Using Workspace ONE with Office 365

For organizations that use Office 365, managing data loss prevention (DLP) settings for Office apps on mobile (iOS and Android) requires the Intune App Protection Policies. Together with Workspace ONE Unified Endpoint Management (UEM) and VMWare Identity Manager (VIDM), an optimal security and end-user experience for Office 365 can be achieved.

Ensure that the following are set up prior to starting:

1. Workspace ONE UEM (SaaS/On-Prem)
    - Workspace ONE
2. VMWare Identity Manager (SaaS/On-Prem)
3. AirWatch Cloud Connector (If your existing deployment syncs users to VIDM from Workspace ONE UEM, then the VIDM connector is not required. For new deployments, use the VIDM connector to sync users from Active Directory (AD) to VIDM)
4. If you have an Identity Provider (IdP) for Single-Sign-On (SSO), then federate the third-party IdP with VIDM . Note that third-party IdPs must support SAML 2.0.
5. Integrate Workspace ONE UEM with Microsoft Intune App Protection Policies DLP.
6. Configure steps 15–18 of the Azure AD Identity Services Integration (needed so that an enterprise wipe in AirWatch will automatically revoke the Azure refresh tokens for the corresponding user), which can be found here.

This whitepaper covers the following:

1. **Why use VIDM for Office apps?**
2. **What is involved in using VIDM ?**
3. **How to use VIDM for authentication and conditional access for Office apps?**
4. **Configure Data Loss Protection for Office apps**
5. **Use Office apps with other non-Office apps**
6. **Configure options for removing corporate data from Office apps**

Why use VIDM for Office apps?

The Workspace ONE platform and VIDM solve two key problems when managing Office apps. 1) Administrator has the ability to secure confidential corporate data stored within high-risk apps (i.e., Office apps) even if the user is accessing the app on an unmanaged/BYOD device, while not being required to enforce the same level of increased security for lower-risk applications. 2) Administrator can extend the capability of her/his third-party IDP to not only authenticate the user but also check for device posture via VIDM prior to authenticating the user to the app. Thus, security controls are based on application, type of device, whether the device is managed and in compliance, and where the user authenticates to the application (i.e., on/off network).

What is Involved in Using VIDM?

VIDM has the capability to act as a standalone federation IdP. It can also integrate with existing IdP and SSO solutions as a federated IdP or service provider (SP).

Federating a third-party IdP or SP would direct users on a mobile device to Workspace ONE to authenticate, then apply policies to map data from the returned SAML assertion into an outgoing SAML assertion to a SaaS application. This gives administrators the flexibility to use VIDM to authenticate mobile device users while the third-party IdP continues to authenticate desktop users.

Workspace ONE never sees a user's password because it is shared only between the user's device and her/his IdP or SP.

It is recommended to create two different mobile authentication flows within the IdP, one for apps accessed via mobile devices that require device management by Workspace ONE and another for apps accessed via mobile devices that do not require device management. This gives administrators the flexibility to redirect mobile traffic from the third-party IdP to VIDM while desktop traffic remains unchanged and is not routed through VIDM. The IdP continues to authenticate desktop users as it did before VIDM was introduced.

This is achieved without altering the SSO that employees are currently used to with the third-party IdP. Moreover, the current SSO experience can be improved with VIDM by leveraging the Mobile SSO certificate for managed devices.

The Mobile SSO certificate used for iOS device authentication uses Kerberos by leveraging VIDM as an identity provider. This authentication method for iOS devices uses a) Workspace ONE UEM as a Certificate Authority and b) VIDM, which acts as a Key Distribution Center (KDC) without the use of a connector or a third-party system.

How to Use VIDM for authentication and conditional access for Office apps?

When a user opens an app on her/his device, the application service provider routes that traffic to the federated IdP. If the application traffic is coming from a mobile device and is whitelisted for redirection to VIDM, then the federated IdP routes this traffic to VIDM. VIDM then checks the application rules specified for conditional access. Apps fall into two categories in this example, namely 1) high-risk apps such as Office apps that require device management to protect data loss and 2) lower-risk apps that do not require device management but have seamless authentication if the device is managed.

For category 1, if the device is managed (i.e., it has the Mobile SSO certificate) and in compliance, then VIDM sends a SAML assertion back to the federated IdP, which authenticates the user and thereby results in the token being delivered to the device from the service provider. If the IdP has a policy that requires Multi-Factor Authentication (MFA), it would further challenge the user for in-app authentication/SMS. Conversely, if the device is not managed (i.e., it does not have the Mobile SSO cert) and/or is out of compliance, then access to the application will be denied at VIDM. Category 2 (lower-risk apps) is the same as category 1 (high-risk apps) above, but if the device is not managed, then access to the application is not denied because VIDM falls back to the federated IdP and the IdP then delivers the credentials page to the application as it would normally without VIDM.

Below is an example of conditional access policies for a high-risk versus lower-risk app that can be set up at VIDM. In this example, MFA is a security requirement for high-risk apps, thus users on managed devices who are not on the corporate network are using the Mobile SSO certificate for the first factor of authentication and SSO credentials (i.e., in-app authentication/SMS) for the second factor of authentication. If users are accessing high-risk apps on devices that are not managed, then access is denied until the user enrolls into Workspace ONE.

For lower-risk apps, users on managed devices are able to authenticate transparently whether or not they are on the corporate network. Users on other non-managed devices must enter their SSO credentials.

Note that below is a common example of how policies are configured, but usually the decision as to how many and which factors are applied in each case is a matter of evaluating the risk to be mitigated.

Table 1a: VIDM Conditional Access Policies for High-risk vs. Lower-risk apps

	High-risk app (Outlook)	Lower-risk app (Concur)
On Network		
Device Managed	**1. Mobile SSO Cert + SSO (optional)**	**3. Mobile SSO Cert**
Device Not Managed	**2. Access Denied**	**4. SSO**
Off Network		
Device Managed	**Mobile SSO Cert + SSO**	**Mobile SSO Cert**
Device Not Managed	**Access Denied**	**SSO**
For Managed Devices Only		
Device Compliance	**Configure compliance in Workspace ONE UEM: Remove Mobile SSO certificate if device is not in compliance, therefore no Corp data will be accessible**	**N/A (as device compliance not enforced for lower-risk apps)**

SSO = Presented via third-party IdP. If MFA requirement, second factor of authentication could include either password, in-app authentication, or SMS.
Mobile SSO Cert = Delivered via VIDM to managed devices only
Device Compliance = Mobile device is not compromised (jailbroken/rooted), or inactive, and/or contains minimum OS version

Best practice is to use Workspace ONE for device compliance instead of VIDM conditional access policies because device posture will be obtained faster and will not require waiting for the sync interval between VIDM and Workspace ONE. Once Workspace ONE detects the device as non-compliant, best practice is to remove the Mobile SSO certificate, thereby preventing access to the high-risk app the next time the user tries to authenticate to the app. More information on configuring Workspace ONE UEM compliance policies can be found here.

a. **High-risk app - Conditional access for apps that contain sensitive or confidential corporate data**

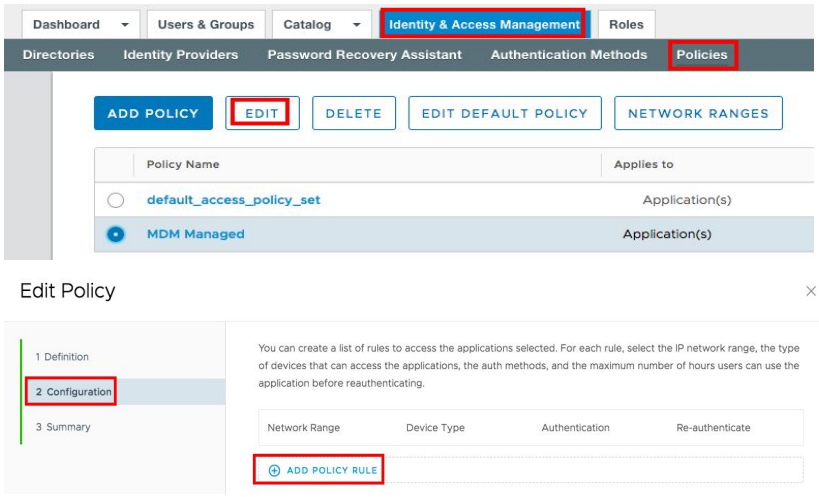
***If user's device is on the Corporate Network (i.e., Corporate Wi-Fi)*:**

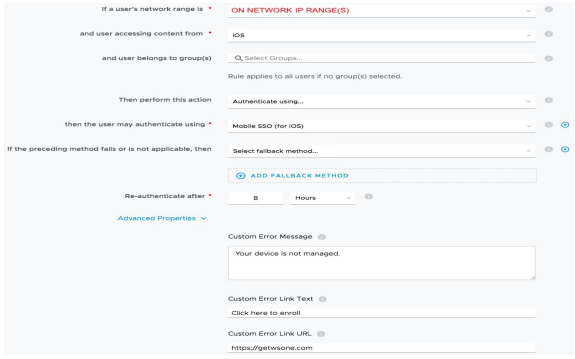
Users enrolled to Workspace ONE will receive the Mobile SSO certificate, which is configured in VIDM. If device management is required for users to access the app, then no fallback must be selected. If the user is not enrolled to Workspace ONE and managed, then she/he will not have the Mobile SSO certificate on her/his device and access will be denied.

Android devices instead would leverage the VMware Tunnel client app and Per-App VPN rules that use an SSO proxy to a VIDM server. More information regarding configuring Android SSO can be found here.

A customized error message can be presented that informs users that *access is denied* and they must enroll to Workspace ONE to be able to authenticate to the app. An example of the iOS mobile policy (Android is nearly identical) as configured in VIDM is shown below.

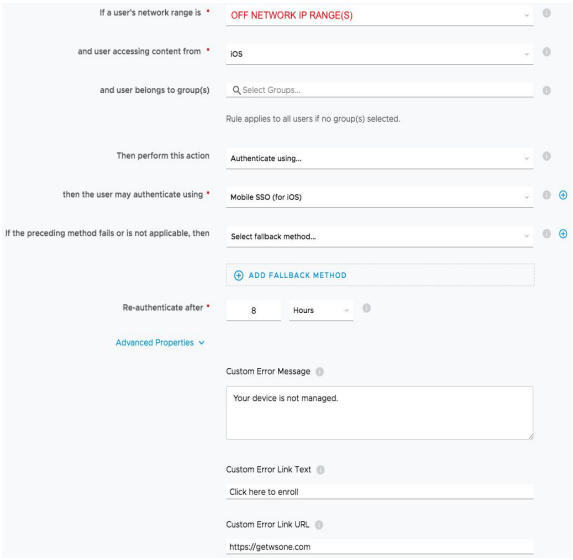
VIDM console > **Identity & Access Management** > **Policies** > select the appropriate ***policy name*** > **Edit** > **Configuration** > **Add Policy Rule**.





If user's device is not on the Corporate Network (i.e., user is working remotely):

Similar to the first point discussed earlier, a corresponding VIDM policy should be created to require device management for an app that a user accesses off the corporate network, as shown below.

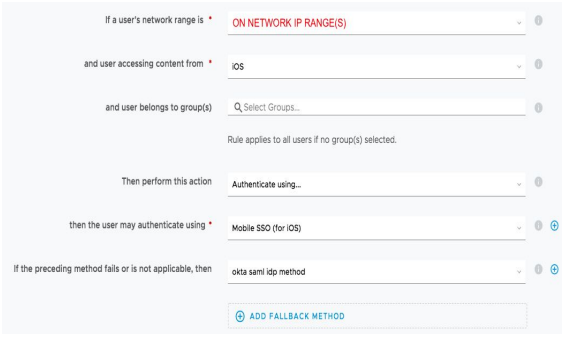


b. **Lower-risk app - Conditional access for apps that do not contain sensitive or confidential corporate data**

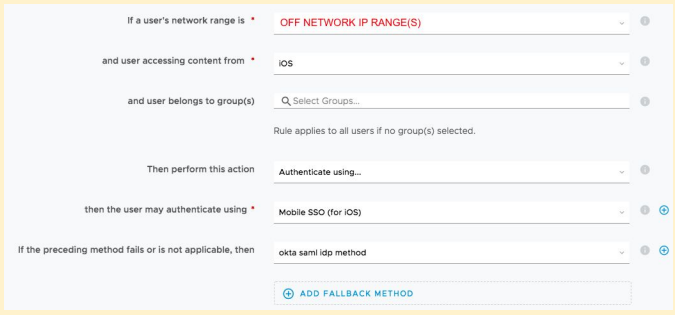
If user's device is on the Corporate Network (i.e., Corporate Wi-Fi)

For apps without sensitive data such as Concur, device management should not be needed and SSO should suffice without increasing the risk for the enterprise. Using a ***fallback*** would continue to grant SSO access via the third-party IdP even when the device is not enrolled and/or the Mobile SSO certificate (from VIDM) is not present on the device, as shown in the VIDM iOS mobile policy below. The corresponding Android policy is almost identical to below.

VIDM console > **Identity & Access Management** > **Policies** > select the appropriate ***policy name*** > **Edit** > **Configuration** > **Add Policy Rule**

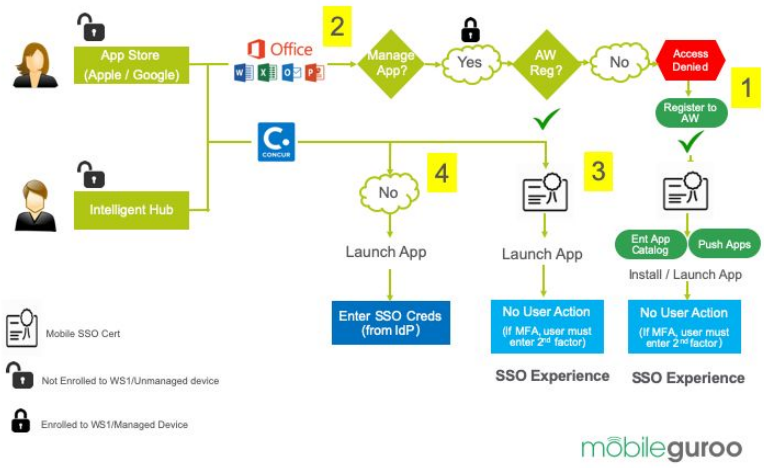


If user's device is not on the Corporate Network (i.e., user is working remotely):
Similar to above, a corresponding VIDM policy should be created to allow a ***fallback*** so that the user is only required to enter her/his SSO credentials in the app deemed low risk and accessed off the corporate network, as shown below.



Note that although you can select specific user groups (i.e., the AD groups that the Connector has synched from the organization's LDAP server to Workspace ONE), because of the user experience, it is recommended to *not* select user groups (thus the conditional access policy will be applied to all users). This is because when applying it to specific user groups, *all* users are prompted by VIDM for their *username* first prior to proceeding with the authentication, which adds an additional step to the SSO.

Table 1b: End User Experience for High-risk vs. Lower-risk apps



1. **End user installs a *high-risk app* (i.e. Outlook) from a public app store/Hub app catalog on a managed device which has the Mobile SSO cert installed. The end user is not prompted for credentials when they authenticate to Outlook. (If Multi-Factor Authentication is optionally required by the IdP, the user is prompted to enter either password or authentication code sent via SMS, or swipe in-app).**
2. End user installs a ***high-risk app*** (i.e. Outlook) from public app store/Hub app catalog on an unmanaged device and access is denied when they attempt to authenticate to Outlook.
3. End user installs a ***lower-risk app*** (i.e. Concur) from a public app store/Hub app catalog on a managed device which has the Mobile SSO cert installed. The end user is not prompted for credentials when they authenticate to Concur. (If Multi-Factor Authentication is optionally required by the IdP, the user is prompted to enter either password or authentication code sent via SMS, or swipe in-app. If the IdP supports different authentication strengths per mobile app, the recommendation would be to not require MFA for lower-risk apps that do not contain confidential company data).
4. End user installs a ***lower-risk app*** (i.e. Concur) from a public app store/Hub app catalog on an unmanaged device. The end user is prompted for credentials from the IdP as they normally would when they authenticate to Concur as lower-risk apps do not require device management.

Note that with *Adaptive Authentication*, the user can download and authenticate to the Intelligent Hub app catalog without their device being managed. Consequently, the apps available within the Intelligent Hub app catalog drive the security policy and whether the device is managed, including for apps that are publicly available.

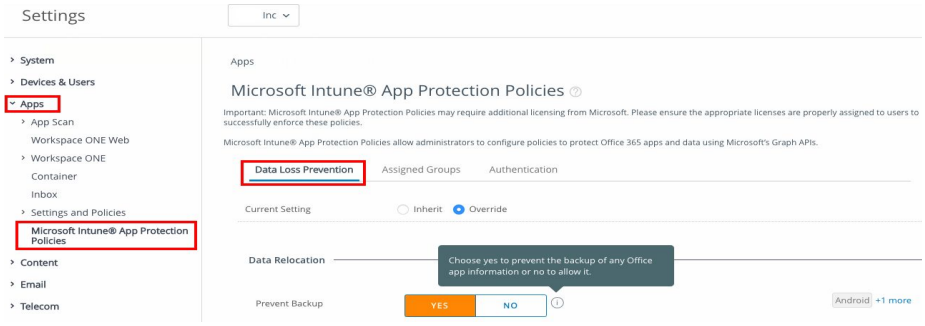
Configure Data Loss Protection for Office apps in the Workspace ONE UEM

Once you integrate Workspace ONE UEM with Microsoft Intune App Protection Policies DLP, manage the DLP policies in Workspace ONE UEM console so that the integration remains current. Because Workspace ONE UEM console syncs with Microsoft Intune App Protection console but not the other way around, changes made in Microsoft Intune App Protection console will not be reflected in Workspace ONE UEM. Note that Workspace ONE does not directly control the Microsoft Intune App Protection policies; the Microsoft SDK applies these policies directly. For this reason, we will provide the recommended configuration in Workspace ONE UEM and where it is not available in Workspace ONE, we will provide the configuration in Azure Portal. More details on the location of these settings in Workspace ONE UEM can be found here.

Note that to apply the Intune App Protection Policies, you must have Microsoft Enterprise Mobility + Security E3 licensing.

1. **Prevent users from backing up from Office apps to iTunes, iCloud, and Android backups**

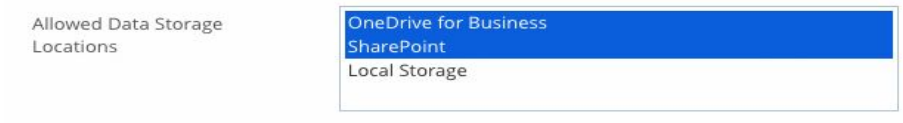
Workspace ONE UEM> Groups & Settings > All Settings > Apps > Microsoft Intune App Protection Policies > *Data Loss Prevention* tab



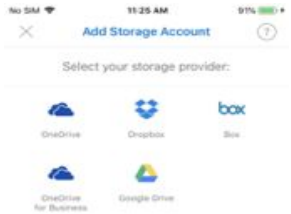
Prevent employees, whether on BYOD, CORP, or COPE owned devices, from performing iTunes/iCloud/Android backups to Office mobile apps containing corporate data/accounts (i.e., Outlook, OneNote, PowerPoint, OneDrive, Excel, Word).

2. **Prevent users from saving corporate Office data to local storage and/or personal cloud storage and allow users to save to corporate cloud storage only, such as SharePoint or OneDrive for Business**

Workspace ONE UEM > Groups & Settings > All Settings > Apps > Microsoft Intune App Protection Policies > *Data Loss Prevention* tab



Within Office mobile apps, users have the ability to save corporate data and attachments to personal cloud or restricted-content sharing sites such as OneDrive (Personal), Dropbox, Box, and Google Drive.



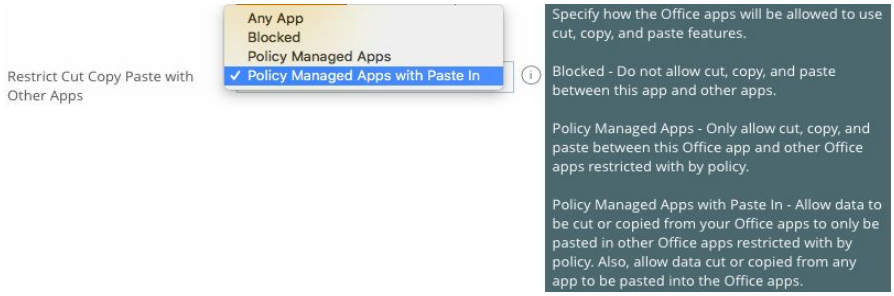
Selecting "***OneDrive for Business***" and/or "***SharePoint***" ensures that employees, whether on BYOD, CORP, or COPE owned devices, cannot save to personal or restricted-content sharing sites. Employees, when signed into their corporate account via any of the Office mobile apps, will only have the option to save their corporate data and attachments to either OneDrive for Business and/or Sharepoint. It is recommended not to allow "***Local Storage***" because if data is saved from the Office app to the mobile device's local storage, then it will not be subject to an enterprise wipe (from Workspace ONE). However, users will be able to save this corporate data stored locally into personal apps including personal cloud-storage repositories.

This setting offers added value for organizations looking to protect their corporate IP and prevent sensitive data from being saved to unauthorized third parties. If data is saved in an unmanaged destination or locally on the device, then it will not be subject to an enterprise wipe via Workspace ONE UEM. To prevent a security breach, the data should either not be stored at all or stored in only corporate-approved locations where security controls and auditing are in place.

With Android Enterprise, the locations to save to are limited to the Work container, but the Intune App Protection policy would further restrict users. For example, a user using Outlook in the Work container would not be allowed to save to a personal Google Drive storage location and only be allowed to save to OneDrive for Business and/or SharePoint. A user using Outlook in the personal side of the device would be blocked from being able to access her/his corporate Outlook account once she/he enters her/his SSO credentials because the device would not be enrolled to Workspace ONE on the personal side.

3. **Prevent users from cut, copy, and paste operations to all but policy-managed apps**

Workspace ONE UEM > Groups & Settings > All Settings > Apps > Microsoft Intune App Protection Policies > *Data Loss Prevention* tab



Select "***Policy Managed Apps with Paste In***" if you are only using Office apps for email and collaboration on iOS devices. This option restricts cut, copy, and paste to among Office apps only. If using a non-Office app for meetings and/or collaboration, consider selecting "***Any app***" because copying a meeting ID or URL from email/calendar into the third-party collaboration app (e.g., Webex) will not work.

If you have Android Enterprise, then selecting this setting will not be needed because the Work container set up via Workspace ONE can prevent cut, copy, and paste from apps in the Work container into personal applications outside the container. Support for cut, copy, and paste exists among any applications within the Work container. Work container apps require corporate approval and are subject to enterprise wipe.

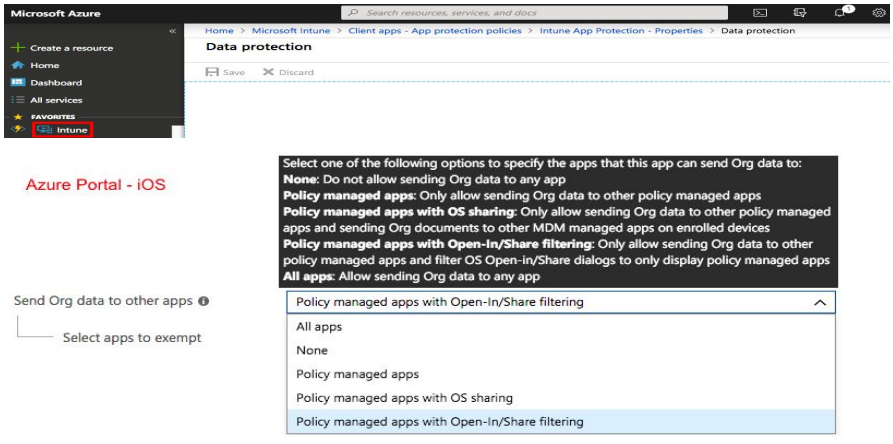
4. **iOS - Office apps only**

Prevent users from Open-In/sending corporate data to non-Office apps, allow users to send only to Office apps

For organizations that only use Office apps on iOS devices, the "***Open-In/Share filtering***" option works best because this setting prevents the usage (i.e., opening and saving) of third-party apps that are not built with the Intune SDK.

Configure in the Azure portal because currently these settings are not available in Workspace ONE UEM console version 1905 (note that you must make this particular policy change for both iOS and Android in Azure so that both platforms are configured correctly).

Azure Portal > Intune > Client Apps > App Protection Policies > *select the iOS policy name*, e.g., Default AirWatch Policy > Properties > Data Protection

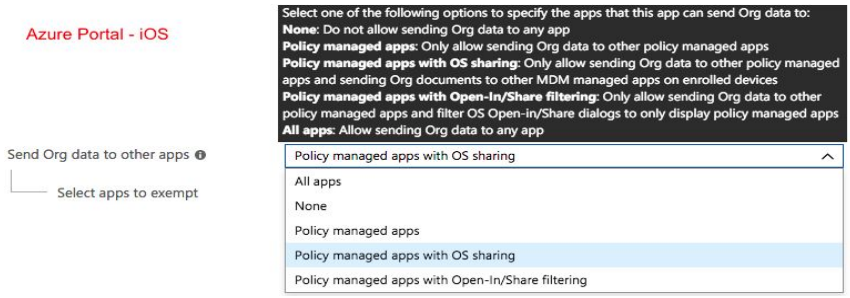


5. **iOS - Office apps plus Box or Slack**

Prevent users from Open-In/sending corporate data to other non-managed apps

For those that standardize and use a corporate file repository such as Box for EMM, instead of OneDrive, the recommendation would be to use the "***OS sharing***" setting so that when opening a file or attachment in an Office app, the user sees the non-Office app (along with the other Office apps) listed as options to share to. To accomplish this, all of the corporate apps including Office apps must be managed by Workspace ONE, which is described below.

Azure Portal > Intune > Client Apps > App Protection Policies > *select the iOS policy name*, e.g., Default AirWatch Policy > Properties > Data Protection

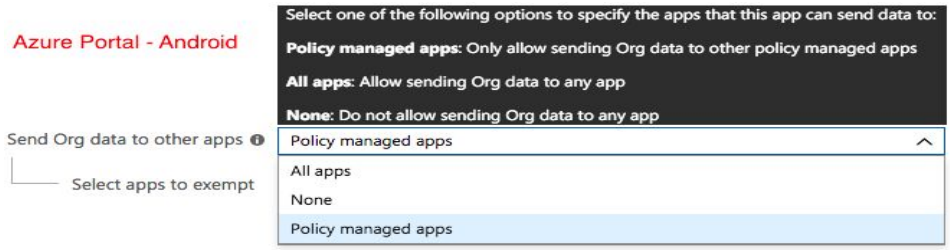


Android Enterprise

Prevent users from Open-In/sending corporate data to other non-managed apps

It is recommended to select "***Policy managed apps***" to allow for sharing of corporate data among Office apps in the Work container, and to restrict sharing of corporate data from the company apps in the Work container to personal apps outside the Work container. Note that if you are using non-Office apps, then there will be some limitations in sharing data among corporate apps in the Work container. In some cases, to overcome this and allow for sharing corporate data with non-Office company apps in the Work container, non-office apps may have an Intune SDK such as Adobe Acrobat Reader for Intune, which will enable sharing of corporate data.

Azure Portal > Intune > Client Apps > App Protection Policies > *select the Android policy name*, e.g., Default AirWatch Policy > Properties > Data Protection



6. **Allow users to sync Office apps to the native contacts app on the device**

This setting is needed if you a) have configured Workspace ONE to push the corporate Exchange ActiveSync mail profile to the native Mail, Calendar, and Contacts on iOS devices and b) support the use of several third-party apps that integrate with the native contacts application. This requires responsible use of this setting: the information security team should blacklist non-approved apps, as necessary, that can access the

native contacts application to extract company contacts, which can be used for malicious intent.

Impact of DLP settings on BYOD and COPE iOS mobile devices

For BYOD and COPE devices that have more flexibility to manage both personal and corporate data on a single mobile device, these restrictions apply only when the user is signed into her/his corporate Office account in any of the Office mobile apps. When signed in with her/his personal account, she/he will be able to add and share to personal apps and locations as she/he normally would on an unmanaged device.

Office mobile apps operate under a different model than do apps such as Box and Slack, who have a different iOS app for both personal and enterprise use. “Box for EMM” and “Slack for EMM” can only be used if the organization has deployed a Mobile Device Management/Enterprise Mobile Management (MDM/EMM) solution such as Workspace ONE UEM and made these apps available in the company app catalog. The upside to this model is that leveraging MDM/EMM controls for the enterprise version of Slack/Box—such as sharing corporate data among managed apps and/or enterprise wiping the corporate data—does not impact personal data because they are saved in a completely separate consumer app. More below on how to preserve the experience in Office mobile apps if using these apps for dual corporate and personal use.

Use Office apps with other non-Office apps

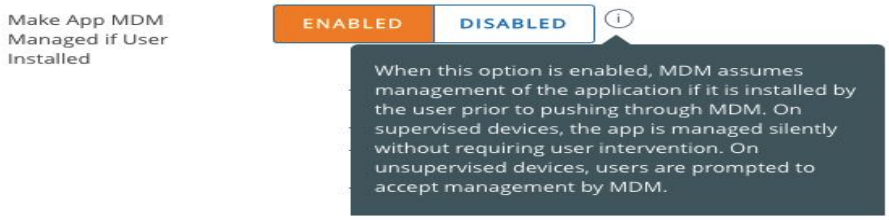
1. **Configure DLP for Microsoft Intune Apps in Azure Portal:**

If in #5 above you are using a mixed environment of enterprise collaboration apps on iOS that include Office apps as well as others such as Box for EMM and Slack for EMM, then select the “***OS sharing***” setting so that when opening a file or attachment in an Office app, the user sees the non-Office app (along with the other Office apps) listed as an option to share to.

2. **Configure app management in Workspace ONE UEM:**

Select “***Enabled***” in the following app setting in Workspace ONE UEM for each of the apps that you distribute and manage via the Hub app catalog. This includes enabling app management for all corporate apps, both Office apps (i.e., Outlook, Word, OneDrive, etc.) and non-Office apps (e.g., Box for EMM, Slack for EMM).

Workspace ONE UEM Console > **Apps & Books** > **Applications** > **Native** > select the corresponding iOS ***app*** and click **Assign** > select the corresponding ***smart group*** and click **Edit** > scroll to the following policy in the Policies section:



Although company apps installed from the Hub app catalog are automatically "managed" on the user's device, many of these apps are publicly available (Outlook, Word, OneDrive, etc.). Thus, users may have already installed these apps from the Apple App Store directly prior to enrolling in Workspace ONE. In that case, once the user enrolls and their device becomes managed, the user will be prompted for app management. If the user accepts the app management prompt, the app they have previously installed will become "managed". Enforcing app management via an MDM solution can be challenging, especially if using a BYOD or non-DEP iOS device.

For corporate iOS devices that are managed by Apple's Device Enrollment Program (DEP), app management can be enforced and not left up to the user. For BYOD or non-DEP iOS devices, Workspace ONE Intelligence can create an advanced compliance policy to notify users and/or administrators and remove profiles such as VPN/Wi-Fi if users have declined management of Office apps.

For organizations that use Box for EMM for storing corporate data, it is recommended to require management for this app. In addition, the administrator must set the iOS Restriction of blocking data transfer from managed sources to unmanaged destinations.

If all corporate apps (including Office and non-Office apps) are managed via Workspace ONE, then this setting will ensure that corporate data will be blocked from being shared and/or transferred from a corporate app (i.e., managed source) to a personal app (i.e., unmanaged destination). If non-Office apps are being used for collaboration, then the Intune App Protection Policy of "***OS sharing***" alone will not prevent corporate data loss.

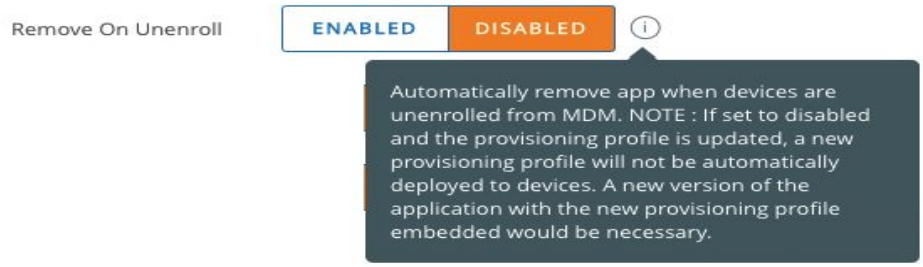
Configure options for removing corporate data from Office apps

If the employee ***exits*** the company or her/his iOS device is ***lost or stolen***, then the Help Desk is responsible for performing an enterprise wipe from the Workspace ONE UEM console. In the case of an exiting employee, best practice has been to configure an automatic enterprise wipe from Workspace ONE UEM console once the employee's AD account has been disabled. However, an enterprise wipe will a) remove all data from the managed app, including any

personal data saved locally within the app, and b) if Microsoft Intune integration is in place, then the Azure Refresh Token will be revoked.

Your user community can use Office apps for both personal and work: for example, users can add personal accounts to the same iOS Outlook app that has their corporate account configured. Because Intune App Protection policies do not apply to the user's personal accounts, they may save files to the local device storage. Thus, if the Outlook app (or any other Office app) is managed, then an enterprise wipe will delete all data in the app, which would include not only the user's corporate data but potentially her/his personal data as well. Given this scenario, it is recommended to disable "***Remove on unenroll***" in **Workspace ONE UEM**.

Workspace ONE UEM Console > **Apps & Books** > **Applications** > **Native** > select the corresponding *iOS app* and click **Assign** > select the corresponding *smart group* and click **Edit** > scroll to the following policy in the Policies section:

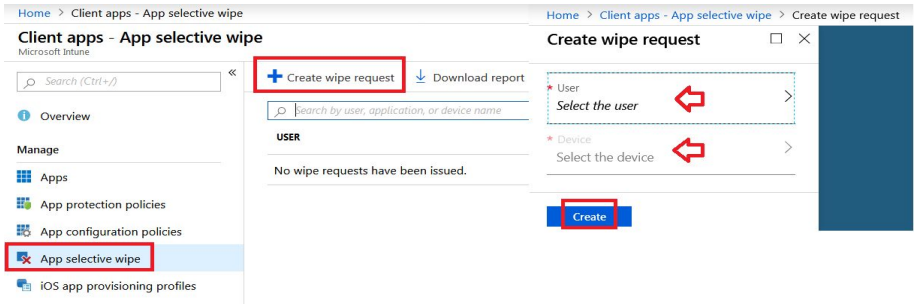


The above setting will not result in any data—corporate or personal—being removed from the Office app upon an enterprise wipe, even if the app is ***managed.***

If Workspace ONE UEM is integrated with Microsoft Intune App Protection policies, then the enterprise wipe command issued by Workspace ONE UEM results in revoking the Azure Refresh Token. This is the case whether Office apps are managed or not. Revoking the Azure Refresh Token causes the default one-hour access token for Office apps to expire and forces an SSO prompt to occur. At this point, users must sign-in using their SSO credentials to regain access to their Office data. However, if the user cancels the SSO prompt, then we have found that corporate data can still be accessed.

Because we have disabled removing corporate (and personal) data for each of the Office apps upon an enterprise wipe, and revoking the Azure Refresh Token does not make corporate data completely inaccessible, it is important to ensure that corporate data is removed when a user exits the company or her/his device is lost or stolen.

To remove corporate data only from the Office app, perform an **App Selective wipe** from the **Intune console**.



This can also be automated if necessary by creating a script that will leverage the Intune MAM GraphAPI. For example, when an enterprise wipe is issued from Workspace ONE UEM, Workspace ONE can issue an API call to Intune so that the app-selective wipe is performed at the same time, resulting in all corporate data being removed from the Office apps.