VMware AirWatch and Office 365 Application Data Loss Prevention Policies

Workspace ONE UEM v9.6

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Add AirWatch by VMware as an Azure Enterprise MDM Application

To enable Workspace ONE UEM and Azure to communicate, add **AirWatch by VMware**application to your Azure environment. This action allows Workspace ONE UEM to manage the DLP policies for Microsoft Intune® App Protection Policies applications.

For the most current procedure, see Microsoft Azure Active Directory Documentation at https://docs.microsoft.com/en-us/azure/active-directory/.

1. In Microsoft Azure, navigate to your Azure Active Directory and Mobility Apps, **Mobility (MDM and MAM)**.
2. Select **Add Application**.
3. Select **AirWatch by VMware** application.
4. Review the application details and select **Add**.
5. In the Mobility (MDM and MAM) area, confirm that **AirWatch by VMware** displays in the list of applications.

Microsoft Intune® App Protection Policies Settings

Configure and apply data loss prevention (DLP) application policies to the Microsoft Intune® App Protection applications and data in the Workspace ONE UEM console. Workspace ONE UEM does not directly enforce policies on applications. The Microsoft SDK controls and enforces the policies.

To configure and apply data loss prevention (DLP) application policies to the Microsoft Intune® App Protection applications the user must be an admin with the privileges to configure app policies in intune.

Complete the following steps to add DLP application policy information to the UEM console:

1. Navigate to **Groups & Settings > All Settings > Apps > Microsoft Intune® App Protection Policies**.
2. Navigate to the **Authentication** tab.

   Office 365 data loss prevention application policies allow administrators to configure policies to protect Office 365 apps and data using Microsoft Graph APIs. To configure Office 365 DLP policies, you need admin credentials to connect your tenant to Workspace ONE UEM.

   Enter the user name and password for the Azure admin. Workspace ONE UEM uses these credentials to search and assign the DLP application policies to the Microsoft Security Groups.

Setting	Description
User name	Enter the user name to configure your tenant to Workspace ONE UEM.
Password	Enter the password that is used to configure your tenant to Workspace ONE UEM.

3. Configure the preferred Microsoft Intune® App Protection Policies DLP application policies.

   Configure DLP app policies for your managed Microsoft Intune® App Protection Policies applications and data. Find these configurations in the UEM console at **Groups & Settings > All Settings > Apps > Microsoft Intune® App Protection Policies**.

Setting	Description
Data Relocation	
Prevent Backup	Prevents users from backing up data from their managed applications.
Allow Apps to Transfer Data to Other Apps	• **All Apps** - Enables users to send data from managed applications to any application. • **Restricted Apps** - Allows users to send data from their managed applications to other managed applications. • **No Apps** - Prevents users from sending data from managed applications to any application.
Allow Apps to Receive Data from Other Apps	• **All Apps** - Enables users to receive data from applications to their managed applications. • **Restricted Apps** - Allows users to receive data from other managed applications to their managed applications. • **No Apps** - Prevents users from receiving data from all applications to their managed applications.
Prevent Save As	Prevents users from saving managed Microsoft Intune® App Protection Policies application data to another storage system or area.
Restrict Cut Copy Paste with Other Apps	• **Any App** - Allows users to cut, copy, and paste data between their managed applications and any application. • **Blocked** - Prevents users from cutting, copying, and pasting data between managed applications and all applications. • **Policy Managed Apps** - Allows users to cut, copy, and paste data between managed Microsoft Intune® App Protection Policies applications. • **Policy Managed Apps with Paste In** - Allows users to cut and copy data from their managed applications and to paste the data into other managed applications. It also allows users to cut and copy data from any application into their managed applications.

Setting	Description
Restrict Web Content to Display in Managed Browser	Forces links in managed applications to open in a managed browser.
Encrypt App Data	Encrypts data pertaining to managed applications when the device is in the selected state. The system encrypts data stored anywhere, including external storage drives and SIM cards.
Disable Contents Sync	Prevents managed applications from saving contacts to the native address book.
Disable Printing	Prevents users from printing data associated with managed applications.
Allowed Data Storage Locations	Enables admins to control where users can store managed application data.
Access	
Require PIN for Access	Requires users to enter a PIN to access managed applications. Users create the PIN upon initial access.
Number of Attempts before PIN Reset	Sets the number of entries users attempt before the system resets the PIN.
Allow Simple PIN	Allows users to create four digit PINs with repeating characters.
PIN Length	Sets the number of characters users must set for their PINs.
Allowed PIN Characters	Sets the characters that users must configure for their PINs.
Allow Fingerprint Instead of PIN	Enables users to access managed applications with their fingerprints rather than PINs.
Require Corporate Credentials For Access	Requires user to access managed applications with their enterprise credentials.
Block Managed Apps from Running on Jailbroken or Rooted Devices	Prevents users from accessing managed applications on compromised devices.
Recheck The Access Requirements After (minutes)	Sets the system to check the access PIN, fingerprint, or credential information when the access session reaches one of the time interval options. • **Timeout** - The number of minutes the access sessions for managed applications are idle. • **Offline Grace Period** - The number of minutes devices with managed applications are offline.
Offline Interval (days) before App Data is Wiped	Sets the system to remove managed application data from devices when devices are offline for a set number of days.
Block Screen Capture and Android Assistant	Prevents users from taking screen shots on their devices when they access managed applications.
iOS	

Setting	Description
Minimum Operating System version required	Enter the required minimum iOS version number that a user must have to gain secure access to the application.
Minimum Operating System version required (Warning alert only)	Enter the recommended minimum iOS version number that a user must have to gain secure access to the application.
Minimum App version required	Enter the required minimum App version number that a user must have to gain secure access to the application.
Minimum App version required (Warning alert only)	Enter the recommended minimum App version number that a user must have to gain secure access to the application.
Minimum App protection policy SDK version required	Enter the minimum Intune Application Protection Policy SDK version that a user must have to gain secure access to the application.
Android	
Block Screen Capture and Android Assistant	If Yes is selected, screen captures and Android Assistant app scanning will be unavailable when using an Office app.
Minimum Operating System version required	Enter the required minimum Android OS version number that a user must have to gain secure access to the app.
Minimum Operating System version required (Warning alert only)	Enter the recommended minimum Android OS version number that a user must have to gain secure access to the app.
Minimum App version required	Enter the required minimum App version number that a user must have to gain secure access to the app.
Minimum App version required (Warning alert only)	Enter the recommended minimum App version number that a user must have to gain secure access to the app.
Minimum Android patch version required	Enter the oldest required Android security patch level a user can have to gain secure access to the app.
Minimum Android patch version required (Warning alert only)	Enter the oldest recommended Android security patch level a user can have to gain secure access to the app.

4. Assign the DLP application policies to the Microsoft Security Groups. The security groups are previously configured in Azure.

Setting	Description
All Security Groups	Enter the name of the security group to assign it to the DLP app policies. Select from the list the system displays after an entry. Select **Add Group** to assign the DLP app policies to the security group.
Security Groups Assigned to Microsoft Intune® App Protection Policies	Lists the security groups assigned to the DLP app policies. Select **Remove Group** to remove the assignment from the security group.

Note: The warning alters for the Operating System version, App version, and the Android Patch version only notifies the user with a warning message. However, the warning alters do not stop the end users from using the app.