

Intune App Protection Policies Integration

VMware Workspace ONE UEM 1907



vmware®

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

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1** Microsoft Intune App Protection Policies Integration 4
- 2** User Experience Differences for Android and iOS When Integrating Microsoft Intune
5
- 3** Requirements to Integrate Microsoft Intune 6
- 4** Configure Microsoft Intune App Protection Policies Settings 7

Microsoft Intune App Protection Policies Integration

1

VMware Workspace ONE[®] powered by AirWatch integration with Microsoft Intune[®] App Protection Policies removes the need to manage 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.

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 Experience Differences for Android and iOS When Integrating Microsoft Intune

2

The user experience on iOS devices and Android devices differs in terms of management.

Experience on iOS

When the device user authenticates to Microsoft Office 365 applications On iOS devices, and if the profile has been pushed successfully, the system displays a popup stating that your organization manages the application. There are no additional steps in the configuration.

Experience on Android

In order 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 need to 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.

Requirements to Integrate Microsoft Intune

3

To integrate Workspace ONE UEM and Microsoft Intune® App Protection Policies DLP, ensure to set listed components.

- Ensure the admin for this integration has the listed permissions.
 - The admin has access to Azure Active Directory with permissions to add enterprise applications and with the `Group.Read.All` and `Group.ReadWrite.All` permissions.
 - The admin has MFA (Azure Multi-Factor Authentication) disabled.

- Add **AirWatch by VMware** in Azure Active Directory as an Azure Enterprise MDM application. Find this configuration in Azure Active Directory in **Azure Active Directory > Mobility Apps > Add Application > AirWatch by VMware**.

If you already have OOB enrollment set up, add **AirWatch by VMware** and do not enter or edit any other settings. If you do enter or edit configurations, you risk breaking the OOB enrollment process.

- Use licenses from Microsoft for Microsoft Intune® App Protection policies and for Microsoft Enterprise Mobility + Security E3 or E5.

Most Microsoft Intune® App Protection Policies are available for Android and iOS platforms.

Configure Microsoft Intune App Protection Policies Settings

4

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.

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.

Prerequisites

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.

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.

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.

| 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. |

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

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 Workspace ONE UEM console at **Groups & Settings > All Settings > Apps > Microsoft Intune® App Protection Policies > Data Loss Prevention**.

| 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 | <ul style="list-style-type: none"> ■ 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 | <ul style="list-style-type: none"> ■ 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 | <ul style="list-style-type: none"> ■ 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. <p>It also allows users to cut and copy data from any application into their managed applications.</p> |
| 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. |
| Settings for Access | Description |
| Require PIN for Access | Requires users to enter a PIN to access managed applications. |

| Settings for Access | Description |
|---|--|
| | 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) | <p>Sets the system to check the access PIN, fingerprint, or credential information when the access session reaches one of the time interval options.</p> <ul style="list-style-type: none"> ■ 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 iOS | 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. |

| Settings for Android | Description |
|--|--|
| 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. |

| Settings for Android | Description |
|---|---|
| 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. Got to **Groups & Settings > All Settings > Apps > Microsoft Intune® App Protection Policies > Assigned Groups**.

| 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 O365 Policies | Lists the security groups assigned to the DLP app policies. Select Remove Group to remove the assignment from the security group. |