supported operating systems for mobile devices is listed later in the What you should consider when planning your implementation section.

There is an **optional** setup stage that may be needed. The reporting that is used to manage and monitor device access and status requires the Microsoft Intune service to service connector to be set up.

The End-user experience:

When the user attempts to access email on the device for the first time, or sync subsequently, the device enrollment and compliance status is checked. The process of enrolling or fixing compliance issues is a guided experience. The end-user is shown the necessary steps to enroll their device and make it compliant without needing to call your IT help desk:

- **If the device is not enrolled**, the sign-in page will show access denied and will prompt for enrollment. On enrollment, the device is automatically registered in Azure Active Directory. Intune checks the device for compliance and provides remediation steps to resolve any non-compliance issues. Once the device is compliant, Intune sets the device compliance status with Azure Active Directory.
- **If the device is enrolled but is not in compliance**, a link with steps to remediate the issues is sent to the device. When the end-user corrects the issue (for example, set password, encryption), Intune which manages the compliance policies updates the compliance status of the device in Azure AD.

Once the device is evaluated as enrolled and compliant, the email sync should happen within a few minutes.

Protect email and email attachments from data leakage

The previous section talked about how you can make sure that only compliant devices can access corporate email. However, the content in the email and email attachments is not protected just by securing access. The content can be copied, moved, saved to a different location, or shared with another user. EMS solves this problem using mobile application management policies.

Managed apps are apps that are deployed by your IT admin that comply with your companies security requirements. With these apps, IT has direct control over deployment, ongoing management like inventory or updates, and selective wipe of the apps and their associated data. Additionally, through a set of mobile application management (MAM) policies, **Intune** lets you modify the functionality of apps, and restricting sharing of data like:

- **Block copy and paste**, or prevent **data transfer** from a managed app to an app without MAM policy.
- **Prevent backup** to personal cloud storage, preventing **Save as**, etc.
- **Secure app access** by requiring PIN/passcode or corporate credentials on a MAM-protected app.
- Configure the application to open all web links inside the Intune **Managed Browser**.

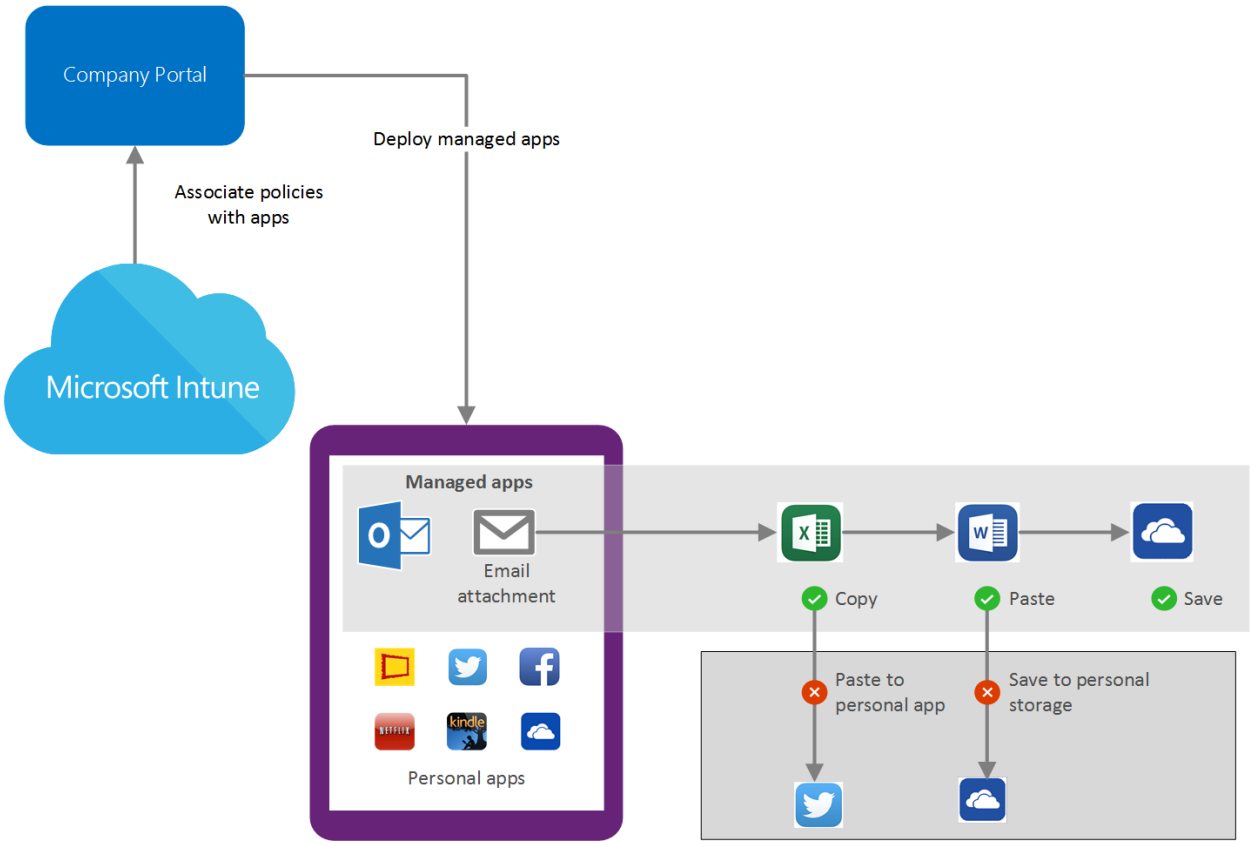
- **Selectively wipe** only data that is associated with the managed app. When a device is lost, stolen, or is no longer managed by your IT, a selective wipe can remove all corporate data from the apps, leaving only personal app data behind. This is known as **multi-identity**.

With **Azure Rights Management Services**, you can extend email protection in the following ways:

- Email messages can be encrypted so only the right users can read or view the content whether within your company or outside the company.
- Users can protect email messages and the recipient can read and use protected email messages sent to them.
- An administrator can set rules to:
    - Automatically apply the rules to a specified group of recipients or create templates for specific departments.
    - Automatically detect and apply rules to email messages with sensitive content. The rule can be based on sender, recipient, message subject, or content.
    - Detect sensitive content and alert the sender to apply the protection rules before sending the email.

Managed App Components

- **Microsoft Intune** is where you configure the policies, associate the policies with the app, or use the app wrapping tool to enable an in-house app to use mobile application management policies.
- **The Company portal** is an app that either runs natively on each device or is browser based. Your IT deploys the managed apps to users or devices, and end-users can install the app from the portal. The policies associated with the apps are carried over to the device with the apps.



The IT admin experience:

Your IT admin creates the mobile application management policies, associates the policy to the app, and deploys it to users or devices. When the managed app is installed on the device, the app restrictions take effect. Creating and deploying managed apps involve little or no additional effort:

- There are existing apps that already have the App SDK which allows you to apply restrictions to the app. These require no other processing, but just adding a link pointing to an app store such as iTunes or Google Play. Read this article to see the list of managed apps.
- If you want to manage apps that are created in-house, you can repackage the apps with Microsoft Intune App Wrapping tool. The tool repackages the app which allows you to apply restrictions to the app.

The End-user experience:

End-users can install managed apps and use them to do their work. They will only be able to move or share data between managed apps. Any attempt to move data out of the managed app ecosystem will be blocked.

Operations and Incidence Response

Once you have implemented the solution, you need to manage the environment and identify potential security risks. Both Intune and Azure AD have monitoring and reporting capabilities that can help in monitoring and responding quickly in case of a security incident.

Here are some of the reporting capabilities:

- Intune reports and alerts help you **monitor the status and health of devices** managed by Intune.
- Azure AD has **auditing and activity** logging. You can monitor things like **password changes** and **user management**. Azure Active Directory premium includes advanced **anomaly security reports** and alerts. These alerts are based on detailed machine learning based reports showing sign in activity, inconsistent access patterns, and potential threat areas.

On-premises implementation

If you have an existing implementation of System Center Configuration Manager, Active Directory and/or Exchange Server you can extend the existing infrastructure by integrating with Intune, Azure AD and Office 365. Using this hybrid implementation, you can provide a consistent management experience across devices on-premises and in the cloud. Intune and Configuration Manager offer a similar set of capabilities to allow restricted email access based on the device state.

For Exchange Online Dedicated implementations, whether you can take advantage of the cloud based solution described previously, or the hybrid implementation depends on what your current implementation looks like. Talk to your account team to determine what your implementation will involve.

What you should consider when planning your implementation

- **Device platform support:** You must also consider if you want to allow email access on platforms that are not supported by Intune. Intune mobile device management supports the following operating systems:

    - Apple iOS 7.1 and later (previously enrolled iOS 6.0 and 7.0 devices remain enrolled but new devices cannot enroll)
    - Google Android 2.3.4 and later (includes Samsung KNOX)
    - Windows Phone 8.0 and later
    - Windows RT and later
    - Windows 8.1 computers and later

- **Type of email apps**: The EMS solution currently supports clients that use EAS protocol, and Outlook apps (previously Accompli on iOS and Android).
- **Policies:** The EMS solution and its components have several policies through which security and access is managed. Determine what policies your IT admin needs to configure. The three key policies to be used for research and plan when securing access to email and email data are:
    - **Device Compliance Policies:** Determine what compliance means for your company. Intune includes several rules that you can set, but all of those rules may or may not apply to your company. You can change policies anytime, but it is good practice to

determine a basic set of policies for you company. Compliance policies are targeted at Intune user groups and device groups.

- **Conditional Access Policies:** Conditional access policies are targeted at Azure AD Security Groups. Determine which users will be targeted by the policies and if there are users who need to be exempt. Conditional Access is supported by both the cloud based solution and the hybrid implementation.
- **Mobile Application Management:** Determine what apps should be managed and the MAM policies you need to apply to these apps.

- **Device management considerations:** Select the device management option that best meets the requirements for your organization before you implement the solution. There are two options:
  - Unify System Center Configuration Manager with Microsoft Intune to manage all devices through a single console. This is called the **Hybrid implementation**.
    - Advantages of this approach:
      - **Single management console** with rich rights-management controls to manage both on-premises PCs as well as mobile devices
      - Rich **targeting** and **deployment** capabilities
      - High **scale** for very large enterprises
  - Manage the mobile devices through Microsoft Intune separately from the on-premises devices using System Center Configuration Manager. **This is called Intune Stand-alone implementation**.
    - Advantages of this approach
      - **Simple** web-based console tailored specifically for mobile device management
      - Rapid access to the **latest features**

  While migration is always possible, we strongly recommend that you make this decision before implementing it, since it will influence a lot of the decisions you will make in the roll out process.

- **Your Exchange environment:**
  - Deployment of Exchange connectors and how they connect when network load balancers are implemented.
  - Exchange Online – is it multi-tenant or dedicated?

    If it is dedicated, find out which architecture your tenant is on. This will determine whether Azure AD-based conditional access can be used, or if an on-premises connector is required.

- **Azure AD synchronization and Active Directory Federated Services (ADFS), or another third-party federated service:**
  - **Conditional Access** is designed to work for customers who have federated their identity service to ADFS. Client access rules will generally still apply, however it is recommended that full testing be conducted. Requirements for directory synchronization and ADFS are no different than for Office 365.

- **Third-party federation services** like Ping should also work. Testing before implementation is recommended.

Where to go from here

- Try/Evaluate: Watch this video to learn how to sign up for a trial account and get started.

Additional Resources

- EMS Architecture: http://aka.ms/emposter
- Intune capabilities: Read the Intune evaluation guide to learn about Intune features, choosing an implementation that works for your company, and how to get started on Intune.
- Azure Active Directory:
  - What is Azure Active Directory
  - How does Azure Active Directory support Office 365, Microsoft Intune, and other Microsoft services?
  - How does Azure Active Directory help you manage identities
- Azure Rights Management Service
  - What is Azure Rights Management?
  - How Applications support Azure Rights Management
    Automatically protecting emails with Exchange Online and data loss prevention policies

* IDC: "Worldwide Mobile Worker Population 2011–2015 Forecast"

** Experian "Quarterly email benchmark report" (Q3 2014)

*** Forrester Research: "BT Futures Report: Info workers will erase boundary between enterprise & consumer technologies," Feb. 21, 2013