Microsoft Endpoint Manager

Configure App Protection Policies

HASHMAT
IT SOLUTION

Overview

Things to Cover:

1. App Protection Policies and Windows Information Protection WIP
2. Review the Azure AD MDM/MAM configuration
3. Create the WIP Policy
4. Monitor WIP Policy

HASHMAT
IT SOLUTION

App Protection Policies **and** Windows Information Protection **WIP**

App protection policies are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app.

A managed app is an app that has app protection policies applied to it and can be managed by Intune.

HASHMAT
IT SOLUTION

How WIP works

- App Protection Policies will use Windows Information Protections on devices
- It uses EFS (encrypted file System) to protect your data
- You can have options to restrict data copy within your company Boundary network
- User will not be able to Copy data from Managed Apps to un-managed Apps
- WIP Policy can protect both Enrolled Devices by MDM or non-Enrolled devices via MAM
    - MAM – protect data on personal Device which are not enrolled by MDM. Ex: personal Device
        - Personal Device needs to be Azure AD Registered
        - Enable MAM only for users/groups that are using personal Device
        - Do Not Enable MAM for all users, it will overwrite the MDM device enrollment into MAM

Differences between MDM and MAM for WIP

- You can create an app protection policy in Intune either with device enrollment for MDM or without device enrollment for MAM. The process to create either policy is similar, but there are important differences:
- MAM has additional Access settings for Windows Hello for Business.
- MAM can selectively wipe company data from a user's personal device.
- MAM requires an Azure Active Directory (Azure AD) Premium license.
- An Azure AD Premium license is also required for WIP auto-recovery, where a device can re-enroll and re-gain access to protected data. WIP auto-recovery depends on Azure AD registration to back up the encryption keys, which requires device auto-enrollment with MDM.
- MAM supports only one user per device.
- MAM can only manage enlightened apps.
- Only MDM can use BitLocker CSP policies.
- If the same user and device are targeted for both MDM and MAM, the MDM policy will be applied to devices joined to Azure AD. For personal devices that are workplace-joined (that is, added by using Settings > Email & accounts > Add a work or school account), the MAM-only policy will be preferred but it's possible to upgrade the device management to MDM in Settings. Windows Home edition only supports WIP for MAM-only; upgrading to MDM policy on Home edition will revoke WIP-protected data access.

Enlightened versus unenlightened apps

- Apps can be enlightened or unenlightened:
- **Enlightened apps** can differentiate between corporate and personal data, correctly determining which to protect, based on your policies.
- **Unenlightened apps** consider all data corporate and encrypt everything. Typically, you can tell an unenlightened app because:
    - Windows Desktop shows it as always running in enterprise mode.
    - Windows **Save As** experiences only allow you to save your files as enterprise.
- **WIP-work only apps** are unenlightened line-of-business apps that have been tested and deemed safe for use in an enterprise with WIP and Mobile App Management (MAM) solutions without device enrollment. Unenlightened apps that are targeted by WIP without enrollment run under personal mode.

Device Requirements

Operating system	Management solution
Windows 10, version 1607 or later	Microsoft Intune -OR- Microsoft Endpoint Configuration Manager -OR- Your current company-wide 3rd party mobile device management (MDM) solution. For info about 3rd party MDM solutions, see the documentation that came with your product.