Intune App Protection Policies Integration

VMware Workspace ONE UEM 2105

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Microsoft Intune App Protection Policies Integration

1

VMware Workspace ONE® powered by AirWatch integration with Microsoft Intune® App Protection Policies removes the management of DLP policies for your Microsoft Intune App Protection policies in two consoles.

You can configure the data loss prevention (DLP) application policies for your Microsoft Intune App Protection in Workspace ONE UEM. After you integrate the two systems, manage the DLP application policies in the Workspace ONE UEM console so that the integration stays current.

Most Microsoft Intune App Protection Policies are available for the Android platform and the iOS platform.

Manage in the Workspace ONE UEM Console to Stay Synced

After you integrate the two systems, manage the DLP application policies in the Workspace ONE UEM console so that the integration stays current. Workspace ONE UEM does not receive changes that are made in other parts of the integration. The DLP application policies or security group assignments can get out of sync.

User Experiences on Android and iOS

The iOS and Android platforms have different and similar user experiences when users first access apps after a successful integration with Intune.

Experience on iOS

When the device user authenticates to Microsoft Office 365 applications on iOS devices, and the profile pushed successfully, the system displays a pop-up stating that your organization manages the application. There are no additional steps in the configuration.

Experience on Android

To manage Android and Android Enterprise devices, users must install the Intune Company Portal application. This application acts as a broker for the Intune App SDK the same way the Workspace ONE Intelligent Hub acts as a broker for Workspace ONE UEM applications.

Common Experience on iOS and Android

Both platforms must set Intune as the MDM Authority on the device. You can configure this setting on the device in **Azure Tenant > All Resources > Intune**. Enable **Intune MDM Authority** from the **Getting Started** notification.

Do These Actions in Azure to Integrate Microsoft Intune

For integration, create a user account and assign the user the listed Microsoft licenses.

Those environments that do not have the Azure AD integration in Directory Services in the Workspace ONE UEM console, you must add the **AirWatch by VMware** app in Azure. Access Configure Workspace ONE UEM to Use Azure AD as an Identity Service for details.

Important If you already have Out of the Box Enrollment (OOBE) set up with any other MDM provider other than Workspace ONE UEM, add **AirWatch by VMware** and do not enter or edit any other settings in Azure. If you do enter or edit configurations, you might break the existing enrollment process.

- Create a service account (a user) in Azure, and assign the user the proper roles.

  Note These steps are general. For current details about configuring Azure, see Microsoft documentation.

  a Go to your Azure portal by entering `portal.azure.com` in your browser.

  b Create a user or sync a user with On-Premises Active Directory.

  Disable MFA (multi-factor authentication) for this user's domain.

  c Assign this user the listed roles.

  - **Intune Administrator**
  - **Application Administrator**
  - **Directory Reader**
  - **Directory Writer**

- If you created a user in Azure AD, use this account to log in to Azure at `portal.azure.com`. Ensure that the password is valid and does not need updating.
- You must assign the user the listed licenses in Azure.
  - Microsoft Intune App Protection Policies

- Microsoft Enterprise Mobility + Security E3 or E5

Configure Intune Settings

In the Workspace ONE UEM console, configure and apply data loss prevention (DLP) application policies to Microsoft Intune® App Protection applications and data. Configure the Authentication tab first so the systems can communicate. Then configure your DLP settings and assign them to groups.

Workspace ONE UEM does not directly enforce policies on applications. The Microsoft SDK controls and enforces the policies.

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

Prerequisites

To configure and apply DLP application policies to Intune applications, you must have the privileges to configure app policies in Intune.

Procedure

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

2 Select the **Authentication** tab and enter the user name and password for the Azure admin.

Administrators can use Office 365 DLP application policies to protect Office 365 apps and data with Microsoft Graph APIs. To configure Office 365 DLP policies, you need admin credentials to connect your tenant to Workspace ONE UEM.

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

Workspace ONE UEM uses these credentials to search and assign the DLP application policies to the Microsoft Security Groups.

3 Select the Data Loss Prevention tab and 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.

Settings for Data Relocation	Description
Prevent Backup	Prevents users from backing up data from their managed applications.
Allow Apps to Transfer Data to Other Apps	■ **All** - Users can send data from managed applications to any application. ■ **Restricted** - Users can send data from their managed applications to other managed applications. ■ **None** - Prevents users from sending data from managed applications to any application.
Allow Apps to Receive Data from Other Apps	■ **All** - Users can receive data from applications to their managed applications. ■ **Restricted** - Users can receive data from other managed applications to their managed applications. ■ **None** - 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** - Users can 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** - Users can cut, copy, and paste data between managed Microsoft Intune App Protection Policies applications. ■ **Policy Managed Apps with Paste In** - Users can cut and copy data from their managed applications and to paste the data into other managed applications. Users can also cut and copy data from any application into their managed applications.
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	Admins can control where users can store managed application data.

Settings for Access	Description
Require PIN for Access	Requires users to enter a PIN to access managed applications. Users create the PIN during their initial access.
Number of Attempts before PIN Reset	Sets the number of entries users attempt before the system resets the PIN.
Allow Simple PIN	Users can 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.

Settings for Access	Description
Allow Fingerprint Instead of PIN	Users can access managed applications with their fingerprints rather than PINs.
Require Corporate Credentials For Access	Users can 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 validate the access PIN, fingerprint, or credential information when the access session reaches one of the time intervals. ■ **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.

Settings for Android	Description
Block Screen Capture and Android Assistant	If **Yes** is selected, screen captures and Android Assistant app scanning are 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 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 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 Android security patch level a user can have to gain secure access to the app.

4 Select the **Assigned Groups** tab and 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 and assign it to the DLP app policies. Select from the list the system displays after an entry. Select **Add Group** and assign the DLP app policies to the security group.
Security Groups Assigned to O365 Policies	Lists the security groups assigned to the DLP app policies. Select **Remove Group** and remove the assignment from the security group.

Warning Messages for Deleted and Modified Policies

After the Microsoft Intune App Protection Policies load, Workspace ONE UEM console checks for deletions and modifications in Intune in the Azure portal. It is possible for managed policies to get out of sync with the deployed policies. To warn admins about possible deletions and modifications, the Workspace ONE UEM console displays warning messages based on the scenario.

-
  ```
  Policy was deleted on the Microsoft Intune Portal. Click Delete Settings to delete the policy
  settings from UEM.
  ```

  The Workspace ONE UEM console displays this message after someone deletes one or both iOS and Android policies deployed in Intune. Selecting **Delete Settings** removes the settings of both policies from the Workspace ONE UEM console without modifying anything on the Azure side. The console page does not refresh automatically.

  Users can deploy new iOS and Android policies to Azure without error.

  Note If only one of the policies, iOS or Android, is deleted in Azure, the other policy still remains in Azure. Users must manually delete the other policy if they choose not to keep the past settings.

-
  ```
  Policy settings were updated on the Microsoft Intune portal and are out of sync with Workspace
  ONE UEM. Click Sync Settings to update this policy in UEM.
  ```

  The Workspace ONE UEM console displays this message after someone modifies both iOS and Android policies in Intune in the Azure portal and the policy settings still match between the two policies. Selecting **Sync Settings** updates the settings of both policies in Workspace ONE UEM to match those pulled from the policies in Azure. The console page does not refresh automatically.

  Note This senario excludes settings that are specific to iOS or Android such as iOS SDK settings and Android Assistant settings.

-
  ```
  "Receive data between other apps" policy is different for Android policy and iOS policy in Azure
  Portal. This setting needs to be the same for Workspace ONE UEM to sync the Android and iOS
  policy. Contact IT administrator to resolve the issue.
  ```

  ```
  "Receive data between other apps" and "Send org data to other apps" policies are differet for
  Android policy and iOS policy in Azure portal. These settings need to be the same for Workspace
  ONE UEM to sync the Android and iOS policy. Contact IT administrator to resolve the issue.
  ```

  ```
  "Prevent Backups", "Receive data between other apps", and "Send org data to other apps" policies
  are different for Android policy and iOS policy in Azure portal. These settings need to be the
  same for Workspace ONE UEM to sync the Android and iOS policy. Contact IT administrator to
  resolve the issue.
  ```

The Workspace ONE UEM console displays these messages after someone modifies both policies in Intune in the Azure portal but the policy settings do not match between the two policies. The messages list the setting discrepancies between the two policies in Azure. They also list the policy names listed in Azure and not the ones used by the Workspace ONE UEM console.

Resolve the conflicts listed in the messages before using the **Sync Settings** menu item in the Workspace ONE UEM console.

Note This senario excludes settings that are specific to iOS or Android such as iOS SDK settings and Android Assistant settings.

The **Delete Settings** menu item and the **Sync Settings** menu item do not modify any settings in Intune in the Azure portal.